

Distributed ReStart

Lot 2 – Design Phase

Final Report

Author: Conan Malone, Sean Norris, Roger Jefferiss, Douglas Wilson, Andreas Glatz, Tony Nutley

Reference: GE-D_RESTART-DRZC_CYBER_DESIGN

Version: 1

Date: 17/12/2021



© GE Digital 2021. All rights reserved. Information contained in this document is indicative only. No representation or warranty is given or should be relied on that it is complete or correct or will apply to any particular project. This will depend on the technical and commercial circumstances. It is provided without liability and is subject to change without notice. Reproduction, use or disclosure to third parties, without express written authority is strictly prohibited.

Contents

1	Introduction.....	13
1.1	Scope and Deliverables.....	13
1.2	Limitations	14
1.3	Standards and Frameworks.....	14
2	Communications Design.....	16
2.1	Bandwidth Considerations for Design.....	22
3	Network Design.....	23
3.1	Security Controls.....	26
4	Data Flows Design.....	30
4.1	Synchrophasor Data.....	30
4.1.1	C37.118	30
4.1.2	IEC 61850-90-5 R-SV	34
4.2	Control Scheme Data	39
4.2.1	IEC 60870-5-104	39
4.2.2	DNP3.0.....	44
4.2.3	IEC 61850-90-5 R-GOOSE.....	49
4.3	Admin/Management	54
5	Desktop Study – Penetration Techniques for Designs	59
5.1	Network Attacks.....	59
5.2	Protocols Attacks	59
6	Design Strategies for Cyber Security.....	60
6.1	Comms Strategies.....	60
6.2	Network Strategies.....	61
6.3	Protocol Strategies	62
7	Change Impact Analysis.....	64
7.1	Electricity System Operator	64
7.1.1	Interfaces.....	64
7.1.2	Systems.....	65
7.1.3	Telecommunications	65
7.1.4	Training.....	65
7.1.5	Staff	66
7.1.6	External Factors	66
7.1.7	Security	67

7.2	Transmission Operator	67
7.2.1	Interfaces.....	67
7.2.2	Systems.....	67
7.2.3	Telecommunications	68
7.2.4	Training.....	69
7.2.5	Staff	70
7.2.6	External Factors	70
7.2.7	Security	70
7.3	Distribution Network Operator	72
7.3.1	Interfaces.....	72
7.3.2	Systems.....	73
7.3.3	Telecommunications	76
7.3.4	Training.....	77
7.3.5	Staff	79
7.3.6	External Factors	80
7.3.7	Security	80
7.4	Distributed Energy Resource.....	84
7.4.1	Interfaces.....	84
7.4.2	Systems.....	84
7.4.3	Telecommunications	86
7.4.4	Training.....	86
7.4.5	Staff	87
7.4.6	External Factors	87
7.4.7	Security	88
8	Future Operating Service Models	91
8.1	Vulnerability Management.....	91
8.2	Patch Management	91
8.2.1	Secure Patch Retrieval.....	92
8.2.2	Patch Frequency	93
8.3	Software Lifecycles	96
8.3.1	Operating Systems	96
8.3.2	Products.....	98
8.4	Hardware Lifecycles	98
8.4.1	Controllers.....	98
8.4.2	Servers	99

8.4.3	Network Devices	99
8.4.4	PMUs/RTUs	99
8.5	Changes in Cyber Security	100
8.6	Transition to IEC 61850	100
9	Appendices.....	102
9.1	Bandwidth calculations using IEC 104 for fast balancing.....	102
9.2	Bandwidth calculation using R-GOOSE for fast balancing	107

Figures

Figure 1 Example communications for ESO, TO, DNO and DERs with single communications	17
Figure 2 Power resilient communications requirements	18
Figure 3 Power resilient communications requirements w/ dual DNO WANs.....	19
Figure 4 Low latency communications for BlackStart.....	21
Figure 5 Higher latency communications for BlackStart.....	22
Figure 6 Example DNO central control network architecture	24
Figure 7 Example central DRZ controller and anchor generator site	25
Figure 8 Example of fast and slow balancing sites where multiple are available per zone	25
Figure 9 Example of fast and slow balancing sites where only one fast balancing site is available in the zone.....	26
Figure 10 IP whitelisting	27
Figure 11 Sandbox testing environment.....	27
Figure 12 Network isolation.....	28
Figure 13 Mutual TLS.....	29
Figure 14 Synchrophasor data flows using IEEE C37.118	31
Figure 15 Synchrophasor data flows using IEC 61850-90-5 R-SV and IEEE C37.118	35
Figure 16 Control data flows using IEC 60870-5-104.....	40
Figure 17 Control data flows for DNP3	45
Figure 18 Control data flows using IEC 61850-90-5 and IEC 60870-5-104/DNP3	50
Figure 19 Admin and management data flows.....	55
Figure 20 Bridged PKI infrastructure.....	56
Figure 21 Bridged PKI infrastructure with independent KDC infrastructure	57
Figure 22 Data flows for CA or KDC	58

Tables

Table 1 TO data flows for IEEE C37.118	32
Table 2 TO to DNO data flows for IEEE C37.118	32
Table 3 DNO data flows for IEEE C37.118	33
Table 4 DER data flows for IEEE C37.118	34
Table 5 TO data flows for IEC 61850-90-5 R-SV	36
Table 6 TO to DNO data flows for IEC 61850-90-5 R-SV	37
Table 7 DNO data flows for IEC 61850-90-5 R-SV	38
Table 8 DER data flows for IEC 61850-90-5 R-SV	38
Table 9 ESO to TO data flows for IEC 60870-5-104	41
Table 10 DNO data flows for IEC 60870-5-104	42
Table 11 DER data flows for IEC 60870-5-104	43
Table 12 ESO to TO data flows for DNP3	46
Table 13 DNO data flows for DNP3	47
Table 14 DER data flows for DNP3	48
Table 15 ESO to TO data flows for IEC 61850-90-5 R-GOOSE	51
Table 16 DNO data flows for IEC 61850-90-5 R-GOOSE	52
Table 17 DER data flows for IEC 61850-90-5 R-GOOSE	53
Table 18 ESO change impact analysis to interfaces	64
Table 19 ESO change impact analysis to systems	65
Table 20 ESO change impact analysis to telecommunications	65
Table 21 ESO change impact analysis to training	66
Table 22 ESO change impact analysis to staff	66
Table 23 ESO change impact analysis to external factors	66
Table 24 ESO change impact analysis to security	67
Table 25 TO change impact analysis to interfaces	67
Table 26 TO change impact analysis to systems	68
Table 27 TO change impact analysis to telecommunications	68
Table 28 TO change impact analysis to training	70
Table 29 TO change impact analysis to staff	70
Table 30 TO change impact analysis to external factors	70
Table 31 TO change impact analysis to security	72
Table 32 DNO change impact analysis to interfaces	73
Table 33 DNO change impact analysis to systems	76
Table 34 DNO change impact analysis to telecommunications	77
Table 35 DNO change impact analysis to training	79
Table 36 DNO change impact analysis to staff	80
Table 37 DNO change impact analysis to external factors	80
Table 38 DNO change impact analysis to security	84
Table 39 DER change impact analysis to interfaces	84
Table 40 DER change impact analysis to systems	85
Table 41 DER change impact analysis to telecommunications	86
Table 42 DER change impact analysis to training	87
Table 43 DER change impact analysis to staff	87
Table 44 DER change impact analysis to external factors	87

Table 45 DER change impact analysis to security..... 90

Glossary

Acronym	Description
AD	Active Directory
ADMS	Advanced Distribution Management System
BESS	Battery Energy Storage System
CA	Certificate Authority
CAF	Cyber Assessment Framework
CDMA	Code Division Multiple Access
CIS	Centre for Internet Security
CPU	Central Processing Unit
DER	Distributed Energy Resource
DMS	Distribution Management System
DMZ	De-Militarized Zone
DNO	Distribution Network Operator
DNP3	Distributed Network Protocol 3
DO/DSO	Distribution Operator/Distribution System Operator
DRZC	Distributed Restoration Zone Controller
EAD	Ethernet Access Direct
EMS	Energy Management System
ENA	Energy Networks Association
ESO	Electricity System Operator
FEP	Front End Processor
FPS	Frames Per Second
GPG	GNU Privacy Guard
GPS	Global Positioning Satellite
GSM	Global System for Mobile communications
GSP	Grid Supply Point
HTTPS	Hypertext Transfer Protocol Secure
HMAC	Hash-based Message Authentication Code
IACS	Industrial Automation and Control Systems
ICCP	Inter-Control Centre Communications Protocol

ICS	Industrial Control Systems
ICV	Integrity Check Value
IDS/IPS	Intrusion Detection System/Intrusion Prevention System
IED	Intelligent Electronic Device
IEMS	Integrated Energy Management System
IP	Internet Protocol
KDC	Key Distribution Centre
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
MFA	Multi-Factor Authentication
MIT	Main Interconnected Transmission System
MMS	Manufactured Message Specification
MPLS	Multi-Protocol Label Switching
NCSC	National Cyber Security Centre
NGESO	National Grid Electricity System Operator
NGET	National Grid Electricity Transmission
NTP	Network Time Protocol
OPCDA	Open Platform Communications Data Access
OS	Operating System
OT/IT	Operational Technology/Information Technology
PBC	Primary Balancing Control
P-class	Protection Class
PDC	Phasor Data Concentrator
PDH	Plesiochronous Digital Hierarchy
PLC	Programmable Logic Controller
PMU	Phasor Measurement Unit
PR	Proportional Regulation
PSTN	Public Switched Telephone Network
PTP	Precision Time Protocol
QoS	Quality of Service
RAM	Random Access Memory

R-GOOSE	Routable Generic Object Orientated Substation Events
RoCoF	Rate of Change of Frequency
RT	Real Time
SAT	Site Acceptance Testing
SBC	Secondary Balancing Control
SCADA	Supervisory Control and Data Acquisition
SDH	Synchronous Digital Hierarchy
SDLC	Software Development Life Cycle
SHA	Secure Hash Algorithm
SIEM	Security Information and Event Management
SiL	Software in the Loop
SLA	Services Level Agreement
SOAR	Security Orchestration, Automation and Response
SPEN	Scottish Power Energy Networks
SPR	Scottish Power Renewables
SS	Substation
SSH	Secure Shell Protocol
SSO	Single Sign On
ST	Structured Text
STM	Synchronous Transport Module
SW	Software
T&M	Time and Materials
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TLV	Type-Length-Value
TO/TSO	Transmission Owner/Transmission System Operator
UDP	User Datagram Protocol
UFLS	Under Frequency Load Shedding
UI	User Interface
UPS	Uninterruptible Power Supply
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network

VPP	Virtual Power Plant
VSAT	Very Small Aperture Terminal
VT	Voltage Transformer
WAMS	Wide Area Management System
WAN	Wide Area Network
WF	Wind Farm
WPD	Western Power Distribution

1 Introduction

The purpose of the Distribution Restoration Zone (DRZ) is to enable distribution resources to participate in the BlackStart and restoration plan for the GB power system. Conventional BlackStart services have traditionally assumed a top-down approach to start large generators, energise the high voltage transmission network, and finally pick up the distribution system. Since the conventional capability for BlackStart is becoming scarce due to the energy transition, the Distributed ReStart project explores a bottom-up approach using smaller distributed generation in controlled zones. The distribution island is started, and grown to energise the zone and reconnect customers, and provides a resource for wider grid energisation.

The purpose of this development is to implement a Distribution Restoration Zone Controller (DRZC) and associated control logic and infrastructure and to trial the process in a Hardware-in-the-Loop (HiL) environment. The control scheme provides the automation and control to manage the network and the power balancing resources with the aim of creating a live power island, bringing customers back online and providing a resource either to energise further into other areas of the transmission or distribution networks, or to sustain supply to customers until it can be resynchronised with the transmission system.

This document specifies the detailed designs for a Distributed ReStart solution with regards to the communications, networks and data. For communications, the required physical connections between ESO, TOs, DNOs and DERs is highlighted with an emphasis on the different availability metrics for different designs. The minimum requirements for communications derived from the requirements report is highlighted, with connections that require high or low latency, or connections that must be power resilient to deliver a successful BlackStart.

Network designs are given in high-level format with examples of the different systems existing on different networks and the security controls in place. Network architecture depicting the DNOs hosting the DRZC and DER sites hosting the field controllers are given, with the interconnections between the different networks shown. *Please note – network architectures will vary from organisation to organisation, each with their own cyber security requirements and processes. These network diagrams are given as high-level examples.*

Finally, the designs of data for control, monitoring and management are highlighted to demonstrate the flow of traffic within the organisation and between organisations. Different protocols and interfaces are shown to accommodate the different party's current infrastructure and to allow for future expansion. Information on how each data flow is secured is also given.

A change impact analysis for the designs is outlined in the later sections, with regards to the different parties and the new processes, procedures and technologies the Distributed ReStart system brings to each. Finally, future operating models for the Distributed ReStart system are discussed with a focus on system lifecycles and patch management.

1.1 Scope and Deliverables

The following networks are in scope for this report:

- National Grid OpTel Network

- SPEN Operational Network (Transmission and Distribution)
- DNO Operational Networks (SPEN and WPD)
- DER sites (Ewe Hill WF and Glenlee Hydro)

And the following systems are in scope for this report:

- General Electric (GE) IEMS XA21 V17
- National Grid Operational Telecommunications Network/SCADA
- SPEN Operational Telecommunications Network/SCADA
- General Electric (GE) E-terra
- General Electric (GE) PowerOn Advantage
- General Electric (GE) WAMS PhasorPoint/PhasorProcessor
- General Electric (GE) WAMPAC PhasorController

1.2 Limitations

The following limitations are in place for this scope of work:

- Supplier is not expected to survey all existing assets of Partners. Partners are responsible for supplying most asset information.
- Supplier is not expected to be granted access to live systems or data unless there is a risk assessed and supervised (and need-to-know) basis that inhibits any task.
- Supplier may not be granted access to select sensitive documents for security reasons. Instead, redacted documentation, overview of documentation or interview techniques are used to gain the necessary information for complete analysis.

1.3 Standards and Frameworks

Standard	Description	Component
IEEE C37.118	Synchrophasor	PMU, WAMS
IEC-61131	PLC	PLC in DRZC
IEC 60870-5-104	Master/slave commanding protocol	DRZC, ADMS
IEC 60870-6 ICCP	Supervisory control and data acquisition	ADMS, EMS
IEC-61850	Substation communication language	DRZC
IEC 62351	Security for Control protocols	Cybersecurity, IEC 61850
IEC 62443	Secure development	Cybersecurity, All
NIST 800-53	Security and Privacy controls for Info Systems and Organisations	Cybersecurity, All

NCSC CAF	Security for Critical National Infrastructures	Cybersecurity, All
ISO 27001	Best practice for information security management systems	Cybersecurity, All
CIS Benchmarks	Best practice for secure configuration	Cybersecurity, secure configuration
Cyber Essentials Scheme	Government backed scheme for protecting organisations against common cyber threats.	Cybersecurity, supply chain

2 Communications Design

The following section discusses the communications design for Distributed ReStart, with a focus on power resiliency and latency requirements derived from the final cyber security requirements report delivered as part of the OST workstream. The proposal for the communications is to utilise the current ICCP links between DNOs and ESO for visualisation of the distribution network and extend the DNO networks to the DER sites to exchange control and measurement data required by the DRZC.

Figure 1 shows the communications design for a sample BlackStart architecture. From previous analysis, it is noted that the following participants are required for a successful BlackStart using the DRZC scheme:

- ADMS – this is likely located in a DNO’s central control centre (and typically replicated between secondary/backup control centres).
- Central DRZ controller – this is likely located in the DNOs main grid substation; however, it may also be located in different locations in the DNOs network.
- Proportional Regulation sites – Anchor generators and other generators with frequency droop control.
- Primary Balancing Control sites – Load banks or BESS with fast power setpoint control. Requires fast response times over physical communications.
- Secondary Balancing Control sites – Constrained generation with slow dispatch control (e.g. wind farms) or sheddable loads used as last resort control action to preserve the anchor generator. Does not require fast response times over physical communications.

