Distributed ReStart

Energy restoration for tomorrow

Organisational, Systems and Telecommunications Design Stage II

December 2020

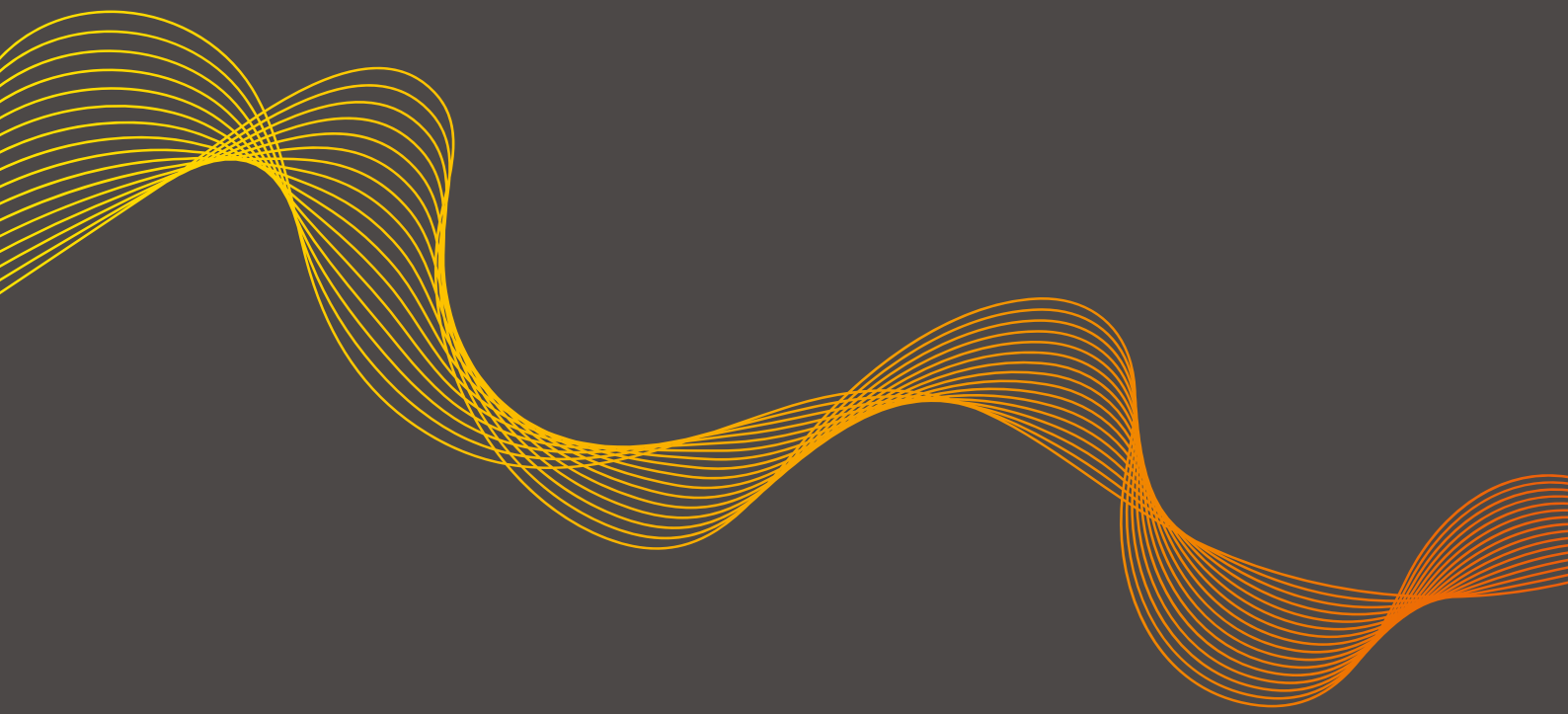
In partnership with:

tnei

SP ENERGY NETWORKS

nationalgridESO

Table of Contents



Abstract

The Distributed ReStart project is a partnership between National Grid Electricity System Operator (ESO), SP Energy Networks (SPEN) and TNEI (a specialist energy consultancy) that has been awarded £10.3 million of Network Innovation Competition (NIC) funding.

The project is exploring how distributed energy resources (DER) can be used to restore power in the highly unlikely event of a total or partial shutdown of the National Electricity Transmission System as part of a Black Start procedure. Past and current approaches rely on large power stations but as the UK moves to cleaner, greener and more decentralised energy, new options must be developed. The enormous growth in DERs presents an opportunity to develop a radically different approach to system restoration. Greater diversity in Black Start provision will improve resilience and increase competition leading to reductions in both cost and carbon emissions. However, there are significant technical, organisational and commercial challenges to address.

The project will tackle these challenges in a three-year programme (Jan 2019 – Mar 2022) that aims to develop and demonstrate new approaches, with initial implementations of Black Start service from DERs from mid-2022 if deemed feasible and cost effective. Case studies on the SP Distribution (SPD) and SP Manweb (SPM) networks will be used to explore options then design and test solutions through a combination of detailed off-line analysis, stakeholder engagement and industry consultation, desktop exercises, and real-life trials of the re-energisation process.

Project Description

The project is made up of five workstreams. The Project Direction and Knowledge Dissemination workstreams cover the effective management of the project and sharing of learning. The other three workstreams cover the wide range of issues to enable Black Start services from DERs:

The Organisational, Systems and Telecommunications (OST) workstream is considering the DER-based restoration process in terms of the different roles, responsibilities and relationships needed across the industry to implement at scale. It will specify the requirements for information systems and telecommunications, recognising the need for resilience and the challenges of coordinating Black Start across a large number of parties. Proposed processes and working methods will be tested later in the project in desktop exercises involving a range of stakeholders.

The Power Engineering and Trials (PET) workstream is concerned with assessing the capability of GB distribution networks and installed DERs to deliver an effective restoration service. It will identify the technical requirements that should apply on an enduring basis. This will be done through detailed analysis of the case studies and progression through multiple stages of review and testing to achieve demonstration of the Black Start from DER concept in 'live trials' on SPEN networks. Initial activities have focused on reviewing technical aspects of DER-based restoration in a number of case study locations that will support detailed analysis and testing within the project. Each case study is built around an 'anchor' resource with 'grid forming' capability, i.e. the ability to establish an independent voltage source and then energise parts of the network and other resources. Then it is intended that other types of DERs, including batteries if available, join and help grow the power island, contributing to voltage and frequency control. The ultimate goal is to establish a power island with sufficient capability to re-energise parts of the transmission network and thereby accelerate wider system restoration.

The Procurement and Compliance (P&C) workstream will address the best way to deliver the concept for customers. It will explore the options and trade-offs between competitive procurement solutions and mandated elements. It uses a strategic process to develop fit for purpose commercial solutions that are open and transparent, stakeholder endorsed, and designed end-to-end with the commercial objectives of the project and workstream in mind. It will feed into business as usual activities to make changes as necessary in codes and regulations.

For an overview of the project and current progress click on the link:
nationalgrideso.com/future-energy/projects/distributed-restart

Executive Summary

This report is the second part of the Design Stage deliverables from the Organisational, Systems and Telecommunications (OST) workstream. It should be read alongside the Design Stage I report published in October 2020. The report analyses the latest Government guidance for cyber security, and details the functional requirements for telecommunications, control systems and cyber security to ensure a fully functional, resilient and robust Distributed ReStart service. The Design Stage outputs of the Organisational, Systems and Telecommunications workstream have been split between the Design Stage I report published in October 2020 and this Design Stage II report. The work will continue into 2021, with the detail of the central organisational model being refined alongside the functional specifications for operational telecommunications, control systems and cyber security.

The Design Stage I report focused on:

- methodology for development of the operational telecommunications functional specifications
- initial cost estimates and methodology for development of cost case studies
- initial end-to-end cyber-resilience methodology and mitigation assessment
- systems considered essential to Distributed ReStart
- an introduction to the DER control interface.

This Design Stage II report focuses on:

- regulatory guidance for cyber security
- functional specifications for operational telecommunications
- costs associated with the operational telecommunications case studies
- end-to-end cyber-resilience analysis
- gap analysis of the current and required DER control interface.

Regulatory Guidance for Cyber Security

The project conducted an analysis of the Distributed Energy Resources Cyber Security Connection Guidance document developed by BEIS and Energy Networks Association (ENA), published in September 2020, and assessed its impact upon the Distributed ReStart project designs.

The analysis showed that with increased interconnectivity between large numbers of stakeholders, and a potentially greater reliance upon automation and control systems, it could result in increased levels of cyber security risk and a broader attack surface. More specifically, where systems become more interconnected and interdependent in order to deliver a distributed restart service, the impact of a cyber-attack could have an impact far beyond the system owner/operator. This risk remains unchanged with the introduction of the Cyber Security Connection Guidance document.

To help reduce the levels of cyber security risk, a number of mitigations have been recommended to develop in future work. The mitigations cover the main risks affecting the capability and include the supply chain, third parties, people, processes and technologies and are summarised below:

- **There is no specific guidance for distributed restart generators:** Where DERs (either transmission or distribution-connected) are contracted as Black Start generators, clear cyber security requirements should be included within contracts. Where applicable, these should be tailored specifically to the DERs and be derived from

risk assessments, (i.e. risk-based). In addition to developing specific cyber security requirements, ENA should also consider developing supporting guidance for those DERs, to which the additional requirements apply, to support their implementation.

- **Role of anchor generators:** It is recommended that an additional DER grouping be created that will cover anchor generators and distributed restart DERs.
- **Communications service providers are not considered as 'external functions':** Within contracts, the division of responsibility between National Grid ESO, DNOs and DERs needs to be made clear. Contracts with DNOs and DERs should make clear who owns the requirements for ensuring cyber resilient communications exist between DERs and DNOs/National Grid ESO to meet day-to-day and distributed restart requirements.
- **Guidance does not fully align with the Networks and Information Systems Cyber Assessment Framework (NIS CAF):** When developing contractual requirements for DERs involved in a distributed restart, the designated authority should consider developing requirements that are fully aligned to the NIS CAF.
- **NIS applicability should be reassessed:** Particular attention should be given to those DERs that provide a distributed restart capability, with a focus upon those that are anchor generators, as these may be considered as providers of essential services.
- **Cyber Security of third parties:** Clear cyber security requirements should be placed upon third-party communications providers, as well as those DERs that are considered Black Start/Distributed ReStart generators, with particular focus being placed upon anchor generators. The requirements should cover security of key operational systems, their provision, maintenance and monitoring, as well as the personnel security controls required to provide appropriate levels of security assurance and protection.

Cyber Security Analysis

Further, ongoing review has been conducted to align the cyber security risk analysis presented in the design I report with the central organisational model. In this model the DNO leads the localised power island growth as part of a pre-defined plan. Once this plan is executed National Grid ESO becomes the strategic lead and directs further growth options. This requires interconnection of systems, distributed responsibility and makes use of an automated interface through a Distribution Restoration Zone Controller (DRZ-C). As a result of this proposal and the intent for a secure by design approach, each aspect of the communications network architecture and control design should be considered. The chosen communications network architecture must reliably provide data on-time and be robust enough to withstand any foreseeable disaster. Additionally, an out-of-band communication channel should be established to ensure trusted communication in the event of a cyber incident and as a fallback plan in the event of network outages. The network resiliency approach must include spare equipment and a backup strategy should a clean sheet recovery be necessary.

Regardless of whether the end-to-end connection model is via the National Grid ESO OpTel network or DNO networks, a required connection architecture and mandated set of technical controls must be implemented. By furnishing a common interface and expected data flow, one can create a repeatable design and decrease the monitoring burden for security personnel.

The entity or entities who are connected to DERs must have the economic ability to provide the necessary infrastructure and security controls to ensure the connection is monitored and secured. The cost of staffing, spare equipment, and maintenance should be factored into the overall budget of the connected party or parties.

Network security monitoring with Security Information and Event Management (SIEM) integration coupled with competent security personnel can drastically improve the overall cyber security posture of a system. Using an active defence of continuous monitoring, response, threat intelligence consumption, and environmental manipulation can provide a security posture that static alerting alone cannot. Should an incident occur, a well-defined sharing mechanism between parties must be established to distribute indicators of compromise to establish the scope and impact of the breach.

Functional Specifications for Operational Telecommunications

The functional specifications for operational telecommunications required to support a Distributed ReStart service are detailed in chapter 3. They have been derived with significant input from stakeholders, including ENA Strategic Telecoms Group and Joint Radio Company members. The functional specifications have been grouped under:

- technical requirements
- configuration, environmental and other requirements
- bandwidth requirements

- resilience requirements
- supported protocols
- cyber security considerations.

The proposed Central Model for organisation under a Black Start from DER introduces a level of automation by incorporating a DRZ-C, hence would need to meet the specifications for the automated restoration process. Upgrades to existing telecommunication networks may be required. Latency and bandwidth are key technical requirements for this type of restoration. Some DRZ-C resources are required in a stringent time window (fast response resource) and some in a slower time (slow response resource) and this in turn will impact on the latency and bandwidth requirements for the network.

The project has also drawn up functional specifications for a manual restoration process, as it is envisaged that participants would be at different stages of the automation journey and would therefore need to continue using the manual process.

The current operational telecommunications networks used by transmission operators and DNOs align with the technical requirements for manual restoration. The provision of at least 72-hour independent power resilience and its extension to the DER sites is a key requisite.

The voice telephony functional requirements remain the same for the manual and automated restoration processes. The key requirements are availability, voice call clarity and end to end 72-hour independent power resilience.

Factors such as cost, existing technology utilised by participant and familiarity, terrain and access to site, maintenance and support for the technology, reliability, availability, policies and regulations play crucial roles in determining preferred solutions for participants in Distributed ReStart services.

Operational Telecommunications Costs

Working with the ENA Strategic Telecoms Group, case studies were undertaken by National Grid ESO and participating DNOs to provide an indication of average costs for service roll out. These have been developed through use of the cost methodology proposed in the Design Stage I report. Please note that these costs are indicative but are summarised here:

- The cost of providing each individual Black Start Voice Service typically equates to £2,000 per annum normalised over the 15-year life time of the voice service although in some instances this could be as high as £9,000 per annum dependent on the technology required or deployed. These costs are primarily driven by the power resilience requirements of the Black Start services and not by the voice element of the service.
- The additional costs of providing the data service are less significant over and above the initial costs of providing the Black Start Voice Service. Typically, this cost equates to circa £400 per annum per data service normalised over the 15-year life time of the data service but for some it could be as much as £2,000 per annum.
- On average the costs of providing Black Start Voice and Data per site is likely to be £2,400 per annum if normalised over 15-year life time but this is site specific and could be as much as £11,000 per annum over 15 years, dependent on the technology required.

DER Control Interface

A case study based review of synchronous DER technologies has been conducted with a particular focus on steam turbine installations and engine installations. This section finds that there is currently a limited communication link between DNOs and DERs. In particular where sites are installed under G59 engineering recommendation (pre 2019), there is no consistent requirement for this data exchange and it will have been developed only where a specific need was identified by the DNO. Exceptions are where ANM schemes are installed, although information exchanged is typically limited to metering data and curtailment signals.

For unmanned DER installations that are controlled remotely, communications links are provided over Openreach infrastructure with backup connection often provided via the cellular network. These links provide visibility of the sites' operation externally to the facility alongside the control capabilities. Many functions of the plant may be automated with physical intervention only being required in the event of faults. For this reason, many of the local capabilities are supplementary and do not function as the primary control in normal operation.

The output of this analysis demonstrates that there is no specific blocker at a DER installation which means that it could not be modified to accept external control commands from the DNO and provide feedback. However, this will require specific alterations to be made for the purpose of Black Start and in particular, existing communications or auxiliary control system resilience may require an increased sizing for battery and UPS due to the increased power draw from this additional control and monitoring equipment.

Automated Control Interface

Many of the communications requirements between the DRZ-C, the DER, and the DNO SCADA are analogous to existing Active Network Management (ANM) schemes. Most required functionality is supported using the protocols presented for both variants of ANM roll out explored in this report (Hardwire and DNP3).

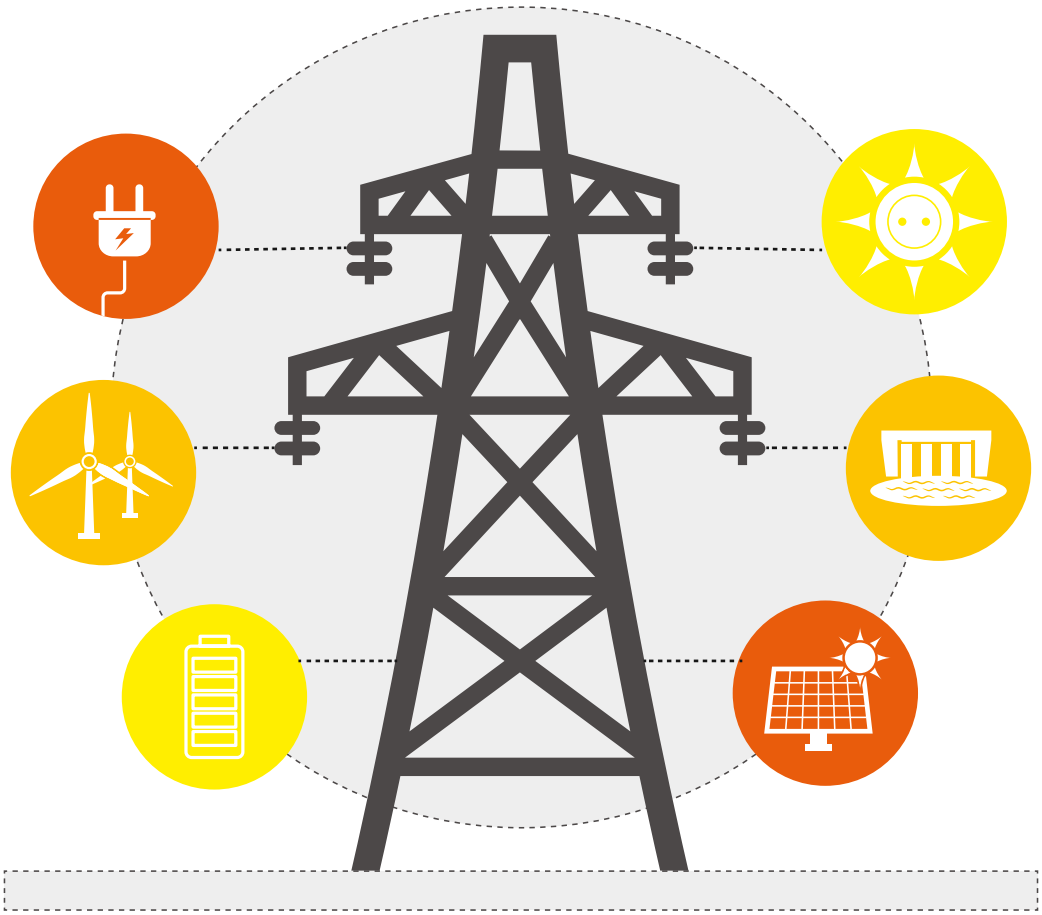
However, fast balancing actions required to maintain stability of the very low inertia system, require extremely low latency. This requires the introduction of different specialised protocols between the DER and the RTU, and between the central controller and the RTU to reduce response times. This is captured in the automated functional specification.

For integration with the DNO Distribution Management System (DMS), an ICCP link or direct DMS control is required, which is analogous to existing ANM schemes. Due to the high latency tolerance of these activities it can make use of existing communications infrastructure and protocols where available.

A DRZ-C would require the introduction of these specialised communications protocols in addition to the existing communications infrastructure. The gap between an ANM scheme and a DRZ-C is limited to low latency power resilient communications and the specific control logic used.

Conclusion

This report presents the telecommunications requirements necessary to facilitate a Black Start and identifies the gaps between existing infrastructure and protocols compared with the functional specifications. These proposals represent a baseline technical requirement which can be built upon across the project refine stage through use of further consultation, design and build, and testing through desktop exercises.



1. Introduction

1.1 This Report

This report builds on the Design Stage I report (nationalgrideso.com/document/178271/download) and 'Organisational, Systems and Telecommunications Viability' report (nationalgrideso.com/document/156216/download) delivered in October 2020 and November 2019 respectively.

Our focus for the 'Viability Report' was to identify the main challenges to delivering Distributed ReStart and consider a range of options to meet these. At that stage, we presented all widely known operational telecommunication options and developed a set of organisational models to illustrate possible stakeholder roles in delivering Distributed ReStart. The report did not propose solutions at this stage.

