nationalgridESO

ESRS - Communication Infrastructure WG Report

Contents

1 Introduction

The Electricity System Restoration Standard (ESRS) requires The Electricity System Operator (ESO) to have sufficient capability and arrangements in place to restore 60% of regional demand within 24hrs and 100% of Great Britain's electricity demand within 5 days. Whilst our current approach plans to achieve restoration of 60% of national demand within 24 hours, there are regional variations and time taken for full system restoration is based on a probabilistic assessment of shutdown scenarios, reflecting the range of severity of events, to determine likely timescales for differing stages of restoration. The ESO must ensure that everything is in place to comply with this standard by no later than 31 December 2026.

The Communication infrastructure Work Group is one of the seven working group established to understand and recommend changes required to achieve the ESRS standard. The working group comprised of stakeholders from across the industry - Electricity System Operator, Energy consultancy companies, Transmission Operators, Telecommunication companies and Distribution Network Operators. The working group provided regular progress updates to coordination team and steering committee, which sits above this working group.

In accordance with the terms of reference, the purpose of this working group was to develop an understanding of the role communications play in restoration and enable the delivery of a secure and resilient communications infrastructure to meet the ESRS.

The inputs to the working group include:

- NGESO strawman
- Relevant consultation responses
- Relevant codes
- Glossary & definitions

The outputs from the working group includes:

- Current and future challenges for Communications across GB (including cybersecurity)
- A testing process for all communication for Primary Restoration Service Providers including Cyber security resilience
- Regular progress updates to coordination team and steering committee
- Final report includes:
    - List of current/future challenges for communication including, as a minimum, a comparison of all key comms technologies and related advantages/limitations and related mitigations
    - A testing regime for each communications service provider
    - Risks and mitigations
    - Impact on Industry.

2 Telecommunication Requirements

This section of the report lists the communication requirements, technical and non-technical telecommunication requirements for Primary Restoration Service Providers needed to meet the restoration standard. These requirements will pertain to the Electricity System Operator (ESO), Transmission Operators (TO), Distribution Network Operators (DNO) and Primary Restoration Service Providers (RSP).

It should be noted that these requirements apply to the network over which the restorations services run across and where the service is applicable for example, teleprotection requirements will apply where teleprotection service is required. This will typically be the ESO, TOs and DNOs' networks. The Primary Restoration Service Providers will liaise with the Network Operators to ensure interoperability. These requirements will also apply to the Restoration Service Providers if the network is extended into the Restoration Service Provider's network for restoration services. The power resilience requirements for a site will usually be provided by the site owner.

2.1 Communication Interface

The communication infrastructure is required to support the following services during restoration:

- Real time data telemetry traffic for operating the network – SCADA, Protection
- Real data to provide status information and situational awareness
- Voice communication between parties

The type of communication and interaction between parties during the restoration process is shown below. It should be noted that the interaction covers all the possible interaction at different stages of the restoration process, and it is not necessarily happening at the same time. The interface covers both the traditional transmission led Primary RSPs and distribution led RSPs (Anchor and Top Up services)

The following gives a high-level requirement for communication infrastructure and detailed in the respective sections.

- Resilience of Data & Voice communications is required at all primary restoration sites (72 hrs mains independence).
- High bandwidth, low latency communications upgrades may be required at Distributed Network Operators Operational telecommunication network and interface to Primary restoration providers (new protocols introduced for Distributed Restoration Zone Controllers) for automation in DNO network
- Inter-Control Centre Communications Protocol (ICCP) used to map Distributed Management System changes to ESO's Energy Management System giving situational awareness.