Hence there is a requirement to have physical communications channels between the DRZC and PR, PBC and SBC sites for data exchange. Comms also must extend from DRZC to ADMS. From previous analysis, the physical comms between the DNOs network and different DER sites are currently very limited (or non-existent). DNO networks will need to extend to at least 1 PR, PBC and SBC site for BlackStart, however it is recommended that multiple sites per zone are included in the network.

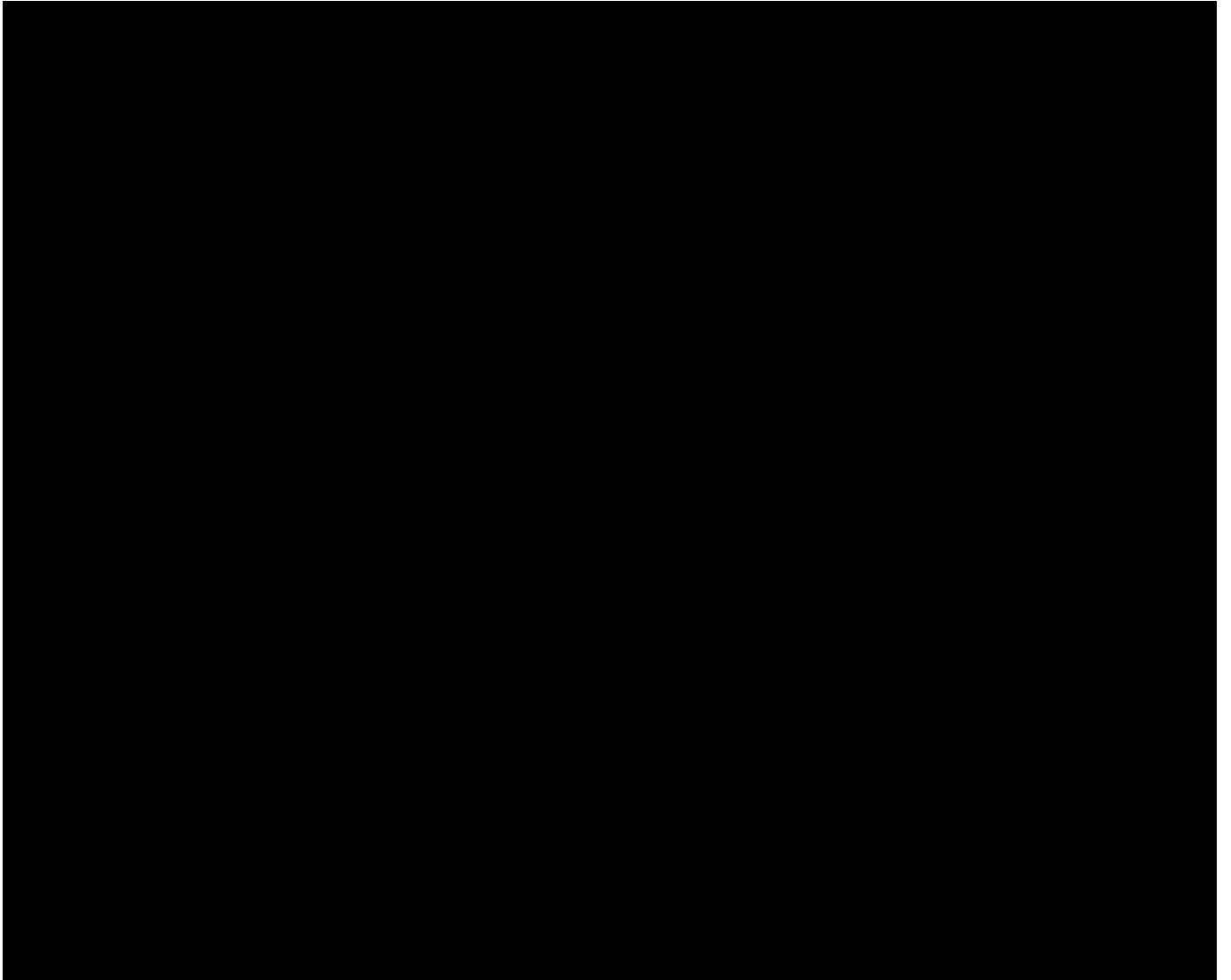


Figure 2 expands the communications design further and highlights the elements where power resilient communication channels are required for BlackStart (**shown in Grey**). According to Ref. DRZC-RN-1 (*Distributed ReStart Lot 2 – Requirements Phase Final Report*) the following links must have power resilient communications to successfully complete a BlackStart using the DRZC model.

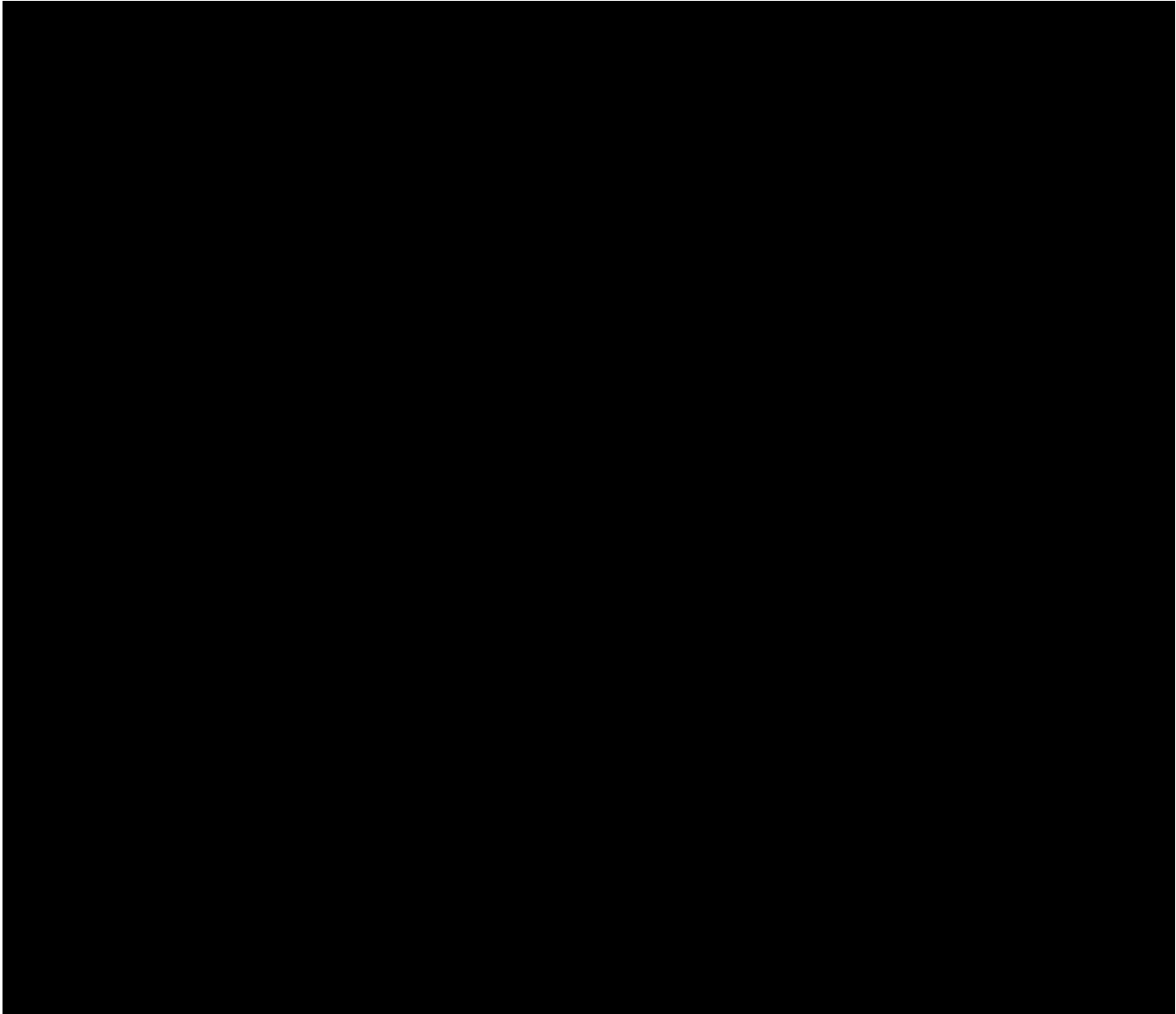
DNO must ensure power resilient comms:

- Between ADMS and central DRZC.
- DRZC to all sites designated Primary Balancing Control (PBC), i.e. batteries and load banks for fast response*
- DRZC to all sites designated Proportional Regulation, i.e. anchor generator and other frequency proportional sites**
- ADMS and the Grid Supply Point(s) feeding primary substation loads to be picked up.

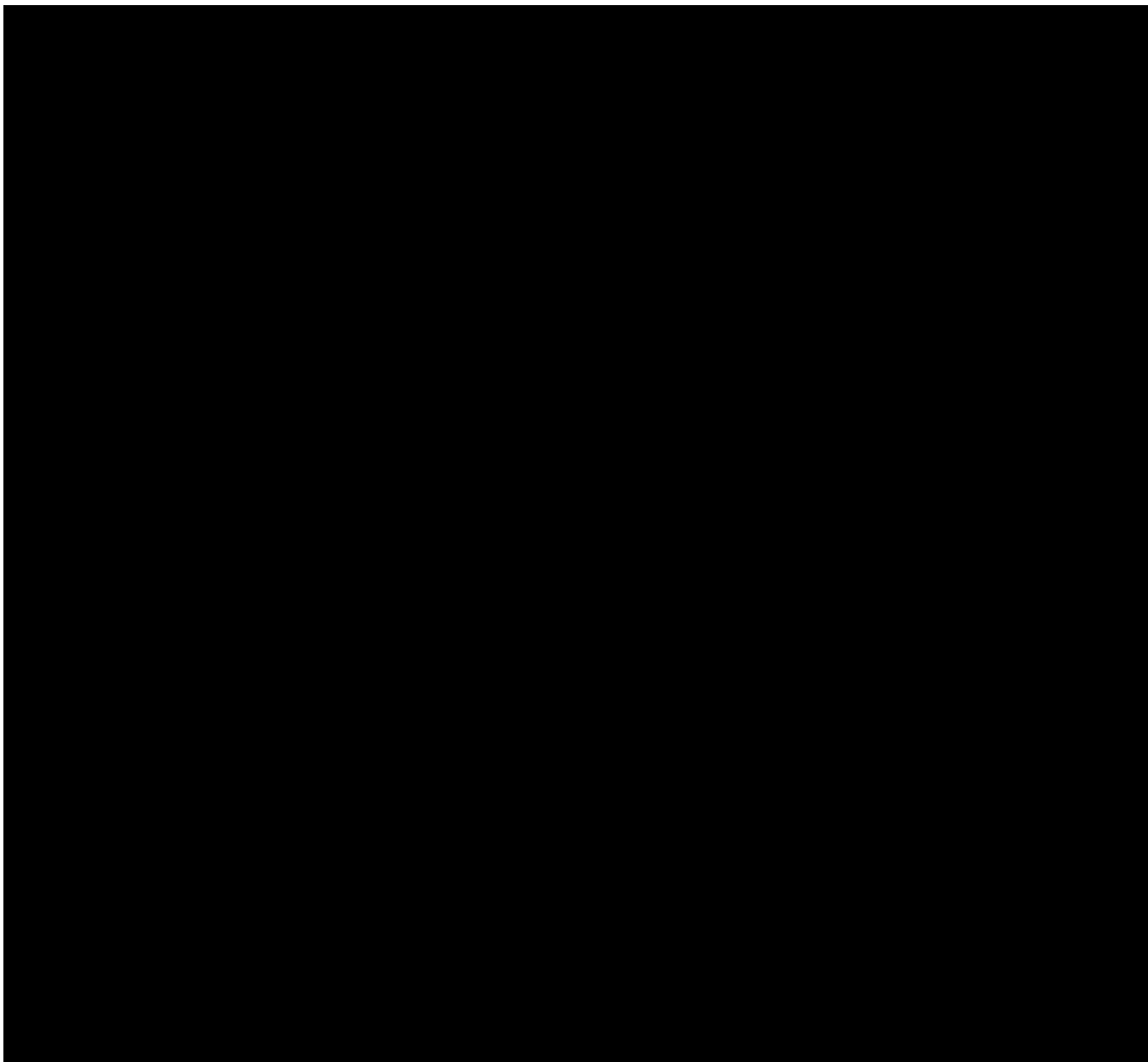
** the requirement is for the DRZC model is 1 PBC site available to perform a BlackStart, however, to increase resiliency, multiple PBC sites should have power resilient comms between site and*

DRZC. In some cases, the DRZC may be co-located with a fast-balancing resource (e.g. load bank), so power resiliency is only required for the local DRZC connection to the resource.

*** as above, the DRZC may be co-located on the anchor generator site. However, it is unlikely there are more than 1 anchor generator per zone.*



During the Failure Modes and Effects Analysis (FMEA), it was discovered that a single comms architecture; where the comms between DNO control centre, central DRZC and the minimum required edge substations (anchor generator, PBC and SBC site) utilise a single WAN connection, provides an availability rating of 0.99992999 (or 4-nines). In contrast, figure 3 depicts the communications designs utilising a dual WAN connection between the key sites for DRZC BlackStart. From the FMEA, the availability rating for the dual WAN architecture is 0.9999999307 (or 7-nines).



The limiting factor in the design may be the power system. Availability statistics on the power system are not currently known, so cannot be compared to the availability statistics of the telecoms. If the power system provides availability less than that of the telecoms, the requirement for dual WANs to provide increased availability decreases the effectiveness to that of the single WAN, however it may still be worthwhile to account for unexpected disasters.