Our focus for the Design Stage I report was to refine our thinking by developing four organisational models initially and then adopting a preferred way forward for the organisational design; the Central Model, which enables local DNO leadership whilst maintaining National Grid ESO national and regional coordination. Initial functional requirements for operational telecommunications and technology frameworks were developed, and we carried out end to end cyber security assessments for the four organisational models.

Our focus for this report – Design Stage II is to complete the drafting of the functional specifications for the Central Model, including the manual restoration process. The costs for providing the functional specifications were derived through a case study assessment to give average costs for service roll out. The project carried out a review of the recently published DER Cyber Connection Guidance, analysed what that would mean for Distributed ReStart and made recommendations on additional areas that need to be addressed. Further Cyber analysis centered on the Central Model was carried out with recommendations. In addition, a review of the DER communication and control interface was carried out with the view of incorporating learnings into the Distribution Restoration Zone Controller DRZ-C design and build.

1.2 Report Structure

In this report we completed the outstanding work started in the Design Stage I report, incorporating information from the DRZ-C design papers and feedback from industry and stakeholder engagement.

1.2.1 Regulatory Guidance for Cyber Security

Since the publication of the Design Stage I report in October 2020, cyber security guidance for the connection of DERs has been published by ENA and BEIS. A review of this guidance and the implications for Distributed ReStart cyber security requirements is included.

1.2.2 Cyber Security Analysis

In addition to the cyber security risk assessment presented in the Design Stage I report, the project has assessed the proposed Central Model against options to provide a cyber resilient operational telecommunications system for Black Start. This review includes consideration of the impacts of data and network availability on cyber resilience and economic considerations for the cyber design. Furthermore, it reviews the impact of different communication system configurations on cyber resilience, inclusive of mitigation strategies for identified threats. Finally, specific Black Start cyber resilience is considered, and options to improve the overall cyber security of a Black Start event are provided.

1.2.3 Functional Specification for Operational Telecommunications

The key output of this report and analysis, is functional specifications for the operational telecommunications required to facilitate the Central Model as outlined in the Design Stage I report. This reviews the technical and non-technical requirements for an operational telecommunications system which can facilitate an automated DRZ-C process. It is noted that the manual process is required to mitigate against the risk of automation failure or as an initial option for deployment without use of a DRZ-C.

These specifications detail the technical requirements, configuration and environmental requirements, resilience requirements, bandwidth requirements, and protocols which can facilitate these. In addition, the standards that must be met for cyber compliance are highlighted.

Specific voice communication functional requirements are separated out to enable early stage deployment of Distributed ReStart without the use of a DRZ-C.

Finally, a review of technologies which are suitable for providing this functional specification is given using the requirements outlined in this report.

1.2.4 Operational Telecommunications Cost Review

A cost study covering multiple DNOs and National Grid ESO has been used to benchmark the costs for service roll out. This incorporated feedback from National Grid ESO and the DNOs who were consulted through the ENA Strategic Telecommunications Group. A case study method has been used to capture a range of costs and provide an average for each linked element. This allows for the variance introduced by terrain, existing telecommunications technology and DER location to be included, giving a range appropriate for wider GB roll out.

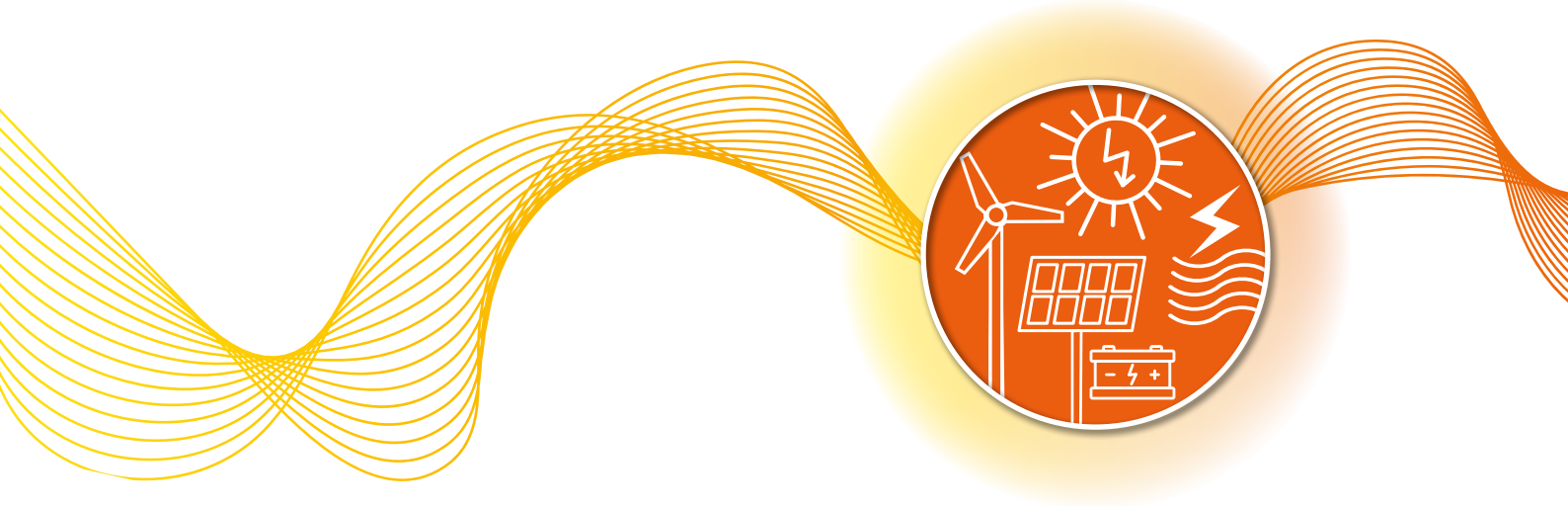
1.2.5 DER Communication and Control Interface

In chapter 6, DER communication and control interface which currently exists is shown to be dependent upon the DER technology type. A review of existing communications protocols for standard DER installations is provided which will be used to refine processes for site attendance and communication protocols with a mind to reduce cost impact from the service.

Chapter 7 reviews options currently used to interface between Active Network Management schemes (ANM) and DERs. This allows for gaps to be identified and incorporated into the design and build stage of the DRZ-C, using existing and preferred communication methodologies where possible within the design.

1.2.6 Conclusions and Next Steps

The intent of this report is to provide a framework for review across the refine stage of the project where desktop exercises, further system design, build and hardware in the loop testing, and stakeholder consultation will feed into contractual requirements for service participants and procedures for control engineers to follow should a restoration event using DERs be enacted. Our conclusions and next steps (chapters 8 and 9 respectively) summarise the key outputs of this framework and our plan for delivery across this final project stage.



2. Regulatory Guidance for Cyber Security

This document presents an analysis of the Distributed Energy Resources Cyber Security Connection Guidance[1], developed by the Department for Business, Energy and Industrial Strategy (BEIS) and the Energy Networks Association (ENA), and assesses its impact on Distributed ReStart.

2.1 Introduction

On 29 September 2020, the Energy Networks Association (ENA) published guidance on cyber security connection for Distributed Energy Resources (DERs). Commissioned by BEIS and the ENA, the guidance is aimed at improving the cyber resilience of DERs. In response, the project has conducted a review of this guidance against Distributed ReStart requirements and proposals from prior risk analysis.

The guidance identifies that, as DERs continue to play an increasingly important role in the UK's electricity generation mix, the impact of a cyber-attack could be significant and wide ranging. Given the role DERs will take within the UKs Critical National Infrastructure (CNI), BEIS and the ENA identified a requirement for clear cyber security guidance tailored specifically to DERs (to include certain supporting services).

The risks highlighted in the Design Stage I report cyber security risk assessment, associated with interconnecting large numbers of stakeholders, are repeated in the foreword to the Cyber Security Connection Guidance, which states that "improving cyber security will help ensure that we have a secure and resilient energy system **…"**[1].

2.2 BEIS Cyber Security Guidance

2.2.1 The Role of the Networks and Information Systems (NIS) Regulations

Transposed into UK law in 2018, the NIS Regulations aim to "raise levels of cyber security and resilience of key systems…"[2]. Their primary objective is to ensure that elements of CNI, including energy generation, transmission and distribution assets, are resilient to cyber threats.

Despite this objective, DERs do not currently fall under the definition of an 'Essential Service', that is "a service which is essential for the maintenance of critical societal or economic activities"[3], as set out within the NIS Regulations. Therefore, there is no legal requirement for operators of DERs to ensure that they follow and implement the requirements it contains.

In order to address this gap, BEIS and the ENA have developed the Cyber Security Connection Guidance. As its name suggests, the guidance is intended to define cyber-security good practice for DERs and support its implementation by owners and operators as assets are connected directly to the UK's electricity transmission and distribution networks. To close the gap in requirements, as the guidelines undergo formal review and are adopted/implemented within the sector, it is envisioned that they will be converted into connection codes in the future – though no timescales are provided.

2.2.2 Development of the Guidance

The guidance developed by BEIS and the ENA has adapted the approach developed by the UK National Cyber Security Centre (NCSC) within the NIS Cyber Assessment Framework (CAF).The NIS directive is EU-wide legislation on cyber security to ensure a common standard of security across Critical National Infrastructure. It is outcome-based, identifying the effects that should be achieved by owners and operators of DERs without providing prescriptive requirements, and is fully aligned with the 4 objectives, 14 principles and 39 outcomes it contains (included in Appendix B). There is also a significant overlap with the Indicators of Good Practice (IGPs) within the CAF. The IGPs are based on 3 principles:

- **Purpose:** It is intended to help inform expert judgement.

- **Scope:** Give important examples of what an assessor will normally need to consider, which may need to be supplemented in some cases.
- **Applicability:** It is designed to be widely applicable across different organisations, but applicability needs to be established.

By adopting this approach, it is intended that a common baseline for cyber security can be established for DERs, whilst also supporting alignment with the wider energy sector and other elements of CNI, to which the NIS Regulations apply.

Applicability

The guidance is designed to be equally applicable to both new and existing DERs and is intended to help establish a common cyber-security baseline across a range of organisations, including, but not limited to, generators, service providers and aggregators.

The scope includes all non-domestic DERs (including wind, solar, gas, hydro, battery storage, etc) that are connected to electricity distribution networks, as well as supporting third-party organisations (e.g. aggregators and control centres)[1].

Classification of DERs

To support the adoption of the connection guidance, and to ensure it may be tailored to specific DERs, groupings based upon the number of sites and installed capacity have been identified. In total, four groupings (baseline, small, medium and large) are identified within the connection guidance, as shown in figure 1, below.

In addition to the four groupings identified, the guidance also outlines the following additional groups that directly support DERs[1]:

1. control centres
2. third party support or managed services
3. dedicated operational technology
4. remote access.

Figure 1, below, taken from the DER – Cyber Security Connection Guidance[1], shows all eight groupings and the criteria to be applied when identifying which group a DER belongs to. Note: these groupings are expected to remain under review and will be updated as the technology matures.

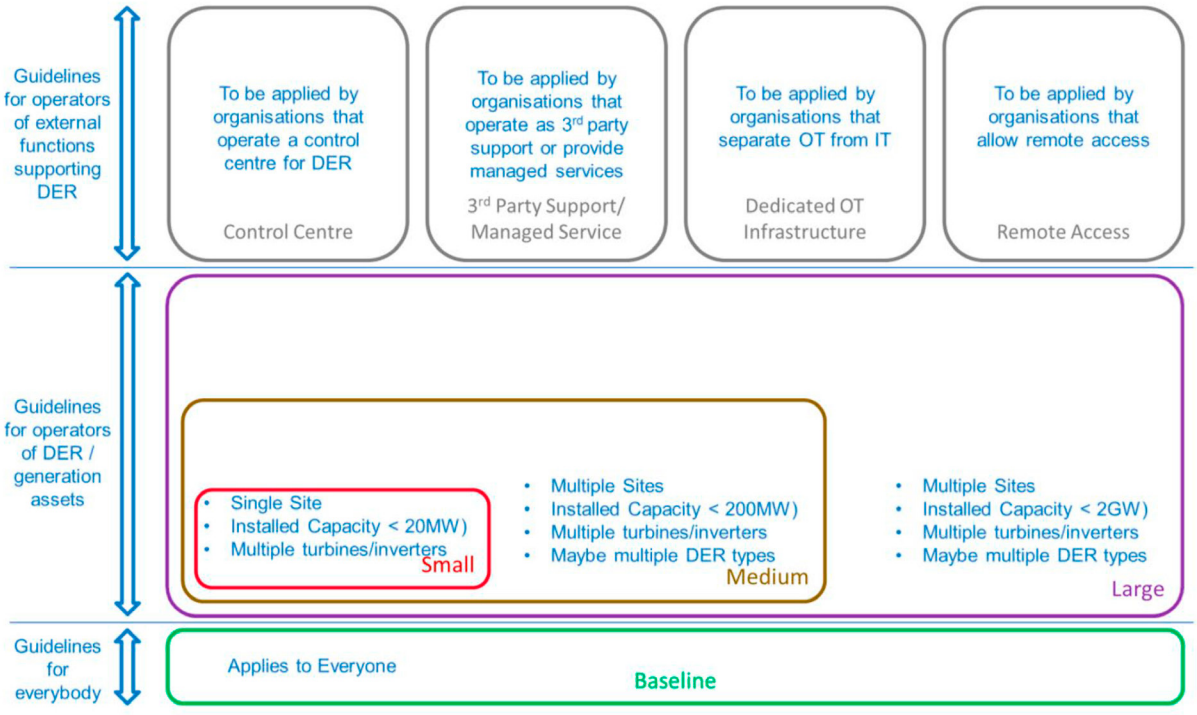


Figure 1: DER Groupings from Cyber Security Connection Guidance[1]

Compliance with the Guidance

To support adoption of the guidance and support a risk-based approach, BEIS and ENA proposed a three-tier approach to identifying the levels of compliance for DERs (including those of 'external functions supporting DERs') that will be required to be achieved against the guidelines. These are defined as follows[1]:

Foundational – This tier would be considered 'Not Achieved' within the NIS CAF, with foundational compliance requiring that DERs satisfy a subset of the 'Partially Achieved' IGPs from the CAF.

Light – Broadly aligned to 'Partially Achieved' within the CAF but, in some cases, may also include IGPs from the 'Achieved' level.

Full – Fully aligns with the 'Achieved' IGPs contained within the NIS CAF.

An overview of the guidelines associated with each of the tiers (i.e. foundational, light and full) aligned to the 39 outcomes of the NIS CAF is presented within table 3 of Cyber Security Connection Guidance – (see Appendix B).

2.3 Findings

This section presents an overview of the key findings and recommendations resulting from our assessment of the Cyber Security Connection Guidance.

2.3.1 Key Observations and Recommendations

In reviewing the Cyber Security Connection Guidance, it is clear that the intention is to improve the overall cyber resilience of DERs to ensure that they are able to satisfy their operational requirement – to meet electricity demands within the distribution networks to which they are connected. However, it is considered that, in their current form, the guidelines do not fully address the unique operating environment of Distributed Restart.

The following observations, relating specifically to the impact on the project, and recommendations have been made:

1. **Applicability is limited.** Whilst the scope of applicability applies to DERS that are controlled through National Grid ESO and NIS regulations applies to transmission connected generators with aggregate of 2GW and above, there is no guidance for transmission connected generators below 2GW.

   Recommendation 1: Clarity should be sought from BEIS and the ENA regarding the applicability of the guidance to transmission-connected generators <2GW. Where there are specific legal and/or regulatory requirements that include transmission-connected generators within their scope (e.g. the NIS Regulations), this should be clarified within the connection guidance. Where gaps remain, National Grid ESO/TOs should develop bespoke cyber security guidance specifically covering transmission-connected generators. Any guidance or contractual requirements developed by National Grid ESO/TOs will require that National Grid ESO/TOs or DNOs ensure that the generators are audited, either independently (e.g. as in smart metering) or by National Grid ESO/TOs to ensure ongoing compliance, as they may not be covered by external organisations.

2. **There is no specific guidance for distributed restart generators.** The current guidance does not consider the role of distributed restart generators (i.e. those DERs designed and contracted to fulfil a distributed restart requirement).

   Recommendation 2: Where DERs are contracted as Black Start generators, clear cyber security requirements should be included within contracts. Where applicable, these should be tailored specifically to the DERs and be derived from risk assessments (i.e. risk-based). In addition to developing specific cyber security requirements, ENA should also consider developing supporting guidance for those DERs, to which the additional requirements apply, to support their implementation.

3. **Role of anchor generators.** In developing the DER groupings, the guidance includes various impacts, ranging from loss of supply, to frequency instability, to disconnection of DERs from the distribution network. However, the impact statements developed do not consider whether DERs, where required, will be able to act as an anchor generator within a DRZ, whether they play a crucial role in delivering a distributed restart, or the proportion of the required supply the DER provides within a given DRZ. As a result, DERs are grouped based upon impact to normal operations and not all circumstances are covered.

   Recommendation 3: It is recommended that an additional DER grouping be created that will cover anchor generators and distributed restart DERs.

4. **Groupings do not consider the impact on DRZs.** The sizing thresholds to be used in grouping DERs are top-down (based upon combined generating capacity) and do not consider the importance of a DER to meet frequency and supply demands within a given DRZ. As the UK moves towards more distributed resources, the impact of a loss of failure of a DER would likely be limited to the distribution network to which it is connected. Failures associated with the loss of multiple DERs may affect multiple, independent zones.

Recommendation 4: When placing contracts with DERs to deliver a distributed restart capability, the designated responsible party should take into account the importance of the asset within a DRZ (e.g. if a 'small' DER provides 50% of capacity in a DRZ it may be required to have more stringent cyber security requirements).

5. **Communications service providers are not considered as 'external functions'.** Whilst there is a group which focuses upon the provision of remote access, there appears to be no consideration as to how this capability is achieved. Similarly, there is no consideration of how communications networks and control systems are extended to DERs. The groupings within the existing guidance do not identify communications service providers, some of which may be external to National Grid ESO, TOs and the DNOs, as a specific group.

   Recommendation 5: Within contracts, the division of responsibility between National Grid ESO, TOs, DNOs and DERs needs to be made clear. Contracts with DNOs and DERs should make clear who owns the requirements for ensuring cyber resilient communications exist between DERs and DNOs/National Grid ESO/TOs to meet day-to-day and distributed restart requirements.

6. **Guidance does not fully align with the NIS CAF.** Whilst aligned to the CAF, the DER cyber security connection guidance document does not follow exactly the same process and can appear confusing. This may cause problems in baselining the cyber resilience of DERs against that of other Operators of essential services (e.g. National Grid ESO, TOs and DNOs) as they will not be required to satisfy the same IGPs or comply with the same baseline standards.

   Recommendation 6: When developing contractual requirements for DERs involved in a distributed restart, National Grid ESO/TOs or designated authority should consider developing requirements that are fully aligned to the NIS CAF. By aligning the requirements in this way, it will be possible to map the levels of compliance across the different stakeholders (e.g. National Grid ESO, DNOs and DERs).

7. **NIS applicability should be reassessed.** De-centralisation and digitalisation, driven by a need for decarbonisation, means that the UK energy supply will become increasingly reliant upon DERs of all types in the future. This transition means that DERs will provide an increasingly significant role in meeting the UK's energy demands and should be designed and built in a manner that ensures they are, and remain, resilient to cyber threats. At present, DERs are not currently considered essential services under the NIS Regulations and, based upon the DER connection guidance, it is unclear whether or not this is a future aspiration.

   Recommendation 7: To ensure all DERs are designed, constructed and operated with cyber resilience in mind, and to support a common baseline to be established across the industry, it is recommended that BEIS consider whether DERs should be considered essential services now or in future. Particular attention should be given to those DERs that provide a distributed restart capability, with a focus upon those that are anchor generators.

2.4 Conclusion

The assessment identified increased levels of risk.

The initial risk assessment presented in the Design Phase I report found that the increased interconnectivity between large numbers of stakeholders, and a potentially greater reliance upon automation and control systems, could result in increased levels of cyber security risk and a broader attack surface. More specifically, where systems become more interconnected and interdependent to deliver a distributed restart, the impact of a cyber-attack could have an impact far beyond the system owner/operator. This remains unchanged with the introduction of cyber guidance as the project will need to increase DER cyber resilience beyond the scope of this guidance.

Risk mitigations were identified, including cyber security of DERs.

To help reduce the levels of cyber security risk, a number of mitigations were identified. The mitigations cover the main risks affecting the capability and include the supply chain, third parties, people, processes and technologies.