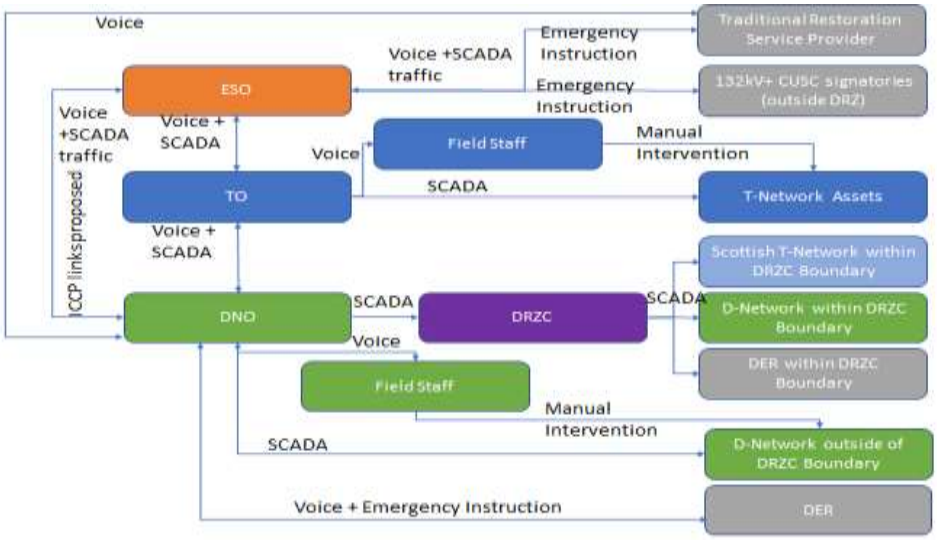

Figure 1: Primary Restoration Providers communication interface

2.2 Technical Requirements for Telecommunications Infrastructure

This section lists the technical requirements for telecommunications infrastructure to support data and voice communication for the restoration process. This also included the requirement for incorporating a Distribution Restoration Zone Control System in the distribution network. The infrastructure cuts across the primary restoration service participants – ESO, TO, DNOs and Restoration Service Providers.

Requirements	Description	Values
End-to-End Delay	This defines the maximum allowable communication channel `end-to-end' delay for teleprotection services.	The maximum allowable communication channel `end-to-end' delay for the different categories should not exceed the specifications for tele protection systems. Category 1 - 6 milliseconds Category 2 – 10 milliseconds Category 3 – 30 milliseconds SCADA services – 100 milliseconds ENA 48-6-7, Section 5.4 The Distribution Restoration Zone Control System 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 for teleprotection services.	The maximum admissible differential delay for the different categories should be as specified. Category 1 - 400 microseconds Category 2 – 10 milliseconds

		Category 3 – 30 milliseconds ENA 48-6-7, Section 5.5
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 enabling manual/disabling automatic switching where required.	It shall have the ability to disable automatic switching for specific services.
Specifications for Communications Protocol requirements	The requirements to specify the communication protocol that needs to be supported for teleprotection services.	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.
Voice user requirements	This defines the control centre and substation voice user requirements.	The voice system shall be designed to meet the Control Telephony Electrical Standard. (See section on voice user requirements)

Table 1: Technical Requirements

2.3 Non-Technical Requirements for Telecommunications Infrastructure

The non-technical requirements for the restoration processes. These include environmental factors, segregation, power resilience and other factors. This is required for services provided across the ESO, TO, DNO and Primary Restoration Service Provider's network used for restoration services. It should be noted that this will apply to Primary Restoration Service Provider where the service extends across their network.

Requirements	Description	Values
End-to-end Service availability	The end-to-end availability for a single-routed 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, Section 5.2
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 maloperation 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
Restoration of Service	Priority to restoration of service.	Priority to restoration of service in accordance with ENA 48-6-7 Issue 2, Section 6.5
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, Section 5.7. This shall be risk assessed if the above is not achievable.
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.
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, Section 5.8

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. ENA 48-6-7 Issue 2, Section 5.2
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	All equipment installed in substations meets the EMC requirements stated and

	the substation by compromising the existing earthing arrangements.	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

2.4 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 Restoration event.

In view of this standard and the recommendation, the 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.