The requirement for end-to-end latencies is dependent on the type of resource required for the function of the BlackStart sequence. For the anchor generator, where the key inertia provision is sited, the latency should be around 100ms with a maximum latency no more than 200ms. It should be noted that the anchor generator may exist as a generator only site, or a generator and fast balancing (PBC) resource site. The key difference between the two is that if the site is also a PBC, it will receive control signals from the DRZC. If it is an anchor generator only, it will be providing PMU measurements to the DRZC only. However, these are critical measurements and

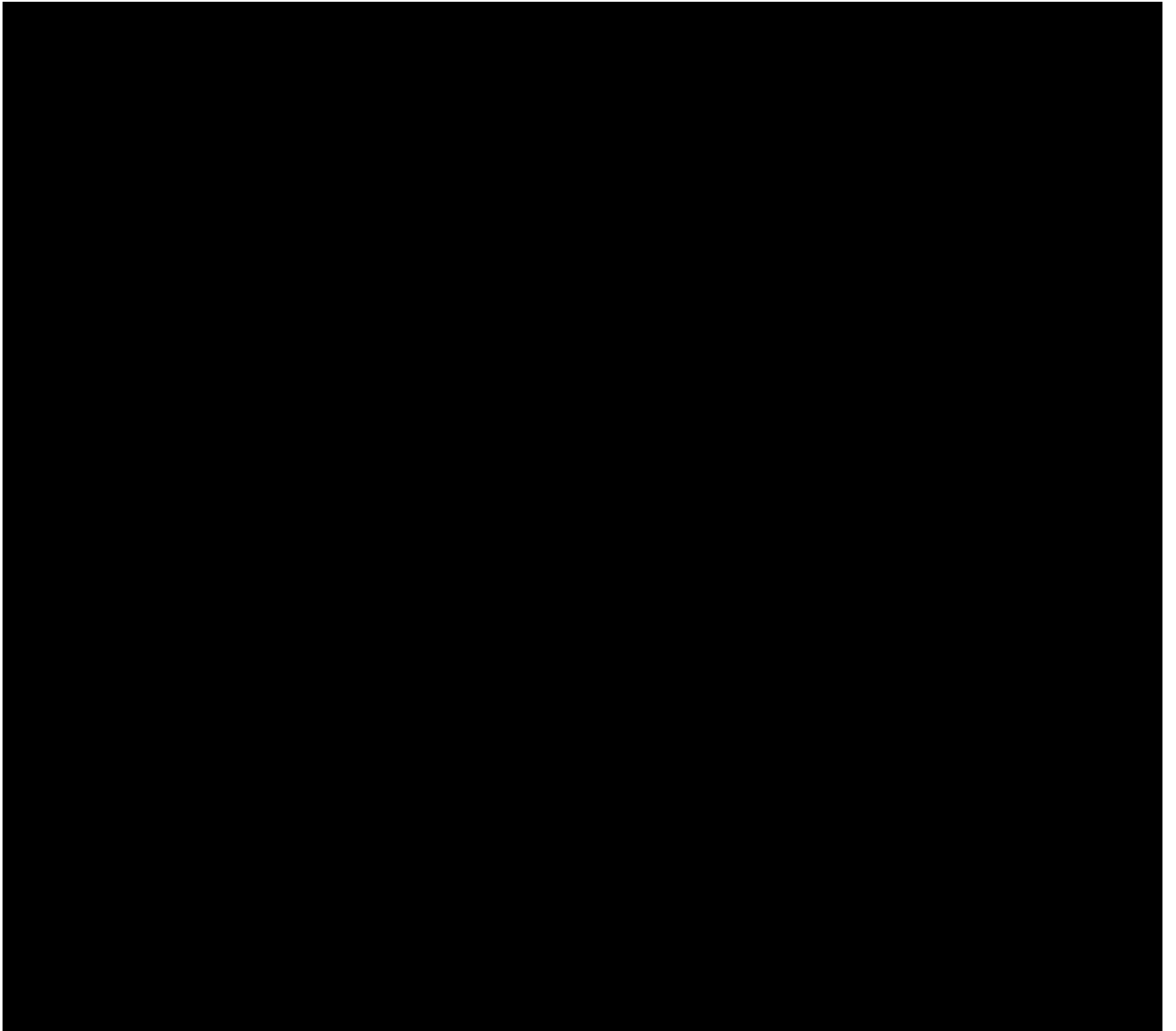
therefore the same requirement on latency is there, as latency in these measurements affects the total round trip time of response. Therefore, anchor generator sites regardless of it being PBC or not should target 100ms response. (Note that measurement latency includes latencies within the PMU of 40ms for a P-class PMU which means that for 100ms latencies on measurements, the communications latency must be no more than 60ms.)

This is a similar case for the PBC sites, where the fast-balancing resources are located and may be independent of the anchor generator sites. These would include battery resources, load banks for example. The latencies down to these sites from the DRZC for the receipt of control signals should again target 100ms and should not exceed 200ms. Therefore, the communications links between DRZC and anchor generator, DRZC and PBC sites and anchor generator and PBC sites should not exceed 200ms*

** in many cases, an anchor generator will contain an PBC (e.g. battery or load bank) on site, so there need not be a fast comms link between anchor generator and PBC sites. Further, in the event where the DRZC controller is situated at an anchor generator site, which also contains a PBC resource, there is no requirement for a fast (<200ms) data link over the WAN.*

Figure 4 highlights the communications paths extended from DNO to DER sites that require low latencies to account for the fast response times to/from the DRZC (**shown in Red**). Analysis during the requirements phase showed that fibre optic lines, microwave links, 5G and (in ideal circumstances) 4G. Technologies such as VSAT or 3G do not provide sufficient speeds for this medium.

For SBC sites, there is less need for low latency comms as these resources do not need to respond fast to the DRZC, instead they bring slow dispatch loads into the DRZC power island. The maximum latency for these comms should not exceed 2s (where possible a maximum of 1s is preferred). As above, the same technologies are sufficient for extending the DNO network to the SBC sites (fibre, microwave, 5G/4G) along with the slower technologies (VSAT, 3G). Figure 5 demonstrates the requirement for communications with SBC sites (**shown in Green**).



As the ESO-DNO link is solely for visualisation in this BlackStart architecture design, there is no specified requirement for latency over the comms. However, from previous analysis, it is known that the ICCP link has sufficient latency statistics for control.

2.1 Bandwidth Considerations for Design

As the communications design focused mainly on power resiliency and latencies, it is also critical for the individual participants to understand the bandwidth requirements over the different communications paths. As these are very granular and vary depending on the protocol selection, a detailed table is provided in Appendix 6.1 and 6.2 with the necessary information.

3 Network Design

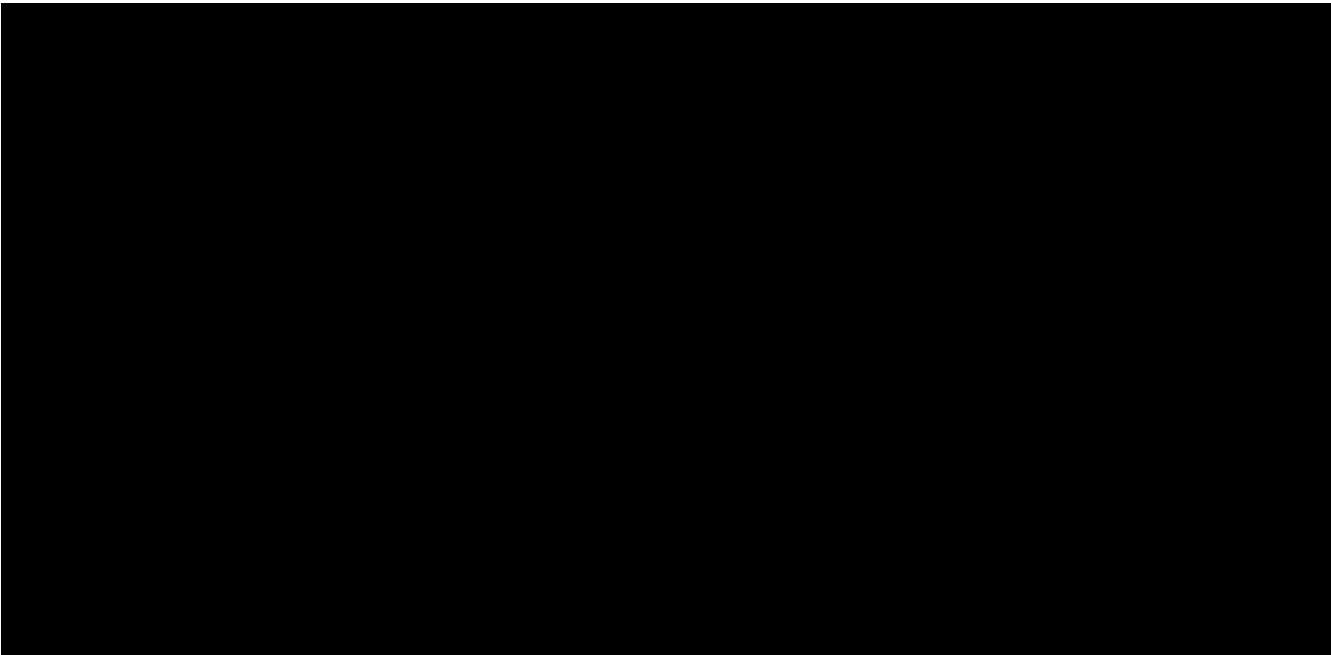
The next section depicts the network design architecture for the multi-party environments and security for Distributed ReStart. The designs are high-level and should be used as a guidance for the distribution network operators when implementing the new systems that are required on the networks to achieve an automated BlackStart using the DRZC. It is highly likely that the network designs vary between the DNOs and that the designs depicted may never truly represent the exact nature of the organisations own internal networks. Network diagrams should be carefully designed on each use case when implementing this architecture, and should include the organisation's network architects, OT network and security teams and IT network and security teams.

Figure 6 highlights an example network architecture, with security controls implemented to protect the network from common vulnerabilities and attacks.

The network should adopt a back-to-back firewall approach to separate the SCADA domain from the corporate domain. A Demilitarised Zone (DMZ) also adds an additional layer of security between the domains. In the following example, multiple example machines are placed in the DMZ which provide a degree of separation between IT and OT networks.

Jump servers may be utilised to access the controllers, ADMS and/or WAMS systems – these jump servers can implement strong authentication (MFA) and access control lists to further protect access to the critical BlackStart systems. Anti-virus/malware is updated with latest checks via corporate and scans the SCADA network to protect the trusted network from untrusted malicious code or viruses.

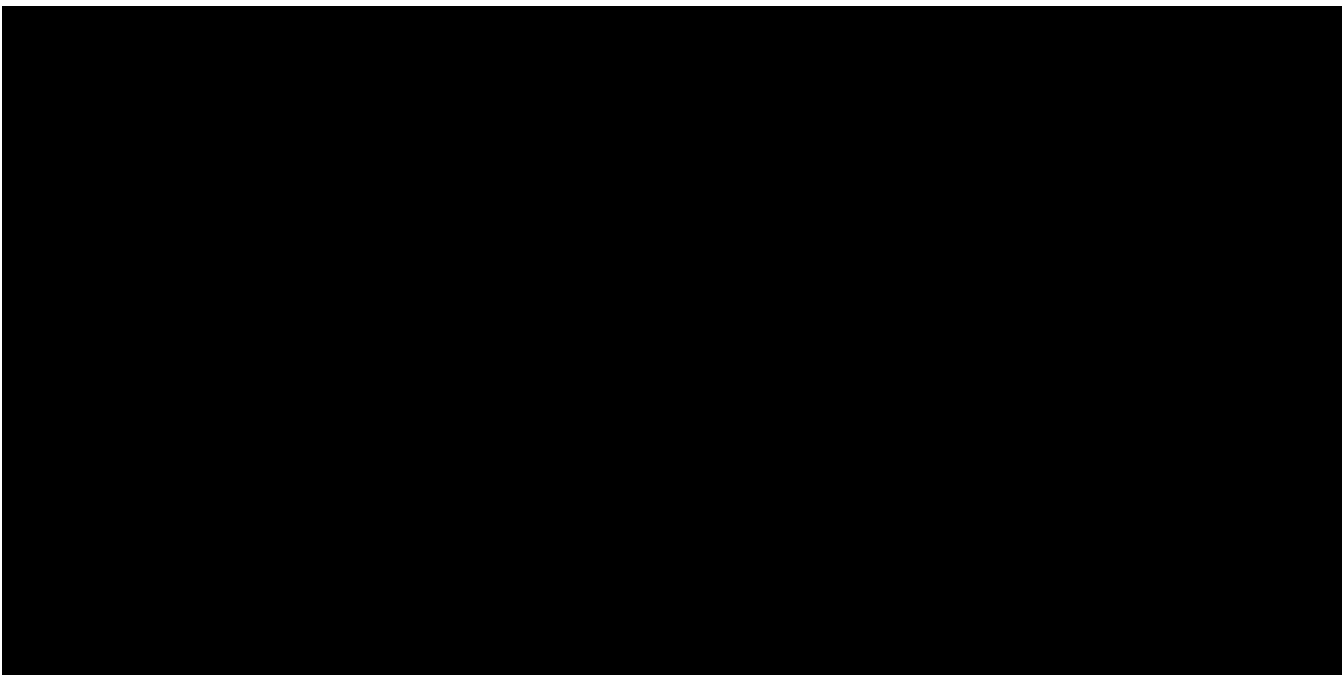
Protocol converters should be installed adjacent to each FEP within the SCADA networks, if multiple FEP servers are in use (for replication over the ADMS cluster), then a protocol converter (i.e. Field Interface Unit) at each FEP is required. There is no need for HA protocol converters at each FEP as the ADMS will typically be clustered over multiple locations/networks. Protocol converters may also be placed in a DMZ.



From the DNO central control centre (or backups), mainly any location containing a FEP/ADMS/Protocol converter – there is the requirement for these systems to exchange data with the central DRZ controller (along with the protection devices owned by the DNO). In figure 6, the network extends into the DNO WAN, where the physical comms are routed into the DNO substations which host the central DRZ controller (see Figure 1).

Figure 7 demonstrates the network connectivity between the central DRZC and proportional regulation (anchor generator) site. Back-to-back firewalls are installed between sites with physical communications extended from DNO to DER. Central DRZC is not a distributed site therefore requires redundancy of systems contained within the local area network. Redundant controllers are deployed with dual network interface cards on redundant comms, the use of dual switches with rapid spanning tree protocol or parallel redundancy protocol capabilities ensures redundant paths and interconnection between LAN and WAN. Where IEC 61850-90-5 is used, the network routers must support multicast routing through IGMP and multicast routing protocols for IP networks. These routers are depicted between DNO substation and DNO control centre, and DNO substation and DER site; however, only the router between DNO firewall and WAN requires the multicast routing capabilities, as 61850 data is not traversed between organisations.

Similarly, it is likely that only one anchor generator will exist within each distributed restoration zone, hence the need for local redundancy is required within this site (as above). Where zones contain multiple anchor generator sites, redundancy is provided on the site level rather than locally, an example of this can be seen in Figure 8 (demonstrating network architecture where multiple sites are available in a DRZ).



Distributed restoration zones typically will comprise of multiple primary and secondary balancing control sites (e.g. load banks or wind farms). The requirement for an automated BlackStart using the DRZC model and scheme is one primary balancing and one secondary balancing control site made available per zone. Redundancy is therefore supplied at the physical level rather than the network level. Figure 8 shows the single comms and device architecture for each PBC and SBC site, where the network extends from site to central DRZC firewalls and subsequently through to