Of relevance to this review is the mitigation relating to the security of third parties, which recommended that contractual requirements be placed onto communications providers and DERs to ensure proportionate cyber security controls are in place. The mitigation recommends that:

"Clear cyber security requirements should be placed upon third-party communications providers, as well as those DERs that are considered Black Start/distributed restart generators, with particular focus being placed upon anchor generators. The requirements should cover security of key operational systems, their provision, maintenance and monitoring, as well as the personnel security controls required to provide appropriate levels of security assurance and protection."

The intention of this requirement is twofold:

- to protect DNO and National Grid ESO communications networks and operational systems/services from attack from DER networks, such that they are able to deliver a distributed restart
- to ensure DERs are able to respond to demand instructions from microgrid controllers within specific Distributed Restoration Zones (DRZs) and meet electricity demands.

3. Cyber Security Analysis

Cyber security is a crucial element of ensuring a reliable, resilient power system. A review has been used to highlight possible risks and mitigations.

3.1 Introduction

The cyber risk assessment presented in the Design Stage I report on the initial four organisational models found that:

- private networks have significant advantages over public networks, including limiting the potential attack surface and avoiding connections to the public internet
- fixed networks have the advantage over wireless and satellite as jamming and interception of traffic are generally more challenging
- point-to-point network links make a cyber-attack more challenging as physical access or proximity is required
- private networks will require security expertise to be deployed to design, build, operate, and maintain the network. These tasks can be outsourced, provided the risks associated with third parties are well managed
- privileged insiders need to be managed using a set of security controls and procedures to ensure they do not deliberately or accidentally disrupt the network
- nation-state actors may have the ability to undertake attacks on the fixed, wireless, and satellite networks in order to pre-position for a conventional attack. The use of private networks may limit the threat of hostile state actors and those associated with the supply chain.

Further, ongoing review has been conducted to align this work with the central organisational model. In this model the DNO leads the localised power island growth as part of a pre-defined plan. Once this plan is executed, National Grid ESO becomes the strategic lead and directs further growth options. This requires interconnection of systems, distributes responsibility and makes use of an automated interface through a Distribution Restoration Zone Controller (DRZ-C).

The findings of this review are presented in this chapter covering telecommunication options, end to end risk assessment and mitigation strategies. In addition, more general considerations for cyber security in a Black Start situation are provided.

3.2 Additional Cyber Considerations

Additional factors were considered in the assessment such as network availability and data latency from one point to the other, which can have a significant impact on the overall security of the system.

Network availability is critically important when considering which telecommunication option to use. Other factors to consider include latency, redundancy, or environmental factors and it is quite possible that these factors may drive the decision on a final telecommunication option more than the perceived security risk of the option.

Economic factors could also play a role in determining the final telecommunication option. It may be more economically feasible to choose one option over another while providing a similar security posture.

The following section provides a general overview of additional factors that are important to consider when making a final decision on a telecommunication option.

3.2.1 Data and Network Availability

Latency and redundancy are critical components in determining which network option to use. The inherent latency in some technologies, such as satellite communications, may prevent them from delivering data in the required time

frame. A lack of network redundancy and geographically diverse network paths could lead to the inability to coordinate a Black Start, depending on the cause of the blackout.

The initial cause of a blackout could have a critical effect on the ability of the network to maintain communications. It is important to consider both the power engineering scenario and other blackout scenarios and the effects they might have on the ability to execute a Black Start.

A kinetic physical attack or a natural disaster could lead to devastating infrastructure damage. A network architecture that does not include network redundancy and diversity of network paths could critically hinder the ability to deliver the communications required for Black Start.

A cyber-attack that is focused on meaningful impact to Critical National Infrastructure will require a high level of confidence by the attacker. To perpetrate this type of an attack, an adversary will require an in-depth knowledge of the system architecture, operation, and controls; this will require the adversary to establish a significant network presence before executing the attack. A blackout caused by this type of high-confidence cyber-attack could also lead to a network availability problem. It is plausible that every action taken using the compromised network would be seen by the adversary, who could then take remedial action. This would also extend to voice communications, i.e. if the voice communications are established through the same networks as data communication. In this scenario, it would be imperative to identify the compromised network and have an alternate communication medium available.

The recommendation is to establish an out-of-band communication channel where the channel should use different physical infrastructure than the final telecommunication option channel. An acceptable out-of-band communication channel is one that would remain operable during a blackout and should be tested periodically. Out-of-band communications are critical for incident response and disaster recovery scenarios. Without a trusted channel, it would be impossible to react to a dynamic situation during a high-confidence attack or to coordinate a disaster response during a loss of the primary network.

3.2.2 Economic Factors

While it is technically possible for public and private telecommunications options to be equally able to provide security controls, it may not be economically feasible. It is reasonable to consider that a large organisation such as a public network provider may have an advantage in the economic ability and experience to provide network redundancy and the qualified personnel needed to monitor and maintain the network. It is important to note that decreasing the exposure of internet-connected links does generally reduce the attack surface, but it does not eliminate risk. There are few truly air-gapped networks, as most Operational Technology (OT) networks have links indirectly connected to the internet through Demilitarised Zones (DMZs) which are connected to the enterprise environment. Furthermore, there are numerous other vectors that are commonly used to infiltrate OT environments such as widely published phishing campaigns, use of USB storage devices, and compromised websites.

It is possible that a public internet provider could provide a resilient and secure network due to its investment in personnel and equipment. However, this would still require a significant investment to ensure compliance with contractual agreements on security controls and service-level agreements. Using a public service provider would also require the use of an encrypted transport mechanism and consideration of the implications of key management.

3.3 End-to-End Cyber Risk

It is important to have a wide range of information on the security controls of the multiple parties and integration of the networks in order to fully assess the end-to-end cyber risk.

There are several factors that need to be considered when deciding on an end-to-end communication model and before moving forward into an implementation phase.

As described in the Design Stage I report, when networks with varying levels of security controls and maturity are connected, the increased connectivity will lead to increased cyber security risk. To decrease this risk, it is important to consider the current structure of the network and the ability of the connected entity to recognise and respond to a cyber event.

3.3.1 DER Connectivity via National Grid-Provided Network Only

The connection of DERs directly to the National Grid-provided network presents a level of homogenous risk. In the DER connectivity to the National Grid-provided network only model, a low-level risk can lead to a large impact due to the centralised nature of the National Grid-provided network and the existing connections into DNO networks. Furthermore, a catastrophic incident on the National Grid-provided network could cause loss of communication between all other networks in this system architecture.

Connecting the DERs to the ESO networks would also most likely lead to more standardised security requirements and enforcement strategies as National Grid security requirements are applied to DER connections.

Additionally, the National Grid-provided network may increase overall system resiliency.

3.3.2 DER Connectivity via DNO Network Only

DER connectivity via DNO networks adds a level of abstraction between the National Grid-provided or TO networks and the DER. This may have the effect of adding a layer of protection to the National Grid ESO networks.

The localised nature of the DNO networks could also improve the ability of the DNO to monitor the DER traffic and ensure that appropriate controls are enforced. In other words, having fewer DER sites to monitor may help with visibility, assuming that the DNOs have a robust cyber security strategy and sufficient resources to effectively monitor and enforce security requirements of the DER to DNO network connections.

3.3.3 DER Connectivity via National Grid Network or DNO Networks

The hybrid strategy of allowing DER connections to either the National Grid network or the DNO network may have the greatest economic benefit. By allowing DERs to connect into the system at the nearest geographic location, infrastructure cost could be reduced.

A possible disadvantage with this model is the lack of standardisation. A lack of standardisation would likely lead to greater difficulty in security monitoring and analysis for the connected entities. This, in turn, would lead to disparity in requirements and enforcement of security controls for the connected DERs.

3.4 Mitigation Strategy Assessment

Applying an established governance model such as the National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF) or the United States National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) can significantly enhance the security of the connected entities. The DER-Cyber Security Connection Guidance bases much of its guidance on the NCSC CAF. This can be further enhanced by applying specific use case and mitigation strategies such as the MITRE ATT&CK for ICS framework (collaborate.mitre.org/attackics/index.php/Main_Page). The MITRE ATT&CK for ICS framework is a resource that provides known attack vectors and techniques commonly used by adversaries and their mitigations. Using this specific threat-versus-control methodology can help an organisation ensure it is maximising the return on its security controls investment.

The policy and administrative controls mentioned in the Design Stage I report are good security practice. The technical controls mentioned, such as anti-malware and system hardening, do provide some protection against established threats. However, there is a need for controls to provide additional protection against emerging or zero-day threats as they are likely to be encountered when dealing with an advanced threat actor. In other to achieve the desired secure-by-design posture, it is important to realise that some additional technical controls will be required to achieve a level of network visibility that is sufficient to mitigate advanced attack vectors.

While it is important to maintain an established electronic security perimeter, firewall monitoring alone is not enough. Significant security advantages can be gained by employing continuous network security monitoring (NSM) and security information and event management (SIEM) integration. These technologies can be further enhanced by employing a deny-by-default network architecture at the local area network (LAN) level using products such as deterministic software defined network (SDN) technology for OT networks.

3.4.1 Adversary Mindset

Since the focus of the current phase is the viability and security of current communication paths, it is imperative to remember that a skilled adversary such as a hostile state actor or a technically advanced cybercriminal would likely be focused on maintaining a presence on the network for an extended period of time. The heterogeneous nature of OT networks requires a significant amount of skill and time to learn the operation of the system in preparation for a high-confidence and/or cyber-kinetic attack.

Network security monitoring is essential. One should not assume that a cybercriminal or hostile state actor will act as soon as their presence is established on the network. It is highly unlikely that an adversary would be able to maintain this presence without causing some type of observable anomaly such as accidental settings changes, abnormal machine-to-machine communications, or unexpected device behaviour. For this reason, robust technical controls must be mandated, implemented, and monitored. These controls should include a combination of network security monitoring and traffic analysis.

3.4.2 Incident Response

As the networks between the National Grid ESO, DNOs, and DERs become more interconnected, the scope of required monitoring and response grows exponentially and will require a high level of organisation and cooperation between the connected parties.

One should also consider incident response in determining the end-to-end connection strategy. A detailed inventory of all network connected assets, a holistic view of network communication paths, and a baseline of expected conversations between nodes should be established and monitored.

When an incident is identified, indicators of compromise must be shared with interconnected organisations to establish the scope of the breach. Iterative sharing of specific threat indicators and coordinated action can severely affect the ability of the attacker to establish a meaningful presence on the system or systems. This will also help in the forensic analysis to determine the intent of the adversary and the vector of the intrusion.

3.4.3 Security Return on Investment

As a system architecture is evaluated, it is important to consider where, how, and by whom security controls will be implemented. In general, securing a system is on a sliding scale of cost versus reward in the terms of security posture. System architecture provides the most security value and the least economic impact and offence offers very little value for the cost and may result in ethical and legal implications (see figure 2).[4]

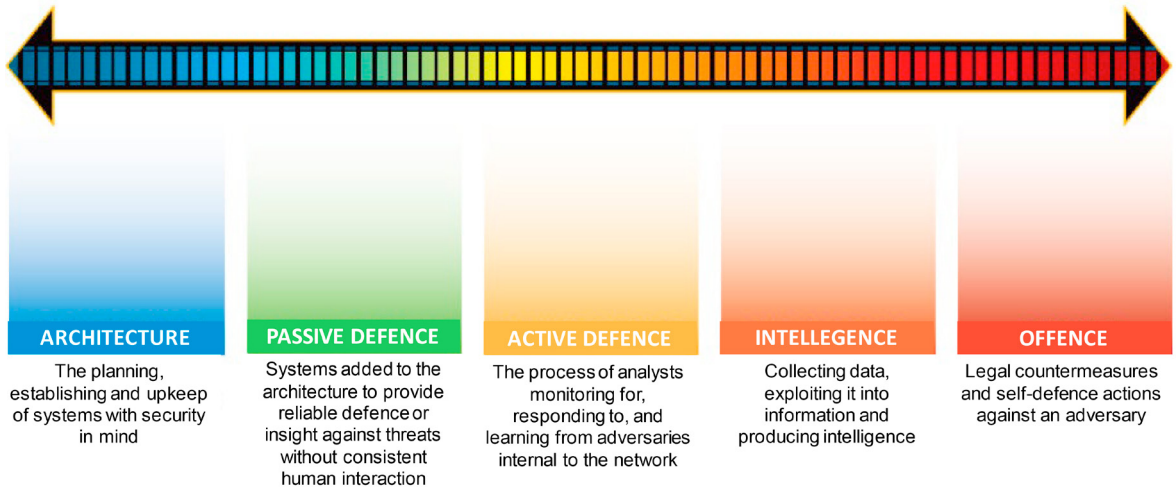


Figure 2: The sliding scale of cyber security[4]

While the current focus of this assessment is on backbone communication architecture, it is important to keep in mind that an integrated system of passive defence is also critical to effective network defence. This will require investment in tools and personnel. The ability of the organisation/entity to meet these requirements should be considered when choosing telecommunication options, DER connection strategy, and future system requirement phases.

3.5 Considerations for Black Start

3.5.1 Complexity of Recovery

As the network architecture grows and spans across multiple organisations, recovering from an attack or disaster becomes much more complex. Coordination between National Grid ESO, TOs, DNOs, and DERs becomes paramount. Furthermore, having a well-organised plan that has been exercised helps reduce confusion and prevents lengthy delays in recovery.

3.5.2 Key Spare Equipment

Sometime between late 2008 and early 2010, a small digital weapon Stuxnet, was released in Iran on the Natanz uranium enrichment plant. The Stuxnet “worm” sabotaged the centrifuges that were being used to enrich uranium, making them fail at a high rate. The failure of this equipment slowed and at points stopped Iran’s ability to enrich uranium. Having spare equipment available if key primary equipment fails is essential. Whether such a failure is caused by a cyber-attack, natural disaster, or design failure, not having enough spare equipment to replace key online equipment reduces the ability to perform a successful Black Start.

Spare equipment will require a maintenance and testing strategy to ensure that it is operational. The cost of maintenance and procurement of required spare equipment will need to be factored into the operational budget and the contracts of any new systems.

Spare equipment is essential to react to a cyber-kinetic attack where equipment may be unrecoverable. However, in the case of self-propagating network malware or a worm, it is probable that previously un-infected equipment would be compromised as soon as it is connected to the network. This further illustrates the importance of a robust detection and response strategy.

3.5.3 Latency/Bandwidth

Network latency is of concern to protection communication. The ability to provide wide area protection communication is even more important when the Black Start involves distributed renewable energy resources, because of the low inertia and determinism of these energy sources. Additionally, the network must be purposefully designed to ensure that adequate bandwidth is provided.

3.5.4 Out-of-band Communication (Manual Restart)

Black Start exercises should be conducted to test responses to a cyber-attack. For this scenario, it could be assumed that the blackout was caused by a cyber-attack in which an adversary attacked the electronic devices within the substation. This attack would not only affect Intelligent Electronic Devices (IEDs), but also the networking infrastructure (e.g. switches and firewalls) of the LAN and Wide Area Networks (WAN).

Without communications, troubleshooting and restoration is greatly slowed by the need to physically travel between substations. To reduce restoration time, multiple out-of-band communication systems should be used. These techniques could include a separated network, an emergency long distance Wi-Fi network, or a military radio system. Even an intermittent voice link provides a significant improvement over the no-communication option. The key lesson is the value of ancillary communication channels that are decoupled from the utility infrastructure under attack.

3.5.5 How Do You Trust Known Good Configurations?

Nearly all Information Technology (IT) and OT professionals have experienced equipment failures and accidental configuration changes that have made systems stop performing as designed. In some cases, the hardware failed and had to be replaced, in other cases settings were changed and the system acted abnormally. With hardware failures, having a clean and trusted backup is crucial. In the case where changes are made, a backup configuration should be used to compare the current configurations to a last known good configuration. But how do you know those backup configurations are accurate?

Last Known Good Configurations

All changes to equipment should be approved and documented. Any changes to the architecture should be noted on existing diagrams and published. When a configuration change to settings must be made, a board of subject matter experts should review those changes and approve them prior to the changes being made. Prior to and after a settings change, a backup of the current configuration should be made. These backups should be encrypted, a cryptographic hash value should be generated, and a copy of these files stored offline and offsite.

These backup files will be used to revert to a known good state when an outage occurs. Additionally, these files can be used to compare a current configuration against a last known good backup.

3.5.6 Network Security Monitoring

Network Security Monitoring (NSM) is another key item in protecting IT and OT networks. NSM helps administrators keep track of access to equipment and changes to equipment settings.

Expanding software defined network (SDN) equipment should be considered. SDN solutions eliminate unnecessary network traffic, allow better control of communication between devices, and improve security. The advantages SDN has over traditional networking are traffic programmability, more cyber security awareness, and the ability to create policy driven network communication.

With SDN, only allowed communication paths are programmed into the network equipment; any additional communication is blocked by a default “deny all” rule. Communication that is blocked by the default “deny all” rule is called a “miss”. These “misses” in communication can then be sent to a central server where they can be viewed for analysis. Unlike traditional IT network switches that allow all communication, SDN only allows devices to transmit and receive what has been deterministically engineered. Anything not programmed is an alert to cyber security personnel to investigate the new traffic. NSM and SDN are two great tools to help cyber security personnel detect and deter threats to their networks.

Communication Providers, DERs, and Contractors

It is not uncommon to see contractors from other companies working within the confines of one's organisation. This allows direct access to equipment and networks by outside personnel. Physical security should be of the utmost importance when allowing outside personnel into one's facilities and areas of work. Disabling all unused network ports, denying the use of USB devices on the equipment, requiring all contractors to be escorted, and limiting access to areas where sensitive equipment is housed are big steps in preventing physical changes to the equipment.

3.5.7 Continuity of Operations (COOP)

The UK Government defines continuity of operations as the "ability to maintain critical functions and to ensure that they can continue to perform their functions in the event of an emergency, so far as is reasonably practicable. The duty relates to all functions, not just their emergency response functions."[4]

Every organisation should develop a COOP plan and test this plan regularly to ensure that leadership and those responsible for maintaining operations are aware of what is required of them. This plan should include the following areas:

- Readiness and Preparedness Phase
- Activation and Relocation
- Continuity of Operations
- Reconstitution of Operations.

For Black Start operations, a plan should be developed, reviewed, and signed by all parties, and a simulation should be conducted with those parties responsible. The simulation should consider scenarios where primary and possibly secondary forms of communication have failed. Also consider adding changes to Black Start procedures in which a key element in the restart process is not available; how would those responsible for restoring operations work around it?

How to Conduct Tests

The test can be as simple as key personnel coming together for a desktop exercise. The desktop exercise will present different scenarios that will test the knowledge and processes of key personnel on their roles in restoring power from a Black Start. In many organisations people move out of roles or take jobs with other companies, so it is important to conduct these tests to maintain knowledge and to teach new employees.

The project recommends testing Black Start equipment to restore power by using key personnel to direct the operations of the restart to evaluate their ability to command and control the operation.

What to Test?

The purpose of the test should be to see how personnel respond during a blackout scenario, and how power would be restored. Different scenarios of how power was disrupted should be given as each may require different methods of recovery and in some cases different personnel.

3.6 Conclusion

To achieve the secure-by-design posture desired by the Distributed ReStart project, each aspect of the network architecture and control design should be considered. The chosen network architecture must reliably provide data on time and be robust enough to withstand any foreseeable disaster. Additionally, an out-of-band communication channel should be established to ensure trusted communication in the event of a cyber incident and as a fallback plan in the event of network outage. The network resiliency approach must include spare equipment and a backup strategy should a clean sheet recovery be necessary.

Regardless of whether the end-to-end connection model is via the National Grid-provided network or DNO networks, a required connection architecture and mandated set of technical controls must be implemented. By furnishing a common interface and expected data flow, one can create a repeatable design and decrease the monitoring burden for security personnel.

The entity or entities who are connected to DERs must have the ability to provide the necessary infrastructure and security controls to ensure the connection is monitored and secured. The cost of staffing, spare equipment, and maintenance should be factored into the overall budget of the connected party or parties.

Network security monitoring with SIEM integration coupled with competent security personnel can drastically improve the overall security posture of a system. Using an active defense of continuous monitoring, response, threat intelligence consumption, and environmental manipulation can provide a security posture that static alerting alone cannot. Should an incident occur, a well-defined sharing mechanism between parties must be established to distribute indicators of compromise to establish the scope and impact of the breach.

4. Functional Specifications for Operational Telecommunications

The functional specifications required for the telecommunications systems suitable for manual and automated restorations, standards, resilience and technology suitability have been determined through engagement with participants, suppliers and stakeholders.

