Transmission System Operator to Distribution System Operator Agreement Guidelines

Document Control

Version	Date	Reason for change
0.1		
0.2	24/03/11	Review comments
0.3	25/03/11	Further review
0.4	31/03/11	Further review comments
0.5	04/04/11	Update to contingency table
0.6	06/04/11	Final review
0.7	17/10/11	Legal Review
1.0	21/03/13	DN Review and population of appendices.

Development of Rules

The procedure to review and modify the Transmission System Operator to Distribution System Operator Agreement Guidelines is specified in Section N1.2 of the Offtake Arrangements Document"".

These "Guidelines" can only be modified in accordance with the procedures adopted by the Offtake Committee in accordance with Section N 1.2.5 of the Offtake Arrangements Document, while the Document Control Section records changes which have been made to "the Guidelines". The document is published on the Joint Office of Gas Transporters' website, www.gasgovernance.co.uk

1. Contents

2. Definitions

Unless otherwise stated, terms in the Transmission System Operator to Distribution System Operator Agreement Guidelines ("Guidelines") shall have the meaning given to them in the Uniform Network Code. Such terms will be capitalised within quotation marks where first used in the Guidelines.

In these Guidelines:

"**Distribution System Operator**"
The department of the "Distribution Network Owner" responsible for the safe control and operation of their gas supply and storage system(s).

"National Grid Transmission System Operator"
The department of National Grid Transmission responsible for the safe control and operation of the National Transmission System.

"UK Gas Supply Network" –
Includes all the gas supply networks owned and operated by National Grid Transmission and Distribution Network Operators.

"Control Systems"
SCADA systems used by the National Grid Transmission System Operator and Distribution System Operators in the control and operation of the UK Gas Supply Network.

"IS Systems" -
Information Systems and communications network infrastructure, which shall include Control Systems where appropriate, employed by the National Grid Transmission System Operator and Distribution System Operators used to monitor and control their UK Gas Supply Networks.

"**Party**"
For the purposes of these Guidelines a Party is either the National Grid Transmission System Operator or a Distribution System Operator.

"Parties"
For the purposes of this document the Parties are both the National Grid Transmission System Operator and the Distribution System Operators.

NRO
Non-Routine Operation.

Service Desks
Points of contact for raising IS System faults / incidents for the National Grid Transmission System Operator and each Distribution System Operator.

3. Background

The System Operations Managed Service Agreement (SOMSA) came into effect on the 1st May 2005 and set out the terms and conditions under which National Grid Gas (NGG) managed gas networks on behalf of the independent Distribution Network Operators (iDNs).

With the termination of the SOMSA there remains a number of areas where the "**National Grid Transmission System Operator"** and a "**Distribution System Operator" (the Parties)** will need to share information and provide mutual support to allow efficient and safe operation of the "**UK Gas Supply Network"**. To ensure this happens effectively, there is a requirement for enduring arrangements between the Parties.

4. Purpose

These Guidelines have been created to detail the arrangements and clarify the responsibilities of the Parties in order to fulfil the processes defined within these Guidelines. These Guidelines have been included as an Offtake Subsidiary Document within the UNC Offtake Arrangements Document (OAD) which details the governance for amendments to these Guidelines.

These Guidelines apply to the processes associated with information sharing between the Parties' IS Systems and creates the agreements that will govern the transfer of any such data and the processes by which the appropriate support is provided to ensure that all data that is required by impacted Parties is maintained effectively.

5. The Guidelines

The different agreements covered by these Guidelines have been developed to cover all the obligated and other agreed data transfers required between the Parties, and are summarised below with full details included in the appropriate annex.

For the avoidance of doubt, where there is a conflict between the provisions of these Guidelines and those contained within the UNC OAD, those provisions within the UNC/OAD will take priority.

6. Business Planning

It is recognised that from time to time a Party may need to amend / replace their System(s) or processes and that this may impact upon the other Parties' business planning processes or systems. The initiating Party must notify affected Parties of plans in sufficient time to permit plans to be developed to support these changes.

These Guidelines specify the requirements and responsibilities placed upon the Parties for ensuring that affected Parties are engaged in good time and follow appropriate processes to implement changes.

The full details of the process are covered in Annex 1.

7. IS System Fault Management

These Guidelines provide the framework that the Parties will use to manage faults or failures in IS Systems leading to a potential loss of data to another Party and details the support required from other Parties to resolve and achieve a return to normal service.

