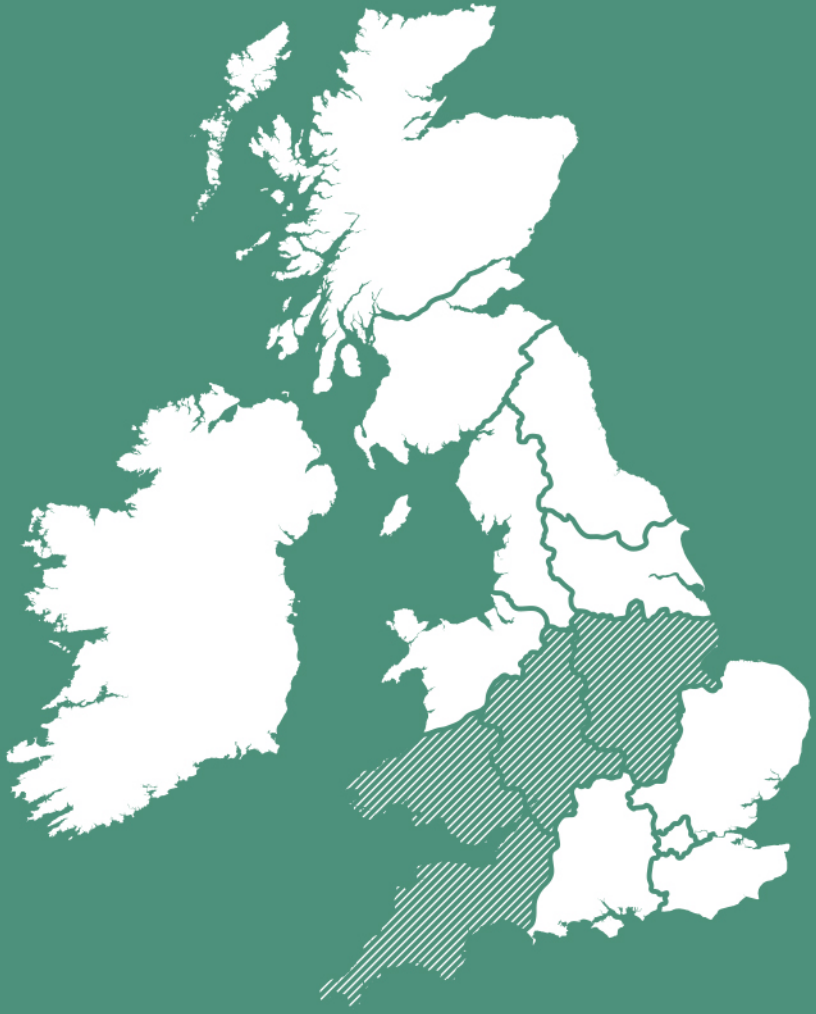
WESTERN POWER DISTRIBUTION

INNOVATION

NEXT GENERATION NETWORKS

INTERCONNECTION OF WPD AND NGC SCADA SYSTEMS

CLOSEDOWN REPORT



LCN Fund
Low Carbon Networks

Report Title	:	INTERCONNECTION OF WPD AND NGC SCADA SYSTEMS CLOSEDOWN REPORT
Report Status	:	FINAL
Project Ref	:	WPDT1001
Date	:	20/09/2016

Document Control

	Name	Date
Prepared by:	Steven Burns /Jonathan Berry	01.12.2016
Reviewed by:	Roger Hey	01.12.2016
Approved (WPD):	Nigel Turvey	01.12.2016

Revision History

01/12/2016	V2.0	Rebrand and Update

Contents

DISCLAIMER

Neither WPD, nor any person acting on its behalf, makes any warranty, express or implied, with respect to the use of any information, method or process disclosed in this document or that such use may not infringe the rights of any third party or assumes any liabilities with respect to the use of, or for damage resulting in any way from the use of, any information, apparatus, method or process disclosed in the document.