4.1 Introduction

The previously published Distributed ReStart reports for Organisational, Systems and Telecommunications (Viability Report, Design Stage I report) presented the assessment of the current telecommunications infrastructure of the electricity industry participants – National Grid ESO, TOs, DNOs and distributed energy resources. These reports identified the various technologies that are available now and in the near future, identified gaps between what is currently deployed and what will be required to provide resilient end-to-end telecommunications to support Distributed ReStart.

The Distributed ReStart project is now able to provide a set of technical and non-technical requirements for telecommunications that technology providers will need to satisfy to enable a resilient Distributed ReStart service. The approach that has been taken is to recommend solutions that are technology agnostic and are not necessarily 'one size fits all'. Industry participants may choose to adopt any technology or combination of technologies and solutions to suit their circumstances but must meet the functional requirements.

As described in the Design Stage I report published in October 2020, there are several factors that play a crucial role in determining the preferred solution for each industry participant. These include:

- cost – capital and operational
- existing technology utilised by participant and familiarity
- terrain and access to site
- maintenance and support for the technology
- reliability
- availability
- policies and regulations in place and future roadmap.

4.2 Approach

As described earlier, rather than specifying a technology, the Distributed ReStart project seeks solutions that are technology agnostic. The approach taken has been to develop a set of functional specifications that will support the organisational models developed by the project and described in earlier Organisational, Systems and Telecommunications reports. Four organisational models were initially explored (National Grid ESO automated control, National Grid ESO manual control, DNO automated control, DNO manual control) which has now led to the development of the Central Model. The telecommunications solutions for the Central Model align with the DNO automated control model.

It is anticipated that the roll out of telecommunications solutions would be a gradual process across GB networks and wouldn't be 'one size fits all'. Therefore, functional specifications have been developed that would support both the manual and automated control models. The functional specifications for the manual control model would support participants who haven't installed a Distribution Restoration Zone Controller (DRZ-C), while the functional specifications for the automated control model would support participants that have installed a DRZ-C and have adopted the roles and responsibilities of the Central Model.

In developing the functional requirements for the manual control model, the project concluded that the existing functional requirements for the National Grid OpTel and DNO telecommunications networks support the functionalities

required for a manual Distributed ReStart. These functionalities are for telemetry, frequency monitoring, tele-protection and voice communication. However, these requirements need to be extended to DER connections.

In addition to these functionalities, the automated control model incorporates the requirements for a DRZ-C. The project engaged the services of vendors to develop these DRZ-C functional requirements.

The project engaged extensively with stakeholders to help shape the functional requirements. The resulting outputs aim to give guidance on the technical and non-technical requirements that would enable a suitable technology and solution to support a Distributed ReStart restoration service.

4.3 Functional Requirements

The telecommunications functional requirements to support Distributed ReStart are broken down into the following sections:

- technical requirements
- configuration, environmental and other requirements
- bandwidth requirements
- resilience requirements
- supported protocols
- cyber security considerations.

4.3.1 Technical Requirements

This section lists the technical requirements for telecommunications infrastructure to support data and voice communication for both the manual and automated control models. Current GB Black Start restoration processes are based on the manual control model, hence do not support the use of a DRZ-C. The automated control model incorporates a DRZ-C within the network design. The preferred Central Model falls into this category.

The technical requirements to support the telecommunications networks are described in terms of various considerations including interfaces, protocols, bandwidth, latency, environmental, configurations and power requirements. The technology type and network configuration play a crucial role in determining whether the technical requirements criteria are met, the critical parameters being data rates, latency, bandwidth and independent power resilience of the end-to-end solution.

Requirements	Description	Values
End-to-End Delay	This defines the maximum allowable communication channel ‘end-to-end’ delay.	The maximum allowable communication channel ‘end-to-end’ delay for the different categories should not exceed the specifications for teleprotection systems (ENA 48-6-7). Category 1 – 6 milliseconds Category 2 – 10 milliseconds Category 3 – 30 milliseconds SCADA services – 100 milliseconds The Central Model which incorporates a DRZ will require the following: Fast balancing action/Phasor measurements – 30 milliseconds Slow balancing action – 90 milliseconds No time critical data – 100–200 milliseconds
Differential Delay	The requirements for differential delay under steady state conditions.	The maximum admissible differential delay for the different categories should be as specified. (ENA 48-6-7). Category 1 – 400 microseconds Category 2 – 10 milliseconds Category 3 – 30 milliseconds

Jitter	This defines the maximum permissible jitter.	The maximum permissible jitter shall be according to ITU-T G.823 (2048kbit/s) specifications for a digital service, ITU-T G.824 (1544kbit/s), ITU-T G.825 (SDH) as appropriate.
Manual Switching	This will define the capability for manual and automatic switching.	It shall have the ability to disable automatic switching for specific services; e.g. SCADA and protection services.
Specifications for Communications Protocol Requirements	The requirements to specify the communication protocol that needs to be supported.	It should support protocols required for SCADA, protection and voice services such as DNP3.0, 6870-5-110, IEC 608705 – 101, ICCP (60870-6), 61850 Secure File Transfer Protocol (SFTP) SNMP v3 (for device management) TCP/IP, MPLS,61850, 61870-104, Modbus, C37.94. x21, RS232/485, audio. The protocol requirement for an automated restoration is listed in protocol table (table 5).
Telephone User Requirements	This defines the control centre and substation telephone user requirements.	The operational telephony system shall be designed to meet the control centre and substation user requirements. (See section 4.5).

Table 1: Technical requirements

4.3.2 Configuration, Environmental and Other Requirements

The non-technical requirements apply to all manual and automated restoration processes. These include environmental factors, segregation, power resilience and other factors.

Requirements	Description	Values
End-to-end Service Availability	The end-to-end availability for a single-routed service (an un-switched service).	1. This shall be minimum of 99.94% over a rolling 12-month period. 2. There shall be no more than one break in service of greater than 10 seconds duration in any one year for any single service. 3. The difference between the total number of severely errored seconds and the total number amount if unavailable time expressed as a percentage of total time shall not be greater than 0.002%. ENA 48-6-7.
Service Density Fast Communication Services	During normal operation, the maximum percentage of fast communication services to be carried on one physical communications link between any two nodes.	It shall not exceed 10% of all fast communication services.
Service Density: SCADA, Operational Telephony and Operational Data	The maximum percentage of SCADA, operational telephony or operational data services to be carried on one physical communications link between any two nodes.	It shall not exceed 15% of all services in the respective category. (Excluding the Control Centre services).

Failure Isolation Procedures	The compliance with the principle of no knock-on failures and have proactive automatic shutdown procedures in place to prevent a failure of network equipment triggering mal-operation of other non-directly interconnected network equipment or systems within the application layer.	Compliance with principle of no knock-on failures as in the description. ENA 48-6-7 Issue 2.
Restoration of Service	Priority to restoration of service.	Priority to restoration of service in accordance with ENA 48-6-7 Issue 2.
Physical Separation Design	Requirements for physical separation between specified separately routed telecommunication services along the entire route for cabled services.	Minimum of five metres physical separation between specified separately routed telecommunication services along the entire route. ENA 48-6-7 Issue 2. This shall be risk assessed if the above is not achievable. This applies to wired services.
Segregation of Circuits	Requirements for segregation of network for localised disaster events, such as storm damage, flooding etc, not to cause degradation of service.	Circuits should be segregated such that localised disaster events (storm damage, flooding etc) would not result in degradation of service. This applies to wired services.
Location of Equipment	Requirements for location of equipment securely and away from areas liable to flooding.	Required as in the description.
Change of Routes	Requirements for continued service operation where service route has changed, e.g. due to network failure or planned infrastructure change.	Required as in the description. ENA 48-6-7 Issue 2.
Power Source	Requirements for type of power source, redundancy and specifications.	The telecommunications equipment shall be designed to operate from a 24V/48V DC power source. The equipment shall be capable of being powered from two separate supplies. ENA 48-6-7 Issue 2.
High Voltage Sites	Requirements for installations and safety at hot sites.	All fibre inlet cables and cross-site links must not contain any metallic elements e.g. foils or strength members. If copper is used at hot sites (e.g. for PSTN, ISDN, SCADA, operational data or telephony services) then the metallic conductors shall be isolated from earth by an approved isolation barrier. No joints are permitted in the hot zone. Only hot site trained personnel are permitted to install or work on copper delivered infrastructure.
Environmental Performance	Requirements for environmental and test performance of equipment at HV electrical substations.	Equipment located in substations and power stations shall be immune to electrical interference. All proposed equipment shall comply with BS EN 61850-3.

Equipment Design	Requirements for equipment to work without error or degradation for the environmental conditions specified for these locations.	It shall be designed to work without error or degradation for the environmental conditions specified for these locations.
Operation in Extended Temperature Ranges	Requirements for equipment to work at certain temperatures.	Where mounted within an enclosure, it shall be capable of normal operation at a temperature 15°C higher than the upper temperature limit of the environmental class. When operating in extended temperature ranges the equipment should use passive cooling to minimise power requirements and to avoid reliance on any active components such as fans.
Earthing in Substation Telecommunications Room	Requirements for earthing in substations.	The earthing policy adopted should be such that the performance of existing substation equipment will not be impaired. See also ENA 48-6-7 Issue 2.
EMC Requirements	EMC requirements so it does not impair the performance of any other equipment in the substation by compromising the existing earthing arrangements.	All equipment installed in substations meets the EMC requirements stated and does not impair the performance of any other equipment in the substation by compromising the existing earthing arrangements.
Safety and Site Access	Requirements for safe access to site and safety of equipment.	There is a requirement for the equipment to be in a secured location and safe access for personnel.
Business Continuity and Disaster Recovery	Requirement for Business Continuity and Disaster Recovery procedures.	DR procedures should be capable of switching or re-routing of operational telecommunications services 24 hours per day, 7 days a week, within 15 minutes of being instructed to do so.

Table 2: Configuration, environmental and other requirements

4.3.3 Resilience Requirements

The electricity industry, with support of the UK Government (BEIS) and the regulator (OFGEM) reviewed the resilience of GB to Black Start events after a series of major blackout around the world. Exercise Phoenix in 2006 recommended that the loss of supply resilience of the grid and primary substations for the GB electricity networks be extended to a 72-hour period. According to Engineering Recommendation ENA G91, the baseline requirement is for the core transmission and distribution substations to be designed so that they are resilient for a minimum period of 72 hours. This means that the substation protection, control and SCADA functions should be available such that the site can be safely energised within 72 hours of the inception of a Black Start event.

In view of this standard and the recommendation, Distributed ReStart functional specification specifies the following:

Mains Independence Resilience	Requirements for mains independent electricity supplies to telecoms rooms at substations and control centres.	In the event of a mains failure, there shall be no loss or disruption of communications services for at least 72 hours. This provision will not require manual intervention to achieve. Mains independence shall be maintained during outage and planned maintenance conditions. To achieve this, all the active devices (any device that requires power to operate) in the end to end telecommunication path for Distributed ReStart services shall be independent power resilient lasting up to 72 hours at least.

Table 3: Resilience requirements

4.3.4 Bandwidth Requirements

The introduction of a DRZ-C within the existing telecommunications network would impact the bandwidth requirements. This section articulates the bandwidth requirements for an automated Distributed ReStart. The bandwidth requirements for a manual process is considered to be the same as the normal operations of the power system in providing data and voice communication.

There are various considerations that determine or impact the bandwidth requirements. These include:

- type of interface
- number of interfaces
- protocol
- configurations such as encryption.

Interfaces can be split into 4 categories:

- Digital Only – fast balancing requirements
- Analogue and Digital – fast balancing requirements
- Analogue and Digital – slow balancing requirements
- SCADA.

Communication/Interface Type	Estimated Bandwidth
Fast balancing communication link	For IEC 61850-9-2LE up to 5.760 Mbps per analogue measurement may be expected.
Slow balancing communication link	This is expected to be low due to the relatively slow polling rate of the protocols used (expected to be 1–2 seconds). Using DNP3.0 protocol, the bandwidth requirement is about 20 kbit/s.

Table 4: Bandwidth requirements

The table below gives an indication of the bandwidth requirements for the fast balancing communication channel using 2 different protocols (with encryption).

Location	Bandwidth Required (kbps)	
	IEC 61850 R-GOOSE	**IEC 60870-5-104**
Central Control Site (2 fast resources)	11600	2700
Control Centre	1940	1940
Outstations (fast) (each)	6600	1800
Outstations (slow) (each)	1800	1800
Measurement only locations	1700	1700

Table 5: Bandwidth requirements per communication protocol

This is based on bandwidth calculated (x2 showing that there are two resources and R indicates a redundant system (e.g. twice the bandwidth required with a single communications link) shown in figure below.

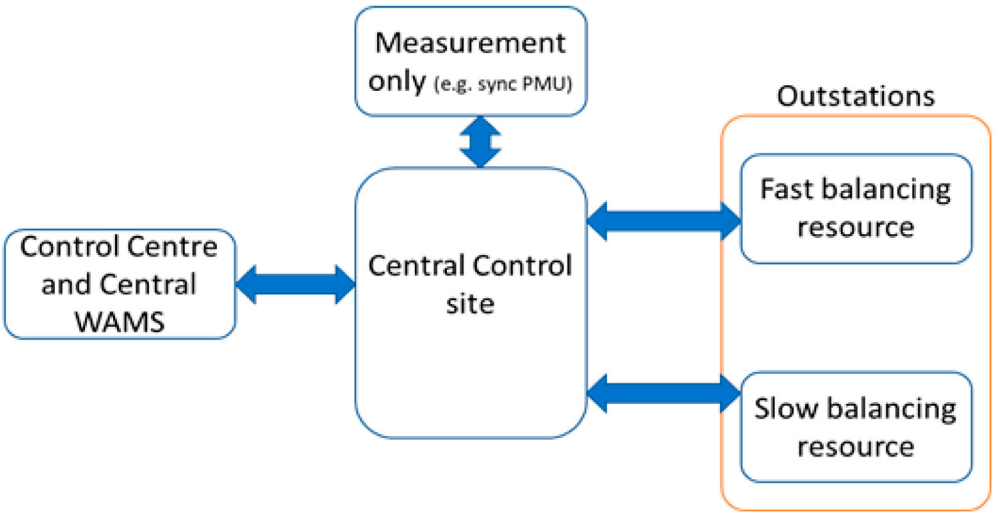


Figure 3: Schematic of architecture on which bandwidth of table 1 was calculated

4.3.5 Protocol Requirements

The Distributed ReStart project undertook design work for DRZ-C with vendors and identified the following protocols that may be required. The protocols used could in turn influence the configuration and functional requirements. These protocols are applicable to the automated restoration process and hence the preferred Central Model.

Protocol	Purpose	Type
IEEE C37.118	Synchrophasor format for frequency and phasor data.	Periodic with 50 Hz data rate.
IEEE 1588 PTP	Time synchronisation protocol for PMUs and PhCs.	Periodic.
IEC 61850 GOOSE	Fast control/protect protocol for local control actions (within substation).	Event based.
IEC 61850 R-GOOSE	Fast control/protect protocol for wide-area control actions, potential use for fast balancing.	Event based.
IEC 60870-5-104	Non-encrypted data stream to get data/commands from legacy equipment such as resources/DMS.	Poll based, but can be polled periodically.
IEC 60870-5-104 (with TLS)	Authenticated and encrypted data stream to get data/commands across the wide-area network securely. Used for general commands/data, possible for fast balancing with development.	Poll based, but can be polled periodically, typically slower than GOOSE.
IEC 61850 MMS	Used for monitoring of the scheme, reports from devices, management of test modes and settings changes for the scheme.	Reports can be period, or user based for settings/control.
NTP	Network Time protocol for WAMS server.	Periodic.
DNP 3.0	Distributed Network Protocol used in process automation systems such as data acquisition and control systems.	Poll based, solicited and unsolicited.
SSH	Secure Shell is a cryptographic network protocol for operating network services securely over an unsecured network.	Various authentication methods.

Table 6: Protocol requirements

4.4 Cyber Security Standards

The cyber security standards listed have been identified as essential in the setup of a DRZ-C and hence are required in the automated restoration options including the Central Model.

Name	Description
IEC62351 (Components)	Standards for Securing Power System Communications.
IEC62443 (Processes and Functions)	Flexible framework to address and mitigate current and future security vulnerabilities in industrial automation and control systems (IACSs).

Table 7: Cyber security standards

4.5 Voice Telephony Functional Requirements

The voice telephony functional requirements considered the user requirements, configuration requirements and responsibilities for providing voice services to enable a Distributed ReStart service.

These requirements are extracts from the Grid Code requirements for Control Telephony – CC 6.5.2, Technical Requirements for Control Telephony – CC 6.5.5 and the Control Telephony Electrical Standard that applies to National Grid ESO's provision of telephony services to DNOs and power stations for the operation of the power system.

These standard voice telephony requirements apply to both the manual and automated restoration processes. The need for voice communication between ESO/DNOs and generators may not be required for non-anchor DERs in an automated model. However, it will be required for anchor DERs and as an exception for other non-anchor strategic DERs where automation has failed for effective restoration.

Voice Telephony Requirements
When National Grid ESO or Distributed Network Operator agree with a Distributed ReStart generator that a Black Start telephone is required at any site, the relevant host in co-ordination with National Grid ESO or DNO will provide one Black Start phone in addition to a control telephone using an infrastructure and configurations that meet the recommended standard.
End-to-end voice telephone infrastructure should have at least 72-hour mains independence. The host at where the telephone is being provided will be responsible for providing 72-hour mains independent power for the active devices that support the Control Telephony and Black Start equipment. The host will also be responsible for installing the internal infrastructure e.g. local cabling between the relevant National Grid ESO/DNO equipment in the communications room and the control room desk.
The telephone terminal should be installed in a prominent position at the site, suitable for use by operational staff.
The telephone terminal should have pre-programmed memory buttons with the key contacts programmed and labelled accordingly for ease of making Black Start calls.
The telephone system should be configured such that Black Start calls should not encounter network congestion, or it should automatically override network congestion if it occurs.
Black Start calls should be presented with a distinctive ringing signal (where possible) at the National Grid ESO, DNO control centres and Black Start DER ends.
If incoming calls are queued by the host's system, Black Start calls should be given priority over other calls at the host's end.
Unanswered incoming calls to the telephone shall normally time out after 120 seconds. The exchange shall have the option of varying this time supervision period including the option to ring indefinitely (with a practical limit of 8 hours). The setting for each site will be agreed and configured prior to deployment.
Telephone instruments in substations shall be robust and be capable of operation in harsh electrical environments with the absolute minimum of maintenance. Telephones will be expected to operate first time despite not having been used for long periods (years in some cases) and no routine maintenance.
The telephone network should be configured in the main as a Closed User Group with immunity from public network congestion and the reception of unwanted public network calls. The equipment shall provide mechanisms to support this requirement with Allow/Block/Digit length tables on inbound calls.

Black Start calls from separate desks at the Network Operator Control Centre or Black Start generator sites are required to be identified uniquely.
For Network Operators/generators that have both Main and Contingency Control Centres, when the contingency site is operational, arrangements must be invoked to transfer Control Telephony calls to the contingency site. For each Network Operator, actual provision of services and changeover arrangements will require separate technical and operational agreements between National Grid ESO or DNOs where applicable.
National Grid ESO/DNO/DERs will implement frequent testing of the end to end telephone infrastructure to ensure they are in good working order and the operational staff are familiar with its use.

Table 8: Voice telephony requirements

4.6 Technology Suitability Summary Based on Functional Specifications

The table below lists the different technologies that Distributed ReStart considered in the Viability Report against the functional requirements for the preferred Central Model and automated restoration process. The table analysed these technologies in terms of the latency, data rates and cost. The suitability of the technology for use in Distributed ReStart is largely dependent on meeting the latency requirements. The cost of deploying the technology as discussed in the Design Stage I report could vary depending on several factors, including if it is a new technology deployment or extension of technology already in use at a particular site.

	Data Rate	Voice	Latency	VPN	Range	Relative Cost	Age	Restrictions	Suitable
VHF/UHF	35 Kb/s	N	<50 ms	Y	Wide Area	Moderate	Dated	Low Data rates	N
TETRA	80 Kb/s	Y	<50 ms	Y	Wide Area + inbuilding	Very High	Dated	Low Data rates	N
LTE 4G/5G	10 Mb/s	Y	variable up to 500 ms	Y	Wide Area	Low	Evolving	Latency/Power Resilience/ Emergency availability	N
Private LTE	*	Y	*	Y	Wide Area + inbuilding	High**	Evolving	Subject to spectrum availability	Y
Microwave	up to 1000 Mb/s	Y	<50 ms	Y	LoS	Low/ Moderate	Evolving	LoS Antenna Mounting/ Alignment	Y
Fibre	up to 1000 Mb/s	Y	<50 ms	Y	Variable	Low to Very High***	Evolving	Accessibility/ Availability	Y
Copper Line	100 Mb/s	Y	<50 ms	Y	Variable	Low to High	Dated	End of Life	N****
Satellite	Kb/s	Y	125ms – 500ms	Y	UK Wide	Low/ Moderate	Evolving	Latency	Dependent on type *****

Table 9: Technology evaluation against functional specification

* Private LTE performance is dependent upon design and guaranteed service.