The full details of the process are covered in Annex 2.

8. IS System Change Management

Accurate transfer of data between Parties is essential to efficient System operations. It is recognised that from time to time, a Party may need to carry out planned work on their System(s) that may impact upon other Parties. In this situation the initiating Party must ensure that potentially impacted Parties are consulted in sufficient time to permit discussions to agree how the change is managed effectively.

These Guidelines specify the requirements and responsibilities placed upon the Parties for ensuring that changes that impact data transfer (or have the potential to impact) are communicated to the appropriate Parties in sufficient time and detail.

The full details of the process are covered in Annex 3.

9. SCADA Configuration Management

Consistent and accurate configuration of Control Systems by all Parties is essential to support the accurate transfer of data between the Parties' Control Systems and associated Systems.

These Guidelines define the process for ensuring consistent mapping between the Parties' Control Systems and for managing any changes to the mappings in a timely and efficient manner.

These Guidelines specify the requirements and responsibilities placed upon the Parties for ensuring that changes that affect data transfer are communicated to other affected Parties in sufficient time and that data extracts are provided to support validation of mapping between Control Systems.

The full details of the process are covered in Annex 4.

10. Contingency requirements

It is recognised that System issues suffered by one of the Parties may impact on other Parties, and procedures have been developed and agreed to manage the provision of affected Party's(ies) key data in such an occurrence.

These Guidelines specify the requirements and responsibilities placed upon the Parties for ensuring the effective communication and transfer of key data items in the event of failure of normal processes.

The full details of the process are covered in Annex 5.

11. System Security

All Parties to these Guidelines are expected to protect the confidentiality, integrity and availability of those information assets, shared in the course of ongoing operation, with recognised good practice security controls.

Controls shall be put in place by each Party to ensure that whenever confidential information, including any personal data, is shared, only those individuals required by their job role and authorised to do so are able to access that confidential information.

All Parties shall carry out good practice vetting of staff, appropriate to the individual job role and the information access granted to their own and shared information assets.

Each Party shall also put in place arrangements to ensure the security of its own computing and communications infrastructure when that infrastructure is connected to a third party. These arrangements shall include, but are not limited to, appropriate methods of protection against malicious software.

In the event there are any concerns regarding the level of security then a Party may request evidence of such security standards.

12. Hardware Demarcation

The supply, transfer and receipt of data is reliant on IS Systems being in place. The demarcation point for the ownership of this hardware is at the handoff router:

- Typically, a Party will procure and install a network link, terminating at a handoff router within the connected Party's IS System.

- Both Parties will have infrastructure (servers) associated with the sending/receiving system and ownership of these will align with the location of the equipment. The effects of exceptions to this, such as xoserve utilising the National Grid Transmission System Operator IS System, are covered by commercial arrangements and separate to this document.

- Either Party may also have an IS System to manage the file transfer process (FTP) and again ownership of this will align with the location of the equipment.

Ownership includes the responsibility for fault/support and maintenance of the equipment.

13. Business Continuity Management

In order to ensure that the contingency processes are fully effective, it has been agreed by all Parties that these will be tested on an annual basis and will be included in the annual emergency desk top exercise.

14. Annexes

Annex 1 - Business Planning
Annex 2 – IS Systems Fault Management
Annex 3 – IS Systems Change Management
Annex 4 - SCADA Configuration Management
Annex 5 - Contingency Requirements

Annex 1. Business Planning

Scope

Due to the reliance of Parties on data transfer from other Parties, it is important that a coordinated approach is taken to business planning for Systems changes where those changes affect more than one Party.

Where a Party, as part of its business planning process, identifies a requirement to make such changes or replacements to its Systems that will significantly impact another Party due to changes to interfaces, or a requirement for significant testing of interfaces, then the initiating Party will make this known to all impacted Parties in sufficient time to allow the affected Parties to take this into account in their own business planning.

Process

The Parties will agree indicative timescales, impacts, processes for project implementation/issue resolution and funding arrangements (i.e. which Party will pay for which elements of the work).

During project delivery, each Party should follow its own project management methodology, however, this should follow industry best practice. As a key part of this, throughout the life of the project, the initiating Party will engage effectively in a pre-agreed manner with affected Parties to allow for appropriate planning to be carried out and for agreement on key issues to be achieved in appropriate timescales.

In the event of conflicting requirements between affected Parties, these will be resolved via a suitable Transporter Forum, such as the System Operators Forum, to find an optimum solution.

