1 Communications Standards

For Electronic Data, Communication Facilities, Operational Metering and Automatic Logging Devices

NESO
National Energy System Operator

Contents

1 Introduction

This document defines the process for connecting registered Balancing Mechanism Units to the Balancing Mechanism, whether using the internet-based Wider Access API, or dedicated communication links from Trading Points and Control Points to The Company's Operational Wide Area Network (WAN). This document covers the physical means for the configuration of communication circuits together with the associated routing, protocol and security arrangements necessary for a Balancing Mechanism Unit to be integrated into the Balancing Mechanism.

Compliance with the communication requirements in this document is a condition of approval of requests for connections into The Company's Operational WAN. This includes EDL and EDT circuits to participants main sites and participants Disaster Recovery (DR) sites.

The scope of this document does not include the server platforms, software applications or workstations which utilise the communication links, although some details of application protocols are included for completeness.

2 Overview of Responsibilities

The submission of Bid Offer Acceptances to Control Points is an activity undertaken by The Company. There are two ways in which The Company can provide these services. For larger units, The Company normally elect to provide and own dedicated EDL communication circuits to Control Points whereas, for smaller units, the Wider Access API may be a more appropriate communications mechanism.

When implementing dedicated EDL communications circuits, the requirement for Automatic Logging Devices to be installed at Control Points, and therefore EDL communication circuits, is specified in Grid Code CC.6.5.8 (or ECC.6.5.8). Where requested by market participants, The Company shall use its discretion to decide whether to provide EDL link(s) to:

I. A Control Point not covered by the provisions of CC.6.5.8 (or ECC.6.5.8); and
II. Non-standard Control Points – e.g. where there are discrete Control Points used at different times or duplicated Control Points.

The number of EDL links provided to a Control Point is at the discretion of The Company, being dependent upon the operational need for this facility at the sites in question.

When implementing communications via the Wider Access API, The Company expect the market participant to provide suitable internet connectivity with appropriate security control in line with NIS guidelines.

It is a Trading Party's responsibility to submit Physical Notifications, Export & Import Limits and Bid Offer Data prices to The Company, and therefore, if not using the Wider Access API, to provide and own the circuits from Trading Points to The Company's premises which would be specified in the Bilateral Connection Agreement.

Notes with regards to submissions over dedicated communications circuits:

I. Submissions of Dynamic Parameters and short term Export & Import Limits (i.e.: up to 4 hours ahead of real time) are made from Control Points, and such submissions will therefore take place over the EDL circuits which are also used by The Company for Bid Offer Acceptances and other instructions; and

II. Longer term submissions of Export and Import Limits must be made via EDT links.

Unlike Wider Access API which utilises a common interface, in those cases where The Company provide and own communication links to a Control Point which is also designated as a Trading Point, the standard arrangement is to have separate circuits for EDL purposes and EDT purposes; i.e. these services do not share common communication links.

3 Registering for Services

Companies wishing to register for new Balancing Mechanism services, or wishing to undertake modifications to existing services, should send an e-mail précis of their requirements to The Company at bmu.registration@nationalenergyso.com.

If the query concerns the registration of new Balancing Mechanism Units (BMUs), details of the procedures involved will be provided via return e-mail.

In the case of requests for new or modified communication links for EDL or EDT purposes, or access to the WA API, a questionnaire will be sent out in response to e-mail enquiries.

Completing and returning this questionnaire is the first step in the approval process for arranging communications links into The Company's Operational WAN. Following receipt of the completed questionnaire, applicants will receive a follow-up telephone call from The Company to discuss their requirements.

4 NESO Connections Strategy

The Company recognises the need the embrace the Internet of Things (IoT), but at the same time maintain the resilience the of the Balancing Mechanism, by ensuring that Market Participants have appropriate levels of connectivity and Power-Supply (loss of mains) resilience protection.

Traditionally, communication services between The Company and participants have been solely through the use of fixed-line Multi-Protocol Label Switching (MPLS) connections, for EDL/EDT services. It is recognised that these services can be potentially cost-prohibitive, especially for Market Participants wishing to enter the Balancing Mechanism for the first time.

The Company has embraced IoT technology, making available the WA API and the Operational Metering hub to Market Participants. Market Participants are free to use such technologies, until such time that their portfolio of BM Units exceeds certain thresholds or for Market Participants who are Defence Service Providers or a Restoration Contractors. Above these limits, the participants will be required to move over to fixed-line and RTU technology, where power-resilience is guaranteed through telecom service providers.

Data latency (transmission time between the Market Participant and The Company boundary) should be kept as low as possible, but it is recognised that maximum limits may need to be applied. Such limits will remain under constant review by The Company and published by The Company on The Company's Website though they would not be expected to apply retrospectively.

Table 1.0:- Communications requirements based on Control Point Threshold

Control Point Threshold per Site (MW)	**BM Unit Thresholds (MW)**		**API**	**EDL/EDT (Fixed Lines)**	**Operational Metering**		**Telephony**	**24/7 (Staffed Operations)**
	Aggregated	**Primary or Sub-assets**			Hub	RTU		
≤10	NA	NA	✓	O	✓	O	System	O
≤50	NA	NA	✓	O	✓	O	System	O
<100 **	NA	NA	✓	O	✓	O	Control	M
<300	NA	<100	✓	O	✓	O	Control	M
<300	NA	>100	X	O	✓	O	Control	M
<600	<300	<100	✓	O	2nd independent VPN*	O	Control	M
<600	NA	>100	X	M	2nd independent VPN*	O	Control	M
<600	>300	NA	X	M	2nd independent VPN*	O	Control	M
<1000	<300	<100	✓	O	2nd independent VPN*	O	Control	M
<1000	NA	>100	X	M	X	M	Control	M
<1000	>300	NA	X	M	X	M	Control	M
≥1000 to 3600	NA	NA		M	X	M	Control	M
>3600	Fixed-line (MPLS) Connection required 3600MW is the Maximum industry limit for use of the API							

* a second independent and unique VPN (or a second resilient link in the case of MQTT (Message Queuing Telemetry Transport) protocol is required in order to avoid a single point of failure.