Glossary

Abbreviation	Term
NGC	National Grid
WPD	Western Power Distribution
ICCP	Inter-Control Centre Communications Protocol
CPNI	Centre for the Protection of National Infrastructure

Executive Summary

The background to this project is relatively simple but the potential ramifications of what it set out to achieve are industry changing. Due to the increasing volume of distributed generation, it is becoming increasingly important for National Grid (NGC) to gain visibility of the real-time output of generation connections on distribution networks. This is currently not possible to achieve as there is no end to end visibility of the network to NGC.

The benefits of having that visibility could be potentially quite significant when it comes to operational efficiency and system balancing. Therefore in discussion with NGC it was decided that it was worth undertaking a feasibility study or proof of concept to establish with cross- network visibility could be achieved without increasing any security threat.

This project, in collaboration with GE, sought to create a link between the control systems of NGC and WPD, using the Inter-Control Centre Communications Protocol (ICCP). Establishment of the link has been successful with data being transferred between the systems in real time in a secure manner. An initial assessment of the cyber security risks has identified a potential risk with establishing multiple links through ICCP to NGC. Further assessment of these risks will be assessed and learning shared through the Centre for the Protection of National Infrastructure (CPNI).

Note: this report has been updated to reflect updated information, including reference to PowerOn instead of ENMAC. More information has been provided on the Idaho National Laboratory work mentioned within this report.

1 Project Background

At present there are areas of electrical network configuration and information that are of mutual interest to both NGC and WPD that can only be viewed from one operator’s SCADA System. Visibility of these areas of interest, especially the extent of running distributed generation, are becoming increasingly important to both companies and therefore it is proposed to create an environment where data from one system can be seen on the other and vice versa.

At present, whilst WPD has real time visibility of EHV and significant HV connected distributed generation, NGC does not. Such visibility could aid NGC operational timescale forecasting, with particular reference to generation scheduling / spinning reserve. The project did not attempt to initiate any form of control on the other’s network.

2 Scope and Objectives

The scope of the project was to establish a real time link between the SCADA systems operated by NGC and WPD using the ICCP protocol such that data on either system could be viewed on the other in real time. This was of course not an insubstantial challenge but we set the objectives deliberately to determine its viability and not to be an “operational” norm as it was agreed that the security risks needed to fully explored before any normalisation of this concept could be considered. This we believe to be a common sense approach to this idea.

The main project objectives were to:

- Establish the link between the two systems
- Establish access to the data and the necessary methods of viewing the data

- Establish the security measures required to ensure the security of the link to both of the systems against Cyber-attack for the purposes of the trial with follow on work to explore the full detailed threats to be detailed subsequent to this project

3 Success Criteria

The success criteria detailed below were identified at the point of project registration. These success criteria were used to determine the positive and negative learning throughout the project. This was relatively short project because it was a proof of concept and as such the success measures were confined to proving the viability of the idea not the operational control of networks on either side which would have been an entirely different project all together.

Success Criteria	Status
The ability of staff in both control environments to view data from the other system.	✓
An evaluation of the security of the environment against Cyber-attack.	✓

It is extremely encouraging that we were able to meet the stated objectives and we detail in this report what work was required and discuss a little more the issues that still remain in order to take this forward. It is worth stating that it needs to be taken forward with more information and assessment of the security risks before it could be considered a viable part of the network management process.

4 Details of the work carried out

4.1 Background

Western Power Distribution (WPD) has seen and continues to see a significant increase in the amount of generation connecting to the distribution network and this is across all voltage levels. This includes the development of large scale wind farms, photo-voltaic arrays, CHP and Biomass installations, a trend that is being replicated across the whole UK.

This is a shift from the traditional large-scale power stations connected directly to the National Grid. While these larger plants continue to underpin the majority of the UK’s energy needs, the generation connected to distribution networks is playing an increasingly important role. However this also creates a number of operational challenges associated with managing load flows and system balancing. Whereas in the past load would have flowed one way from National Grid down through the distribution networks, some parts of the system are now net exporters of power rather than consumers. This in itself is a significant change to the way that energy flows in the UK and one that as a key player, WPD feels it to be important to explore ways to better manage information flows.