Communications

At the initiation stage of a Project/issue resolution the Parties will agree and provide details for key points of contact, including e-mail addresses and telephone numbers.,

Annex 2 – IS Systems Fault Management

Scope

These Guidelines are applicable to the Parties for the management of faults on IS Systems which impact upon the operations of other Parties, or require support from other Parties to resolve.

Arrangements for planning and management of maintenance and change of applicable IS Systems are outside the scope of these Guidelines.

Where a Party encounters a fault with a System or communication link that could affect another Party, they will communicate and co-ordinate their response through established points of contacts as described in Appendix A.

Process

1. Fault/Incident Reporting

The Party that detects the fault shall report the fault to their respective "**Service Desk"** for a fault reference to be raised and appropriate support teams within their organisation to be mobilised. In addition, where appropriate, Control Room to Control Room communication will be initiated by the originating Party to focus on necessary operational contingency arrangements.

Service Desk to Service Desk communication will be initiated by the originating Party to mobilise fault resolution activity.

Reporting of faults within each organisation is the responsibility of each organisation.

Parties are expected to agree and manage faults at similar priority to those of the initiating Party.

Where a fault is raised and the initial diagnosis determines that the problem lies with the initiating Party, other Parties will carry out high level checks and be prepared to participate if called on (e.g. if NGG raise a call for a problem that appears to be a fault on a NGG system, other Parties will check their systems and prepare to be called upon should the need arise).

This process will result in agreement upon which Party is responsible for leading on resolution of the fault/incident.

2. Fault/Incident Management

During fault/incident resolution each Party shall be responsible for managing impacts upon their own IS Systems.

Where co-operation is required between Parties this shall be at the direction of the Party agreed as responsible at the outset of the reported fault.

Co-operation may include (as required by the specific circumstances of a fault/incident):

- Attending technical and/or management "bridges" (teleconferences)
- Undertaking remedial activities on Parties' own IS Systems
- Undertaking tests as required
- Agreeing priority/severity
- Co-ordinating communication within Parties
- Allocation of appropriate resources and knowledge
- Other actions which may be necessary to achieve effective and timely resolution
- Contingency co-ordination
- Reporting on progress of actions agreed
- Fault closure will take place through Service Desk to Service Desk communication.

3. Fault/Incident Investigation/Post Event Analysis.

Once a fault/incident is resolved, and co-operation has been necessary, the nominated responsible Party shall initiate appropriate post event and root cause analysis. The objectives of this shall be to learn from the experience in order to avoid future reoccurrence and/or improve the process of fault/incident management.

Where requested, each Party is obliged to contribute to and participate in such analysis and undertake agreed resulting actions.

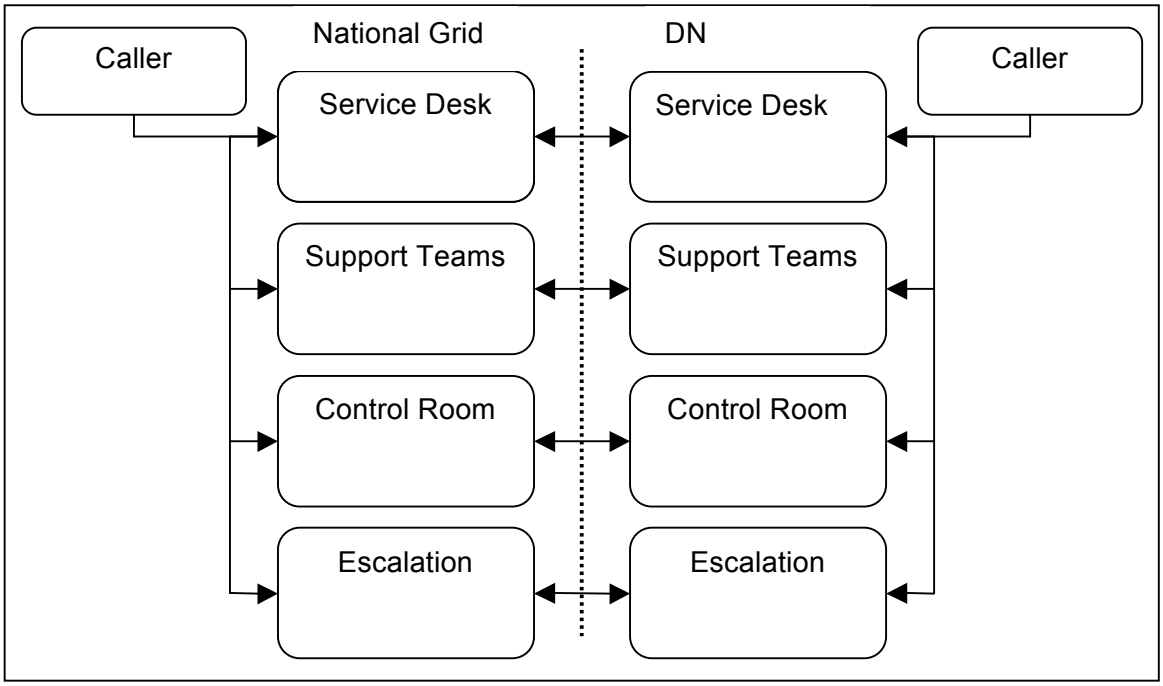
A formal RCA (Root Cause Analysis) Report will be made available for any P1/P2 incident raised and distributed within 10 days of formal closure. The responsible Party should also be responsible for carrying out trend analysis should a persistent problem occur.