Table key

Aggregated BMU – a registered BMU comprising of multiple sub-assets at different locations, but within the same Constrained Group.

Primary BMU – a registered BMU comprising of a single asset located on it's own site and operated independently.

2nd Independent VPN – the connection of another parallel VPN (for Operational Metering) channel, with a different ISP and unique for the HUB VPN.

√ - Compliant to use-

O = Optional

M - Mandatory

X – Service option - Not available

NA – Not applicable as other thresholds determine the availability of the service option

Critical Tools and Facilities are defined in the Grid Code Glossary and Definitions. These Critical Tools and Facilities include items such as EDL, Control Telephony and Operational Metering, all of which require a 72 hour mains resilience period as defined in CC/ECC.7.10.1 of the Grid Code.

Critical Notes: ** Any Control Point managing any asset ≥ 100MW, or any Plant which is owned and operated by a Defence Service Provider or Restoration Contractor, automatically triggers the requirement to upgrade to fixed line/RTU technology.

The Company will adopt an absolute maximum limit of 3600MW, for the total portfolio of BMUs using the WA API. This limit will remain under constant review by The Company and will be subject to the perceived IoT resilience and The Company's communication infrastructure.

5 EDL/EDT

5.1 Support Arrangements

Although each of the communication circuits has a designated formal owner, as defined in section 2.0, the practical maintenance and operation of these circuits requires the active cooperation of parties at both ends of the circuit and the Multi-Protocol Label Switching (MPLS) provider.

It is the formal responsibility of each Trading Party to diagnose and resolve faults and problems on the EDT communication services to their Trading Point. This excludes responsibility for the core communication infrastructure located within The Company's communications provider's MPLS network, but includes responsibility for the communication circuits between the Trading Party and the MPLS network and the EDT routers which terminate these services on the Trading Party premises.

The Company will, however, provide Trading Parties with reasonable assistance in diagnosing and correcting problems on their EDT communication services.

The maintenance of EDL links is the formal responsibility of The Company; this includes the communication circuits and also the EDL communication router which is usually located at each Control Point. The boundary of responsibility is the Local Area Network (LAN) port on the EDL router; i.e. The Company's responsibility does not extend to any networks or network devices which may be connected to the EDL router. Beyond this boundary point maintenance and support is the responsibility of the BM Participant.

BM Participants and their agents are expected to provide The Company with reasonable assistance to resolve faults and problems on EDL communication services.

Faults should be reported to The Company's Service Desk on 0800 917 7111 (overseas callers should use +44 2030334634) and quote EDL or EDT as appropriate. This will ensure that the Service Desk engage the correct resolver group.

5.2 Types of Communication Circuit

The types of communication circuit are described in Appendix A.

5.3 Services to Control Points

The Company will provide a Main Route to each Control Point, and may also elect to provide an Alternate Route depending upon the extent of demand or generation which is controlled from that point. The standard for these is described in Appendix A.

In circumstances where The Company and the BM Participant agree to provide communications to a location other than the Control Point, then The Company will provide communications to this location, and the BM Participant will be responsible for onward communications to the Control Point. All EDL Managed Service Providers must conform to the requirements in this standard. The Company reserve the right not to provide EDL to this other location until these requirements are met. In these situations, on The Company's request, system architecture arrangements shall be shared with The Company.

Main Routes and Alternate Routes will terminate at geographically separate Company premises, with onward linking via The Company's Operational WAN.

The Company will provide, install and configure a router to terminate EDL services at each Control Point, hosting site or alternative location agreed with the BM Participant. Maintenance and operation of the routers is The Company's responsibility.

The network protocol used over these links is restricted to IPv4, with Border Gateway Protocol (BGP or eBGP) for the exchange of routing information. The use of other routing protocols or static routes is not permitted for this purpose.

The application level protocol is as referenced in the Electrical Standards annex to the Grid Code General Conditions. Further details of the EDL application protocol are given in Reference 8.1 of this document.

Where Control Telephony is provided to Control Points, this may be delivered via separate communication circuits to the services used for EDL, however The Company may elect to share communications circuits for both EDL and Control Telephony.

The Company will act as custodian of all network addresses which communicate with The Company's Operational WAN, and will allocate Registered Private IP Addresses for EDL at Control Points in accordance with The Company's standard addressing scheme. These are the only addresses which may be used by Automatic Logging Devices for communication with The Company.

Where The Company and the BM Participant or relevant Restoration Contractor agree that The Company will provide communications to a point other than the Control Point, then the resilience, support and redundancy requirements for the onward communication system to the Control Point is the responsibility of the BM Participant and/or relevant Restoration Contractor and must comply with the following requirements to ensure that systemic risks are mitigated:

1. Data in transit is:
   a. protected between the end user device(s) and the service
   b. protected internally within the service
   c. protected between the service and other services (e.g. where APIs are exposed)
2. The means of communication should be either of the following:
   a. Use a dedicated circuit replicating the current EDL leased line;
   b. If using an internet based connection:
      i. IpSec VPN to
      ii. Minimum of, cryptographic algorithm based on:
         1. Key length 128 bit
         2. Symmetric key algorithm: CAST AES-128
         3. Hashing algorithm SHA-256

iii. Security event and alarm monitoring, making The Company aware of significant breaches

3. The BM Participant and/or Restoration Contractor shall ensure that independent penetration tests and vulnerability assessments are carried out on the hosted environment at least annually, based upon HMG National Cyber Security Centre (HMG NCSC) Cyber Essentials (https://www.cyberessentials.ncsc.gov.uk/) and Security of Network and Information System (NIS) Regulations. Any consequent issues and remediation plans must be shared with The Company.

4. The following table shows the fix times, availability and redundancy requirements for fixed-line (MPLS) connections between The Company operational WAN and the Control Point.