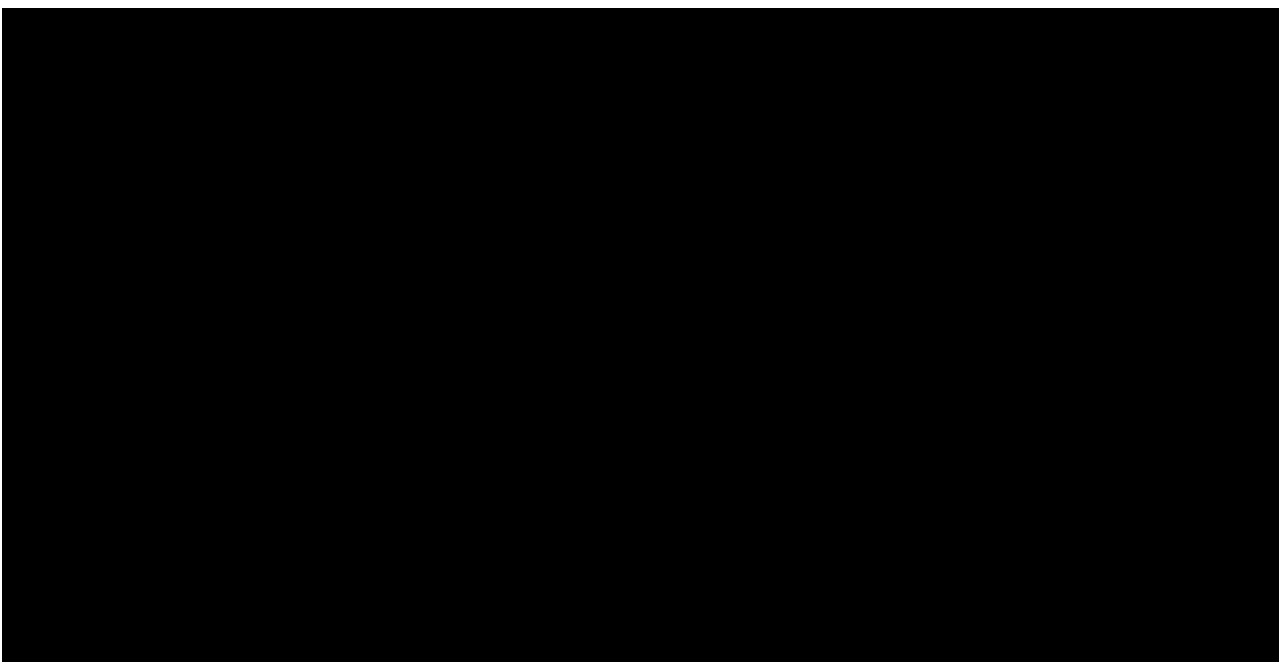
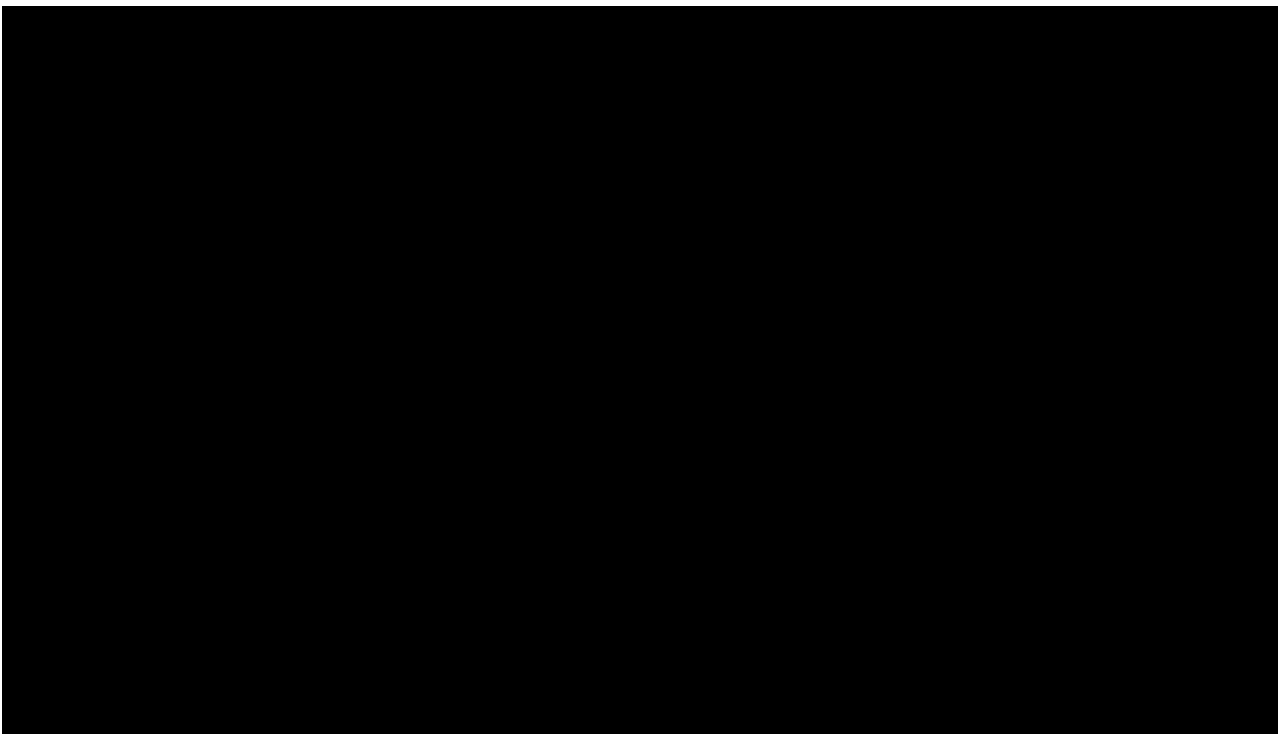


Figure 9 depicts the redundant network architecture for a zone containing only 1 available PBC site – in which case, the redundancy is provided by the sites network and devices similar to

central DRZC and anchor generator sites. This setup is likely uncommon as PBC and SBC sites are abundant in DRZ.

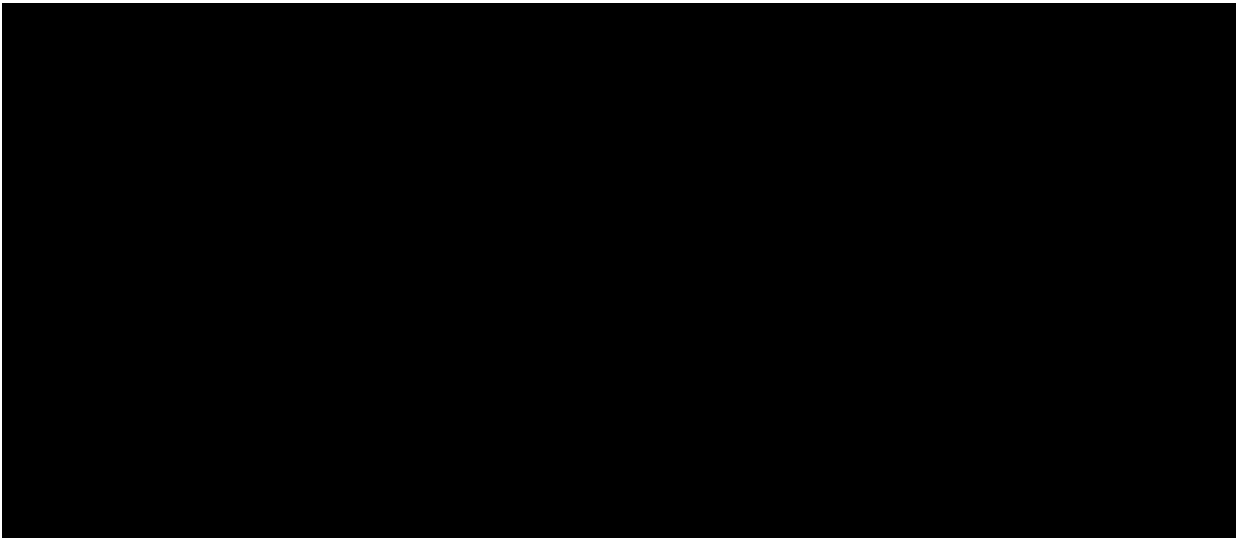


3.1 Security Controls

An attacker may compromise a controller network by either obtaining a controller via supply chain and modifying the device or using their own malicious device and connecting the devices to the network. Once connected, the attacker could passively monitor the local area networks traffic or attempt to brute force controllers without requiring remote access via multiple layers of firewalls (and potentially MFA). Flooding the local network via the switch/firewall is also a big concern where the availability of the controllers is crucial for BlackStart.

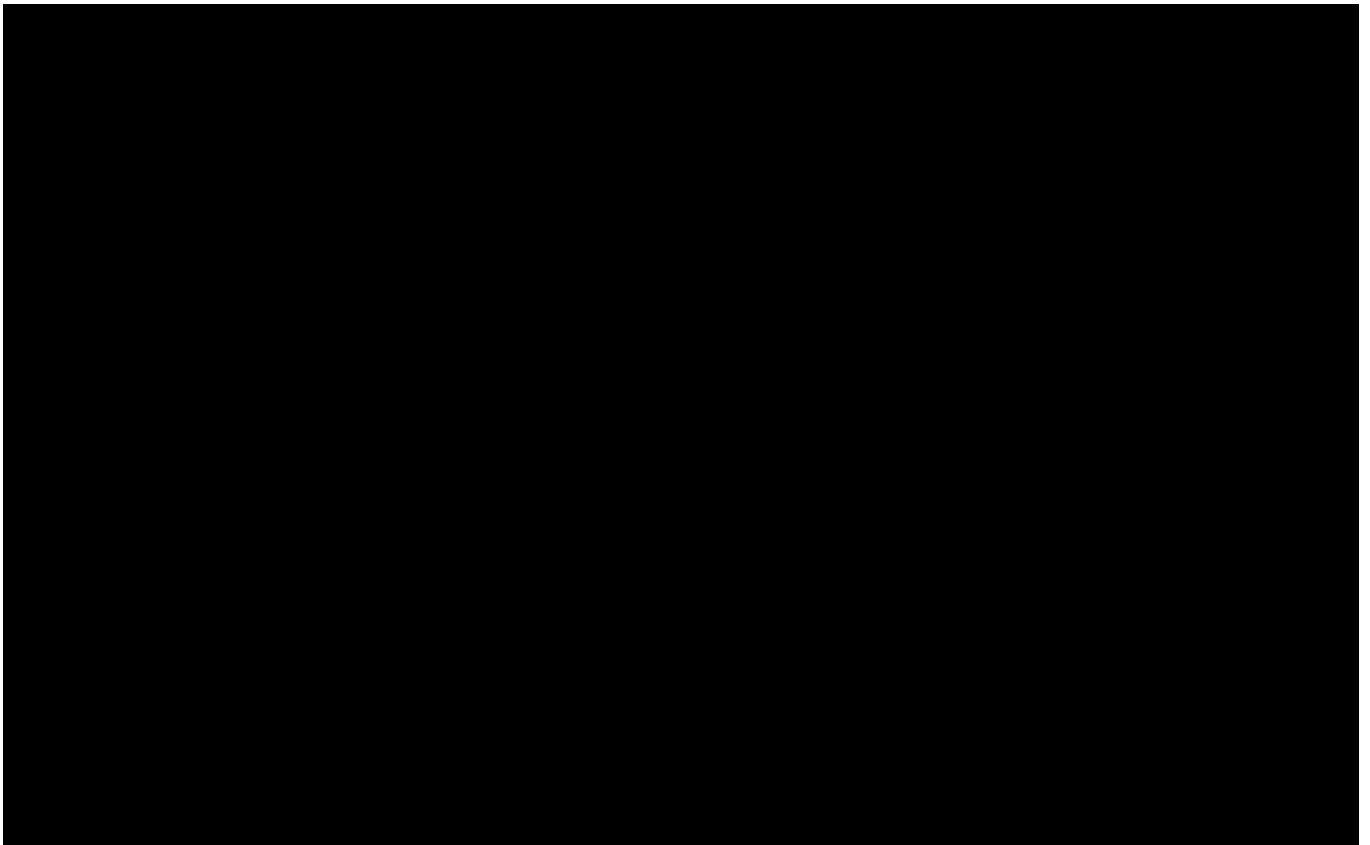
One protection mechanism to help mitigate these attacks is IP/MAC whitelisting. Only devices with specific IP or MAC addresses are granted access to the network, and all other devices are blocked by default. Note these methods do not protect against IP/MAC spoofing. As these techniques are susceptible to spoofing attacks, where an attacker can mimic the IP or MAC address of one that is whitelisted and join the network, certificate whitelisting is the preferred mechanism. Certificates issued by a CA are verified on the network device and confirm the identity of the connecting device. Another alternative is to use 802.1x port authentication with a central RADIUS server, to mitigate the certificate management overhead with using CAs.

CA certificate whitelisting should be implemented where possible on critical networks. IP or MAC whitelisting should be implemented on less critical networks, with MAC whitelisting taking precedence – Figure 10 gives an example of IP whitelisting.

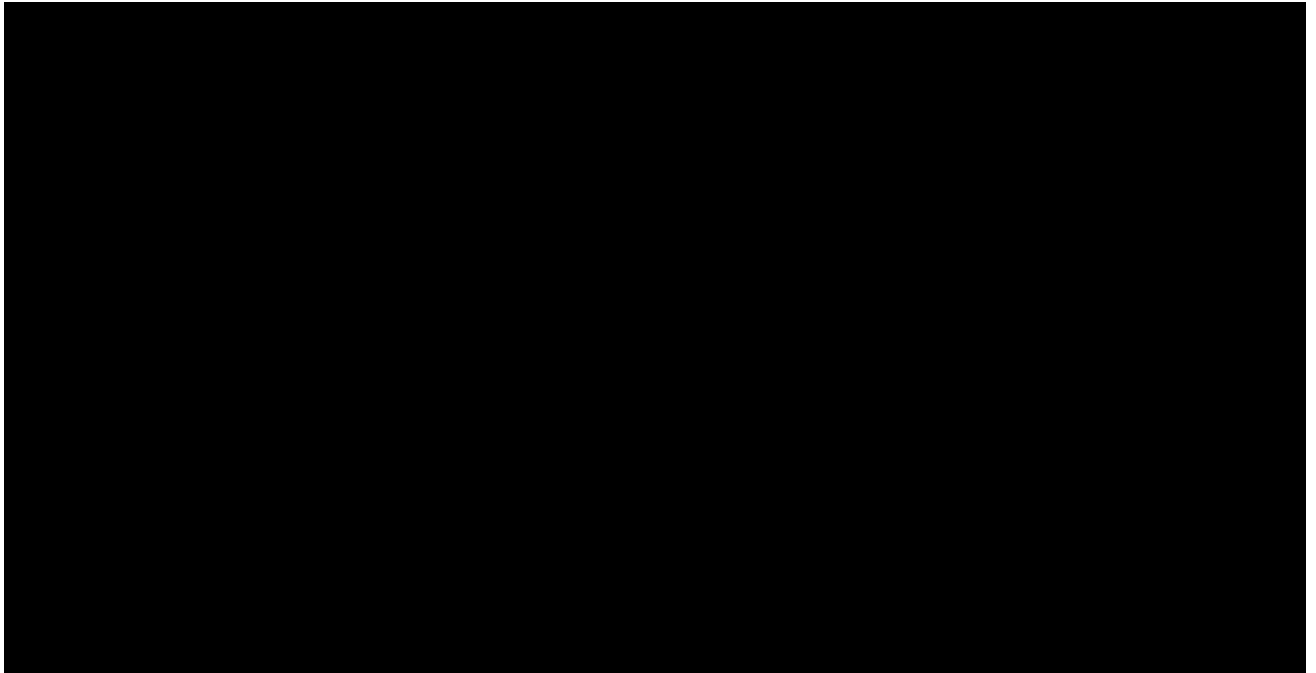


Adding files to servers or devices (such as configuration files for WAMS server or PLC scheme file for controllers), whether this is by secure copy and execution or HTTPS uploads, can lead to a compromised device if the files integrity was not properly verified and contains malicious code. Accidental changes to configurations of live environments can lead to catastrophic consequences, so the use of sandbox environments is crucial.

Each participant of BlackStart should incorporate a sandbox or testing environment into their infrastructure – isolated from the live systems these environments are used for training (refreshers on BlackStart processes) or pre-configuration changes. Figure 11 shows an example of a sandboxed test environment.



In the event a device or network is compromised, it is crucial to isolate and contain as quickly as possible to limit the spread of the attack. Firewalls should be configured with isolation profiles that when enabled, can quickly block the connections to and from a device or network. Some NGFWs will provide automated functionality for isolating devices using logging and any unusual behaviour recognised by the firewall (e.g. a sign of a DOS attack may trigger a network isolation profile). An



As discussed in later data flow designs, some of the protocols used do not provide full end-to-end encryption on the application layer and instead require a method for security on the network layers. Specifically IEEE C37.118, which does not provide a method for message authentication, requires a mechanism for both server and client to verify the authenticity of the device sending the data. Mutual TLS provides the benefits of encryption from standard TLS, with client-side authentication using a client certificate generated from the server sides certificate authority.

All data flows in the BlackStart architecture (see section 4) that require the use of TLS (as apposed to multicast encryption for 61850 protocols) will use the mutual TLS mechanism to provide encryption and verification of both client and server. This is between DER field controllers and central DRZ controller, and from DRZC to ADMS protocol converter. The version of TLS used is 1.3.

Figure 13 shows the typical client/server exchange for mutual TLS.