The Party responsible for leading the fault/incident shall lead on the post event analysis.

Communications

A single point of contact (SPOC), phone number and email account will be maintained and communicated by each Party to enable effective reporting, management and where required escalation of IS System issues (the information required is detailed in Appendix A). The SPOC should be available 24 hours a day, 7 days a week in order to effectively manage this incident process. Each Party will be responsible for maintaining and communicating the contact details for its SPOC.

The following diagram provides an overview of the various elements of the entire restoration team for all faults/incidents affecting the National Grid Transmission and Distribution System Operator. Also shown are the communication activities that will be co-ordinated between technical, management and business groups, including the relevant escalation routes.



Request for Access

In some instances the physical location of a Party's equipment may be on another Party's site. When a Party requires access to this equipment it will be managed via a request to the other Party's Service Desk.

Annex 3 – IS Systems Change Management

Scope
Any changes to non-SCADA systems (referred to as business applications) which may impact other Parties' systems should be managed via the IS Change Management process. This will allow the impact of any proposed business application changes to be assessed in sufficient time to permit discussions to agree how the change is managed effectively.

The table below describes the types of work to be carried out for each classification of IS systems change and the notice periods that are required between parties prior to the work being carried out (Where the work being carried out cannot be clearly placed under a specific classification then Parties will agree on a classification for the work)

Classification	Nature of Work	Notice Period	Typical Work	Typical Impact	Comments
Notification	Routine	5 Business Days	Server swaps	Generation of alarms on system used by other Party. Brief loss of telemetry (typically less than 3 minutes).	
Minor Impact	Non Routine	10 Business Days	System upgrades. Software release to applications. Remedial work post incidents.	Generation of multiple alarms on system used by other Party. Several instances of brief loss of telemetry (typically less than 3 minutes).	Work to be managed under an "**NRO"**. Impacted Parties receive copy of NRO for information only.
Major Impact	Non Routine	30 Business Days	Replacement of IS Systems. Maintenance / testing of telemetry.	Loss of data over extended period(s).	Work to be managed under an NRO. Impacted Parties to approve the NRO.

Process

The Party initiating the work shall identify and advise impacted Parties of the date/time of work, duration, content, impact upon the operation of data transfer and measures to mitigate the effect of the outage. Other Parties will be invited to comment on any aspect of the proposed change which impacts their data flows or system.

In all cases, details including impact assessment, method statement and back out plan to be provided, where applicable these shall be incorporated within the NRO. Those carrying the work will contact the impacted Control Room(s) and IS support before work commences and upon completion of work and make arrangements for contact during the work. Consideration should be given to use of a telephone conference to manage co-ordination between Parties.

To support remedial work following faults/incidents, the Parties will work together to facilitate short notice plan changes.

Communications

The Parties shall each nominate a single point of contact (SPOC) for co-ordination and provide contact details, including an e-mail account address and telephone number. The required level of information for the SPOC is detailed in Appendix B. Each Party will ensure the SPOC details are maintained and communicated as appropriate.

Prior to changes that have a major impact upon another Party, meetings shall be held between the Parties to discuss the change and evaluate the impact upon all Parties (see below).

Parties will be expected to manage each change in a considered way, taking account of constraints of other Parties. If the other Party is subject to difficulties because of the method or timing of the change, the Parties will work together to minimise these.