Table 2.0 – Fix times, availability and redundancy requirements for fixed line MPLS Connections

Total MW capacity at risk / affected	**No. of BM Units at risk / affected**	**Fix Time within**	**Average Availability**	**Minimum Redundancy**[1] [Schematic in Appendix A]
0 – <100MW	n/a	12 hrs 24/7	< 12 hrs downtime pa	Not specified [Example 1, 4a]
100 – <300MW	n/a	12 hrs 24/7	< 12 hrs downtime pa	Dual redundancy on communication links[2][Example 2, 4]
300MW – <1 GW	n/a	12 hrs 24/7	< 4 hrs downtime pa	Dual redundancy on communication links[3] [Example 2,4]
1 GW – <3.6 GW	<=20			
1 GW – <3.6 GW	>20	12 hrs 24/7	< 4 hrs downtime pa, or < 1 hr downtime pa (preferred)	Dual redundancy on comms links. [Example 2,4] Preferred dual redundancy throughout system (no single event[4] will remove service) [Example 3,5]
3.6 GW or more	n/a	12 hrs 24/7	< 1 hr downtime pa	Dual redundancy throughout system (no single event[5] will remove service) [Example 3,5]

5. Where The Company has agreed with the BM Participant to provide the EDL connection to an alternative location, the communications between that location and control point, may use IoT technology in accordance with the requirements specified in Section 4 for WA API.

6. The BM Participant must tell The Company (via bmu.registration@nationalenergyso.com) which EDL Managed Service Provider they intend using. The Company may review the individual arrangements on a case by case basis and track the underlying risks, e.g. multiple EDL Managed Service Providers inadvertently using the same Data Centre, to ensure that this standard is met and that the risks have been mitigated sufficiently.

[1] Where National Energy System Operator has a communication link to the Control Point and to the EDL Managed Service Provider, then National Energy System Operator may use this to provide additional redundancy

[2] E.g. loss of a cable duct should not impact service

[3] E.g. loss of a cable duct should not impact service

[4] E.g. loss of a remote Control Point or Datacentre should not impact service. Geographic redundancy of at least 60km between remote Control Points or Datacentres required

[5] E.g. loss of a remote Control Point or Datacentre should not impact service. Geographic redundancy of at least 60km between remote Control Points or Datacentres required

7. The health of the communications route through to the Control Point must be indicated back to The Company to ensure The Company's Control Room knows whether electronic instructions will get to the Control Point in question.
8. If an EDL Managed Service Provider is identified by HMG NCSC as an "Operator of Essential Services" (OES), the service will be subject to the HMG NIS Directive.

If necessary The Company may revert to standard EDL arrangements to the Control Point.

5.4 Services from Trading Points

The Company will expect the Trading Party to implement communication links for EDT using one or more of the circuit types described in Appendix A.

Where a Trading Party provides an Alternate Route, it is recommended that this terminates on geographically separate Company premises to the Main Route, with onward linking via The Company Operational WAN.

Participants who do not wish to provide an Alternate Route may wish to utilise an ISDN (Integrated Services Digital Network) service as their Main Route, rather than an MPLS Circuit. This is because an ISDN service, which operates as a dial-up link, may be rapidly reconfigured to communicate with alternative Company sites, such as The Company DR site. In contrast to this, it would take a period of weeks to establish a new dedicated circuit to The Company DR site.

Participants who opt for a single communications route are also advised that they will lose the ability to submit data to The Company if their sole main route fails, until such time as the route is returned to service.

The Company recommended standard for termination of all routes at the Trading Point premises is a Cisco router or compatible alternative.

The Trading Party must agree their selected options with The Company in advance of placing any orders for communication circuits.

The network protocol used over the links will be IPv4, with Border Gateway Protocol (BGP or eBGP) for exchange of routing information. The use of other routing protocols or static routes is not permitted for this purpose.

Exchange of data is as referenced in the Electrical Standards annex to the Grid Code General Conditions. Further details of the EDT FTP file formats are given in Section 8.2 of this document.

The Company will act as custodian of all network addresses which communicate with The Company's Operational WAN, and will allocate Registered Private IP Addresses for EDT to Trading Parties in accordance with The Company's standard addressing scheme. These are the only addresses which may be used by Electronic Data Communication Facilities for communication with The Company.

5.5 Data Transmission Security

5.5.1 Application Level Security

5.5.1.1 Links to Trading Points

Each link from a Trading Point will have an EDT account on The Company servers which is dedicated for use by that Trading Party only. The accounts will have the minimum access rights which are necessary for data transfer. Submission accounts will have write-only access to a single directory, and notification accounts will have read-only access to a single directory.

The changing of EDT account passwords is carried out at the discretion of participants, and it is recommended that this be done at minimum intervals of 90 days. Participants wishing to change their passwords should submit an e-mail notification to The Company at bmu.registration@nationalenergyso.com.

The Company will respond to these requests by contacting one of the Authorised Parties previously nominated by the Participant, and agreeing details and timing of the required change.

5.5.1.2 Links to Control Points

EDL links to Control Points will use direct application-to-application data transfer using The Company-specific Master Message Server and Client Message Server protocol. This protocol has built in security mechanisms, under which client connections are automatically established by The Company's Master Message Server to the remote EDL Client Server. There are no manual password changes associated with these protocols.

5.5.2 Router Level Security

5.5.2.1 IP Addressing

All routed connections will be firewalled at The Company's end of the circuit, to restrict access rights to designated source and origin IP addresses only, via designated network IP addresses.

ISDN routes will have the additional protection of Point-to-Point Protocol (PPP). Under this protocol the routers at both ends of the link are configured with a password, and exchange of passwords is necessary before any data can be passed in either direction.

In order to ensure that participant data can pass through The Company firewalls participants should only use the Registered IP Address assigned to them by The Company at the time their communication links are commissioned. A number of options are available to accommodate the Registered IP address within individual participant addressing schemes:

i. Use the IP address as a native address where this does not conflict with existing participant addressing schemes.

ii. Use dual-homed servers with two Network Interface Cards to co-reside in two different addressing domains.

iii. The BM Participant implements Network Address Translation.