National Grid undertakes a critical role in the provision of power by balancing the amount of electricity generation with the quantity of load being used. This affects a number of key network parameters such as system frequency. Any significant variations in frequency can cause load or generation to be lost through the operation of network protection systems. At present NGC has little or no real time visibility of the generation on distribution networks, and therefore only a partial view of the whole UK energy picture. This creates a potentially challenging situation because there is no current mechanism for flowing information back to NGC on the distribution network.

For both WPD and NGC, system operations are controlled using network management software produced by GE. While NGC utilise the XA/21 SCADA system, WPD operate PowerOn , a product that is used by the majority of network operators in the UK.

This project, in collaboration with GE, sought to create a link between these control systems using the Inter-Control Centre Communications Protocol (ICCP).

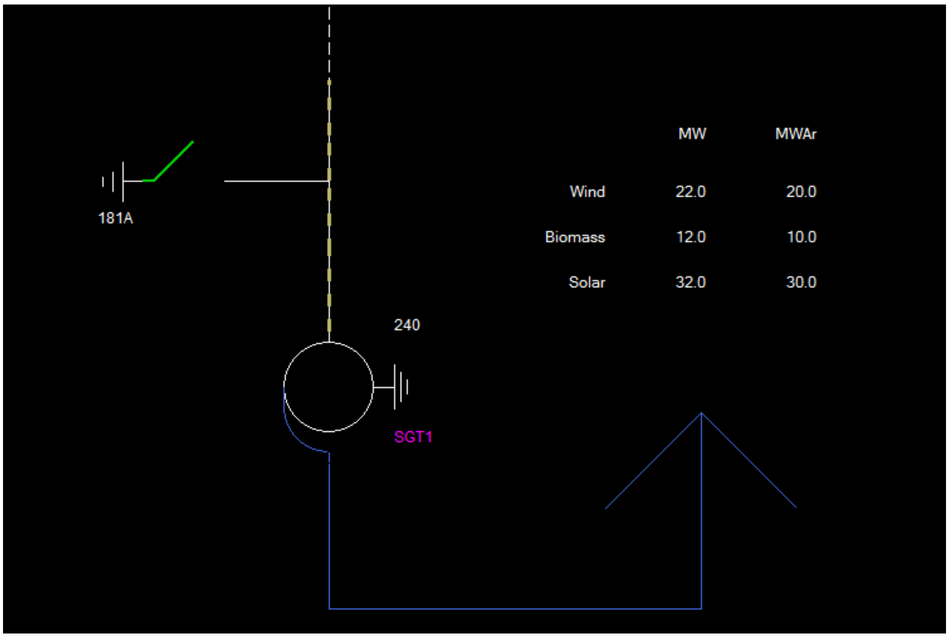
ICCP is part of the IEC 60870 suite of standards and has been developed to allow the real time data exchange between utilities. An ICCP link was applied within the project to allow data to be passed between the two control systems, allowing greater visibility of distributed generation for NG. Whilst this was a test in the truest sense of the word, i.e. the data seen at NGC was “data packets”, the intention of the project was to prove the concept not operational visibility of the network, this was done for security reasons with additional, parallel work done to investigate the level of threat.

4.2 Project Works

A number of key works were required to establish the ICCP link between the two organisations. Firstly a Virtual Private Network (VPN) had to be created between WPD and NG. This allowed a secure link to be established over the internet utilising standard best practices. This work included the configuration of firewalls to allow data to be passed between the organisations.

While ICCP is a standard function within later versions of PowerOn, configuration works are required to activate the protocol. This work was initially to be completed on the control systems for the South West and Wales. However, in the South West and South Wales use is made of predecessor SCADA software set to that used in the Midlands and it was decided that it would be better to use PowerOn for the project in a subtly different application. Additional IT infrastructure was commissioned as part of the scheme; including the installation of two ICCP servers by WPD that act as an interface between ICCP and the data transfer process. The first machine was designated the main server, with a secondary, replicated server being available for resilience purposes.

To enable the link to be trialled, a place holder for aggregated data was created by WPD in PowerOn that would act as a dummy data point. This would allow values to be manually input and then transferred over the ICCP link to be viewed by NGC.