In the event of conflicting requirements between affected Parties, these will be resolved via a suitable Transporter forum, such as the System Operators Forum, to find an optimum solution.

Governance of System Changes

Each Party will follow internal governance processes for changes. The initiating Party may be called upon to provide information to support approval of the work but may not be required to participate in the governance process.

The other Party may not form part of the formal governance group and therefore may not have the power to prevent changes occurring if they are considered necessary by the initiating Party.

However, all Parties will be expected to manage each change in a considered way and if the other Party will be subject to difficulties because of the timing of the change, the initiating Party shall take that into account before finalising the implementation timescales.

Annex 4 – SCADA Configuration Management

Scope

1. Management of Changes

Trigger of Changes
Changes can be initiated by either Party as a result of:

(a) Addition of new assets to existing sites
(b) New sites/telemetry rebuilds
(c) Decommissioning of sites/removal of assets
(d) Correction of errors

Process
Data items and controls to be mapped between Systems are as listed in the Offtake Arrangements Document Section E Annex E-1 and the Supplemental Agreement for each site.

Any additions, changes or deletions to data items mapped between Control Systems shall be communicated to the other Party in line with the timescales below.

The Party that initiates the changes has responsibility for liasing with the other Party to agree the inter Control System configuration that shall be in accordance with the agreed convention.

Details of changes shall be sent to the other Party via fax or e-mail. Details to be provided include (but are not limited to) database addresses, ranges, state names and in the case of changes which require SCADA picture changes, an ELD marked with points at which measurements are taken.

Details of any non standard or unusual operating arrangements relating to a site which may affect the other Party shall be communicated to support monitoring/operation of the site or development of alarm responses.

The initiating Party's change shall ensure that testing between Control Systems is included within the initial site commissioning / end to end tests. In addition, testing can be arranged via the agreed points of contact, at the request of either Party, to validate the data transfer following changes made to the database on either System.

Notification of changes

- Minor changes (e.g. addition of new measurement, change to existing measurement) shall be communicated to the other Party no less than 5 Business Days before the change is to be applied. Significant changes (e.g. new site or telemetry rebuild) shall be communicated to the other Party no less than 60 Business Days before the change is to be applied.

Unplanned changes such as those required to accommodate emergency reconfiguration of a gas network, urgent change to project timescales, or correction of errors shall be allowed.

Where changes are to take place in stages, the other Party shall provide data relevant to each stage of the change along with proposed implementation dates.

2. Validation between Systems

Scope

Requirement for validation – an initial validation of database configuration shall be carried out by using full dataitem to dataitem check between Control Systems and subsequent changes shall be managed as described above. However, the nature of the database configuration on the Control Systems introduces a risk of configuration mismatch between Control Systems. To mitigate this risk, a process shall be introduced to provide the other Party with an extract of the SCADA Database to allow each Party to carry out validation checks to confirm the integrity of the data transfer.

Process

An extract of the SCADA Database mapping required to support the SCADA – SCADA data transfer shall be provided to the other Party fortnightly, or upon request.

The extract shall take the form of an Excel spreadsheet using format agreed between Parties and shall be sent to the nominated email account.

Communication

Each Party shall each nominate a single point of contact (SPOC) for coordination, including an email account address. The information required for the SPOC is detailed in Appendix C and each Party will ensure these are maintained and communicated as appropriate.

It is not envisaged that regular liaison meetings will be required. However, these can be arranged by either Party should the need arise to discuss changes for a significant project, e.g. site rebuild.

Annex 5 – Contingency Requirements

Scope

The table below details the critical data that is required by the affected Party in the event of a failure of normal procedures, this is intended to compliment the existing contingency arrangements including those stipulated in the Offtake Communications Document.