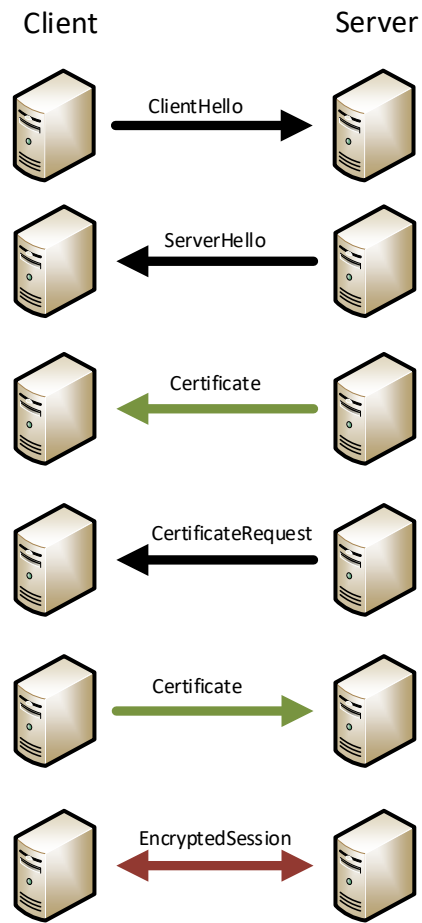


Figure 13 Mutual TLS

4 Data Flows Design

All unencrypted communications channels over local area networks (when not using 61850) that can utilise encryption between measurement devices or RTUs (where legacy devices are not used) should prioritise using encryption. The use of unencrypted communications over the local area networks in the following designs are shown to accommodate the use of legacy devices within substations.

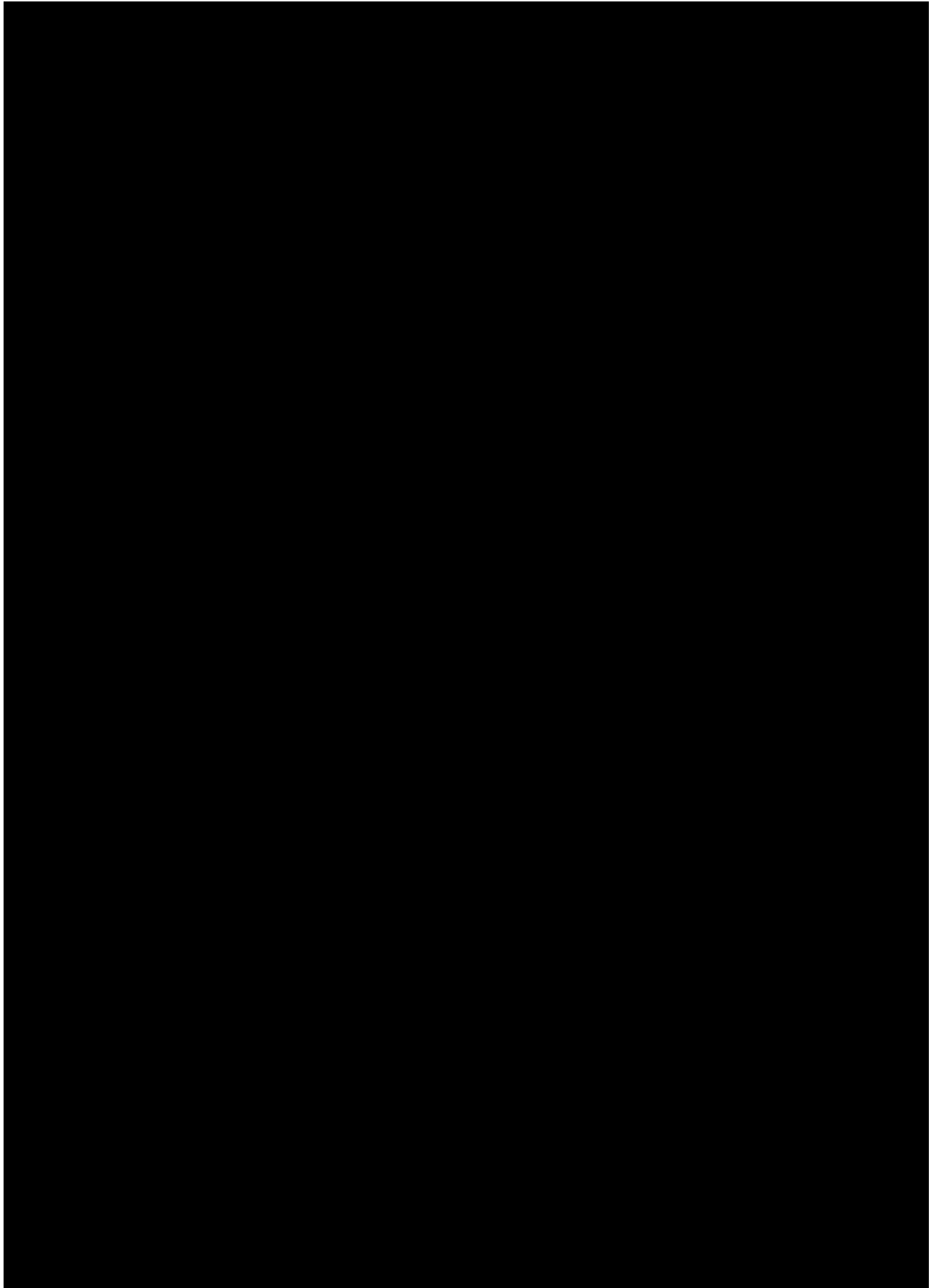
4.1 Synchrophasor Data

The following designs describe the data flows between the DNOs, ESO, TO and DER sites, where synchrophasor data is required by the central DRZC controller to measure the state of the system through electrical measurements of voltage, current and frequency. The controller will use these quantities to assess the state of the system continuously, detect when the system is being disturbed and determine restorative actions. The quantities are high-resolution so that events can be detected quickly within the system ensuring adequate time for taking corrective actions before instabilities can occur. The particular requirement for the TO synchrophasor data comes from the need for a resynchronisation mechanism. In some locations, the presence of synchro-check relays will mean that PMU data from a TO is not required. However, there may exist particular DRZC zones which will be synchronised across a TO-DSO boundary where there are no synchro-check relays and the DZRC will instead need to make the determination based on measurements from both sides of the boundary. In such cases, measurements from the TO side are necessary within the DRZC.

4.1.1 C37.118

As discussed in the Lot 2 – Requirements Final Report (Section 6.3.1) IEEE C37.118 is a viable option for carrying synchrophasor data over wide and local area networks. IEEE C37.118 should be encrypted using TLS with accordance to IEC 62351-3 and utilise mutual TLS with client certificate authentication to provide verification of identity of the client and server.

See Figure 14 for the IEEE C37.118 data flows.



Transmission Operator:

Prerequisites:

- Implement encrypted tunnel (e.g. VPN) from substation to TO PDC to securely transmit data over WAN.

Data flows:

Index	Data/Protocol	Source	Destination	Comms	Security Controls
1	IEEE C37.118 (synchrophasor)	PMU	Substation LAN	Ethernet (LAN)	Encrypt if possible
2	IEEE C37.118 (synchrophasor)	Substation LAN	PDC	Available comms e.g. fibre, microwave, 4G/5G etc. (WAN)	Encrypt data over WAN, use TLS where possible or VPN.

Table 1 TO data flows for IEEE C37.118

1. PMU collects measurements from transmission substation as synchrophasor data in IEEE C37.118 format.
2. IEEE C37.118 data is transmitted over WAN to TO PDC. Data is aggregated and available for forwarding to DNO via PDC.

Transmission Operator to Distribution Network Operator:

Prerequisites:

- TO PDC contains DNO PDC client certificate in TO PDC trust store.
- DNO PDC contains TO PDC client certificate in DNO PDC trust store.
- TO PDC to DNO PDC use available communications channels between sites (e.g. OpTel fibre link or existing ICCP link).

Data flows:

Index	Data	Source	Destination	Comms	Security Controls
3	IEEE C37.118 (synchrophasor)	TO PDC	DNO PDC	Available comms e.g. fibre, ICCP link etc. (WAN)	Encrypted and authenticated using mutual TLS with client/server certificates

Table 2 TO to DNO data flows for IEEE C37.118

3. Synchrophasor data from transmission substation is transmitted securely to DNO PDC. Data is made available on DNO network for forwarding to central DRZC controller. Mutual TLS is used to verify the authenticity of both PDCs and ensures data is encrypted while in transit.

Distribution Network Operator:

Prerequisites

- DNO PDC contains client certificate for central DRZC controller in trust store.
- Central DRZC controller contains client certificates for all DNO owned field controllers, DER owned field controllers and DNO PDC.

Data flows:

Index	Data	Source	Destination	Comms	Security Controls
4	IEEE C37.118 (synchrophasor)	PMU	DRZC/Field controllers	Ethernet (LAN)	Encrypt if possible
5	IEEE C37.118 (synchrophasor)	Field controllers	Central DRZC controller	Available comms e.g. fibre, microwave, 4G/5G etc. (WAN)	Encrypted and authenticated using mutual TLS with client/server certificates
6	IEEE C37.118 (synchrophasor)	Central DRZC controller	PDC	Available comms e.g. fibre, microwave, 4G/5G etc. (WAN)	Encrypted and authenticated using mutual TLS with client/server certificates
7	IEEE C37.118 (synchrophasor)	PDC	Central DRZC controller	Available comms e.g. fibre, microwave, 4G/5G etc. (WAN)	Encrypted and authenticated using mutual TLS with client/server certificates
8	IEEE C37.118 (synchrophasor)	PDC	WAMS/Offline monitoring	Co-located	Data is contained within host.

Table 3 DNO data flows for IEEE C37.118

4. Sites with PMUs available collect synchrophasor measurements and send data to local central/field controllers via IEEE C37.118 over substation LAN.
5. Field controllers send synchrophasor data via output streams to central DRZC controller. Mutual TLS is used to verify the authenticity of both controllers and ensures data is encrypted while in transit.
6. Central DRZC controller receives synchrophasor data from field controllers, aggregates the data and sends to DNO PDC via output stream. Mutual TLS is used to verify the authenticity of both controller and PDC and ensures data is encrypted while in transit.
7. PDC forwards synchrophasor data from TO substations (from index 3) to central DRZC controller via output stream. Mutual TLS is used to verify the authenticity of both controller and PDC and ensures data is encrypted while in transit.
8. PDC sends all available synchrophasor data via infrastructure stream to WAMS for offline monitoring and visualisation of data. PDC is co-located with WAMS service and uses local loopback address to exchange data.

Distributed Energy Resource:

Prerequisites

- DER field controllers contain client certificates for central DRZC controller
- DER sites use available communications channels extended to central DRZC controller site (e.g. fibre, microwave, 5G link etc).

Data flows:

Index	Data	Source	Destination	Comms	Security Controls
9	IEEE C37.118 (synchrophasor)	Field controllers	Central DRZC controller	Available comms e.g. fibre, microwave, 4G/5G etc. (WAN)	Encrypted and authenticated using mutual TLS with client/server certificates

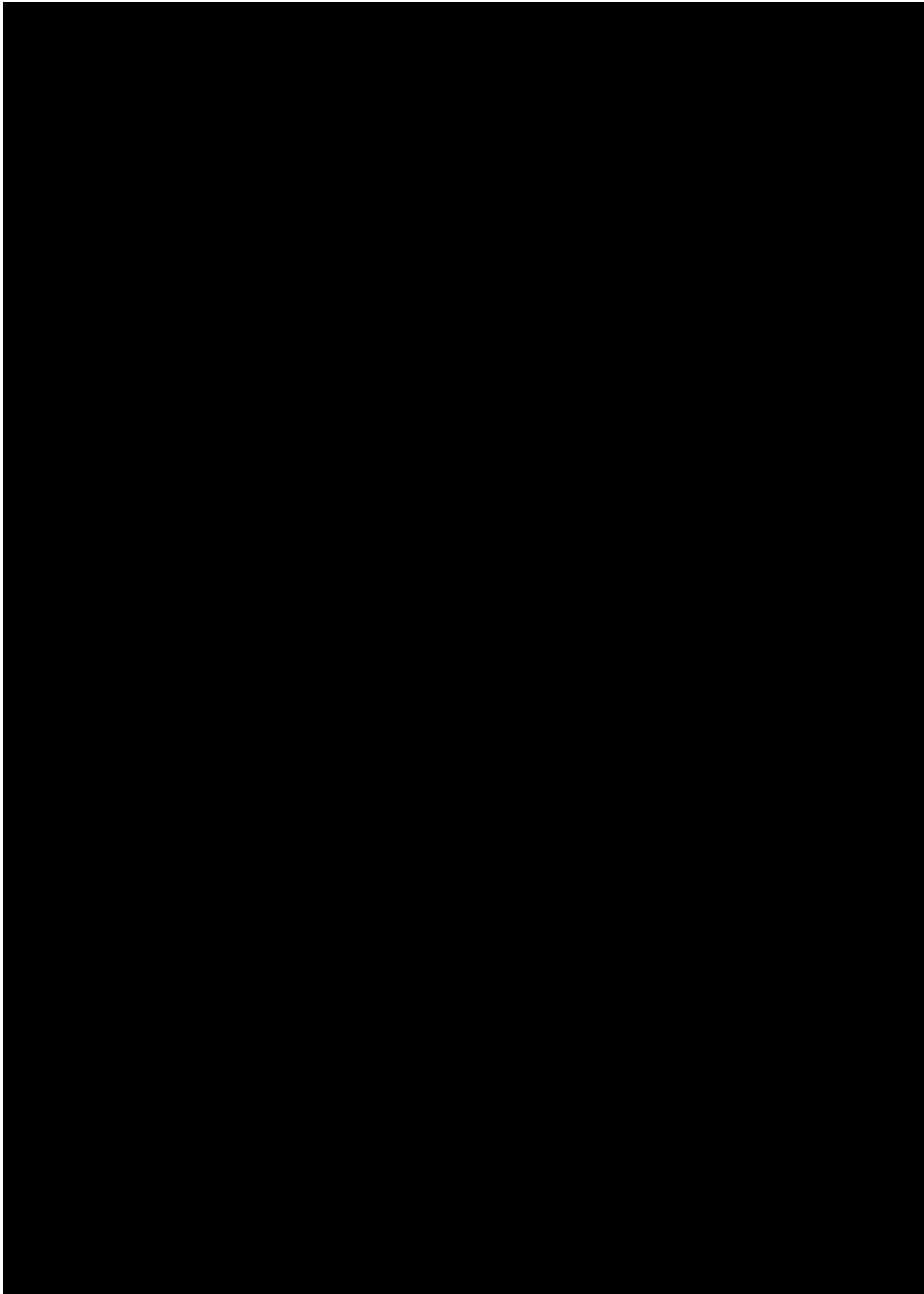
Table 4 DER data flows for IEEE C37.118

9. DER field controllers with access to PMUs and synchrophasor data send C37.118 data to central DRZC controller via output streams. Mutual TLS is used to verify the authenticity of both controllers and ensures data is encrypted while in transit. Mutual TLS between parties using different CAs presents a challenge for certificate management, which is discussed in Section 4.3.

4.1.2 IEC 61850-90-5 R-SV

As discussed in the Lot 2 – Requirements Final Report (Section 6.3.1) IEC 61850-90-5 is a viable option for carrying synchrophasor data over wide and local area networks within a single party environment (note that IEC 61850-90-5 is still relatively new and not widely available or used as of today but will become more widespread in the coming years). IEC 61850-90-5 provides encryption and authentication of data using symmetric keys issued from a central KDC, with accordance to IEC 62351-6 and IEC 62351-9. IEEE C37.118 is also required for cross-party communications and utilises TLS with accordance to IEC 62351-3.

See Figure 15 for the IEC 61850-90-5 R-SV data flows.



Transmission Operator:

Prerequisites:

- PDC and 61850 compliant synchrophasor measurement devices configured to connect with KDC and receive (via PUSH mechanism) symmetric keys to encrypt and authenticate data. Connection to KDC must be initially authenticated (e.g. via mutual TLS).