Option (iii) is the most commonly implemented configuration on participant EDT services, and is used by The Company on all EDL services to Control Points. Further advice on this topic can be obtained via e-mail to bmu.registration@nationalenergyso.com.

5.5.3 Security Monitoring

The Company will carry out routine security monitoring of external communication links to The Company's Operational WAN. In the event that activity upon any external link presents a threat to network integrity, the links may be blocked, and associated access rights suspended until the situation is resolved. The circumstances in which this action may be taken include the following: -

i. There is reasonable cause to believe that the links are being used for unauthorised purposes, or being accessed by unauthorised parties.

ii. Breaches of agreed security arrangements on client premises jeopardise the peripheral security of The Company's network.

iii. Excessive levels of data traffic are detected upon the links, which is outside normal operational parameters to the extent that the ability of application servers to process the data is put at risk.

iv. Corrupt or abnormally formatted data is received which presents a risk to application processing.

The Company will normally make all reasonable efforts to contact the parties concerned before any action is taken to block a communications link. The blocking of links without any warning will only occur in circumstances where there is an immediate and unacceptable risk to The Company's operational networks and/or systems.

Access to authorised user accounts on The Company's servers will also be monitored for security purposes. Where three successive failed login attempts are made upon such an account, the account will be frozen until the authorised user of the account contacts The Company support on the telephone number given in section 5.1 and a new password (and if necessary a new user ID) is issued.

5.6 FTP File Transfers

The standard method used by Trading Parties to transfer EDT submission files to The Company is via FTP (File Transfer Protocol), with submission files 'pushed' to the submission directories and corresponding notification files 'pulled' from notification directories. The following guidelines should be followed in relation to this:

i. Participants should only establish FTP connections to The Company servers when they have data to submit, or notifications to retrieve. FTP connections should not be left 'permanently' open.

ii. FTP connections should be terminated when submission of data is complete and notification of this has been received. Participants should not rely upon The Company's inactivity timeout for this purpose.

iii. The Company currently supports a maximum of 3 concurrent FTP sessions from any single Trading Party EDT account.

iv. Participants should not send rapid sequences of FTP connection requests at short intervals to The Company. This may be construed as abnormal traffic and could result in the disconnection of the participant's link.

v. It is, however, permissible to poll The Company’s servers with FTP connection requests at intervals when submissions are due to be sent, or notifications are awaited. The interval between successive connection requests should be no less than 20 seconds.

vi. Once established, a single FTP connection can be used to alternately push submission files and pull notification files.

5.7 Disaster Recovery Sites

5.7.1 Control Points

The Company will not normally provide disaster recovery communication circuits relating to the loss of Control Points. The loss of a site on which a Control Point is situated would normally imply that the physical plant controlled from there is no longer available to accept instructions.

Exceptions to this may be made from time to time at the discretion of The Company in cases where a Control Point is acting as a control agent for a number of geographically dispersed supply or demand blocks. When making such decisions, The Company will take into account the total amount of supply or demand which is under control, and the operational need to re-establish electronic despatch if the Control Agent site is lost.

5.7.2 Trading Points

Requests for communication circuits to Trading Party DR sites should be submitted for approval in exactly the same way as requests for connections to Trading Party main sites. If approved, then The Company will assign a specific IP address for use by the Trading Party for their DR servers. This will be a different IP address to that assigned for the main site servers.

In the event that participants lose facilities at their main site and need to invoke DR facilities, then The Company Operational WAN should already be configured to allow access from the IP address assigned for DR use. It may, however, be necessary to contact The Company support (on the telephone number given in section 5.1) for other reasons, for example to align EDT sequence numbers.

5.8 Network Access Tests

All new communication circuits to The Company Operational WAN must undergo Network Access Tests (NATs) before they can be approved for the transfer of live operational data. These tests are normally conducted using offline servers within The Company.

If participants are commissioning new EDL or EDT servers, additional tests to confirm the functionality of the application software running upon the servers are also needed. This may also apply when participants make software modifications to their existing servers.

Participants should contact The Company at bmu.registration@nationalenergyso.com at an early stage in drawing up their programme of work in order to determine the extent of testing required, and to agree any test dates.

All tests, whether involving network access or application software, shall be agreed in advance with The Company.

Where participants are undertaking development work at the same time as they are running existing production systems, The Company may assign an additional IP address to the participant to use for development system testing.

6 WA API

6.1 Support Arrangements

The Company provide an internet-based API for providing access to the Balancing Mechanism.

It is the formal responsibility of each Trading Party to diagnose and resolve faults and problems on the communication services between their Trading Point and The Company Wider Access API. This excludes responsibility for the core communication infrastructure located within The Company.

The Company will, however, provide Trading Parties with reasonable assistance in diagnosing and correcting problems on their Wider Access communication services.

The maintenance and availability of the Wider Access API is the responsibility of The Company; the boundary of responsibility, however, is the point of Hand-off from The Company's Network to the Internet. Infrastructure between this boundary and the BM Participant's Hand-off to the Internet is treated as an external infrastructure. The Company will, however, provide Trading Parties with reasonable assistance in diagnosing faults in this.

Faults should be reported to The Company's Service Desk on 0800 917 7111 (overseas callers should use +44 2030334634) and quote API as appropriate. This will ensure that the Service Desk engage the correct resolver group.

6.2 Types of Communication Circuit

The Trading Party is responsible for selecting and managing suitable connectivity to the Internet but The Company recommend that it is a permanent link with appropriate SLA and uses fixed IP addresses. It is the Market Participant's responsibility to ensure the SLA with their provider supports their intended hours of operation and recovery in the event of a problem.

6.3 Wider Access API Services

The Company will provide a Main Access Point (URL) for BM Participants to access the inbound Wider Access API Services over the Internet. This URL will have a FQDN that always point to the Wider Access API irrespective of whether The Company is under normal or DR operation.