** Initial network cost would be high as it would require the capital investment for network roll-out but with ongoing costs relatively low. This represents one use case of the many that would be supported by a Private LTE network designed for energy network operators.

*** If fibre is already present then cost will be modest, if it's not then the potential cost of deployment can be very high.

**** Expected withdrawal of service.

***** Satellite has traditionally been considered a high latency, high cost technology but a new emerging satellite network offering lower operational costs and latency is currently being developed and rolled out. Latency for a geostationary orbit is approximately 500ms; latency for a medium-Earth orbit network is around 125ms, and latency for low-earth orbit networks could be as low as 20ms (sometimes, lower than a fibre connection). However, these new LEO satellite platforms are not currently operational and or commercially available.

4.7 Conclusion

The functional specification required to support Distributed ReStart has been grouped under:

- technical requirements
- configuration, environmental and other requirements
- bandwidth requirements
- resilience requirements
- supported protocols
- cyber security considerations.

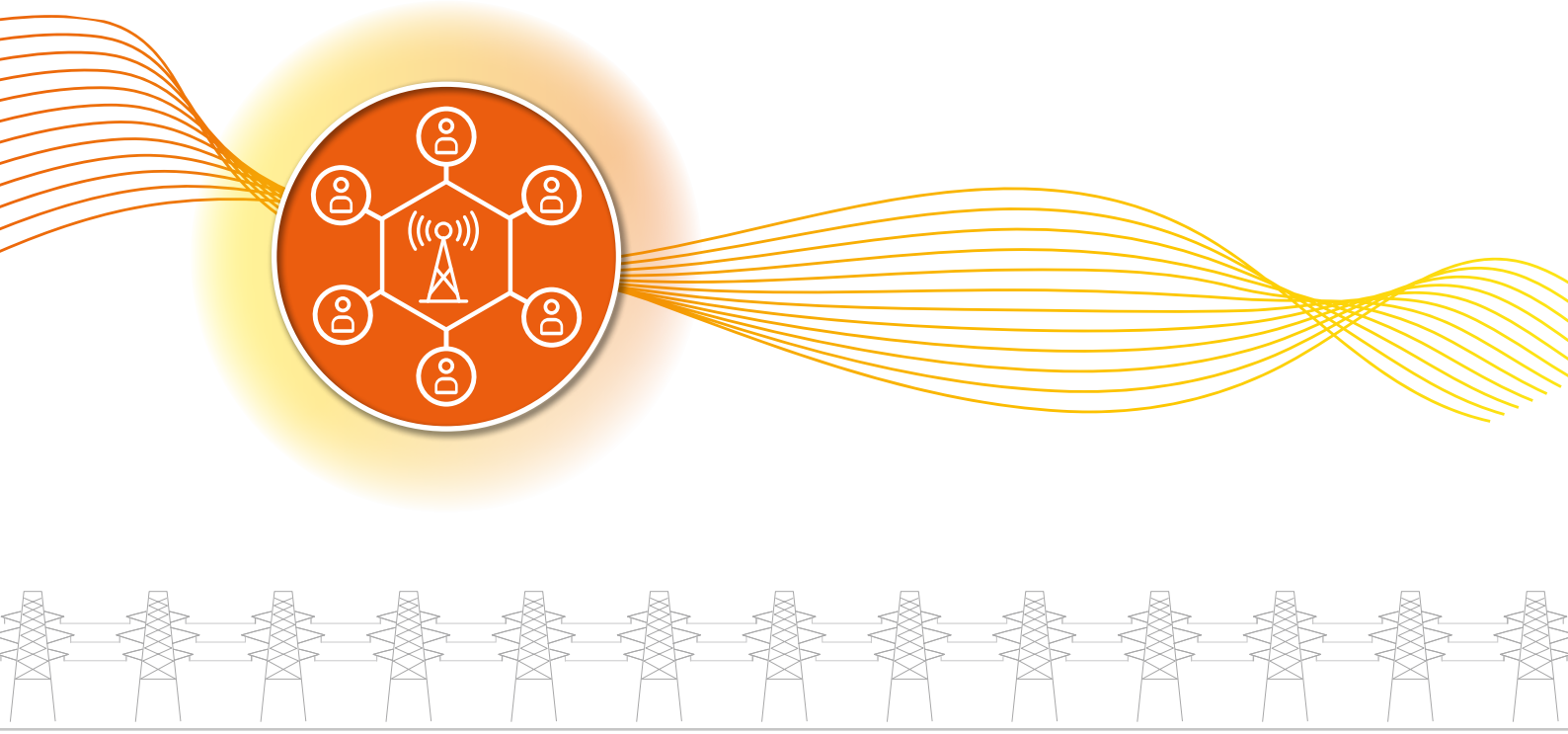
The project has adopted a Central Model which introduces a level of automation to the restoration process by incorporating a DRZ-C and hence would be required to meet the specifications for automated restoration process. However, the project is also drawing up a specification for a manual restoration process as it is envisaged that the participants would be at different stages of the technology journey, i.e. gradually introducing automation and initially may still be using the manual process.

The current operational networks used by the transmission operators and DNOs align with the technical requirements for manual restoration. The provision of at least 72-hour independent power resilience and its extension to the DER sites is a key requirement to ensure compliance.

The automated restoration requirements align with the preferred Central Model. This utilises a DRZ-C which may require upgrades to existing telecommunications networks. The latency and bandwidth are key technical requirements for this restoration. Some DRZ-C resources are required in a stringent time window (fast response resource) and some in a slower time (slow response resource) and this in turn will impact on the latency and bandwidth requirements for the network.

The voice telephony functional requirements remain the same across the manual and automated restoration processes. The key requirements are availability, voice call clarity and end to end 72-hours independent power resilience to ensure availability of the communication during the restoration process.

The available technologies have been compared with the functional specifications to highlight suitability for use in the Central Model. Aside from using the functional specifications, several factors such as cost, existing technology utilised by participant and familiarity, terrain and access to site, maintenance and support for the technology, reliability, availability, policies and regulations in place and future roadmaps play crucial roles in determining the preferred solution.



5. Cost Case Studies

Costs for providing the functional specifications have been done through a case study assessment to give average costs for service roll out.

The project designed a cost template to capture sample costs for technologies to understand the implication for implementing the preferred Central Model for Black Start restoration. In coordination with the ENA Strategic Telecommunications Group, case studies were undertaken by National Grid ESO and participating DNOs that provided a collation of sample costs and technologies if the DNO and/or National Grid ESO implement the communications that are compliant with the functional specifications of the Central Model.

The following criteria were used in the cost template that was used in the case studies:

- **Quantity Modelled:** Indication of how many of each has been considered in formulating the response.
- **1st Installed Cost (£k):** The average cost to provide in the first instance.
- **Annual Operating Cost (£k):** The average cost to maintain and operate per annum.
- **15 Year Lifetime Cost (£k):** The average cost to provide for 15 years including any anticipated asset or service refresh cost such as end of life replacement.
- **Lifetime Cost Variance (£k):** The maximum variance in costs from the average to provide for 15 years.
- **Solution Description:** A description of how the requirement would be provided.

The results in the tables were based on responses from 5 participants from ENA Strategic Telecommunications Group members representing National Grid ESO and the DNOs.

5.1 Provision of Distributed Black Start Voice Services

The distribution of costs to provide Distributed Black Start Voice Services to the DER Control Rooms, DER Sites, DNO Grid Supply Point (GSP) Substations and DNO Primary Substations using the DNO/National Grid ESO infrastructure are summarised below:

	1st Installed Cost Average (£k)	Annual Operating Cost Average (£k)	15 Year Lifetime Cost Average (£k)	Lifetime Cost Variance MAX – min (£k)
DER Control Room	7.70	1.28	32.30	138.50
DER Sites	7.70	1.28	32.30	138.50
DNO GSP Substations	6.30	1.2	28.30	140
DNO Primary Substations	6.30	1.2	28.30	140

The technologies recommended to be deployed to provide the Distributed Black Start Voice Services are mixed and varied from DNO to DNO. These consist of:

- VSAT satellite technology
- Private Fibre
- Voice Over IP
- Private Mobile Radio
- Leased MPLS service.

5.2 Provision of Distributed Black Start Data Service

The additional costs to provide Distributed Black Start Data Services using the DNO/National Grid ESO infrastructure are summarised below. These costs are above and beyond the previous stated costs to provide Distributed Black Start Voice Services.

	1st Installed Cost Average (£k)	Annual Operating Cost Average (£k)	15 Year Lifetime Cost Average (£k)	Lifetime Cost Variance MAX – min (£K)
DER Sites to DNO Grid Supply Point Substations	4.20	0.18	7.30	21.00
DNO SCADA to DNO Grid Supply Point Substations	4.20	0.18	7.30	21.00
DNO Primary Substations to DNO Grid Supply Point Substations	4.20	0.18	7.30	21.00
Interconnection of ESO SCADA with DNO SCADA	250.00	4.00	560.00	

Excluding the interconnection of National Grid ESO SCADA with DNO SCADA, the additional technologies deployed to provide the Distributed Black Start Data Services were limited to the on-site provision of the additional data services using the Wide Area Network infrastructure previously deployed for Distributed Black Start Voice Services, with the exception of 'Line of Sight Microwave, required by one of the DNOs'.

5.3 Summary

The cost of providing each individual Black Start Voice Service typically equates to £2,000 per annum normalised over the 15-year life time of the voice service although in some instances this could be as high as £9,000 per annum dependent on the technology required or deployed. These costs are primarily driven by the power resilience requirements of the Black Start services and not by the voice element of the service.

The additional costs of providing the data service are less significant over and above the initial costs of providing the Black Start Voice Service. Typically, this cost equates to circa £400 per annum per data service normalised over the 15-year life time of the data service but for some it could be as much as £2,000 per annum.

On average the costs of providing Black Start Voice and Data per site is likely to be £2,400 per annum if normalised over 15-year life time but this is site specific and could be as much as £11,000 per annum over 15 years, dependent on the technology required.

The specific costs associated with interconnection of National Grid ESO SCADA with DNO SCADA are for those DNO control rooms that do not already have ICCP links with National Grid ESO. It is not anticipated that this is considered a direct service roll out cost because it is identified as a requirement as part of the ENA 'real time data exchange & forecasting' report for the wider enablement of Distribution System Operation[5]. However, it forms part of the requirement for effective allocation of responsibilities and operational visibility in the Central Model and is therefore an essential part of the telecommunications design.

6. Synchronous DER Control Interface

The project has conducted a review of the existing control interface with synchronous DERs with an aim to inform options for Distribution Restoration Zone Controller (DRZ-C) development.

6.1 Thermal Case Studies

The project has gathered information on control systems and interfaces with DNOs on synchronous installations through discussions with subject matter experts and DER owners/operators. To effectively frame information gathered as part of these works, a generic case study approach has been adopted. This is to allow the commonalities of the main types of thermal technologies containing synchronous generation to be considered. Actual sites and installations will vary from the generic cases considered in this exercise, however each site will be broadly similar in many respects to one of the case study sites outlined.

A review has been conducted for installations using engines and steam turbine based plant. Through this review, steam and engine based DERs are evaluated using generic case studies, grouped by their relevant commonalities. This section breaks down each of these case studies in more detail, discusses the intention behind each case study selected and how each provides valuable insight into the DERs currently in operation in the GB electricity market.

The two case study types for thermal installations have been selected as:

1. Steam based generation; these installations are technically complex and are required to be staffed on a 24/7 basis for operational reasons. An operator will control the DER from an onsite control room via a distributed control system (DCS).

2. Engine based generation; these installations typically comprise several engines, connected to a common network, with a single connection to the DNO network. They are typically dispatched from a remote location using a SCADA system.

A wide-ranging review of a-synchronous technologies is currently being conducted and will be published in further work. However, the project has prioritised the communications interface review for synchronous resources as a result of the known complexities with introducing remote controlled capabilities at these sites.

6.2 G99 Engineering Recommendations

Prior to the introduction of G99 Engineering Recommendations there is no consistent approach to the control interface with DNOs. This means installations from before 2019 which follow G59 may have limited communications with the DNO regardless of technology type. G99 sets standards for operational metering which requires the DNO to install their own telecontrol/SCADA outstation at each DER generating module. G99 requires that a DER should be capable of exchanging information with the DNO at this point of connection. The information a DER is required to monitor includes: fault recording and dynamic readings for active power, reactive power and frequency (although further monitoring capabilities may be included as part of the connection agreement). Notably G99 does not set specific protocols or operational telecommunication requirements for this data exchange and this format should instead be agreed between the DER and the DNO. This means that whilst information captured is consistent, the method by which this is transferred is different between DNO areas.

6.3 Steam Turbine Installations

Steam turbine based plants that are connected to the 11kV or 33kV networks are typically on the 10–50MW scale and comprise a single generator supplied with steam from one or more boilers. The connections to the DNO network are governed by ENA Engineering Recommendation G59 up until 2019 and G99 thereafter.

Steam plant falls into two main fuel types, those using fuels, such as wood and agricultural residues, and those using reclaimed fuels known as energy from waste plants (EfW), utilising municipal solid waste or refuse derived fuels.

Steam based projects are characterised as typically being supported by renewable subsidies based on energy generated or, in the case of EfW, the gate fee for the waste used as feedstock. For this reason, they seek to operate at base load. These sites are staffed at all times, allowing for any manual operations required to facilitate the provision of services in a Black Start scenario to be conducted at site.

The Point of Connection (POC) is closely monitored by both parties for protection, indication and metering purposes allowing power to be exchanged between the DER and wider network as determined by the site-specific grid agreement and in accordance with G59 or G99 as applicable. The DER will typically have unit switchboards at 11kV to facilitate the connection of the generation assets and 400V to provide power to site auxiliary loads required for the operation of the installation.

6.3.1 Existing Capabilities

Control and Monitoring Facilities

Control of the relevant items of plant is carried out by an on-site operations team on a shift pattern for 24/7 coverage. During the day, the on-site team consists of maintenance technicians and senior management, with operators present through the night. Operators are required on-site for a variety of reasons including management of the fuel bunker, manual intervention with the control system to optimise running, and to operate equipment that is not automated.

Installations are typically provided with a single DCS that provides control of the plant from the control room. The various local control systems, including the turbine control package and burner management systems are interfaced with, and integrated into, the DCS such that the DCS has full supervisory control of the whole plant. Operator workstations are provided in the control room to allow the operators to monitor the automatic operation of the plant and make manual interventions to maintain safety, and optimise operation of the plant. Main plant controls include control of the power set point for the turbine, level of generator excitation, step up transformer tap changer position, and plant process controls including fuel feed, steam conditions, fan and damper set points.

At present there is very limited signal exchange between DER sites and the DNO, and this varies between sites. Sites that were commissioned under Engineering Recommendation G59 do not typically have any signal exchange with the DNO for the purposes of control. However, in the rare exceptions that an Active Network Management (ANM) Scheme is required under the particular connection agreement for the DER site then a ‘constraint panel’ may be provided either on the DER site, or within the DNO substation (if this is located adjacent to the DER). A communications interface using a serial link would typically be used, and would provide a signal to limit generation level.

Installations commissioned more recently, under Engineering Recommendation G99, are required to have a basic communication and signal exchange with the DNO to meet the new requirements. These updated requirements are defined within the G99 document and include the requirement for the DER to exchange information with the DNO. The specific signals to be exchanged are agreed on a project by project basis in consultation with National Grid ESO. Another requirement of G99 is for the DER to respond to a de-load signal issued by the DNO. This signal exchange between DERs and the DNO has been implemented most recently utilising a fibre optic cable connection using DNP3 protocol.

Other than this, contact details of a representative from the DER team are shared with National Grid ESO to maintain communication with the installation via telephone as required by the connection agreement.

Steam based DERs would normally have appropriately trained staff to operate the onsite switchgear at 11kV and 400V as necessary for normal operation including start up, shutdown and maintenance activities.

Power Supply Resilience

Steam based projects typically include several forms of emergency power to protect the site from damage if the main supply is not available for any reason. Emergency power is provided from batteries at DC, uninterruptable power supplies (UPS) for AC. These systems are capable of providing emergency power for a period of 30 minutes up to 4 hours depending upon the specific installation. Emergency supplies would be available in the event of a loss of mains power to maintain the following systems:

- tripping supplies to circuit breakers
- turning gear to maintain rotation of the steam turbine until it has cooled
- DCS and operator workstations
- control room operator work stations
- telecommunications.

For DERs containing a steam plant, an emergency diesel generator (EDG) may also be provided on the site which would be automatically started following loss of main supplies. This would be started if the supply from the DNO is lost and the main generation plant trips, providing power to systems supported by the DC battery systems and UPS on site. A 'day tank' which is typically sized for up to 6 hours operation would be included. Additional fuel could be provided to extend the operational period.

Specific consideration of the design and configuration of a steam based DER would be required before an installation could be considered for use as a Black Start site. This is particularly crucial in relation to LV auxiliary supplies as the presence of an emergency power supply does not translate to the site being capable of Black Start or prolonged operation without a strong grid. Emergency power supplies will require modification or supplementary generation to provide these functionalities. For example, electrical supplies would need to be suitable to start motors for the main balance of plant systems including boiler feed pumps and the induced draft fan.

Upon loss of the DNO network, whether this be due to a fault or loss of mains power, the DER incoming circuit breaker would open according to the G59/G99 protection. It is likely that the steam turbine would also trip at this point, although this is dependent on the commercial drivers of the plant. For a biomass plant that receives subsidies for electricity produced, it would not be desirable for the DER to continue combusting fuel without the accompanying electricity sales and the plant is unlikely to have been designed for operation in island mode.

Following loss of supply to the unit switchboard, emergency supplies from batteries would be required to supply the DCS including communications equipment. Although the DNO substation may have its own LV supply separate to the DER, the DER installation would not normally have a backup LV supply. The site would instead rely on starting its EDG to provide AC power to maintain the emergency supplies.

A number of EfW plants are designed to be able to operate in 'island mode' to allow operations to continue burning waste for commercial reasons should the DNO network not be available, due to either a fault or planned DNO outage. In this case the DER's auxiliary loads can continue to be supplied from the generator's terminals once the incoming circuit breaker from the DNO network is opened. The design would also typically include the functionality to restart the plant using the onsite diesel generator should the steam turbine trip during island mode operation.

Following restoration of the DNO network, the plant would be able to close its incoming breaker to re-energise the unit switchboard following any synchronising process with the EDG. Assuming that there have been no interruptions to the UPS or DC systems then the plant DCS and any communications equipment on the site would continue to be available and the operations team would be able to focus on preparing the steam plant for restart. The time for restart of generation would depend on the period that had passed since the boiler and turbine was tripped. Restarting the boiler and regaining the steam conditions required to provide steam to the turbine may take up to 24 hours.

In the case of an EfW plant that has maintained operation in island mode during a network outage, the plant could be resynchronised with the DNO over the DER's incoming circuit breaker within a short period of time, perhaps 1 hour.

If the site emergency supplies had been interrupted then for a DER installation that is normally staffed, the operators would need to follow additional procedures including restart of the DCS and communications equipment, checks of the condition of the steam turbine, and plant switchgear status.

Steam based DER installations typically have telephone and an internet connection provided over the public switched telephone network (PSTN). This would not be expected to be resilient in the case of an outage of the DNO network.

6.3.2 Future Capability

Control and Monitoring Facilities

There are several options to maintain a state of hibernation of a steam turbine based DER. These may include:

- **Increase capacity diesel fuel storage for the EDG:** the fuel tank for a diesel generator used for emergency shutdown purposes is typically sized for up to six hours of operation. By increasing diesel storage, maintaining emergency power for a period of up to 72 hours could be achieved.
- **Increase in the battery capacity:** batteries to provide power for the UPS or DC system are typically only sized to provide power for 30 minutes to 4 hours in duration. It may be possible to upgrade the battery systems, and chargers to extend the discharge period.
- **Optimisation of standby loads:** it may be possible for DER installations to develop operational procedures to put the plant into a hibernation mode to preserve the existing emergency power supplies such that the site can be maintained in a safe state to restart following a power outage of up to 72 hours without additional hardware or plant modification. However, a steam based plant may require up to 24 hours to start up if the boiler is allowed to cool down.