	MW	MWAr
Wind	22.0	20.0
Biomass	12.0	10.0
Solar	32.0	30.0

Figure 1. Screenshot for PowerOn displaying aggregated dummy data sets

A trace function that would automatically scan the network and aggregate generation data was also developed and tested successfully, utilising the network connectivity to aggregate data. This functionality was though not applied to the live ICCP link.

Testing of the real time link was successfully completed as dummy data packets were input into PowerOn by WPD, transferred by ICCP and ultimately viewed by NGC within the XA/21 system.

5 The outcomes of the Project

This trial was a success, with data from the WPD PowerOn system being visible with the XA/21 control system at NGC. It is therefore envisaged that in the future that the link could be used to allow further real-time data to be collated and transferred, potentially from multiple sources from a DNO to TSO for data sharing purposes once security issues are fully determined.

For WPD to make this live, additional configuration would be required within PowerOn to transfer the aggregation and trace process from a test function to a live application. Additional configuration works would also be required to create the aggregation points, allowing the process to collate data prior to transfer through the ICCP link.

For NGC to take this forward with additional links, further configuration works would be required on a specific case by case basis. This would include the development of a separate Front End Processer (FEP) for each link to ensure security can be maintained.

At initiation of this trial, the ICCP link functionality was at TRL 7. As further work is required to assess the use of the link with multiple connections, it is considered that the TRL is unchanged. It is though extremely encouraging that we were able to make this concept work and we believe that it would be a useful piece of information in the continuing debate on DNO/DSO.

6 Performance compared to the original Project aims, objectives and success criteria

The registration proforma outlined the following core objectives for the project.

- Establish the link
- Establish access to the data and methods of viewing the data
- Establish the security measures required to ensure the security of the link to both of the systems against Cyber attack

The primary objective of the project was achieved through the successful establishment and testing of the ICCP link. This link was acting as a real-time data connection, although the data itself was static for the purposes of the testing. Facilities were developed to gather data from the network in real time using a dynamic trace function. It was deemed to be outside of the core scope of the project to implement this functionality, but would form a core component of any wider deployment.

Another key objective was to develop the ability of staff in both control environments to view data from the other system. This has been met in through the establishment of a link that allows data to be passed through between control systems. Further work would be required to automate this process and allow real data rather than dummy data packets to be passed.

From a security perspective, this project utilised a Virtual Private Network (VPN) and the secure form of ICCP. Both are regarded as best practice for this kind of activity and should be run in conjunction with additional security software to monitor and prevent breaches. More information can be provided on this on request.

At the time of the project work was completed by Idaho National Laboratories (INL) for WPD as part of our Annual Security Audit to evaluate some aspects of the security of an ICCP link. It was intended that the link tested would be the one available between WPD and NGC but, because of concerns, expressed by NGC, the link was established between the WPD servers.

The findings have yet to be reported formally, but in essence there are vulnerabilities in ICCP that give cause for concern. A number of issues have been identified in ICCP that could be exploited and it is intended that INL will return to WPD in 2014 to take a further look at this, and other security issues. Any further information will be reported through the relevant channels for sharing with appropriate stakeholders.

Anecdotal evidence is available from INL which indicates that if two DNOs were connected to NGC it would be possible to hack into one of the DNOs and make changes to data in the other by utilising the ICCP link.

Due to the critical nature that future ICCP links could play, it is not intended to share the reports in the public domain. Instead any further learning on security from INL has been shared with the Centre for Protection for National Infrastructure (CPNI). This will then act as a focal point for DNOs and NGC as part of the knowledge dissemination process. It was anticipated that the initial reports will be available in late 2013, with further output in 2014 and these would be shared where appropriate with the CPNI.

7 Required modifications to the planned approach during the course of the Project

The main variance from the initial plan was to establish the trial against the POWERON system based in the Midlands networks areas, rather than South West and Wales.

From a timescale perspective, this project has taken longer to complete then initially envisaged. This was primarily down to ensuring the data routing and policies within NGC were suitable for this application. Now that works have been complete, it should enable any future ICCP links of this type to be applied more easily.