BM Participants are expected to provide a similar URL for the outbound Wider Access API calls made from The Company to the BM Participant. It is expected that, should a BM Participant enter DR and move their Internet Handoff to a different location, this URL will remain the same and the DNS entry for the URL's FQDN will be updated.

The Company will provide a number of credentials to the BM Participant. This will consist of Developer/Admin credentials for accessing the Development Portal plus system credentials for automated systems to access the API directly. Developer/Admin credentials are limited to a total of 5 per BM Participant. Developer/Admin credentials allow access to the Developer Portal that contains the latest Swagger definitions for the Wider Access API, and allows generation of Access Tokens for testing purposes.

6.4 Data Transmission Security

6.4.1 Application Level Security

The Company limits access to the Wider Access API Services based on the originating IP Address of the incoming traffic. It is important that the BM Participant provides all IP addresses that their traffic may originate from during both normal and DR operation. Failure to provide all IP addresses may result in intermittent connectivity or an increased time to restore access to services should the BM Participant invoke DR.

The Company can make their originating IP Addresses available to the BM Participant upon request.

All API connectivity should be secured using TLS1.3, and all URLs should present suitable Certificates to incoming HTTPS connections. These certificates should be signed by an agreed public Certification Authority. The Company will supply a list of recognised Certification Authorities upon request.

All API Payloads must be signed by the originating party. The Company will provide their public key to the BM Participant as part of the Certification Process. The BM Participant will also need to supply their public key to The Company as part of the Certification and Onboarding Processes. All signatures and public/private keys should use SHA256 with RSA; the keys used must of 2048bits in length.

6.5 Security Monitoring

The Company will carry out routine security monitoring of connections using the Wider Access API. In the event that activity upon any external link presents a threat to network integrity, the links may be blocked, and associated access rights suspended until the situation is resolved. The circumstances in which this action may be taken include the following: -

i. There is reasonable cause to believe that the links are being used for unauthorised purposes, or being accessed by unauthorised parties.

ii. Breaches of agreed security arrangements on client premises jeopardise the peripheral security of The Company network.

iii. Excessive levels of data traffic are detected upon the links, which is outside normal operational parameters to the extent that the ability of application servers to process the data is put at risk.

iv. Corrupt or abnormally formatted data is received which presents a risk to application processing.

The Company will normally make all reasonable efforts to contact the parties concerned before any action is taken to block a communications link. The blocking of links without any warning will only occur in circumstances where there is an immediate and unacceptable risk to The Company’s operational networks and/or systems.

Access to authorised user accounts on The Company’s servers will also be monitored for security purposes. Where three successive failed login attempts are made upon such an account, the account will be frozen until the authorised user of the account contacts The Company's support facility on the telephone number given in section 5.1 and a new password (and if necessary a new user ID) is issued.

6.6 Network Access Tests

All new connections to The Company's Wider Access API Services must undergo Network Access Tests (NATs) before they can be approved for the transfer of live operational data. These tests are normally conducted using offline servers within The Company.

If participants are commissioning new Wider Access API services, additional tests to confirm the functionality of the application software running upon the servers are also needed. This may also apply when participants make software modifications to their existing servers. Participants should contact The Company at bmu.registration@nationalenergyso.com at an early stage in drawing up their programme of work in order to determine the extent of testing required, and to agree any test dates.

All tests, whether involving network access or application software, shall be agreed in advance with The Company.

Where participants are undertaking development work at the same time as they are running existing production systems, The Company may provide the participant with access to an additional Wider Access API environment to use for development system testing.

7 Operational Metering

The Company currently offers three routes for providing operational metering to the balancing systems.

- Connect to an existing GB Transmission Owner's Real-time Remote Terminal/Telemetry Unit (RTU).
- Install a new RTU and provide dedicated telecommunication signals to that location.
- Connect to the SCADA Data Concentrator host.

The Company recognises the need for commensurate solutions dependent on the size of BM participant. The above options offer varying levels of resilience, delivery (connection) time, cost and are based on the size of the BM participant.

The Company has implemented a new Data Concentrator, which is hosted by a third party. The new environment (iHost™) provides limitless capacity which is configurable and scalable, quicker to connect and offers a reduced end-consumer cost of making new connections.

The Company currently offer the following connection protocols:

- The IEC 60870-5 104 protocol over a VPN, to connect to The Company's boundary, or
- The MQTT protocol over an internet tunnel, to connect to The Company's boundary.

Additional connection protocols can be considered on request.

8 Additional Documents References

8.1 EDL Message Interface Specification

https://neso.energy/industry-information/codes/grid-code-gc/electrical-standards-documents

8.2 EDT Interface Specification

https://neso.energy/industry-information/codes/grid-code-gc/electrical-standards-documents

8.3 WA API Overview

https://neso.energy/document/179746/download

8.4 Operational Metering overview - Small BMUs

https://neso.energy/industry-information/balancing-services/balancing-mechanism-wider-access

9 Glossary

The following acronyms are used for the purposes of this document.

Table 3.0 – Acronyms

Acronym	**Description**
API	Application Protocol Interface
EDL	Electronic Data Logging
ADL	Automatic Logging Device
BM	Balancing Mechanism
EDL -	Electronic Despatch & Logging
EDT -	Electronic Data Transfer
FQDN	Fully Qualified Domain Name.
HMG NCSC	His Majesty’s Government National Cyber Security Centre
IoT	Internet of Things
ISDN	Integrated Services Digital Network
MPLS	Multi-Protocol Label Switching.
NESO	National Energy System Operator
NIS	Network and Information Systems
PSTN	Public Switched Telephone Network
RTU	Remote Terminal/Telemetry Unit
SCADA	Supervisory (Substation) Control And Data Acquisition
SLA	Service Level Agreement
WA API	Wider-Access API

10 Definitions

The following working definitions are used for the purposes of this document.