Data flows:

Index	Data/Protocol	Source	Destination	Comms	Security Controls
1	IEC 61850-9-2 SV (sampled values)	MU	Substation LAN	Ethernet (LAN)	Data is encrypted and authenticated at application layer using KDC issued symmetric keys
2	IEC 61850-90-5 R-SV (synchrophasor modelled)	Substation LAN	PDC	Available comms e.g. fibre, microwave, 4G/5G etc. (WAN)	Data is encrypted and authenticated at application layer using KDC issued symmetric keys

Table 5 TO data flows for IEC 61850-90-5 R-SV

1. Merging unit (or other 61850 compliant measurement device) collects sample value measurements from substation and presents these to the LAN over IP multicast, where the controller receives this data as IEC 61850-9-2 SV. The sample value data is transformed with additional data objects to comply with IEEE C37.118.1 synchrophasor data.
2. The IEC 61850-9-2 data is encapsulated in IEC 61850-90-5 R-SV protocol and routed using an IP multicast routing protocol (e.g. IGMP and PIM) over TO WAN to PDC located in OT network. Data is aggregated, converted to IEEE C37.118.2 by the PDC and available for forwarding.

Transmission Operator to Distribution Network Operator:

Prerequisites:

- TO PDC contains DNO PDC client certificate in TO PDC trust store.
- DNO PDC contains TO PDC client certificate in DNO PDC trust store.
- TO PDC to DNO PDC use available communications channels between sites (e.g. OpTel fibre link or existing ICCP link).

Data flows:

Index	Data	Source	Destination	Comms	Security Controls
-------	------	--------	-------------	-------	-------------------

3	IEEE C37.118 (synchrophasor)	TO PDC	DNO PDC	Available comms e.g. fibre, ICCP link etc. (WAN)	Encrypted and authenticated using mutual TLS with client/server certificates
---	------------------------------	--------	---------	--	--

Table 6 TO to DNO data flows for IEC 61850-90-5 R-SV

- Synchrophasor data from transmission substation is transmitted to DNO PDC in IEEE C37.118 format. Data is made available on DNO network for forwarding to central DRZC controller. Mutual TLS is used to verify the authenticity of both PDCs and ensures data is encrypted while in transit.

Distribution Network Operator:

Prerequisites

- PDC and Field/DRZC controllers configured to connect with KDC and receive (via PUSH mechanism) symmetric keys to encrypt and authenticate data. Connection to KDC must be initially authenticated (e.g. via mutual TLS).
- Central DRZC controller contains client certificates DER owned field controllers

Data flows:

Index	Data	Source	Destination	Comms	Security Controls
4	IEC 61850-9-2 SV (sampled values)	PMU	DRZC/Field controllers	Ethernet (LAN)	Data is encrypted and authenticated at application layer using KDC issued symmetric keys
5	IEC 61850-90-5 R-SV (synchrophasor modelled)	Field controllers	Central DRZC controller	Available comms e.g. fibre, microwave, 4G/5G etc. (WAN)	Data is encrypted and authenticated at application layer using KDC issued symmetric keys
6	IEC 61850-90-5 R-SV (synchrophasor modelled)	Central DRZC controller	PDC	Available comms e.g. fibre, microwave, 4G/5G etc. (WAN)	Data is encrypted and authenticated at application layer using KDC issued symmetric keys
7	IEC 61850-90-5 R-SV (synchrophasor modelled)	PDC	Central DRZC controller	Available comms e.g. fibre, microwave, 4G/5G etc. (WAN)	Data is encrypted and authenticated at application layer

					using KDC issued symmetric keys
8	IEEE C37.118 (synchrophasor)	PDC	WAMS/Offline monitoring	Co-located	Data is contained within host.

Table 7 DNO data flows for IEC 61850-90-5 R-SV

4. Merging unit (or other 61850 compliant measurement device) collects sample value measurements from substation and presents these to the LAN over IP multicast, where the controller receives this data as IEC 61850-9-2 SV. The sample value data is transformed with additional data objects to comply with IEEE C37.118.1 synchrophasor data.
5. The IEC 61850-9-2 data is encapsulated in IEC 61850-90-5 R-SV protocol and routed using an IP multicast routing protocol (e.g. IGMP and PIM) over DNO WAN from field controllers to central DRZC controller
6. Central DRZC controller receives synchrophasor data from field controllers, aggregates the data and sends to DNO PDC using an IP multicast routing protocol (e.g. IGMP and PIM) over DNO WAN.
7. PDC transforms TO substation IEEE C37.118.1 data from IEEE C37.118.2 format to IEC 61850-90-5 R-SV, and routes to central DRZC controller using an IP multicast routing protocol (e.g. IGMP and PIM) over DNO WAN.
8. PDC sends all available synchrophasor data via infrastructure stream to WAMS for offline monitoring and visualisation of data. PDC is co-located with WAMS service and uses local loopback address to exchange data.

Distributed Energy Resource:

Prerequisites

- DER field controllers contain client certificates for central DRZC controller
- DER sites use available communications channels extended to central DRZC controller site (e.g. fibre, microwave, 5G link etc).

Data flows:

Index	Data	Source	Destination	Comms	Security Controls
9	IEEE C37.118 (synchrophasor)	Field controllers	Central DRZC controller	Available comms e.g. fibre, microwave, 4G/5G etc. (WAN)	Encrypted and authenticated using mutual TLS with client/server certificates

Table 8 DER data flows for IEC 61850-90-5 R-SV

9. Merging unit (or other 61850 compliant measurement device) collects sample value measurements from DER substation and presents these to the LAN over IP multicast, where the controller receives this data as IEC 61850-9-2 SV. The sample value data is transformed with additional data objects to comply with IEEE C37.118.1 synchrophasor data. Synchrophasor data is transmitted from DER site to central DRZC controller in IEEE C37.118 format, where the central DRZC controller transforms data from IEEE C37.118.2

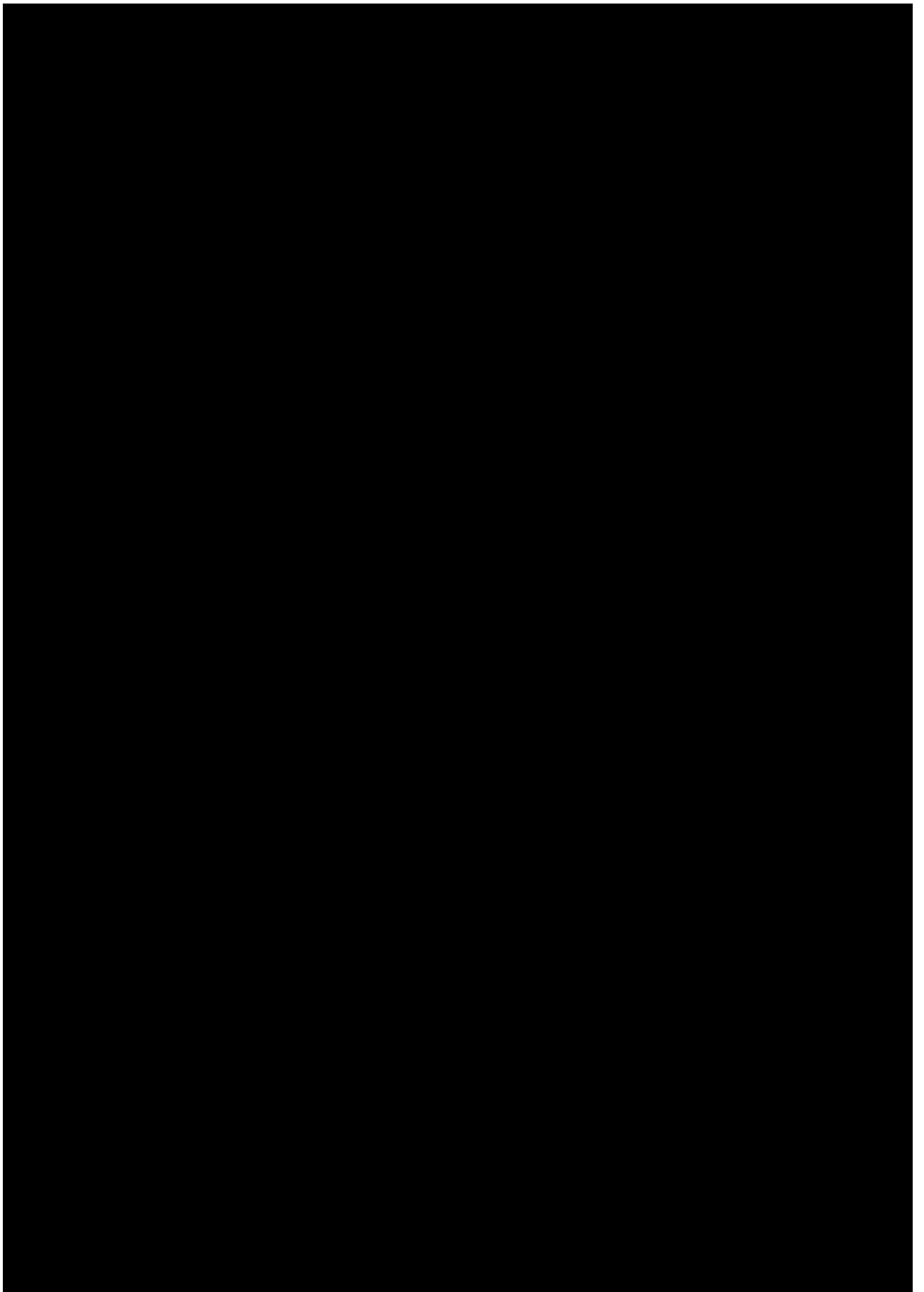
format to IEC 61850-90-5 R-SV (for routing to PDC). Mutual TLS is used to verify the authenticity of both controllers and ensures data is encrypted while in transit.

4.2 Control Scheme Data

4.2.1 IEC 60870-5-104

As discussed in the Lot 2 – Requirements Final Report (Section 6.3.2/6.3.3) IEC 60870-5-104 is a viable option for carrying fast-balancing and slow-balancing control data over wide and local area networks. IEC 60870-5-104 specifies TLS for encryption with accordance to IEC 62351-3, and specifies application layer authentication of data packets using Message Authentication Codes (MAC) with accordance to IEC 62351-5.

See Figure 16 for the IEC 60870-5-104 data flows.



Electricity System Operator to Distribution Network Operator:

Prerequisites:

- ESO EMS to DNO ADMS use available ICCP link between sites.

Data flows:

Index	Data/Protocol	Source	Destination	Comms	Security Controls
1	ICCP	EMS	ADMS	ICCP link	Link should be encrypted between sites

Table 9 ESO to TO data flows for IEC 60870-5-104

1. ICCP link between ESO and DNO is only for visualisation of the distribution network for the ESO, no control is required for the automated DNO BlackStart process.

Distribution Network Operator:

Prerequisites:

- DNO ADMS protocol converter contains central DRZC controller client certificate.
- Field controllers contain central DRZC controller client certificate.
- Central DRZC controller contains DNO and DER field controller and ADMS protocol converter client certificates.
- DER sites use available communications channels extended to central DRZC controller site (e.g. fibre, microwave, 5G link etc).

Data flows:

Index	Data/Protocol	Source	Destination	Comms	Security Controls
2	IEC 60870-5-104	RTU	Central/Field controllers	Ethernet (LAN)	Encrypted and authenticated where possible. IEC 104 messages authenticated via MAC.
3	IEC 60870-5-104	Field controllers	Central DRZC controller	Available comms e.g. fibre, microwave, 4G/5G etc. (WAN)	Encrypted and authenticated using mutual TLS with client/server certificates. IEC 104 messages authenticated via MAC.

4	IEC 60870-5-104	Central DRZC controller	ADMS protocol converter	Available comms e.g. fibre, microwave, 4G/5G etc. (WAN)	Encrypted and authenticated using mutual TLS with client/server certificates. IEC 104 messages authenticated via MAC.
5	DNP3	ADMS protocol converter	ADMS FEP	Ethernet (LAN)	No encryption or authentication (roadmap)
6	IEC 60870-5-104	ADMS FEP	ADMS protocol converter	Ethernet (LAN)	No encryption or authentication (roadmap)
7	IEC 60870-5-104	ADMS protocol converter	Central DRZC controller	Available comms e.g. fibre, microwave, 4G/5G etc. (WAN)	Encrypted and authenticated using mutual TLS with client/server certificates. IEC 104 messages authenticated via MAC.
8	IEC 60870-5-104	Central DRZC controller	Field controllers	Available comms e.g. fibre, microwave, 4G/5G etc. (WAN)	Encrypted and authenticated using mutual TLS with client/server certificates. IEC 104 messages authenticated via MAC.
9	IEC 60870-5-104	Central/Field controllers	RTU	Ethernet (LAN)	Encrypted and authenticated where possible.

Table 10 DNO data flows for IEC 60870-5-104

2. RTUs at DNO sites interface with field and central DRZC controller to provide RTU measurements and breaker statuses via IEC 60870-5-104.
3. Field controllers send RTU measurements and breaker statuses to central DRZC controller via IEC 60870-5-104. Mutual TLS is used to verify the authenticity of both controllers and ensures data is encrypted while in transit.

4. Central DRZC controller sends RTU measurements, breaker statuses, load pickup values and alarms to the ADMS protocol converter via IEC 60870-5-104. Mutual TLS is used to verify the authenticity of both controllers and ensures data is encrypted while in transit.
5. ADMS protocol converter forwards RTU measurements, breaker statuses, load pickup values and alarms (from controllers) to ADMS FEP via IEC 60870-5-104. Encryption and authentication are terminated at the protocol converter, so this data flow does not contain any encryption or authentication.
6. ADMS FEP sends breaker control to ADMS protocol converter via IEC 60870-5-104.
7. ADMS protocol converter forwards breaker control to central DRZC controller via IEC 60870-5-104. Mutual TLS is used to verify the authenticity of both controllers and ensures data is encrypted while in transit.
8. Central DRZC controllers sends setpoints and breaker control to field controllers via IEC 60870-5-104. Mutual TLS is used to verify the authenticity of both controllers and ensures data is encrypted while in transit.
9. Central and field controllers communicate with site resource directly or via RTU issuing setpoints and breaker control from central DRZC controller via IEC 60870-5-104.

Distributed Energy Resource:

Prerequisites

- DER field controllers contain client certificates for central DRZC controller
- DER sites use available communications channels extended to central DRZC controller site (e.g. fibre, microwave, 5G link etc).

Data flows:

Index	Data	Source	Destination	Comms	Security Controls
10	IEC 60870-5-104	Field controllers	Central DRZC controller	Available comms e.g. fibre, microwave, 4G/5G etc. (WAN)	Encrypted and authenticated using mutual TLS with client/server certificates. IEC 104 messages authenticated via MAC.
11	IEC 60870-5-104	Central DRZC controller	Field controllers	Available comms e.g. fibre, microwave, 4G/5G etc. (WAN)	Encrypted and authenticated using mutual TLS with client/server certificates. IEC 104 messages authenticated via MAC.