8 Significant variance in expected costs and benefits

The project has been delivered on budget with all objectives met. The direct benefits of the project were limited to essentially proving the ICCP link with no immediate financial benefits. However, the further implications of the trial could go much wider with the application of further DNO / NGC links. Currently 13 out of the 14 DNO licence areas are utilising GE software to manage the control systems, although some of these systems would require upgrading to the current version of PowerOn to allow ICCP to be enabled. This would deliver an increased benefit to NGC in terms of visibility of the end to end electricity system and deliver reduced system risk to the UK as a whole.

The following table outlines the costs incurred through the project. The majority of the scheme was delivered through GE as a service and reflected in the cost breakdown below.

Description	Cost
Equipment: Servers HP, Hardware Support	£3,574.77
ENMAC software: ICCP SCADA Interface	£50,000.00
3rd party software	£4,392.91
Services (T&L costs included)	£21,225.17
Future Networks Team Project Management	£789.60
Total	**£79,982.45**
Total to be claimed through LCNF	£71,984.21
DNO Contribution	£7,998.25

9 Lessons learnt for future Projects

There were considerable challenges in establishing the firewall link between the organisations. This was partially due to the methods chosen to deliver the data routing within NGC and the unfamiliarity of the way ICCP connections initiated. Standardising the ICCP addressing structure and putting in place tools to decode the exchanged messages allowed these to eventually be overcome. Well documented procedures and upgraded data policies should mitigate this risk in future connections.

There are several other features available in the ICCP protocol that could also be used with minor software enchantments for example

a. Transferring the electrical model (or relevant parts of it) between systems could be used to increase accuracy of sub systems like the state estimator.
b. The transfer of switching schedules between systems

This report is intended to form the core of the knowledge dissemination process, with additional security assessment to be shared with the industry through CPNI. In addition both GE and NGC have had a central role to play in establishing the link and will be critical to any further deployment of future ICCP links with other DNOs. This will also form a route for future knowledge sharing.

10 Planned implementation

PowerOn is currently utilised in 13 of the 14 DNO licence areas. Any wider application would require upgrading the version of PowerOn control systems by some companies to enable ICCP and application of the generation trace functionality. This will be a decision potentially determined by Ofgem and supported by NGC as the operational need for embedded generation real time data increases. Individual DNOs would also need to assess the operational risks associated with upgrading PowerOn, based on the guidance from NGC and their own business cases.

From a cyber-security perspective, an initial assessment was made of an individual link. However, additional studies should be made as to the security implications of multiple DNO / NGC links to ensure there is no increased risk to the varying control system infrastructures. This will also need to include the establishment of multiple Front End Processors within NGC to ensure that security is maintained. If the inherent vulnerabilities with ICCP cannot be resolved, WPD would not allow an interconnection of this type to NGC if other DNOs made the same connection.

To develop further learning from this project, WPD will engage in additional security testing in conjunction with INL as a business as usual activity as part of our Annual Security Assessment. Particular attention is to be given to exploring the risks associated with multiple DNO connections to NGC. Output from these reports will be shared with the industry through CPNI as and when they become available

At present there are no plans to with NGC to deploy ICCP links in the short term and in updating this report we believe this still to be the case. We will continue a dialogue with NGC as to the role the link could play in the future as part of the on-going review of DNO/NGC data sharing processes.

11 Facilitate Replication

The core of the products and services required to establish an ICCP link were all supplied through GE as part of the latest releases of their PowerOn and XA/21 SCADA systems.

The additional IT infrastructure required for this scheme can be obtained from a wide number of sources. More information can be provided on request.

GE has acted as the hub for this project, and would support any further applications of this solution.

12 Contact Details

Future Networks Team
Western Power Distribution
Pegasus Business Park
East Midlands Airport
Castle Donington
Derbyshire
DE74 2TU
e-mail: wpdinnovation@westernpower.co.uk
website: www.westernpowerinnovation.co.uk

Appendices

LCN Fund Registration Pro-forma

WPDT1001 - Tier 1
Proforma - WPD NGC