Table 4.0 - Definitions

Term	Definition
Anchor Restoration Contract	As defined in the Grid Code.
API	A computing interface which defines interactions between multiple software systems.
Authorised Party	The person or persons nominated by a market participant, and agreed by the National Energy System Operator, for the purpose of operating and maintaining communication circuits between the participant's premises and the National Energy System Operator’s premises. This includes persons authorised to receive details of security arrangements relating to such circuits, and to request changes to participant account passwords.
Aggregated BMU	A registered BMU, encompassing a portfolio of secondary assets (generation and/or demand), within the same Constrained Group
Automatic Logging Device	The computer facility at a Control Point capable of receiving Bid-Offer Acceptances and certain other instructions issued by The Company in accordance with Grid Code BC2. This may be, subject to the time-limits to be specified in the Grid Code, an Automatic Logging Device (EDL).
BM Participant	Has the meaning defined in the Grid Code.
Constrained Group	A series of 14 geographical boundaries within Great Britain, which align to Distribution Network Operator boundaries at Vesting.
Control Point	The point at which a market participant receives Bid Offer Acceptances and Ancillary Service instructions from National Energy System Operator and submits Export & Import Limits and Dynamic Parameters to National Energy System Operator. This would normally be a site from which the participant exercises real-time control of demand, or in the case of a power station, the point where this is physically controlled by the BM Participant.
Critical Tools and Facilities	As defined in the Grid Code.
Defence Service Provider	As defined in the Grid Code.

Term	Definition
EDL - Electronic Despatch & Logging	A term used to describe the National Energy System Operator application level protocol used on communication links to Control Points. This is also used in a more general sense to refer to the communication circuits between National Energy System Operator and Control Points.
EDL Managed Service Provider	A company that provides EDL services including provision of EDL communication circuits or links.
EDT - Electronic Data Transfer	A term used to describe the transfer of submission files between Trading Points and National Energy System Operator. This is also used in a general sense to refer to the communication links between Trading Points and the National Energy System Operator.
Electronic Data Communication Facilities	The computer facilities that allow a Trading Point or Control Point to submit specified BM Unit Data and Ancillary Services data to The Company in accordance with Grid Code BC1 and BC2. These may be, subject to the time-limits to be specified in the Grid Code, Electronic Data Communication Facilities (EDL & EDT).
EDL Communication System	The complete system used by The Company and the BM Participant for Bid Offer Acceptances and Ancillary Service instructions, and submitting Export & Import Limits and Dynamic Parameters
FQDN	Fully Qualified Domain Name. An FQDN is a the most complete domain name that identifies a host or server. The format is typically of the format [hostname].[domain].[tld] e.g. wideraccess.nationalenergyso.com
ISDN	Integrated Services Digital Network
Local Joint Restoration Plan	As defined in the Grid Code.
Mains Independence	In the event of loss of external electrical energy supplies, there shall be no loss of, or disruption to, communications services for at least the specified duration. To comply with this requirement an alternative power source is required that is independent of external electrical energy supplies which switches in to service on the failure of the external electrical energy supplies without manual intervention.
MPLS	Multi-Protocol Label Switching. MPLS networks assign labels to customer's data which allows routing decisions to be made by the network infrastructure. MPLS also allows data streams to be segregated enabling separate virtual private circuits to be delivered via the Service Provider's network.
MQTT	Message Queuing Telemetry Transport

Term	Definition
PSTN	Public Switched Telephone Network
Restoration Contractor	As defined in the Grid Code.
RTU	A microprocessor device that monitors and controls field devices, which facilitates the collection and transmission of SCADA signals back to a central point.
Small BMUs	BM Participants whose single asset size < 100MW; or who's aggregated assets within the same BMU are <100MW
Top Up Restoration Contract	As defined in the Grid Code.
Trading Party	The owners and/or operators of a Trading Point.
Trading Point	The point, designated by a market participant, from where Physical Notifications, Export & Import Limits and Bid Offer Data prices are submitted to the National Energy System Operator.
WA API	Wider-Access API

Appendix A: Types of Communication Circuit

Internet Circuits

Market Participants using the Wider Access API will need to ensure they have suitable Internet Circuits installed. These provide connectivity to the Internet which in turn provides a path to The Company's Wider Access API infrastructure.

MPLS (Multi-Protocol Label Switching) Circuit

MPLS circuits are now used for EDL connections because legacy KiloStream private circuits are no longer available. MPLS networks assign labels to customer's data which allows routing decisions to be made by the network infrastructure. MPLS also allows data streams to be segregated enabling separate virtual private circuits to be delivered via the Service Provider's network.

Trading Parties wishing to order MPLS circuits for EDT should contact The Company at bmu.registration@nationalenergyso.com to discuss their requirements before placing orders. Orders should be placed with the same MPLS provider that The Company use. This ensures connection to the correct virtual private network in order to access The Company services. Primary and Secondary (backup) connections can be made using this service.

ISDN Dial-up Circuit

The standard for these is a 64 kbit/s ISDN service, with Primary Rate ISDN presentation on The Company premises and Basic Rate ISDN presentation to the Trading Party or Control Point.

As this is a dial-up service, Trading Parties ordering ISDN links for EDT purposes do not have to specify presentation details for The Company end of the service. Trading Parties should still notify The Company in advance of placing orders for ISDN services, however, in order to ensure that capacity is reserved for them on The Company primary channels.

ISDN services provided by The Company for EDL at Control Points are reserved exclusively as Alternate EDL routes. These ISDN services must not be used for any other purpose.

ISDN along with PSTN is due to be switched off in 2025. The Company are considering alternative technologies such as mobile data or leased data services.

Private Circuit (legacy – no longer available)

The legacy connection method for EDL and EDT was KiloStream Private Circuits which were 64 kbit/s synchronous point circuits with X21 presentation.

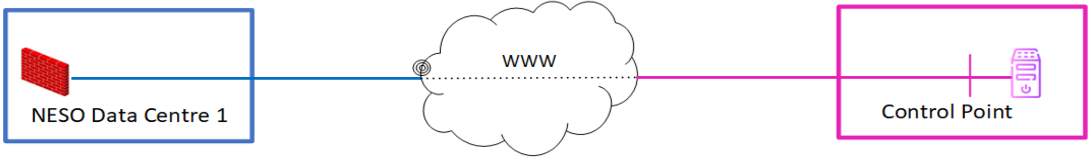
However, BT has ceased to supply KiloStream Private Circuits from March 2016, and will withdraw support for existing circuits by March 2020. Consequently, The Company are no longer using BT KiloStream for new EDL orders and have initiated a programme to replace existing KiloStream circuits used for EDL with MPLS circuits.