- **Maintaining power generation in island mode:** it may be possible to modify DER installations where the steam turbine would currently be required to trip upon loss of the DNO supplies, to allow operation in island mode. The DER installation could then continue to generate sufficient electricity for its auxiliary consumption and be ready for reconnection to the DNO network when required.

Technical

In general, the generator control systems used at steam based DER installations would be capable of following real power (P), reactive power (Q) and voltage set points provided by a DRZ-C. However, at present these are typically set manually by the operator via the DCS. It is expected that these could be changed remotely if a suitable external interface was installed.

Steam based plant is controlled from the control room on site, and especially during the start-up of the plant there would typically be parameters that would need to be carefully monitored including manual operation of certain valves. This type of plant is typically designed for operation at full load, and operation of the boiler at part load is limited. Therefore, changes to the power output in normal operation are required to be carefully supervised by operators who understand the site to avoid tripping the plant. Coordination will be required with the fuel preparation systems and fuel feed systems into the boiler to ensure it matches the required output, as these processes may not be fully automated. For these reasons, it is expected that a plant operator would need to start up the plant, or make significant changes to dispatch that were received from an external party, rather than these being automated.

For start-up of the plant, a DRZ-C could be used to provide the operators with instructions to implement. Even for DERs with existing signal exchange with the DNO, it would be likely that the input/output count would need to be increased to cater for the needs of the DRZ-C. An indicative list of signals may include the following:

- Black Start preparation
- safe to close circuit breaker
- target load level
- able to Black Start
- Black Start initial capacity
- generator circuit breaker position
- ready for load increment
- fuel reserves available (hours)
- governor mode
- AVR mode.

6.4 Engine Installations

Engine based plants typically comprise of several units connected together, forming a common network with a single point of connection to the DNO at 11kV or 33kV. The connections to the DNO network are governed by ENA Engineering Recommendation G59 up until 2019 and G99 thereafter. There are two main types of generation projects using engines; those designed for use as base load, and those used for peaking generation. Both are usually unstaffed with attendance only required during outages and refuelling operations.

Base load plants generally have access to a low-cost fuel, such as recovered gases, or are entitled to receive renewable subsidies for low carbon fuels. Hence, they are operated for as many hours as possible. In contrast, peaking plants typically operate on high cost fuels and only when the electricity price is high. These are therefore dispatchable resources, utilised only when it is financially advantageous for the owner.

The Point of Connection (POC) is closely monitored by both parties for protection, indication and metering purposes allowing power to be exchanged between the DER and wider network as determined by the site-specific grid agreement and in accordance with G59 or G99 as applicable. The DER will typically have unit switchboards at 11kV to facilitate the connection of the generation assets and 400V to provide power to site auxiliary loads required for the operation of the installation.

6.4.1 Existing Capabilities

Control and Monitoring Facilities

These sites are controlled and monitored from a centralised control room situated remotely from the physical location of the generation plant with commands sent via a communications link. Communications links are typically broadband using Openreach digital subscriber line (DSL) or fibre cables. Some sites also operate a backup over the cellular network.

Physical attendance at site is only required for periodic maintenance and when attending to breakdowns. Typically, provision is made for local control at the installation should this be required whilst operators are at the site, but this control is supplementary and is not the primary means of control.

Individual engines are equipped with proprietary controllers to monitor and control each engine and synchronisation with the DNO network. A personal computer, or alternatively a programmable logic controller (PLC) may be used to act as the communications centre for these installations to allow dispatch and control of the engines to be carried out remotely from a control centre off site. Commands are sent from the remote location for initial start-up of the unit(s), to initiate synchronisation, to change the level of generation and to shut down the units. The condition of the engines is also typically monitored with data being provided to the maintenance team to inform planned outage cycles.

Similar to steam-based sites, communications interfaces with the DNO are not typically established as these were not required under G59. However, there may be specific sites which include ANM schemes where exchange of metering data and constraints are required.

For sites providing short term operating reserve (STOR), National Grid ESO has typically provided dispatch signals from a central server via an ISDN or broadband connection to a personal computer which would be based at the DER installation. These signals would be used to bring the generation online and set the power dispatched from the site.

This type of plant can be dispatched by the owner or by traders within the capabilities of the individual DER including its required capacity, start-up times and required duration for operation specific to each site.

Telephone/contact details for the DER owner are commonly used to maintain general contact with National Grid ESO.

Individual engine based DER installations are mainly owned as part of a fleet, and owners put in place arrangements to provide physical attendance to sites when this is required. Typically, this is delivered by in house staff or by fleet operators who employ a range of skilled technicians as sites would need to be attended regularly to perform routine maintenance.

Power Supply Resilience

Engine based DER installations typically have a battery charger and UPS at site to support the auxiliary systems during a loss of mains event. These systems are designed to operate for a short duration only and are present to allow the engines to shut down safely and to preserve communications between the site and remote locations for a limited duration. Emergency power supplies for communications would typically be available for a period of up to four hours.

Some sites have a diesel generator on site to provide emergency power for extended periods where this is required. This is to provide additional resiliency to sites required to maintain emergency supplies to allow management of process safety parameters in the case of landfill gas projects, where flaring of the gas would be required while the gas engines are offline.

Black Start capability would not have been part of the original design criteria for engine-based installations, and so modification would likely be required to achieve this.

Upon loss of the DNO network, the DER's incoming circuit breaker would open according to the relevant G59/G99 protection and the engines would shut down automatically at this point. Following loss of mains supply, emergency supplies from batteries would be available to maintain supply to the site personal computer, engine controllers and communications equipment so that the installation could continue to be monitored remotely. Although the DNO substation may have its LV supply separate to the DER, the DER installation would not normally have a backup LV supply.

The remote-control centre would typically comprise of operator workstations to oversee the SCADA control of a number of DER engine installations. In case of loss of the main electrical supply at the control room, a UPS is typically included to maintain the workstations and communications equipment for up to 4 hours.

Following restoration of the DNO network, the plant would be able to close its incoming circuit breaker to re-energise the unit switchboard following any synchronising process with the EDG, where applicable. Assuming there have been no interruptions to the emergency power supply then the plant control systems and communications equipment on the site would be available to restart. Typically, engine based installations would be available to start generating power within several minutes of a signal to start.

If the site emergency supplies had been interrupted, the plant would typically require a site visit by a technician to restart the facility. This visit would normally be to manually restore the essential power supplies to the control system, engine management systems and control system to regain control of the site. The technician would also carry out basic checks on the condition of the engines and fuel supply status.

DER installations not participating in the STOR market would typically use an internet connection provided via Openreach, with a backup over the cellular network. Communications links to STOR projects would tend to be more resilient than other engine based projects due to the requirements of the Balancing Mechanism which requires a fixed line such as an Integrated Services Digital Network (ISDN) connection. However, ISDN has been declared end of life by Openreach, so, in 2020 National Grid ESO has implemented a Platform for Ancillary Services Application Programming Interface (PAS API). This allows STOR sites to access the dispatch system and exchange the required metering data over a non-fixed line internet connection, and may also use a third-party server. Moving away from a fixed line communications link direct from the dispatch centre to the STOR site may offer less resilience.

The PAS API can be installed on equipment by an owner in a secured central location backed up by a UPS. Backup cloud based APIs are also available. Commands would typically be sent to STOR sites from this location over the PSTN and backup system using the cellular network.

6.4.2 Future Capability

Control and Monitoring Facilities

To maintain a thermal DER in a state ready to start up for a period of up to 72 hours would require a backup power supply to last for the same period. This is to allow communications links to remain open and for essential plant control systems to operate. At present, such supplies would only be available for up to 4 hours, unless an emergency diesel generator is provided to maintain important process safety systems such as gas flaring. There are several options to maintain a state of hibernation of an engine-based DER. These may include:

- increase in the battery capacity at the installation
- segregation of essential and non-essential auxiliary loads to further prioritise the use of emergency power. This may include operating in a bespoke ‘remote start’ mode, facilitating only the loads required for remote starting of the site
- modification to the installation to allow onsite generation to operate in island mode. This would normally require modification of an existing engine and protection, or by the addition of a dedicated emergency generator
- if not already the case, modification of control systems to automatically restart safely following the restoration of power supply.

Technical

Generator control systems would typically be capable of following real power (P), reactive power (Q) and voltage set points. At present these are set manually by the operator via the SCADA from the remote-control centre.

Engines are typically flexible in terms of dispatch and can be readily stopped and started, and can follow load profiles automatically providing there is sufficient fuel available. Minimal human intervention would be required.

For DERs participating in the STOR market with existing signal exchange with the DNO, it would be likely that the input/output count would need to be increased to cater for the needs of the DRZ-C. An indicative list of signals may include the following:

- Black Start preparation
- safe to close circuit breaker
- target load level
- able to Black Start
- Black Start initial capacity
- generator circuit breaker position
- ready for load increment
- Fuel reserves available (hours)
- governor mode
- AVR mode.

6.5 Conclusions

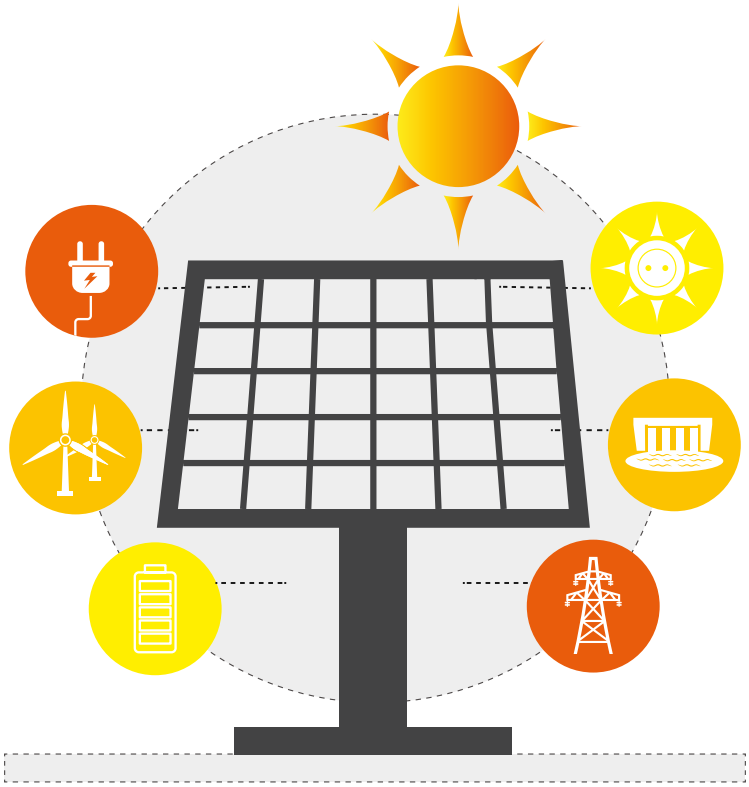
Several consultations with industry members have been used to obtain information relating to the control systems and external interfaces of DERs. The commonalities of these DER sites have been discussed throughout this report section and the key areas of where differences occur. From this consultation, a willingness for industry to collaborate with the development and provision of Black Start services has been demonstrated. This however is on the assumption of the commercial viability of the provision of these services and the ability for each DER owner being able to operate within the market.

Currently there are limited communications links to allow signal exchange between the DNO and DER installations in sites connected under G59 Engineering Recommendations and there may be no connections. Whereas sites connected under G99 Engineering Recommendations have a data exchange requirement under their connection agreements. Exceptions are where ANM schemes are installed, although information exchanged is typically limited to metering data and curtailment signals. It may be possible to use spare signal exchange within these systems to implement rudimentary controls required for Black Start services.

For unmanned DER installations that are controlled remotely, communications links are provided over Openreach infrastructure with backup connection often provided via the cellular network. These links provide visibility of the sites' operation externally to the facility alongside the control capabilities. Many functions of the plant may be automated with physical intervention only being required in the event of faults. For this reason, many of the remote capabilities are supplementary and do not function as the primary control in normal operation.

Following loss of mains power maintaining essential power supplies on a DER site is necessary for the control and communications equipment to function. At present, supplies would typically be provided for up to 4 hours using batteries and diesel generators. In future these could be augmented in a variety of ways to extend the period which emergency power is available.

From a technical perspective, in principle DER installations could be modified to accept external control commands from the DNO and provide feedback. This would require some engineering effort to provide a secure interface and integration into the DER's control system. By enhancing the DER's capabilities to provide Black Start services would likely increase the loading on UPS and battery systems due to the additional control equipment. Specific attention should be paid to these systems as their typical design life is often shorter than the overall site, they are rarely required to operate and can often be omitted from regular maintenance programs. This can result in the battery life of the UPS and battery charger systems being much lower than the quoted values.



7. Automated Control Interface

This section provides a gap analysis between existing automated DER control interfaces and those expected to be introduced through a Distribution Restoration Zone Controller (DRZ-C).

7.1 Introduction

There is no single approach employed for the control interface with DERs across GB. It varies between network areas, generator size and inclusion or exclusion from active network management (ANM) schemes. As the Distributed ReStart project seeks to introduce further automation through use of a DRZ-C, whilst maintaining the facility for manual procedures to be enacted, the interface between the DNO, the controller and the DER requires definition and review.

ANM schemes are increasingly prevalent across GB and provide the closest reference point to a DRZ-C in terms of operational interface. For this reason, an analysis of existing installations and their interface with the DER and the DMS is provided. However, a DRZ-C requires significantly greater functionality than a typical ANM scheme. This section draws out the gaps between existing automated communications interfaces and the proposed front-end engineering designs for further DRZ-C development.[6 7]

7.2 Type of DER

Not all DERs have the same connection protocols in an ANM area, similarly it is not envisaged that every DER within a DRZ will form part of the core restoration service. Table 9 shows key categories of DER, noting similarities in structure between ANM schemes and the proposed DRZ-C structure, alongside the possible emergency actions that can be taken.[8]

Note that these categories are not mutually exclusive, and a generator may belong to multiple generator types.

Generator type	Description	Interface	Emergency action options
ANM generator	A generator which is subject to curtailment as part of a flexible connection offer.	Voice to control point, ANM logic in DNO RTU interacts with DER PLC.	Should follow set point instructions from the ANM scheme. If delivery fails, the DNO circuit breaker can be opened as a means of last resort.
Non-curtailable generator in an ANM area	A generator connected behind a constraint which is being managed by an ANM scheme but is not controlled by the ANM scheme due to legacy arrangements or an MVA size lower than the threshold for inclusion.	Voice to control point, no direct control interface.	Emergency instruction from National Grid ESO via the DNO to turn down only. If delivery fails, the DNO circuit breaker can be opened as a means of last resort.

Anchor DER	Core Distributed ReStart service provider responsible for initiating a DRZ from an unenergised network.	DRZ-C logic to power resilient PLC. Potential requirement for power resilient voice to DER.	Should follow service and set point instructions from the DRZ-C. If automation fails it should follow the redundant manual procedure.
Distributed ReStart top-up service provider	Provider of auxiliary/top-up services required to grow a DRZ and support wider network restoration.	DRZ-C to power resilient PLC, option for power resilient voice to DER.	Should follow service and set point instructions from the DRZ-C. If automation fails it should follow the redundant manual procedure.
Non-contracted DER within a DRZ	A DER included within a DRZ area but without contractual obligation to support the restoration.	Non-power resilient voice to control point only, no direct control interface.	The DNO circuit breaker will need to be opened to prevent a risk to restoration. Areas with a high penetration of uncontrolled intermittent generation resources should be avoided until later restoration stages.
CUSC signatory	A generator which has signed the Connection and Use of System Code.	Voice to control point, may have IP control interface with National Grid ESO for ancillary services.	Obligated to follow Grid Code OC9. National Grid ESO can emergency instruct directly to support power system restoration beyond the DRZ contracted zone. Resilience of communications is a potential blocker.

Table 10: DER contractual classification

7.3 ANM to DER Interface

Existing ANM schemes are limited to set point control of power and/or reactive power from a DER. These are offered as a flexible connection option to manage specific network constraints. Under these schemes the ANM control system calculates the required set point for a DER to meet the constraint requirement and issues this signal through an analogue signal to the DER programmable logic controller (PLC). The PLC decodes this signal and provides the DER control system with an instruction to change output.

Typical installations use either a hardwire current encoded signal or make use of a DNP3 analogue communication protocol. The specific communications protocol varies by DNO but there are two broad variants covered by the case studies below.[9] [10]

7.3.1 Hardwire Protocol ANM Interface

The majority of UK DNOs that have deployed ANM use a hardwired analogue current signal in their ANM schemes to provide the DER with set point instructions. This requires the DER to have a capability to measure and resolve a current signal at its RTU and change the generator output to follow the instructed value. This is a one-way communication protocol and is limited to relatively simple communications whilst limiting the number of network endpoints to make cyber secure.

The hardwired configuration uses a current signal between 4mA and 20mA to represent a 12-bit integer. This integer represents a range in output between -100% to +100% of a given MW classification for demand or generation resources. After calculation by the ANM platform, a control centre panel located at the DNO RTU of a generator connection, generates this representative signal. The DER is expected to respond within a 30 second timeline after which the DNO circuit breaker may be opened to disconnect the generator.

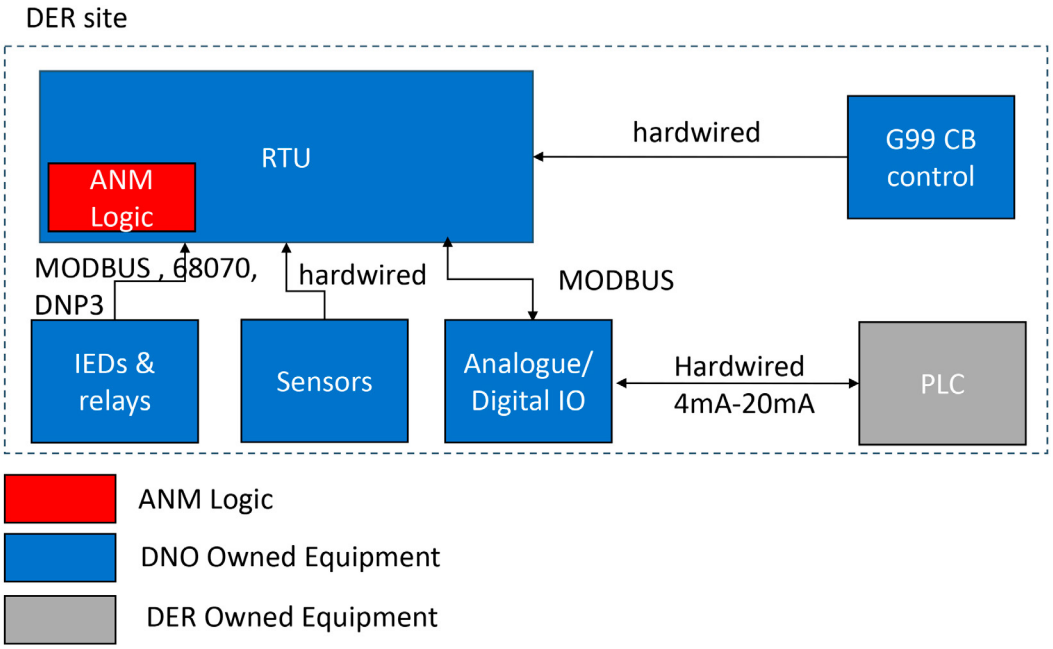


Figure 4: Overview of a current encoded DER interface

7.3.2 DNP3 Protocol ANM Interface

In the DNP3 variant installations, the interface uses IP and serial data, encoded through a secure DNP3 analogue protocol. An analogue set point is issued by the ANM RTU to the DER control system. This allows for setpoints to be transferred but also enables DER weather data or measured values to be shared with the DNO and for time synchronised signals to be issued.