Table 11 DER data flows for IEC 60870-5-104

10. RTUs at DER sites interface with field controllers to provide RTU measurements and breaker statuses via IEC 60870-5-104. Field controllers send RTU measurements and

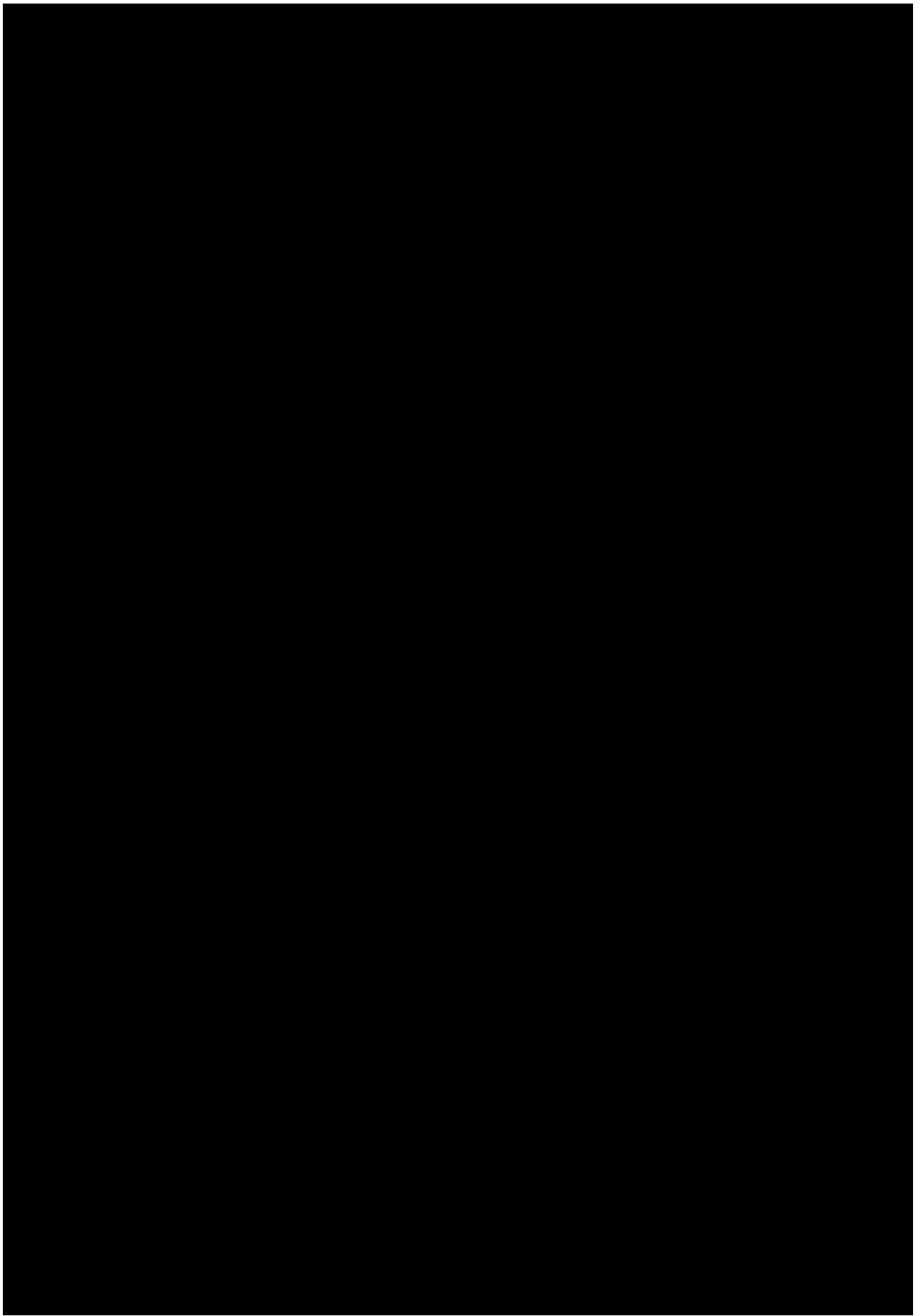
breaker statuses to central DRZC controller via IEC 60870-5-104. Mutual TLS is used to verify the authenticity of both controllers and ensures data is encrypted while in transit.

11. Central DRZC controllers sends setpoints and breaker control to DER field controllers via IEC 60870-5-104. Mutual TLS is used to verify the authenticity of both controllers and ensures data is encrypted while in transit.

4.2.2 DNP3.0

As discussed in the Lot 2 – Requirements Final Report (Section 6.3.2/6.3.3) DNP3 is a viable option for carrying fast-balancing and slow-balancing control data over wide and local area networks. IEEE 1815-2012 does not specify any requirement for encryption of data, however, DNP3 should be encrypted using TLS with accordance to IEC 62351-3. IEEE 1815-2012 specifies application layer authentication of data packets using Message Authentication Codes (MAC) with accordance to IEC 62351-5.

See Figure 17 for the DNP3 data flows.



Electricity System Operator to Distribution Network Operator:

Prerequisites:

- ESO EMS to DNO ADMS use available ICCP link between sites.

Data flows:

Index	Data/Protocol	Source	Destination	Comms	Security Controls
1	ICCP	EMS	ADMS	ICCP link	Link should be encrypted between sites

Table 12 ESO to TO data flows for DNP3

1. ICCP link between ESO and DNO is only for visualisation of the distribution network for the ESO, no control is required for the automated DNO BlackStart process.

Distribution Network Operator:

Prerequisites:

- DNO ADMS protocol converter contains central DRZC controller client certificate.
- Field controllers contain central DRZC controller client certificate.
- Central DRZC controller contains DNO and DER field controller and ADMS protocol converter client certificates.
- DER sites use available communications channels extended to central DRZC controller site (e.g. fibre, microwave, 5G link etc).

Data flows:

Index	Data/Protocol	Source	Destination	Comms	Security Controls
2	DNP3	RTU	Central/Field controllers	Ethernet (LAN)	Encrypted and authenticated where possible.
3	DNP3	Field controllers	Central DRZC controller	Available comms e.g. fibre, microwave, 4G/5G etc. (WAN)	Encrypted and authenticated using mutual TLS with client/server certificates. DNP3 messages authenticated via MAC.
4	DNP3	Central DRZC controller	ADMS protocol converter	Available comms e.g. fibre, microwave, 4G/5G etc. (WAN)	Encrypted and authenticated using mutual TLS with client/server

					certificates. DNP3 messages authenticated via MAC.
5	DNP3	ADMS protocol converter	ADMS FEP	Ethernet (LAN)	No encryption or authentication (roadmap)
6	DNP3	ADMS FEP	ADMS protocol converter	Ethernet (LAN)	No encryption or authentication (roadmap)
7	DNP3	ADMS protocol converter	Central DRZC controller	Available comms e.g. fibre, microwave, 4G/5G etc. (WAN)	Encrypted and authenticated using mutual TLS with client/server certificates. DNP3 messages authenticated via MAC.
8	DNP3	Central DRZC controller	Field controllers	Available comms e.g. fibre, microwave, 4G/5G etc. (WAN)	Encrypted and authenticated using mutual TLS with client/server certificates. DNP3 messages authenticated via MAC.
9	DNP3	Central/Field controllers	RTU	Ethernet (LAN)	Encrypted and authenticated where possible.

Table 13 DNO data flows for DNP3

2. RTUs at DNO sites interface with field and central DRZC controller to provide RTU measurements and breaker statuses via DNP3.
3. Field controllers send RTU measurements and breaker statuses to central DRZC controller via DNP3. Mutual TLS is used to verify the authenticity of both controllers and ensures data is encrypted while in transit.
4. Central DRZC controller sends RTU measurements, breaker statuses, load pickup values and alarms to the ADMS protocol converter via DNP3. Mutual TLS is used to verify the authenticity of both controllers and ensures data is encrypted while in transit.
5. ADMS protocol converter forwards RTU measurements, breaker statuses, load pickup values and alarms (from controllers) to ADMS FEP via DNP3. Encryption and authentication are terminated at the protocol converter, so this data flow does not contain any encryption or authentication.
6. ADMS FEP sends breaker control to ADMS protocol converter via DNP3.

7. ADMS protocol converter forwards breaker control to central DRZC controller via DNP3. Mutual TLS is used to verify the authenticity of both controllers and ensures data is encrypted while in transit.
8. Central DRZC controllers sends setpoints and breaker control to field controllers via DNP3. Mutual TLS is used to verify the authenticity of both controllers and ensures data is encrypted while in transit.
9. Central and field controllers communicate with site resource directly or via RTU issuing setpoints and breaker control from central DRZC controller via DNP3.

Distributed Energy Resource:

Prerequisites

- DER field controllers contain client certificates for central DRZC controller
- DER sites use available communications channels extended to central DRZC controller site (e.g. fibre, microwave, 5G link etc).

Data flows:

Index	Data	Source	Destination	Comms	Security Controls
10	DNP3	Field controllers	Central DRZC controller	Available comms e.g. fibre, microwave, 4G/5G etc. (WAN)	Encrypted and authenticated using mutual TLS with client/server certificates. DNP3 messages authenticated via MAC.
11	DNP3	Central DRZC controller	Field controllers	Available comms e.g. fibre, microwave, 4G/5G etc. (WAN)	Encrypted and authenticated using mutual TLS with client/server certificates. DNP3 messages authenticated via MAC.

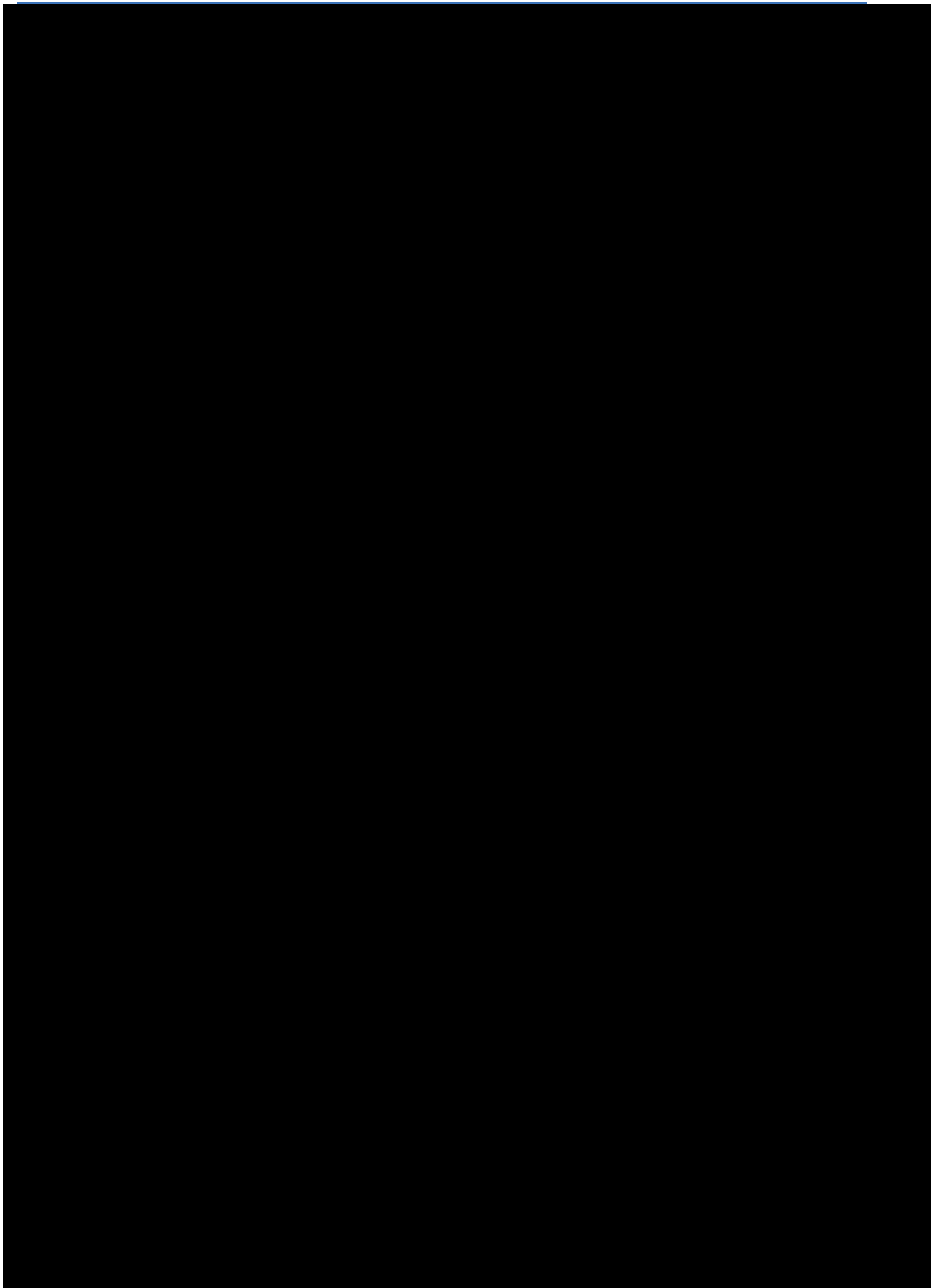
Table 14 DER data flows for DNP3

10. RTUs at DNO sites interface with field and central DRZC controller to provide RTU measurements and breaker statuses via DNP3. Field controllers send RTU measurements and breaker statuses to central DRZC controller via DNP3. Mutual TLS is used to verify the authenticity of both controllers and ensures data is encrypted while in transit.
11. Central DRZC controllers sends setpoints and breaker control to DER field controllers via DNP3. Mutual TLS is used to verify the authenticity of both controllers and ensures data is encrypted while in transit.

4.2.3 IEC 61850-90-5 R-GOOSE

As discussed in the Lot 2 – Requirements Final Report (Section 6.3.2/6.3.3) IEC 61850-90-5 R-GOOSE is a viable option for carrying fast-balancing and slow-balancing control data over wide and local area networks. IEC 61850-90-5 provides encryption and authentication of data using symmetric keys issued from a central KDC, with accordance to IEC 62351-6 and IEC 62351-9. IEEE C37.118 is also required for cross-party communications and utilises TLS with accordance to IEC 62351-3.

See Figure 18 for the IEC 61850-90-5 R-GOOSE data flows.



Electricity System Operator to Distribution Network Operator:

Prerequisites:

- ESO EMS to DNO ADMS use available ICCP link between sites.

Data flows:

Index	Data/Protocol	Source	Destination	Comms	Security Controls
1	ICCP	EMS	ADMS	ICCP link	Link should be encrypted between sites

Table 15 ESO to TO data flows for IEC 61850-90-5 R-GOOSE

1. ICCP link between ESO and DNO is only for visualisation of the distribution network for the ESO, no control is required for the automated DNO BlackStart process.

Distribution Network Operator:

Prerequisites:

- Central DRZC/field controllers (including ADMS protocol converter) and 61850 compliant control devices are configured to connect with KDC and receive (via PUSH mechanism) symmetric keys to encrypt and authenticate data. Connection to KDC must be initially authenticated (e.g. via mutual TLS).
- Central DRZC controller contains DER field controller client certificates.

Data flows:

Index	Data/Protocol	Source	Destination	Comms	Security Controls
2	IEC 61850-8-1 GOOSE	RTU	Central/Field controllers	Ethernet (LAN)	Data is authenticated at application layer using KDC issued symmetric keys. Encryption is not applied due to short response times (IEC 62351-6).
3	IEC 61850-90-5 R-GOOSE	Field controllers	Central DRZC controller	Available comms e.g. fibre, microwave, 4G/5G etc. (WAN)	Data is encrypted and authenticated at application layer using KDC issued symmetric keys

4	IEC 61850-90-5 R-GOOSE	Central DRZC controller	ADMS protocol converter	Available comms e.g. fibre, microwave, 4G/5G etc. (WAN)	Data is encrypted and authenticated at application layer using KDC issued symmetric keys
5	IEC 60870-5-104 or DNP3	ADMS protocol converter	ADMS FEP	Ethernet (LAN)	No encryption or authentication (roadmap)
6	IEC 60870-5-104 or DNP3	ADMS FEP	ADMS protocol converter	Ethernet (LAN)	No encryption or authentication (roadmap)
7	IEC 61850-90-5 R-GOOSE	ADMS protocol converter	Central DRZC controller	Available comms e.g. fibre, microwave, 4G/5G etc. (WAN)	Data is encrypted and authenticated at application layer using KDC issued symmetric keys
8	IEC 61850-90-5 R-GOOSE	Central DRZC controller	Field controllers	Available comms e.g. fibre, microwave, 4G/5G etc. (WAN)	Data is encrypted and authenticated at application layer using KDC issued symmetric keys
9	IEC 61850-8-1 GOOSE	Central/Field controllers	RTU	Ethernet (LAN)	Data is authenticated at application layer using KDC issued symmetric keys. Encryption is not applied due to short response times (IEC 62351-6).

Table 16 DNO data flows for IEC 61850-90-5 R-GOOSE

2. RTUs at DNO sites interface with field and central DRZC controller to provide RTU measurements and breaker statuses via IEC 61850-8-1 GOOSE messages. These are transmitted over the substation LAN via IP multicast.
3. Field controllers send RTU measurements and breaker statuses to central DRZC controller. Controllers encapsulate IEC 61850-8-1 GOOSE messages in IEC 61850-90-5 R-GOOSE protocol and route over DNO WAN using an IP multicast routing protocol (e.g. IGMP and PIM).