Table 3: Power resilience requirements

2.5 Bandwidth Requirements

There is increased demand for bandwidth to support BAU operational functionality and encryption requirements before restoration is considered. In addition, the introduction of a Distribution Restoration Zone Control System within the existing telecommunications network would impact the bandwidth requirements. The below section will detail the bandwidth requirements for an automated distribution restoration.

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.

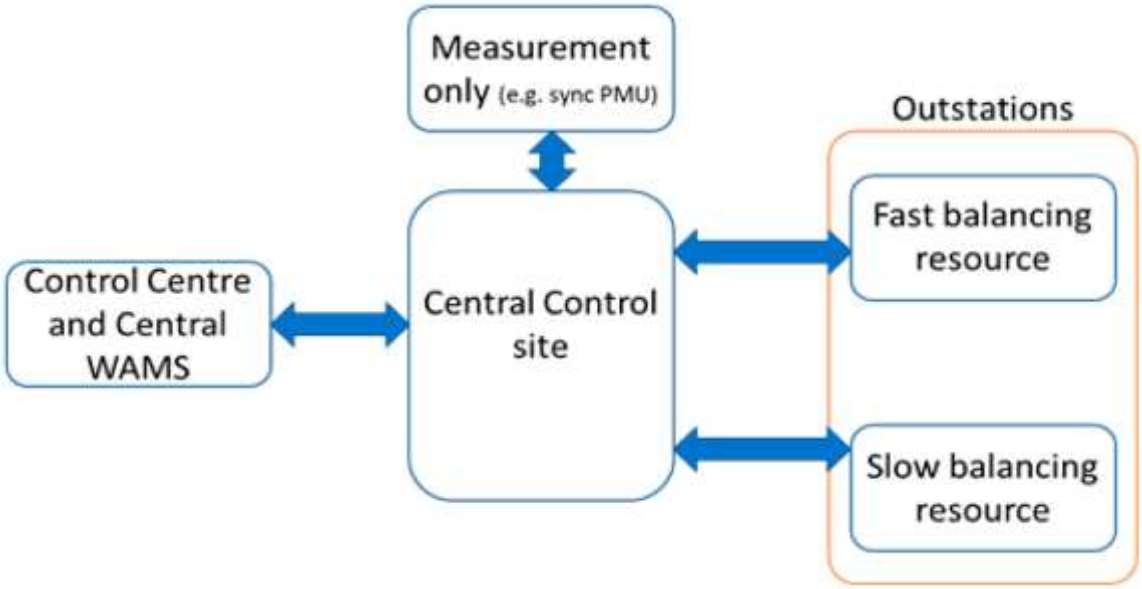

Figure 2: Schematic of architecture on which bandwidth of table 1 was calculated

2.6 Protocol Requirements for Distribution Restoration Zone Control System

The Distributed ReStart project undertook design work for Distribution Restoration Zone Control System with some 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.

Protocol	Purpose	Type
IEEE C37.118	Synchro phasor 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

2.7 Cyber Security Standards

The ESO, TOs, DNOs and Transmission Generators are understood to be classified as Operators of Essential Services (OES). The Network and Information System (NIS) Regulations set out strict compliance obligations for OES to ensure they "take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations". The NCSC (National Cyber Security Centre) has published guidance that describes 4 objectives, covering 14 high-level principles, that OES should meet to comply. OES that fall within the scope of the NIS Regulations are subject to audits by their competent authority.

The proposal is for distribution Primary Restoration Service Providers that are not currently classified as OES i.e. Anchor Generators and Top Up service providers to be classified as such and hence subject to NIS regulation. It is also proposed that all other distributed energy resources should adopt the Distributed Energy Resource Cyber Security Connection Guidance published by Department of Business, Energy, and Industrial Strategy (BEIS) and Energy Network Association (ENA).

The cyber security standards listed have been identified as essential in the setup of a Distribution Restoration Zone Control System, which is required for automated distribution restoration. These standards have been identified as part of the Distributed ReStart project.