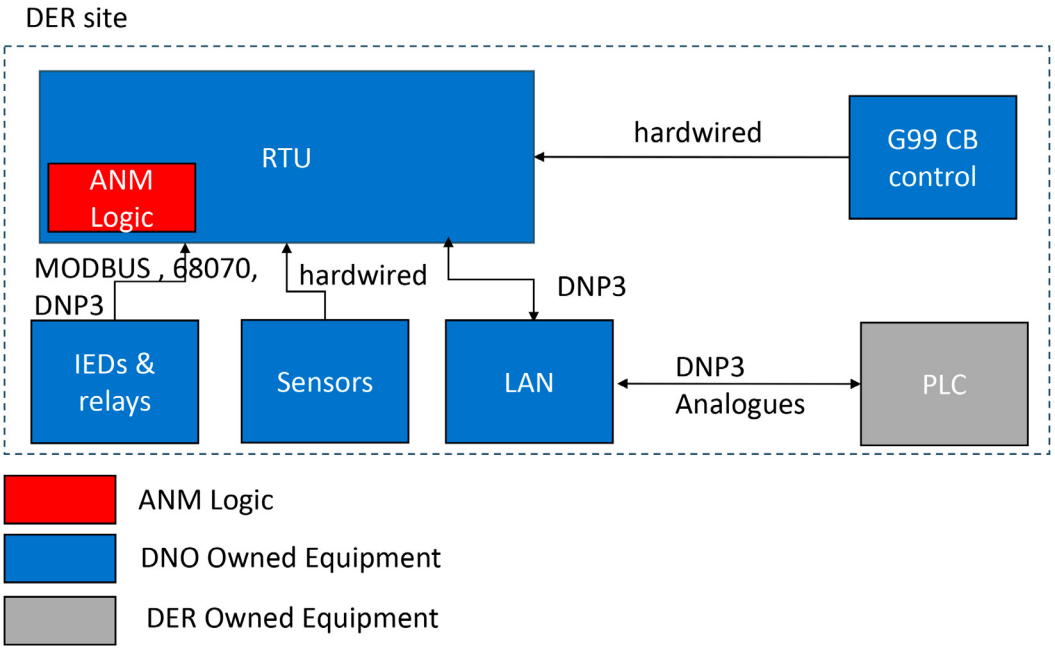


Figure 5: Overview of a DNP3 encoded interface

7.4 DRZ-C to DER Interface

The project has identified a need to automatically send control instructions to DER facilitated by a DRZ-C. This controller acts similarly to an ANM scheme but with greater functionality required to manage the establishment and growth of a power island. However, there is a large commonality in approach to the instruction of DERs amongst the front-end engineering designs which may give DNOs a degree of flexibility in approach to meet their existing ANM to DER connection method. Ongoing commissioned work will aim to demonstrate the controller functionality through hardware in the loop testing, inclusive of testing the communications layer and demonstrating cyber secure functionality. However, the outcomes of preliminary designs are included in this section.

It has been established that a hardwired or IP based interface is required between the DNO RTU and the DER PLC. Table 10 demonstrates the services required and the communications options recommended.

Function	Communication protocol options
Real Power control (slow balancing)	Hardwired analogue or serial/IP communication link supporting Modbus, DNP3/IP, IEC61850, IEC101 and IEC103
Real Power control (fast balancing)	IEC61850 R-GOOSE, IEC60870-5-104, Modbus
Reactive Power control	Hardwired analogue or serial/IP communication link supporting Modbus, DNP3, IEC61850, IEC101 and IEC103
DER synchronisation	IEC61850 R-GOOSE, IEC60870-5-104, Modbus
Voltage regulation	Hardwired analogue or serial/IP communication link supporting Modbus, DNP3, IEC61850, IEC101 and IEC103
Frequency set point	Hardwired analogue or serial/IP communication link supporting Modbus, DNP3, IEC61850, IEC101 and IEC103
Availability signal	Hardwired analogue or serial/IP communication link supporting Modbus, DNP3, IEC61850, IEC101 and IEC103
Metered data	Hardwired analogue where new monitoring equipment is required or interface with existing RTU where monitoring and control already exists (this may require use of IEC101, IEC104, DNP3, DNP3/IP or proprietary legacy protocols)

Table 11: DRZ-C functionality requirements mapped against acceptable communications protocol to facilitate

The functional designs show that a broad range of communications options exist to facilitate most of the required functionality. This means that existing protocols used for the interface with DERs in ANM schemes discussed in 7.3, are suitable for a majority of applications. The key difference highlighted by this review is in fast balancing and synchronisation activities which require very low latency. This may introduce new communication protocols to be integrated into DNO control schemes. Depending on the design implemented, existing metered data may be suitable, or a new phasor measurement unit may be required at the site in addition to the control logic.

7.5 ANM/DRZ-C to DMS Interface

ANM schemes consist of distributed logic controllers at the DER site which interact with the DER as discussed in 7.4. The structure depicted in figure 3 and figure 4 is repeated across multiple DER sites and substations within the scheme and collated using an IP based WAN via DNP3 protocol. The ANM central controller may be a separate standalone system which is integrated into the DMS via an ICCP or directly controlled by the DMS dependent upon the specific design used by the DNO.

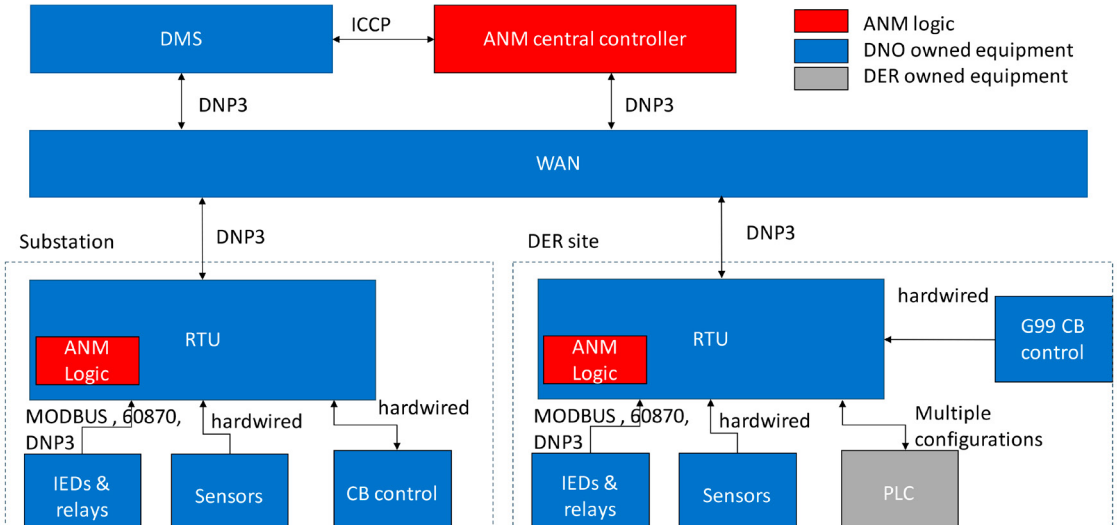


Figure 6: A generic ANM system architecture and DER interface

There is no difference in the interface between the central DRZ-C to DMS, and central ANM Controller to DMS. Designs propose to use existing communications infrastructure where possible. However, there is a need for much lower latency communication than facilitated by the existing channels between the distributed logic controllers and the WAN which means that additional protocols are needed in place of just DNP3. For fast communications protocols, it is recommended that IEC61850 R-GOOSE, IEC60870-5-104 or NGVL are used. Use of standard GOOSE is recommended to be restricted to LAN communications between local resources only and DNP3 is recommended for actions which do not require the very low latency.

7.6 Conclusion

Many of the communications requirements between the DRZ-C, the DER, and the DNO SCADA are analogous to existing Active Network Management (ANM) schemes. Most required functionality is supported using the protocols presented for both variants of ANM roll out explored in this report. Additional options are suggested which may lead to lower latency, but flexibility is retained to use technologies that meet existing DER limitations or DNO-required communications methods.

However, fast balancing actions required to maintain stability of the very low inertia system, require extremely low latency which is not needed in ANM schemes where response times can be up to 30s. This requires introduction of different protocols between the DER and the RTU where a DER participates in this service. Additionally, it requires the use of different protocols between the central controller and the RTU to reduce response times. This is captured in the automated functional specification and it is anticipated that a distributed controller would be required to support several different communication methods. This will enable the use of protocols most suitable for the specific DER which may only accept hardwired or DNP3/IP protocol.

For integration with the DNO SCADA (DMS) an ICCP link or direct DMS control is required, which is analogous to existing ANM schemes. Due to the high latency tolerance of these activities it can make use of existing communications infrastructure and protocols where available and power resilient.

In summary, a DRZ-C will mean the introduction of IEC61850-R-GOOSE, IEC60870-5-104 or NGVL communications protocols in addition to the existing communications infrastructure and protocols which are available across ANM schemes. The gap between an ANM scheme and a DRZ-C is limited to low latency power resilient communications and the specific control logic used.

8. Conclusions

The main conclusions and recommendations in this Design Stage II report centres on the following:

- **drafting of the functional specification for the Central Model, including the manual restoration process**
- **the costs for providing the functional specifications proposed through a case study assessment to give average costs for service roll out**
- **reviewing of the recently published DER Cyber Connection Guidance, what that would mean for Distributed ReStart and making recommendations on additional areas that need to be addressed**
- **further Cyber analysis centred on the Central Model with recommendations – these are summarised below**
- **reviewing the DER communication and control interface with a view to incorporate learnings into the Distribution Restoration Zone Controller (DRZ-C) design and build.**

The next steps will continue to focus on organisational capability and operational telecommunications and systems.

8.1 Functional Specifications

The project has completed the development of the draft functional specifications in consultation with operational telecommunications suppliers and key stakeholders. This is defined against the categories of:

- technical requirements
- configuration, environmental and other requirements
- bandwidth requirements
- resilience requirements
- supported protocols
- cyber security considerations.

The current operational networks used by the transmission operators and DNOs align with the technical requirements for manual restoration. However, the provision of at least 72-hours independent power resilience and its extension to the DER sites is a key requirement to ensure compliance. In addition to ensuring resilience, due to adoption of the Central Model which introduces a level of automation to the restoration process, further communications requirements are needed to meet the specifications for the automated restoration process.

It is recognised that the automated functional requirements may not necessarily be used for early implementations of Distributed ReStart due to where stakeholders are on the technology journey. However, it is seen as a requirement to provide a backup option should automation fail in a Black Start event, giving the plans greater redundancy. Therefore, the manual functional requirements are an essential part of the overall specification.

8.2 Cyber Security

The project reviewed the DER Cyber Security Connection Guidance with a view to understanding the impact on Distributed ReStart and identified additional steps required to ensure the cyber risk to operational telecommunications is minimised.

This highlighted that the guidance in its current form does not fully cover the areas required for Black Start. It proposes reclassification of DERs and contractual cyber security requirements specific to Distributed ReStart providers.

To achieve the secure-by-design posture desired by the Distributed ReStart project, each aspect of the network architecture and control design should be considered. The chosen network architecture must reliably provide data on time and be robust enough to withstand any foreseeable disaster. Additionally, an out-of-band communication channel should be established to ensure trusted communication in the event of a cyber incident and as a fallback plan in the event of network outage. The network resiliency approach must include spare equipment and a backup strategy should a clean sheet recovery be necessary.

Regardless of whether the end-to-end connection model is via the National Grid-provided network or DNO networks, a required connection architecture and mandated set of technical controls must be implemented. By furnishing a common interface and expected data flow, one can create a repeatable design and decrease the monitoring burden for security personnel.

The entity or entities who are connected to DERs must have the ability to provide the necessary infrastructure and security controls to ensure the connection is monitored and secured. The cost of staffing, spare equipment, and maintenance should be factored into the overall budget of the connected party or parties.

Network security monitoring with SIEM integration coupled with competent security personnel can drastically improve the overall security posture of a system. Using an active defence of continuous monitoring, response, threat intelligence consumption, and environmental manipulation can provide a security posture that static alerting alone cannot. Should an incident occur, a well-defined sharing mechanism between parties must be established to distribute indicators of compromise to establish the scope and impact of the breach.

8.3 Cost Case Studies

The costs for providing the functional specifications have been done through a case study assessment to give average costs for service roll out.

The project worked with the ENA Strategic Telecommunications Group and cost case studies were undertaken by National Grid ESO and participating DNOs that provided a collation of sample costs and technologies. These costs assume that the DNO and or National Grid ESO will be providing the distributed Black Start communications that are compliant with the functional specification for the Central Model.

The cost of providing each individual Black Start Voice Service typically equates to £2,000 per annum normalised over the 15-year lifetime of the voice service although in some instances this could be as high as £9,000 per annum dependent on the technology required or deployed. These costs are primarily driven by the power resilience requirements of the Black Start services and not by the voice element of the service.

The additional costs of providing the data service are less significant over and above the initial costs of providing the Black Start Voice Service. Typically, this cost equates to circa £400 per annum per data service normalised over the 15-year lifetime of the data service but for some it could be as much as £2,000 per annum.

On average the costs of providing Black Start Voice and Data per site is likely to be £2,400 per annum if normalised over 15-year lifetime but this is site specific and could be as much as £11,000 per annum over 15 years, dependent on the technology required.

The specific costs associated with Interconnection of National Grid ESO SCADA with DNO SCADA are for those DNO control rooms that do not already have ICCP links with National Grid ESO. It is not anticipated that this is considered a direct service roll out cost because it is identified as a requirement for the wider enablement of Distribution System Operation.

8.4 Review of DER Control and Communication Interface

A review of current DER control and telecommunication interface and resilience for synchronous generators was carried out. This has been done with the view of establishing gaps and subsequently aiding in the design of the infrastructure required for establishing the Central Model which incorporates a DRZ-C.

Several consultations with industry members have been used to obtain information relating to the control systems and external interfaces of DERs. The commonalities of these DER sites have been discussed and the key areas of where differences occur. From this consultation, a willingness for industry to collaborate with the development and provision of Black Start services has been demonstrated. This however is on the assumption of the commercial viability of the provision of these services and the ability for each DER owner being able to operate within the market.

Currently there are limited communications links to allow signal exchange between the DNO and DER installations in sites connected under G59 Engineering Recommendations and there may be no connections. Whereas sites connected under G99 Engineering Recommendations have a data exchange requirement under their connection agreements. Exceptions are where Active Network Management (ANM) schemes are installed, although information exchanged is typically limited to metering data and curtailment signals. It may be possible to use spare signal exchange within these systems to implement rudimentary controls required for Black Start services.

For unmanned DER installations that are controlled remotely, communications links are provided over Openreach infrastructure with backup connection often provided via the cellular network. These links provide visibility of the sites' operation externally to the facility alongside the control capabilities. Many functions of the plant may be automated with physical intervention only being required in the event of faults. For this reason, many of the remote capabilities are supplementary and do not function as the primary control in normal operation.

Many of the communications requirements between the DRZ-C, the DER, and the DNO SCADA are analogous to existing ANM schemes. Most required functionality is supported using the protocols presented for both variants of ANM roll out explored in this report. Additional options are suggested which may lead to lower latency, but flexibility is retained to use technologies that meet existing DER limitations or DNO-required communications methods.

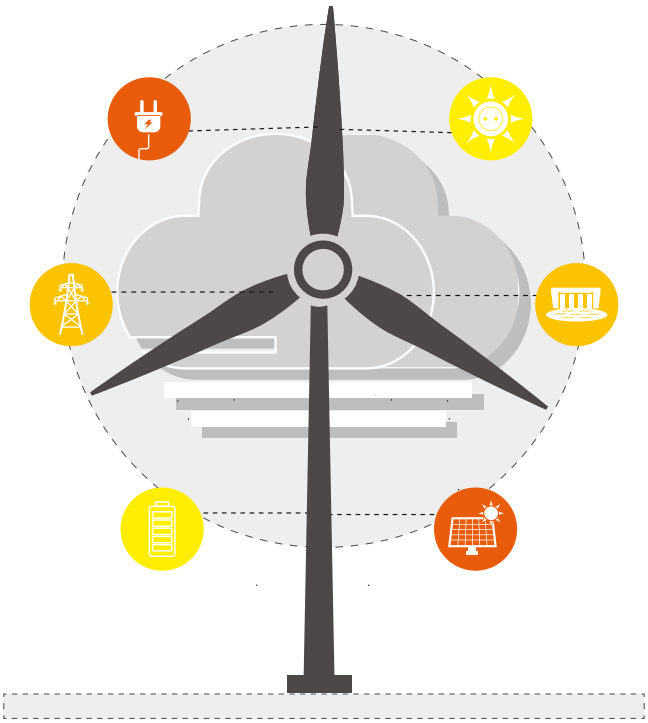
However, fast balancing actions required to maintain stability of the very low inertia system, require extremely low latency. This requires introduction of different protocols between the DER and the RTU where a DER participates in this service. This is captured in the automated functional specifications and it is anticipated that a distributed controller would be required to support several different communication methods.

For integration with the DNO SCADA (DMS), an ICCP link, or direct DMS control is required. This is analogous to existing ANM schemes. Due to the high latency tolerance of these activities, it can make use of existing communications infrastructure and protocols where available and power resilient.

The gap between an ANM scheme and a DRZ-C is limited to low latency power resilient communications and the specific control logic used. To meet this, a DRZ-C will require use of IEC61850-R-GOOSE, IEC60870-5-104 or NGVL communications protocols in addition to the existing communications infrastructure and protocols which are available across ANM schemes.

8.5 Summary

In summary, this report presents the telecommunications requirements necessary to facilitate a Black Start and identifies the gaps between existing infrastructure and protocols compared with the functional specifications. These proposals represent a baseline technical requirement which can be built upon across the project refine stage through use of further consultation, design and build and testing through desktop exercises.



9. Next Steps

9.1 Organisation, Process Design and Desktop Exercises

We will be delivering several desktop exercises to test Distributed ReStart processes in terms of the roles for each Black Start participant, and the timing of the process.

These will also allow us to increase stakeholder participation in Distributed ReStart to gain valuable feedback for process refinement, work through a range of scenarios, and gain information for development of high-level training plans.

We will test the process maps through use of desktop exercises and potential simulation of an event. This coupled with the learnings from live power engineering trials will provide confidence in the efficacy of Distributed ReStart should a Black Start event occur and provide the model for training and assurance of the ongoing service.

We anticipate that significant value will be unlocked from exercises with cross industry participation that focus on communication and decision-making processes. These exercises may be repeated multiple times and will look to test the various scenarios that may lead to a Black Start procedure being enacted to ensure fit for purpose processes that can adapt to different possible needs cases.

9.2 Refine Processes and Organisational Structures

Ahead of issuing a final proposal, we will seek to maximise the efficiency of the processes and organisational structures. In addition to the inputs and consultation discussed earlier, we appreciate that a broader range of views may unlock further insights and more cost and time effective restoration plans. For this reason, the project will conduct a review from a business perspective through organisational design experts.

9.3 Cyber Security Analysis

The threat landscape is evolving and could be subject to disruptive change. Distributed ReStart could be a potential target for highly capable threat sources looking to disrupt CNI. The macro level trends we have identified in technology, digitalisation and accelerating cyber threats suggest that rapid and unforeseen changes in the cyber security landscape could occur between now and 2030.

Considering the above, we would continue work in this area but with greater attention to the design of the DRZ-C. The cyber analysis work will work closely with the DRZ-C design to ensure this is built in.

9.4 Systems and DER Interface

A detailed analysis of the systems and applications required for the Central Model will be completed. Gaps will then be identified and used to define requirements for the DRZ-C design and build.

Appendix A – Bibliography

1. Energy Networks Association, *Distributed Energy Resources – Cyber Security Connection Guidance*, ENA, London, 2020.

2. National Cyber Security Centre, *NIS Introduction,* 30 09 2019. (Online) Available: ncsc.gov.uk/collection/caf/nis-introduction (Accessed 07 10 2020)

3. UK Government, 'The Network and Information Systems Regulations 2018', London: The National Archives, 2018.

4. R. M. Lee, *The Sliding Scale of Cyber Security,* August 2015. (Online) Available: sans.org/reading-room/whitepapers/ActiveDefense/paper/36240 (Accessed September 2020)

5. Open Networks Project, *Real time data exchange & forecasting,* Energy Networks Association, Jan 2020.

6. ENA Open Networks Project, *The interactions between flexible connections (ANM) and flexibility services*, 2020.

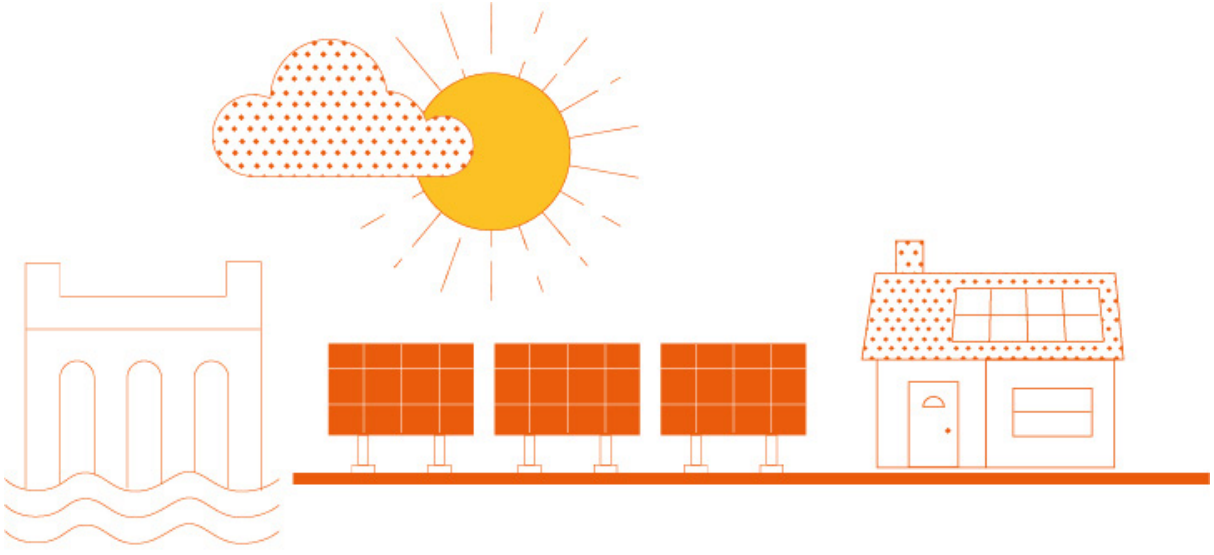
7. ENA Open Networks, *Curtailment process and ANM reliability good practice guide*, 2018.