Trading Parties using BT KiloStream circuits for EDT purposes should make arrangements for their replacement, contacting The Company before any orders are placed so that the form of presentation can be agreed.

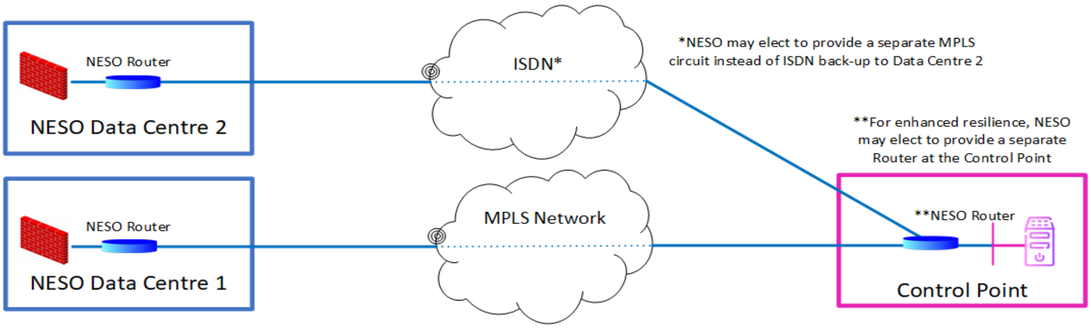
Schematic Diagrams

The diagrams below show the various circuit types

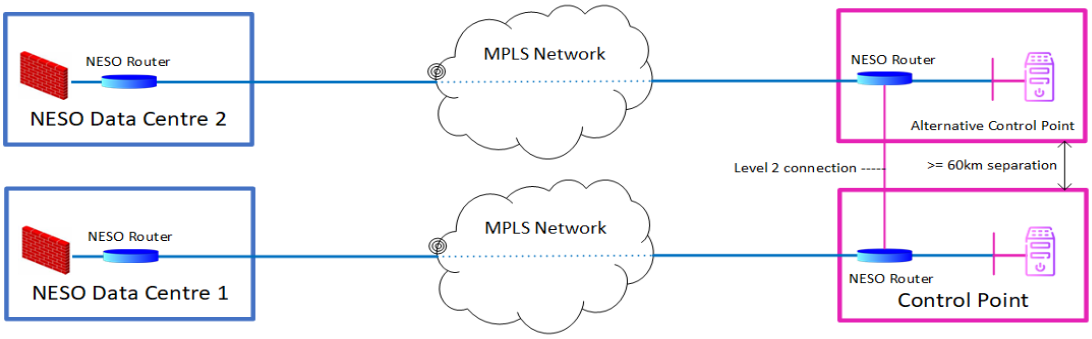
Example 1: EDL via the Internet (Wider Access Services)



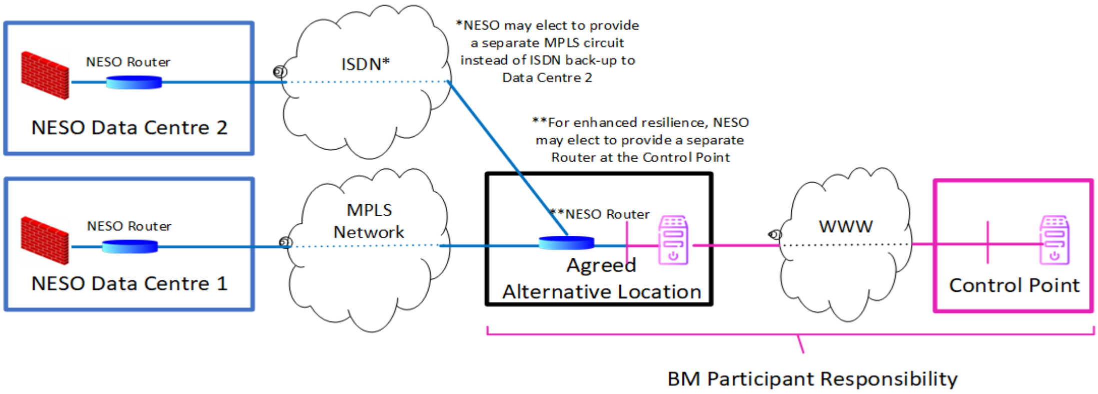
Example 2: EDL MPLS Circuit with ISDN Back-up – Control Point


NESO Router
NESO Data Centre 2
ISDN*
*NESO may elect to provide a separate MPLS circuit instead of ISDN back-up to Data Centre 2
**For enhanced resilience, NESO may elect to provide a separate Router at the Control Point
NESO Router
NESO Data Centre 1
MPLS Network
**NESO Router
Control Point

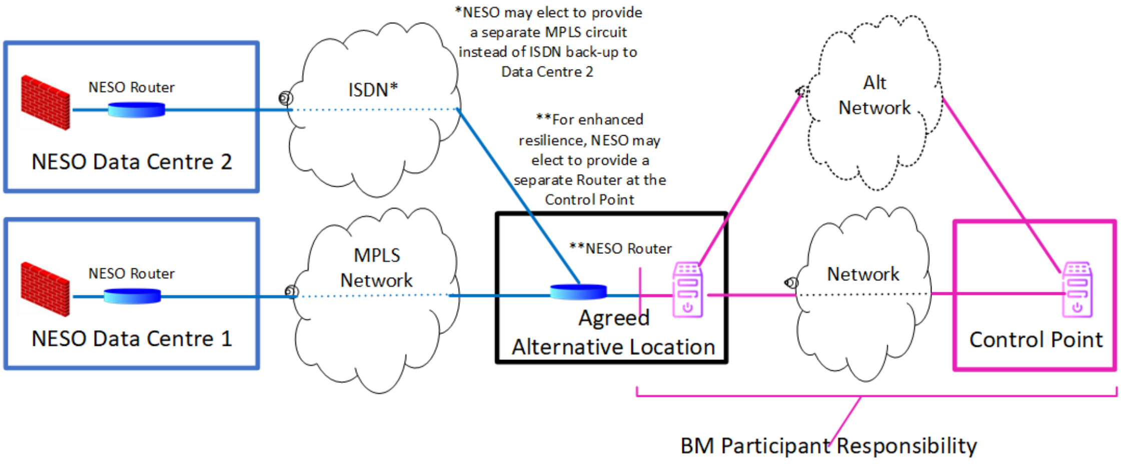
Example 3: EDL Dual MPLS Circuit, Dual Redundancy – Control Point