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

2.8 Voice Service Functional Requirements

The voice service functional requirements considered the user requirements, configuration requirements and responsibilities for providing voice services to enable a wider Restoration service.

The Control Telephony Electrical Standard that is developed and being consulted on under GC0148 is proposed to be the standard that would apply for voice services provision.

This standard is currently being consulted on and details is contained in Annex 10 of the link below.

https://www.nationalgrideso.com/industry-information/codes/grid-code-old/modifications/gc0148-implementation-eu-emergency-and-0#tab-tab-3

3 Viability of Current Technologies

This section outlines the advantages and disadvantages of current technologies, the section also includes a direct specification comparison between technologies and their suitability to be used in the new restoration process.

3.1 Advantages and Disadvantages of Current Technologies

Technology	Advantages	Disadvantages
Satellite Communication **Suitable option**	Requires fewer active nodes, so can be easier to provide power resilience: • Resilience is required at the sending and receiving stations only. • The orbiting satellite has built in power resilience from the sun and rechargeable batteries. during its lifetime.	Can be affected by adverse weather conditions e.g. snow. heavy rain or storm can cause a temporary loss of satellite services as it can block either the signals being sent up to the satellite (uplink) or received (downlink),
	It covers a large geographical zone and it has no distance limitations.	It requires clear sight of the sky for indoor applications. • installation of an antenna for indoor operation can mitigate this
	As a wireless technology, satellite technology does not require road access rights and cabling	As with wireless technology, satellite signal could be intercepted if robust encryption and authentication is not deployed.
	For parties that already have a satellite network, the additional cost of extending the network to DERs could be relatively low. Albeit that existing satellite capability may not be appropriately specified to satisfy the requirements of this use case	Latency for packet transmission from source to destination is high due to distance of satellite from earth is about 36000 Km and so if not properly managed may impact real time applications or communications
	Deployment time can be relatively short, when compared to cabling options	
Fibre Optic Cable **Suitable option**	The communication link is not affected by weather	It requires physical access rights for cabling route
	It has high availability as it is a physical structure with assured link	There is limitation to the length of direct fibre cable that could be used without adding active devices • Limiting which parties could make use of cable
	Any form of interfering with fibre communication will require physical access to the cables or equipment.	Fibre optic installation could take a long time due to the requirement for permissions,

		wayleave agreement and ground digging.
	It provides high speed connection and low latency	Ground installation can have a high environmental impact.
	It is relatively easy to provide power resilience as this is required only at the end points that houses the active equipment.	Proximity of remote assets to fibre solutions may be limited leading to significant cost to deploy dedicated circuits.
Microwave Radio **Suitable option**	It does not require physical access hence suitable for terrains where physical access rights are difficult	It requires line of sight between the microwave dishes to operate
	It provides high speed data and voice transmission	As with wireless technology, microwave signal can be intercepted if robust encryption and authentication is not deployed.
	Installation timescales could be relatively short compared to wired communication	Can be affected by adverse weather conditions e.g.; snow. heavy rain or storm can cause a temporary loss of signal. Potential access issues
	It is relatively easy to implement power resilience as it is required at the end points only	potential third-party dependency on base stations
Private LTE **Suitable option**	It does not require physical access hence suitable for terrains where physical access rights are difficult	As with wireless technology, LTE signal could be intercepted if robust encryption and authentication is not deployed.
	It has the potential to deliver voice and data transmission via LTE network	It will require licensed spectrum to operate
	Base stations could utilise existing substations that have the required power resilience	
	Benefits from global standards and economies of scale.	
Mobile Network 4G/5G **Not suitable for restoration** Due to lack of required power resilience	The mobile network is already available or planned for and could be relatively low cost.	It may pose a challenge for real time SCADA traffic and the required latency and bandwidth
	It does not require physical access hence suitable for terrains where access rights are difficult or impractical.	Providing power resilience could be a huge challenge and outside of Black Start stakeholders' control.
		There are currently coverage issues around many operational sites. Most mobile base station are concentrated around dense urban areas and substations are