8. Cornwall Insight, *Optimal Coordination of Active Network Management Schemes with Balancing Services Markets*, National Grid ESO and WPD, 2020.

9. *Active Network Management ANM implimentation*, Western Power Distribution. (Online) Available: westernpower.co.uk/active-network-management-anm-implementation

10. UK Power Networks, *Engineering Design Standard, RTU logic for ANM schemes*, 2018.

11. Energy Networks Association, *Distributed Energy Resources – Cyber Security Connection Guidance*, ENA, London, 2020.



Appendix B – National Cyber Security Centre Cyber Assessment Framework

Objective A Managing Security Risk	Contributing Outcomes	CSCG Tiers	
A.1 Governance	A.1a Board Direction	Foundational	Existence of a security policy defining the lines of responsibility and accountability for the security of DER assets.
		Light	Clear governance structures in place, clearly articulated risk appetite and risk management policy and processes.
		Full	Appropriate management policies and processes in place to govern the approach to security. Often as part of an industry recognised security management system.
	A.1b Roles and Responsibilities	Foundational	Necessary roles and responsibilities have been identified and are regularly reviewed.
		Light	Appropriately capable and knowledgeable staff fill the identified roles and have the resources and authority to carry them out.
		Full	Roles are filled and there is clarity on who has overall accountability for cyber security.
	A.1c Decision Making	Foundational	Decision makers understand their responsibilities in the context of the risk appetite – as set by senior management.
		Light	Senior management have visibility of key decisions and they are periodically reviewed.
		Full	Risk management decision making is delegated and escalated across the organisation to the people who have the skills, knowledge, tools and authority they need.
A.2 Risk Management	A.2a Risk Management Process	Foundational	Existence of a risk management policy and a process for identifying, assessing and understanding risks to DER assets.
		Light	Following the NCSC Risk Management Guidance to choose a risk management approach that considers the threats, vulnerabilities and impacts relevant to DER. Regular risk assessments carried out.
		Full	Risk assessments are dynamic and updated in light of relevant changes. Threat analysis carried out to understand the implications for the organisation.
	A.2b Assurance	Foundational	Security measures are understood and validated regularly to ensure they remain effective.
		Light	Security deficiencies uncovered during assurance activities are assessed, prioritised and remedied where necessary.
		Full	The organisation takes appropriate steps to identify, assess and understand security risks to the operation of essential functions.
A.3 Asset Management	A.3a Asset Management	Foundational	Existence of an asset list including the location and owner for each asset.
		Light	Existence of an asset management policy and process along with a central asset repository that includes all DER assets, their owners and the dependencies between them.
		Full	Everything required to deliver, maintain or support networks and information systems necessary for the operation of essential functions is determined and understood. This includes data, people and systems as well as any supporting infrastructure.
A.4 Supply Chain	A.4a Supply Chain	Foundational	Awareness of external suppliers and ensuring network connections and data sharing does not compromise the DER.
		Light	Effective specification of security properties for the provision of DER equipment or services from a third party and ensure the protection of data shared with the third party.

A.4 Supply Chain (Cont'd)	A.4a Supply Chain (Cont'd)	Full	The organisation understands and manages security risks to networks and information systems supporting the operation of essential functions that arise as a result of dependencies on external suppliers. This includes ensuring that appropriate measures are employed where third party services are used.
Objective B Protecting against cyber-attack	**Contributing Outcomes**	**CSCG Tiers**	
B.1 Service Protection Policies and Processes	B.1a Policy and process development	Foundational	Basic policies and processes in place related to the securing of DER assets and information.
		Light	Policies and processes are updated in response to major cyber security incidents.
		Full	Policies and processes are reviewed and updated at regular intervals to ensure they remain relevant. Systems are designed so that they remain secure even when security policies and processes are not always followed.
	B.1b Policy and process implementation	Foundational	Basic policies and processes in place related to the securing of DER assets and information.
		Light	Policies and processes actively maintained throughout their lives. Adherence to the policies is checked. Breaches are tracked and assessed to determine actions.
		Full	The organisation defines, implements, communicates and enforces appropriate policies and processes that direct its overall approach to securing systems and data that support operation of essential functions.
B.2 Identity and Access Control	B.2a Identity verification, authentication and authorisation	Foundational	All DER assets are protected with a username and secure password.
		Light	Users are individually authenticated and authorised for remote access. The list of authorised users is regularly reviewed.
		Full	2 factor authentication or hardware backed certificates are used to individually authenticate and authorise access to systems.
	B.2b Device management	Foundational	Assets are physically secure in a locked enclosure.
		Light	All privileged access occurs from dedicated management devices. It is possible to detect and investigate unknown devices connecting to the network.
		Full	Independent assurance is gained for the security of third party devices or networks before the connect to DER assets. Regular scans are performed to detect unknown devices.
	B.2c Privileged user management	Foundational	Separation of operator and administrative access. Periodic review of user and their rights.
		Full	The organisation understands, documents and manages access to networks and information systems supporting the operation of essential functions.
	B.2d Identity and access management (IdAM)	Foundational	User follow a robust procedure to be verified prior to being granted the minimum access rights required.
		Light	All user access is logged and monitoring. Permissions and users are regularly reviewed and revoked when no longer required.
		Full	Users (or automated functions) that can access data or systems are appropriately verified, authenticated and authorised. Attempts by unauthorised users is alerted and promptly investigated.
B.3 Data Security	B.3a Understanding data	Foundational	All important DER data is identified and catalogued together with who has access to that data.
		Light	The location, transmission, quantity and quality of data is periodically reviewed. The impact of a data breach is understood and documented.
		Full	All mobile devices and media that may hold key data are identified and steps are taken to remove or minimise unnecessary or historic copies.
	B.3b Data in transit	Foundational	Data in transit is transmitted over encrypted channels where available (TLS/IPSec for internet traffic).

B.3 Data Security (Cont'd)	B.3b Data in transit (Cont'd)	Light	All data links that carry DER data have been identified and secured by appropriate means, such as cryptography.
		Full	Data transmitted electronically is protected from actions such as unauthorised access, modification, or deletion. Such protection extends to the means by which authorised users, devices and systems access critical data. It also covers information that would assist an attacker.
	B.3c Stored data	Foundational	Data at rest is protected from unauthorised access, modification or deletion.
		Light	Data removal from the system is controlled and data backups are suitable and secured.
		Full	Data stored electronically is protected from actions such as unauthorised access, modification, or deletion. Such protection extends to the means by which authorised users, devices and systems access critical data. It also covers information that would assist and attacker.
	B.3d Mobile data	Foundational	Mobile devices that hold DER data are identified.
		Light	DER data is only stored or processed on mobile devices secured to a similar standard to the rest of the organisation.
		Full	Organisation can remote wipe data help on mobile devices. Data is automatically removed after a specified time.
	B.3e Media/equipment sanitisation	Foundational	All data is removed from device storage prior to disposal.
		Light	All data is securely removed from device storage before the media is destroyed.
		Full	Organisation can remote wipe data help on mobile devices. Data is automatically removed after a specified time.
B.4 System Security	B.4a Secure by design	Foundational	Appropriate expertise is used to design and implement DER systems. Firewalls separating DER from untrusted networks.
		Light	DER systems separated from normal IT systems. Data flows and system recovery mechanisms are simple.
		Full	An organisational understanding of risk to essential functions informs the use of robust and reliable protective security measures.
	B.4b Secure configuration	Foundational	User access control enabled for all assets. Secure platform and device builds are used. Software is verified before installation.
		Light	Boundaries protected and messages content checked. Simple and consistent configurations used across device types.
		Full	Network and information systems and technology critical for the operation of essential functions are protected from cyber-attack. Only permitted software can be installed.
	B.4c Secure management	Foundational	Malware and unauthorised software is prevented and detected.
		Light	Monitoring of essential systems in place. Systems are administered and maintain by authorised privileged users.
		Full	Dedicated management devices are used to maintain the DER systems. Technical knowledge and documentation regularly reviewed and securely stored.
	B.4d Vulnerability management	Foundational	Software updated and patched regularly. Anti-malware measures in place.
		Light	Announced vulnerabilities for DER related systems are tracked and mitigated promptly. Regular testing takes place.
		Full	Regular third party testing is carried out. Only supported software and firmware is allowed in the system.
B.5 Resilient Networks and Systems	B.5a Resilience preparation	Foundational	Understanding of the technologies and interdependencies to aid restore of DER if needed.
		Light	Documented procedures for restoring the DER system in the event of a failure.
		Full	The organisation builds resilience against cyber-attack and systems failure into the design, implementation, operation and management of systems that support the operation of DER.

B.5 Resilient Networks and Systems (Cont'd)	B.5b Design for resilience	Foundational	Capacity of the system managed.
		Light	Segregation between the DER systems and the rest of the organisations IT.
		Full	The organisation builds resilience against cyber-attack and systems failure into the design, implementation, operation and management of systems that support the operation of DER.
	B.5c Backups	Foundational	Regular backups taken and securely stored.
		Light	Automated backups are taken and regularly tested.
		Full	Backups and restore procedures routinely tested. Backups held off site. People and roles are also duplicated.
B.6 Staff Awareness and Training	B.6a Cyber security culture	Foundational	All staff understand their roles and responsibilities with respect to the DER.
		Light	Clear security communications and announcements. Staff understand how to raise a security issue.
		Full	Staff have appropriate awareness and knowledge to carry out their organisational roles effectively in relation to the security of the DER. Issues are routinely reported with any concerns being taken seriously.
	B.6b Cyber security training	Foundational	Cyber security information is easily available.
		Light	Training is defined using a range of techniques. Regular refresher training for staff.
		Full	Staff have appropriate knowledge and skills to carry out their organisational roles effectively in relation to the security of the DER. Training is easily accessible and tracked.
Objective C Detecting Cyber Security Events	**Contributing Outcomes**	**CSCG Tiers**	
C.1 Security Monitoring	C.1a Monitoring coverage	Foundational	Basic monitoring of DER functionality and availability.
		Light	Full monitoring of DER functionality and availability. Basic logging and auditing of user actions.
		Full	The organisation monitors the security status of the DER in order to detect potential security problems and to track the ongoing effectiveness of protective security measures.
	C.1b Securing logs	Foundational	Only authorised staff have access to the logging information.
		Light	Access to logging information is monitored.
		Full	The integrity of logging data is protected such that information cannot be modified or deleted.
	C.1c Generating alerts	Foundational	Alerts from third party security software are investigated. The resolution of alerts is performed regularly.
		Light	Logs are monitored with alerts raised where specific entry types are present.
		Full	Logs and systems are monitored continuously. Alerts are tested to ensure they are genuinely reliable and not false alarms.
	C.1d Identifying security incidents	Foundational	Regular checks with related threat intelligence sources. Regular updates for Anti-virus tools.
		Light	Automatic updates for AV and IDS technologies are applied in a timely way.
		Full	Monitoring and threat intelligence updates are kept up to date and their effectiveness tracked.
	C.1e Monitoring tools and skills	Foundational	Monitoring staff are capable of following most of the required workflows and the tools can make use of some logging information.
		Light	Monitoring tools can capture most unsophisticated and untargeted attacks.
		Full	Monitoring staff are empowered to look beyond the alerts and investigate non-standard threats.

C.2 Proactive Security Event Discovery	C.2a System abnormalities for attack discovery	Foundational	Monitoring for activity that deviates from normal.
		Light	System abnormality descriptions from past attacks are used to monitor for malicious activity.
		Full	The system abnormalities searched for consider the nature of attacks likely to impact on DER operation.
	C.2b Proactive attack discovery	Foundational	Routine checking for system abnormality that may indicate malicious activity.
		Light	Designing of custom 'trip-wires' for the DER assets.
		Full	The organisation detects malicious activity affecting, or with the potential to affect, the operation of DER even when the activity evades standard signature based security prevent/detect solutions.
Objective D Minimising the Impact of Cyber Security Incidents	**Contributing Outcomes**	**CSCG Tiers**	
D.1 Response and Recovery Planning	D.1a Response plan	Foundational	Existence of a documented incident response and recovery plan.
		Light	Use of the NCSC '10 Steps: Incident Management' guidance.
		Full	The response plan is comprehensive and covers likely impacts of both known and unknown tacks. The plan is communicated throughout the business.
	D.1b Response and recovery capability	Foundational	Resources required to undertake response activities are identified.
		Light	Use of the NCSC '10 Steps: Incident Management' guidance.
		Full	There are well-defined and tested incident management processes in place to ensure continuity of essential functions in the event of system or service failure. Mitigation activities designed to contain or limit the impact of compromise are also in place.
	D.1c Testing and exercising	Foundational	Exercise scenarios are documented, regularly reviewed and validated.
		Light	Exercises are based on incidents experienced by varying organisations or from threat intelligence.
		Full	There are well-defined and tested incident management processes in place, to ensure continuity of DER functions in the event of system or service failure.
D.2 Lessons Learned	D.2a Incident root cause analysis	Foundational	Root cause analysis is conducted routinely as a key part of lessons learned activities.
		Light	Root cause analysis is comprehensive and covers both technical and process.
		Full	All relevant incident data is made available to the analysis team for root cause analysis.
	D.2b Using incidents to drive improvements	Foundational	There is a documented incident review process to identify lessons learned.
		Light	Lessons learned are used to improve security measures.
		Full	Analysis is fed back to senior management and included in risk management and continuous improvement.

Appendix C – Glossary

Key Term	Definition
Active Network Management (ANM)	Active Network Management (ANM) connects separate components of an electricity network such as smaller energy generators, renewable generation, storage device, etc by implementing software to monitor and control the operation of these devices.
Electromagnetic Compatibility (EMC)	The ability of electrical equipment and systems to function acceptably in their electromagnetic environment, by limiting the unintentional generation, propagation and reception of electromagnetic energy which may cause unwanted effects such as electromagnetic interference (EMI) or even physical damage in operational equipment.
Anchor Generator	A generator with the ability to establish an independent voltage source (grid-forming capability).
Black Start	The procedure necessary for a recovery from a Total Shutdown or Partial Shutdown.
Connection and Use of System Code (CUSC)	The contractual framework for connecting to and using the National Electricity Transmission System (NETS).
Communication Infrastructure	This is the backbone of the communication system over which telecommunication services are operated like data and voice services.
Critical National Infrastructure (CNI)	Those critical elements of infrastructure, the loss or compromise of which could result in major detrimental impact on the availability, integrity or delivery of essential services. Significant impact on national security, national defence, or the functioning of the state.
Distributed Energy Resource (DER)	DERs are electricity-producing resources or controllable loads that are connected to a local distribution system or connected to a host facility within the local distribution system.
Distribution Restoration Zone (DRZ)	Power island in the distribution network used for Black Start purposes.
Distribution Restoration Zone Controller (DRZ-C)	A system that monitors and controls one or more DRZs.
Distribution Network Operator (DNO)	A company licenced to distribute electricity in the UK.

Distribution System Operator (DSO)	A future entity responsible for actively operating the distribution network. ENA are currently investigating various DSO 'worlds' outlining the division of responsibility and which entity is most appropriate to fulfil this activity.
National Grid Electricity System Operator (National Grid ESO)	National Grid Electricity System Operator Limited (NO: 11014226) whose registered office is at 1–3 Strand, London, WC2N 5EH as the person whose Transmission Licence section C of such Transmission Licence has been given effect.
Emergency Instruction	An instruction issued by The Company in emergency circumstances, pursuant to BC2.9, to the Control Point of a User. In the case of such instructions applicable to a BM Unit, it may require an action or response which is outside the Dynamic Parameters, QPN or Other Relevant Data, and may include an instruction to trip a Genset.
Security Information and Event Management (SIEM)	A set of tools and services offering a holistic view of an organisation's information security. SIEM tools provide: real time visibility across an organisation's information security systems. Event log management that consolidates data from numerous sources.
Out-of-band communication	Out-of-band communication is a communication system that uses a channel or frequency band conceptually independent from the primary communication system used.
Grid Supply Point	A Grid Supply Point where either: (i) (a) the Network Operator or Non Embedded Customer had placed Purchase Contracts for all of its Plant and Apparatus at that Grid Supply Point on or after 7 September 2018, and (b) All of the Network Operator's or Non Embedded Customer's Plant and Apparatus at that Grid Supply Point was first connected to the Transmission System on or after 18 August 2019; or (ii) the Network Operator's or Non Embedded Customer's Plant and Apparatus at a Grid Supply Point is the subject of a Substantial Modification which is effective on or after 18 August 2019.
MITRE ATT&CK	The MITRE ATT&CK™ framework is a comprehensive matrix of tactics and techniques used by threat hunters, red teamers, and defenders to better classify attacks and assess an organization's risk.
Differential Delay	This is the difference in latency between the communication paths in directions end A to end B and end B to end A.
Inter Control Centre Communications Protocol (ICCP)	Also known as IEC 60870-6/TASE.2, is a set of international standards specified by utility organisations to provide data exchange over Wide Area Networks (WANs) between utility control centres, utilities, power pools, regional control centres, and Non-Utility Generators.
Wide Area Measurement Systems (WAMS)	A system that captures measurements in the power grid over a wide area and across traditional control boundaries, and then uses those measurements to improve grid stability and events through wide-area situational awareness and advanced analysis.
Very High Frequency (VHF)	The range of radio frequency electromagnetic waves (radio waves) from 30 to 300 megahertz (MHz), with corresponding wavelengths of ten metres to one metre.
Ultra High Frequency (UHF)	The range of radio frequencies in the range between 300 megahertz (MHz) and 3 gigahertz (GHz), also known as the decimetre band as the wavelengths range from one metre to one tenth of a metre (one decimetre).

Long-Term Evolution (LTE)	Long-Term Evolution (LTE) is a standard for wireless broadband communication for mobile devices. This is based on the GSM/EDGE and UMTS/HSPA technologies and sometimes referred to as 4G LTE.
Latency	This refers to the delay that takes place during communication over a network.
Network Segregation	The process of isolating electricity networks to provide discrete power demand in 'blocks'.
MPLS	Multiprotocol Label Switching (MPLS) is a protocol-agnostic routing technique designed to speed up and shape communication traffic flows across enterprise wide area and service provider networks.
NIS Directive	Networks & Information Systems: EU wide legislation on cyber security.
OpTel	National Grid Electricity Transmission operated power resilient fibre optic telecommunications network.
Power Island	A part of the electricity network that is electrically disconnected from the larger grid and operated in an islanded mode, usually during a partial or total power system shutdown.
PSTN – Public Switched Telephone Network	Circuit switched telephony network, providing infrastructure and services for public communication.
Remote Terminal Unit	An electronic device that interfaces between physical assets and a control system.
Supervisory Control and Data Acquisition (SCADA)	A computer system for gathering and analysing real time data and used to remotely monitor and control equipment. Mostly used in telecommunications, utility, oil and gas industries.
Synchronous Digital Hierarchy	A standard technology for synchronous data transmission on optical media.
Very Small Aperture Terminal	This refers to any two-way satellite ground mounted or a stabilized maritime VSAT antenna with an antenna (dish) that is smaller than 3 metres.
Jitter	Variation in the delay of received information packets.
Terrestrial Trunked Radio (TETRA)	An open digital radio standard for professional mobile radio. TETRA can be used by a company for the communication within a private radio or commercial bases.
Transmission Network Owner (TO)	A company licenced to transmit electricity in the UK.

National Grid Electricity System Operator
Faraday House
Warwick Technology Park
Gallows Hill
Warwick
CV34 6DA
United Kingdom

Registered in England and Wales
No. 11014226

nationalgrideso.com

nationalgridESO