Example 4a: EDL MPLS Circuit with ISDN Back-up – Agreed Alternative location, CP via Internet


NESO Router
NESO Data Centre 2
ISDN*
*NESO may elect to provide a separate MPLS circuit instead of ISDN back-up to Data Centre 2
**For enhanced resilience, NESO may elect to provide a separate Router at the Control Point
NESO Router
NESO Data Centre 1
MPLS Network
**NESO Router
Agreed Alternative Location
WWW
Control Point
BM Participant Responsibility

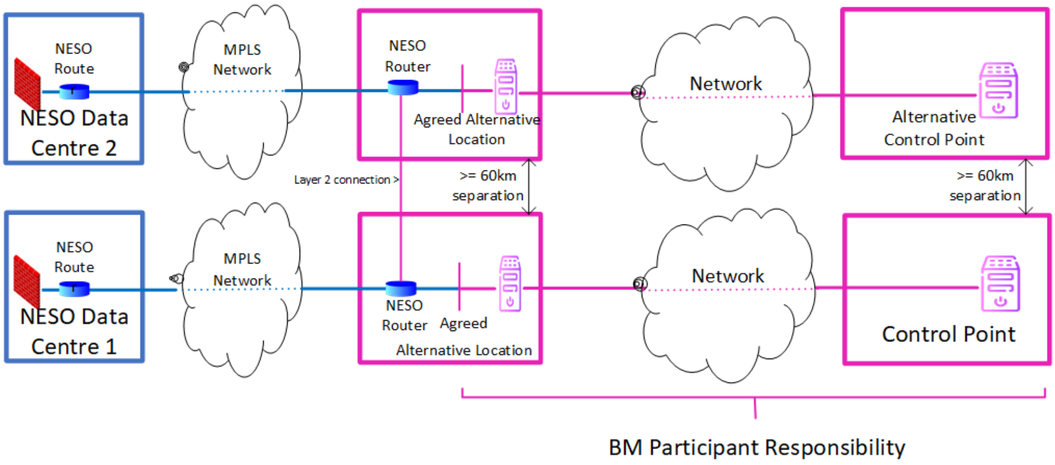
Example 4: EDL MPLS Circuit with ISDN Back-up – Agreed Alternative location, CP via Leased Network



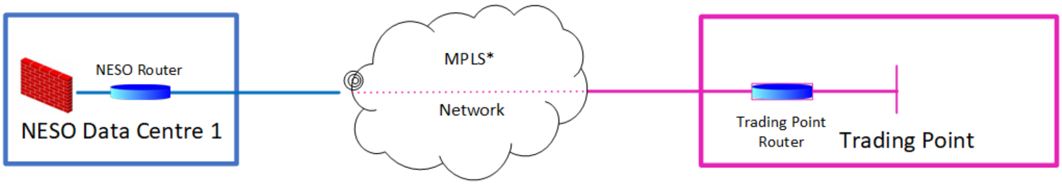
*NESO may elect to provide a separate MPLS circuit instead of ISDN back-up to Data Centre 2

**For enhanced resilience, NESO may elect to provide a separate Router at the Control Point

Example 5: EDL Dual MPLS Circuit, Dual Redundancy – Agreed Alternative location



Example 6: EDT MPLS Circuit (Separate circuit to Data Centre 2 may be provided for resilience)



*The Trading Party may elect to use ISDN or Wider Access Services (future development)

Ownership and Support Responsibility

- NESO
- BM Participant or Trading Party
- Automatic Logging Device (Server or PC running EDL) BM Participant
- NESO Router
- Trading Point Router

Appendix B: Document Information

Author: **Mark Bingham, National Energy System Operator OpTel Manager**

Distribution:

Name	Position	Reason for Distribution
Neil Simmons	Head of UK CNI Applications	Approval
Daniel Holder	Digital Risk and Security	Approval
Mark Bingham	Optel Manager	Approval
Rob Rome	Performance Transformation & Control Systems Manager	Approval

Document Amendment History:

Version	Date	Amended By	Remarks
3.0	28 Mar 2002	Keith Cusson	Issued for NETA go-live
4.0	26 Aug 2015	Steve Roberts	Updated to reflect changes since 2002
5.0	21 Dec 2018	Ivan Kileff	Updated with provisions for Alternative EDL Arrangements and other updates
6.0 draft 1	27 Mar 2019	Mark Bingham	Clarification of redundancy requirements
6.0 draft 2	25 Apr 2019	Mark Bingham	Updated Appendix A Diagrams
6.0 draft 3	8 May 2019	Mark Bingham	Added definition for Mains Independence. Amended National Grid to National Grid ESO
6.1	17 June 2019	Mark Bingham	Added comments from GCRP: updated mains independence definition. Added references to ECC.6.5.8 in Section 3
7.0	30 Dec 2020	John Walsh	Updated on NGESO template, plus additional WA API & Ops Metering chapters
8.0	March 2024	Antony Johnson	Updated in respect of the Electricity System Restoration Standard and changing National Grid ESO to The Company

9.0	08 April 2025	Lulu Isdory	Updated format and style of document

Paper Copies are Uncontrolled