Transfer	Data	Reasoning	Method	Frequency
DSO – TSO SCADA Link	Inlet pressures, CVs & compressibility	To enable monitoring of extremity / key NTS pressures, and update of linepack.	Fax or e-mail	Hourly or as agreed depending upon demand level grid conditions. Dataitems to be supplied as scaled values
DSO – TSO Aggregator Link	Offtake Profile Notifications	To enable calculation / tracking of NTS demands	Fax or e-mail	On change
DSO – TSO Aggregator Link	Forecast demand and stock change (always set to zero) within day and day ahead	To enable calculation / tracking of NTS demands	Fax or e-mail	Forecast times and upon change
DSO – TSO Aggregator Link	End of day volumes for Offtakes (DVols)	To support reconciliation processes	Fax or e-mail	Daily between 06:00 and 08:00
TSO – DSO SCADA Link	Subset of data as identified by each DNO	To enable monitoring of DN gas networks and support DN processes	Fax or e-mail	Hourly or as agreed depending upon demand level grid conditions. Dataitems to be supplied as scaled values
TSO – DSO Aggregator Link	Flow weighted average CV and Billing CV	To support Actual and Forecast demand processes	Fax or e-mail	On change

General

A contingency event will be declared in the event that data has not been received by a Party within the established timescales. If the Party has access to the applicable data, it will be provided by fax or e-mail.

The data received by the National Grid Transmission System Operator in the event of an Aggregator link failure is dependant upon the location/ nature of the fault. Failure of the link between the Distribution System Operator and Aggregator will result in the Transmission System Operator receiving the last good value held within the Aggregator. All other failures will result in no value being received by the National Grid Transmission System Operator.

Where the National Grid Transmission System Operator has data that is appropriate to share with a specific Distribution System Operator, this will be provided in a similar manner to the above, subject to agreement by both Parties.

All Parties will maintain procedures to ensure that the data is transferred manually when there is a failure in the Control Systems and ensure that the transfer procedures are mutually compatible.

To support transfer of SCADA data, each Party will identify and agree the subset of the data required under contingency arrangements. This subset of data will be communicated to the Party providing the data who in turn will create SCADA displays/screens with the required data to send to the other Party.

15. **Appendices**

Appendix A – IS System Fault Management – SPOC details
Appendix B – IS Systems Change Management SPOC details
Appendix C – SCADA Configuration Management SPOC details

Appendix A – IS System Fault Management

Details of SPOC for communications relating to System Fault Management:

Party	IS Points of Contact		Control Room	
	Email	Telephone	Email	Telephone
NGG Transmission	iGMS.SupportTeam@nationalgrid.com	07717447892	Gncc.control@nationalgrid.com	08701910630
Northern Gas Networks	ithelp@northerngas.co.uk	0113 397 5390 or 0796 009 6552	NGN_Operations@northerngas.co.uk	0845 600 3171
Wales & West Utilities	wwutilities@plexus.serco.com	0844 57 65 320	WWU_systemoperation_operations@wwutilities.co.uk	03301 00 00 61
Scotia Gas Networks	Gascontrol.operations@sgn.co.uk	08450737 953	Gascontrol.operations@sgn.co.uk	08450737 953
NGG Distribution	No email or box account for IS helpdesk	0800 917 7111	sysop.dncc.operations@nationalgrid.com	0870 2418701

Details for Service Desk Contact for communications relating to System Fault Management:

Party	Service Desk	
	Email	Telephone
NGG Transmission & Distribution	iGMS.SupportTeam@nationalgrid.com	07717447892
Northern Gas Networks	NGN_sdesk@wipro.com	0808 238 9929
Wales & West Utilities	wwutilities@plexus.serco.com	0844 57 65 320
Scotia Gas Networks	sgngcapp@sgn.co.uk	0788 435 7280

Appendix B - Systems Change Management

Details of SPOC for communications relating to Systems Change Management:

Party	SPOC	
	Email	Telephone
NGG Transmission	iGMS.SupportTeam@nationalgrid.com	07717447892
Northern Gas Networks	NGN_Support@northerngas.co.uk	0191 511 4515
Wales & West Utilities	Wwu_systemoperation_support@wwutilities.co.uk	03301 00 00 64
Scotia Gas Networks	Gascontrol.support@sgn.co.uk	08450737 963
NGG Distribution	dncc.scadatelemetry@nationalgrid.com	0800 917 7111

Appendix C - SCADA Configuration Management

Details of SPOC for communications relating to SCADA configuration:

Party	SPOC	
	Email	Telephone
NGG Transmission	iGMS.SupportTeam@nationalgrid.com	07717447892
Northern Gas Networks	NGN_Support@northerngas.co.uk	0191 511 4515
Wales & West Utilities	Wwu_systemoperation_support@wwutilities.co.uk	03301 00 00 64
Scotia Gas Networks	Gascontrol.scada@sgn.co.uk	08450737 962
NGG Distribution	dncc.scadatelemetry@nationalgrid.com	0800 917 7111