		mostly located outside of these areas.
		Availability and resilience would depend on providers of public infrastructure, it could be difficult to ensure their compliance.
		As with wireless technology, the signal could be intercepted if robust encryption and authentication is not used
		Subject to commercial / technology risk as Public Operators upgrade / withdraw services to address consumer demand.
		No guaranteed quality of service and performance agreements.
Private Radio **Suitable option**	For DNOs (and some power station) that already have private radio, extending the network to DERs could be relatively low cost.	As with wireless technology, the signal could be intercepted if robust encryption and authentication is not deployed
	The base stations could utilise existing substations that have the required power resilience	There may be bandwidth limitations (based on existing spectrum access arrangements) on what can be carried by the radio data modems due to bandwidth required for modern applications and volume of data required.
	It does not require physical access hence suitable for terrains where physical access rights are difficult	
Openreach Ethernet Services **Suitable option**	These could be deployed in relative short time in areas where the services exist	Availability and resilience would depend on providers of public infrastructure, it could be difficult to ensure their compliance.
	Could be a cheap option.	
BT Openreach FTTP **Suitable option**	The communication link is not affected by weather	Availability and resilience would depend on providers of public infrastructure, it could be difficult to ensure their compliance.
	It has high availability as it is a physical and assured link	It requires access along route, right to the premises
	Interference would require physically breaching the cable	Proximity to assets will be limited and hence result in significant cost for deployment and connection.

	It provides high speed connection and low latency as with fibre products	Commercial / Technology risk as operator chooses to upgrade system to address market demand.
	It is relatively easy to provide power resilience as this is required only at the end points that houses the active equipment.	
BT Openreach FTTC **Not suitable for restoration** Due to lack of required power resilience	These could be deployed in relative short time in areas where the services exist	Availability and resilience would depend on providers of public infrastructure, it could be difficult to ensure their compliance.
	It may prove to be cheap compared to other options	The necessary power resilience is not currently in place. Provision may be challenging - it may require multiple active hubs, and these will require independent power to meet black start standard.
	The communication link is not affected by weather	It requires access rights to the premises and wayleave agreement.
	It has high availability as it is a physical and assured link	Proximity to assets will be limited and hence result in significant cost for deployment and connection.
	Interference will require physically breaching the cable	Commercial / Technology risk as operator chooses to upgrade system to address market demand.
		Subject to appropriate product / service availability via Communications Provider
ESN **May be suitable option for voice depending on final configuration.**	This could provide backup voice services to contact field staff or offsite staff.	This network is based on a commercial mobile network which we also know may not have power resilience built into it.
		The rollout has been delayed further
		- ESN is currently considering the requirements of emergency services only and have not considered third parties

Table 8: Advantages and Disadvantages of Different Communications Technology

3.2 Comparison of Key Communication Technologies

The table below lists the different technologies assessed for viability above against the functional requirements (detailed in section 2). The table analysed these technologies in terms of the latency, data rates and cost. The suitability of the technology for use during restoration is largely dependent on meeting the functional requirements. The cost of deploying the technology 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. Hence, no technology should be ruled out if it could be configured or installed to meet the functional specifications irrespective of its classification in the table below.

	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 (Public Mobile)	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	**Depending on Type*****

Table 9: Technology comparison

*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.

*****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 Support and Testing Regime for Service Providers

It is proposed that the telecommunication infrastructure and service support should cover the following broad areas:

- Service Level Agreement (All year round, 7 days a week) in place to cover for service restoration infrastructure failures, application failures, and end terminals equipment failures.
- All infrastructure and services are proactively monitored – faults alerted to a monitoring centre which is staffed all the time.
- Voice communication resilience is tested in normal service where practical e.g. by alternating calls between Main and Alternative routes where applicable.
- New telecoms network provisioning functionality covering restoration services should be proven in lab testing and network commissioning tests. Numerous planned outages and faults to demonstrate it works reliably. All key components proactively monitored.
- Voice communication calls to be tested at predefined intervals by making calls both ways.
- Power Resilience audit to be carried out and it is expected that the Primary Restoration Service participants /site owners would be responsible for carrying this out.
- Cyber resilient test/audit to be carried out in line with the NIS regulations
- Resilience Application test
- Self-test of the application devices

5 Risks & Mitigations

5.1 Table of Risks

Risk Number	Description of Risk	Cause of Risk	Consequence of Risk	Risk Mitigation
001	Unavailability of commercially available telecommunications options that meet functional requirement	Some of the commercially available systems are already in place and were not configured with the functional requirements in mind e.g. requirements for 72 hrs independent power resilience	These commercially available systems are deemed unsuitable for supporting ESRS. This may also discourage the use of certain providers e.g. Offshore based providers	The use of alternative systems, the Operators private network. The option to explore the provision of Emergency Services Network or other jointly provided communication infrastructure that will meet the requirement.
002	High cost of providing telecommunication options to meet functional requirements	The need to provide a resilient network to multiple providers may incur prohibitive cost.	This may discourage the use of some providers leading to insufficient generation capacity to meet ESRS.	The use of alternative systems, the Operators private network. The option to explore the provision of Emergency Services Network or other jointly provided communication infrastructure that will meet the requirement.
003	Increased cyber security risk due to increased attack surface	Increased number of connected networks increases the risk of protecting the systems due to increased attack surface.	This may lead to a less protected network exposing it to a cyber-attack.	End to end Cyber Risk assessment and solution adherence to Cyber security standards e.g. NIS regulations
004	Increased Interoperability risk of interconnecting more systems	Connecting multiple systems which may be different introduces issues with interoperability which may lead to unworkable solution.	Unworkable systems, solution may take longer and costlier to implement.	The use of common standards, whole system approach to solution implementation.
005	Increased risk of getting system to work e.g., automation in a short time scale	Knowhow of new systems, Short time scale to implementation.	Unworkable systems, solution may take longer and costlier to implement.	Early start, field trials and testing.

Table 10: Risks and mitigation

6 Impact on Industry

6.1 Impact on Industry Codes

It is envisaged that code changes will be required to the Grid Code, Distribution Code and System Operator Transmission Owner Codes. These are likely to be numerous changes to ensure that the capability required for ESRS is implemented appropriately. There may also be related changes to the Connection and Use of System Code (CUSC) and Balancing and Settlement Code (BSC).

6.2 Changes on Regulatory Frameworks

Changes made to the industry codes will place additional requirements on the restoration service providers. It is currently understood that there are potential reopeners within the DNO regulatory frameworks for changes associated with ESRS.

For Restoration Service Providers, these will be procured via a tendering process. It follows that costs will be included in their service provision. It is also possible that changes will be required in the secondary (non-commercial) generator providers. Funding mechanisms for secondary restoration activities will be investigated under a separate BSC code panel.

6.3 Route to Change

The ESO have raised Grid Code Modification GC0156 to implement the necessary changes to the Grid Code. The Technology and Locational Diversity Working Group will transfer into GC0156, to formalise the process. It is proposed this is a joint Grid Code / Distribution Code Workgroup which will also develop Distribution Code Changes. There will however need to be separate workgroup under the auspices of the other industry code panels (STC, SQSS, CUSC and BSC) to implement the full suite of measures required. It has been proposed that the combined Grid Code / Distribution Code should be the first formal Code modification established and the other industry code changes will then follow with the Grid Code taking the lead. This will enable the coordination of the Restoration Methodology.

7 Conclusion

The Communication Infrastructure Working Group reported on key areas detailing the different aspect of the communication infrastructure and technologies to support the Electricity system restoration.

The detailed telecommunication requirements including technical and non-technical requirements was reported on with reference to requirements for the Distribution Restoration Zone Control System. These include resilience Requirements, Bandwidth Requirements, Protocol Requirements, Cyber Security Standards and Voice Telephony Functional Requirements.

The Cyber security assessment recommended that Primary Restoration Service Providers be classified as Operators of Essential Services, therefore adhering to the NIS regulations.

The Working Group also reported on the viability of Current Technologies, Advantages and Disadvantages of Current Technologies, comparison of Key Communication Technologies, support and Testing Regime for Service Providers.

Finally, risk and mitigations, the Impact on Industry Codes, Changes on Regulatory Frameworks and Route to Change was reported on.

8 Glossary of Terms

Term	Definition
Primary Restoration Service	The ability for a Restoration Service Provider, or a combination of Providers connected at transmission or distribution, to meet the three basic requirements for Restoration. 1. To start-up (following a Total or Partial Shutdown) independently of external electrical supplies and support the re-starting of other Generators and Network Service Providers. 2. To be able to energise part of the network, and; 3. To be able to provide block loading of demand.
Distribution restoration zone (DRZ)	Part of the Local Distribution Network which has been energised by Anchor Plant following a Total Shutdown or Partial Shutdown. The Distribution Restoration Zone shall include an Anchor Plant and may also include Top-Up Plant owned and operated by one or more Restoration Service Providers;
Power Island	One or more Power Stations, together with complementary local demand.
Primary Restoration Providers	A provider of a Primary Restoration Service
Distribution Restoration Zone Control System" or "DRZ Control System"	A combined automatic control and supervisory system which assesses the equipment status and operational conditions of a DNO's System for the purposes of instructing Anchor Plant and Top-Up Plant and operating items of the DNO's equipment for the purposes of establishing and running a Distribution Restoration Zone;
Hot site	A high voltage site designated as such

9 Appendices

Electricity System Restoration Standard Implementation – Communication Infrastructure Working Group - Terms of Reference

Members

Chair: NGESO to provide
Tech Secs: NGESO to provide

Standing Members:
- NGESO
- NGET
- SPEN-T
- SSEN-T
- SSEN-D
- SPEN-D
- UKPN
- WPD
- ENW
- NPG

By invitation:
- Wind Rep
- Solar Rep
- Synch Gen Rep
- Interconnectors

Logistics

- **Cadence** – Fortnightly full meeting, with interim lighter touch meeting (without the project updates). Scheduled to align with key points in projects. Meetings scheduled for an initial 6months period
- **Duration** – 2 hours
- **Location** – Teams Meeting (for now)
- **Submissions** due and pre-read – slides/papers with clear confirmation of input/decisions needed 5 Business Days prior. Papers are to be read ahead of the meeting.
- **Minutes –** to be taken and circulated with the Action/Decision Log
- **Quorum** – All Standing members to attend. Deputies can attend with full decision-making authority delegated.

Standing Agenda

Items	Owner
1. Safety/Wellbeing/inclusion Moment	
2. Actions Update	
3. Progress/project update	
4. Risk/Issues for escalation to Coordination team	
5. Decisions/Actions	
6. AOB	

Purpose/Scope

Purpose:
- To develop an understanding of the role communications in Restoration and enable the delivery of a secure and resilient communications infrastructure

Inputs

- NGESO Strawman
- Relevant consultation responses
- Relevant codes
- Glossary & definitions

Outputs

- Identify current and future challenges for Communications across GB (including cybersecurity)
- Develop a testing process for all communication for service providers including Cyber security resilience
- Provide regular progress updates to coordination team and steering committee
- Produce a final report to include:
  - List of current/future challenges for communication including, as a minimum, a comparison of all key comms technologies and related advantages/limitations and related mitigations
  - A testing regime for each communications service provider
  - Risks and mitigations
  - In coordination with other industry working groups, the impact on industry codes, including mapping of changes in relevant regulatory frameworks, initial draft of the proposed changes and a route to change (e.g., Grid Code Modification proposal)