4. Central DRZC controller sends RTU measurements, breaker statuses, load pickup values and alarms to the ADMS protocol converter via IEC 61850-90-5 R-GOOSE. Data is routed over DNO WAN using an IP multicast routing protocol (e.g. IGMP and PIM).
5. ADMS protocol converter transforms IEC 61850-90-5 R-GOOSE messages into IEC 60870-5-104 or DNP3 format for compliance with the ADMS. These messages are transmitted over the ADMS LAN. Encryption and authentication are terminated at the protocol converter, so this data flow does not contain any encryption or authentication.
6. ADMS FEP sends breaker control to ADMS protocol converter via IEC 60870-5-104 or DNP3. ADMS protocol converter transforms data back to IEC 61850-90-5 R-GOOSE format. Encryption and authentication are encapsulated in the application layer for IEC 61850-90-5 R-GOOSE.
7. ADMS protocol converter forwards breaker control to central DRZC controller via IEC 61850-90-5 R-GOOSE. Data is routed over DNO WAN using an IP multicast routing protocol (e.g. IGMP and PIM).
8. Central DRZC controllers sends setpoints and breaker control to field controllers via IEC 61850-90-5 R-GOOSE. Data is routed over DNO WAN using an IP multicast routing protocol (e.g. IGMP and PIM).
9. Central and field controllers communicate with site resource directly or via RTU issuing setpoints and breaker control from central DRZC controller via IEC 61850-8-1 GOOSE messages. These are transmitted over the substation LAN via IP multicast.

Distributed Energy Resource:

Prerequisites

- DER field controllers contain client certificates for central DRZC controller
- DER sites use available communications channels extended to central DRZC controller site (e.g. fibre, microwave, 5G link etc).

Data flows:

Index	Data	Source	Destination	Comms	Security Controls
10	IEC 60870-5-104 or DNP3	Field controllers	Central DRZC controller	Available comms e.g. fibre, microwave, 4G/5G etc. (WAN)	Encrypted and authenticated using mutual TLS with client/server certificates. DNP3 messages authenticated via MAC.
11	IEC 60870-5-104 or DNP3	Central DRZC controller	Field controllers	Available comms e.g. fibre, microwave, 4G/5G etc. (WAN)	Encrypted and authenticated using mutual TLS with client/server certificates. DNP3 messages authenticated via MAC.

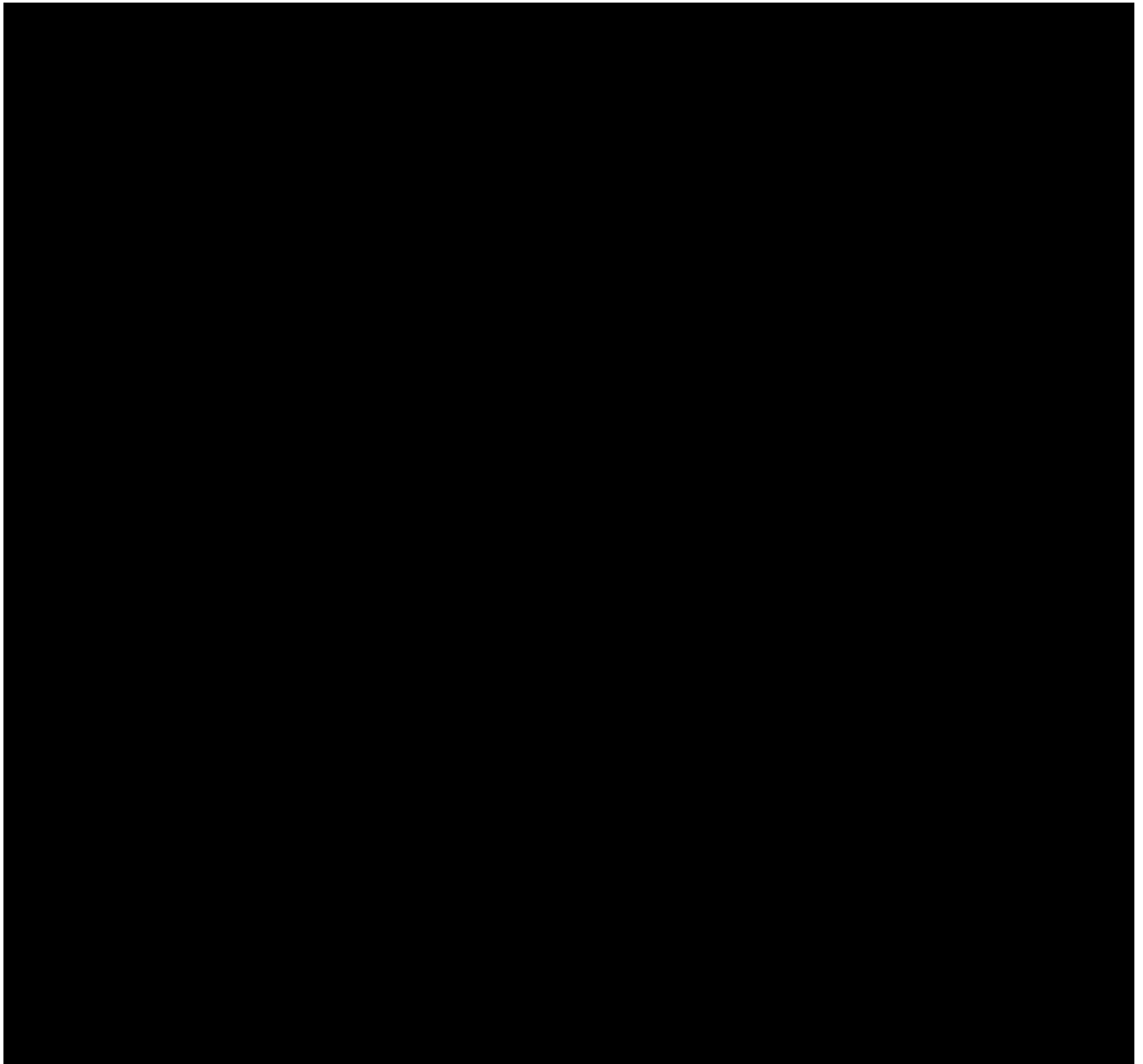
Table 17 DER data flows for IEC 61850-90-5 R-GOOSE

10. RTUs at DER sites interface with field controllers to provide RTU measurements and breaker statuses via IEC 60870-5-104/DNP3. Field controllers send RTU measurements and breaker statuses to central DRZC controller via IEC 60870-5-104/DNP3. Mutual TLS is used to verify the authenticity of both controllers and ensures data is encrypted while in transit.
11. Central DRZC controllers sends setpoints and breaker control to DER field controllers via IEC 60870-5-104/DNP3. Mutual TLS is used to verify the authenticity of both controllers and ensures data is encrypted while in transit.

4.3 Admin/Management

The critical systems in the DRZC architecture all require some management interfacing for configuration or integration purposes. Controllers provide a user interface for managing PDC streams, PLC logic schemes and network configurations whereas ADMS/WAMS require user access for control and monitoring. Access to systems within control centres are likely segregated in their own domain from those on the field, so multiple DMZs with jump hosts may be required for accessing multiple systems. Figure 19 shows a client workstation connecting to a device within the solution, where the connection terminates within the OT DMZ on a jump server. Ingress traffic to the control systems is now initiated from the jump server through the OT firewall.

It is the party's responsibility (based upon onus of controller and location) for the configuration of logic schemes within the controller, as this will vary from site to site. A baseline configuration is supplied with each controller, adhering to security hardening requirements set out in previous reports. However, it is unlikely each generator will have the same interface (e.g. DNP3 or IEC 60870-5-104) so the field controllers will allow for different conversions. The sites integrator is responsible for setting control configurations, as such each DER site will require management access to their controller (highlighted in Figure 19). All management data flows (i.e. accessing the controller's interface for PLC configuration) is secured with encryption and authentication. This is via HTTPS with AD integration (or MFA where strong authentication is required).



One of the main challenges for rolling out a secure Distributed ReStart system across multiple organisations and stakeholders is key and certificate management, for securing control and monitoring data at rest and in transit.

There are two main methods for managing keys are Public Key Infrastructures (PKIs) and Key Distribution Centres (KDCs). Both have different purposes along with advantages and disadvantages such as speed, complexity and security. The purpose of a PKI within an organisation is to manage the generation, storage, distribution and revocation of digital certificates. Digital certificates are used by entities to provide assurance of data confidentiality and integrity, these certificates are signed by trusted actors (certificate authorities or CAs) to provide a root of trust that can be verified by other entities. KDCs on the other hand are standalone (or highly available) systems that generate symmetric keys for groups to enable group members to encrypt and authenticate with other group members. KDCs are required when using IEC 61850 protocols.

The multi-party nature of Distributed ReStart presents challenges for PKIs and the root of trust for verification of the connecting entities (e.g. a DER field controller connecting to DNO central DRZ controller must verify that the controller is trusted by a common CA). Without internet access in the OT networks, field devices must utilise an organisation's private CA to sign their digital certificates and provide a chain of trust. However, with multiple party involvement of independent PKIs and CAs, a connecting party has no way of verifying the chain of trust within a digital certificate without access to the third party's CA. In this case, a Bridge CA is required to provide each organisation with a Root or Intermediate CA that is verified by a commonly trusted party. Certificates for organisation A are issued using their internal CA which issues certificates that are signed by the Bridge CA; organisation B uses their own internal CA to issue certificates which are also signed by the Bridge CA, completing the chain of trust on both sides.

Figure 20 highlights a DER and DNO organisation using independent PKIs, with a Bridge CA issuing the Root certificates for each organisation, allowing for a chain of trust to be completed by both parties. Server-side certificates are rotated on a weekly basis using a certificate management system (CMS) and client certificates distributed between parties after trust is initially established. Initial trust between parties is established by manual intervention on device setup. Once established, client certificates can also be rotated on frequent intervals.

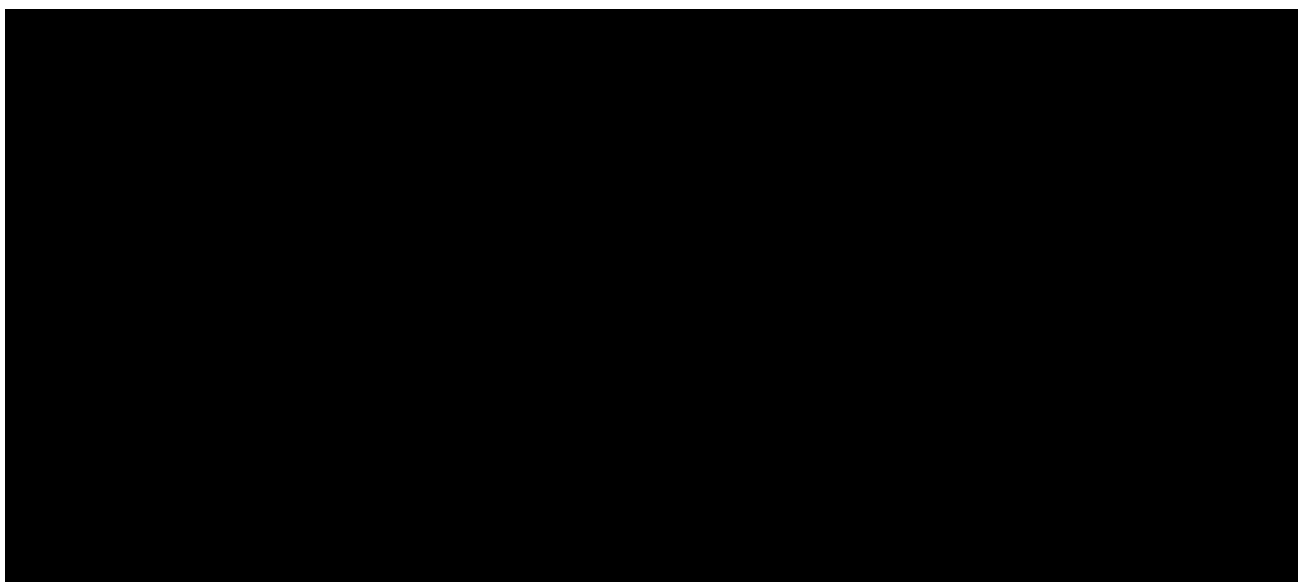
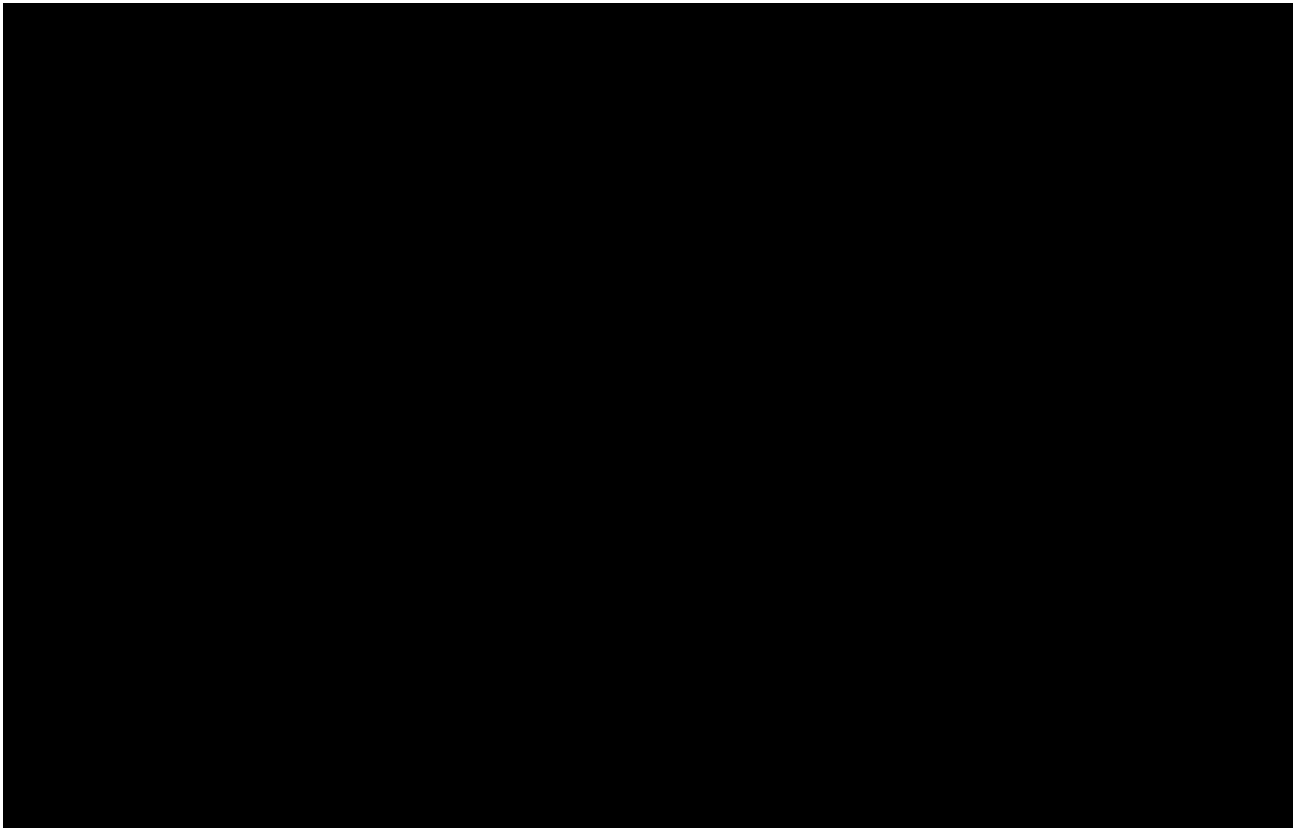


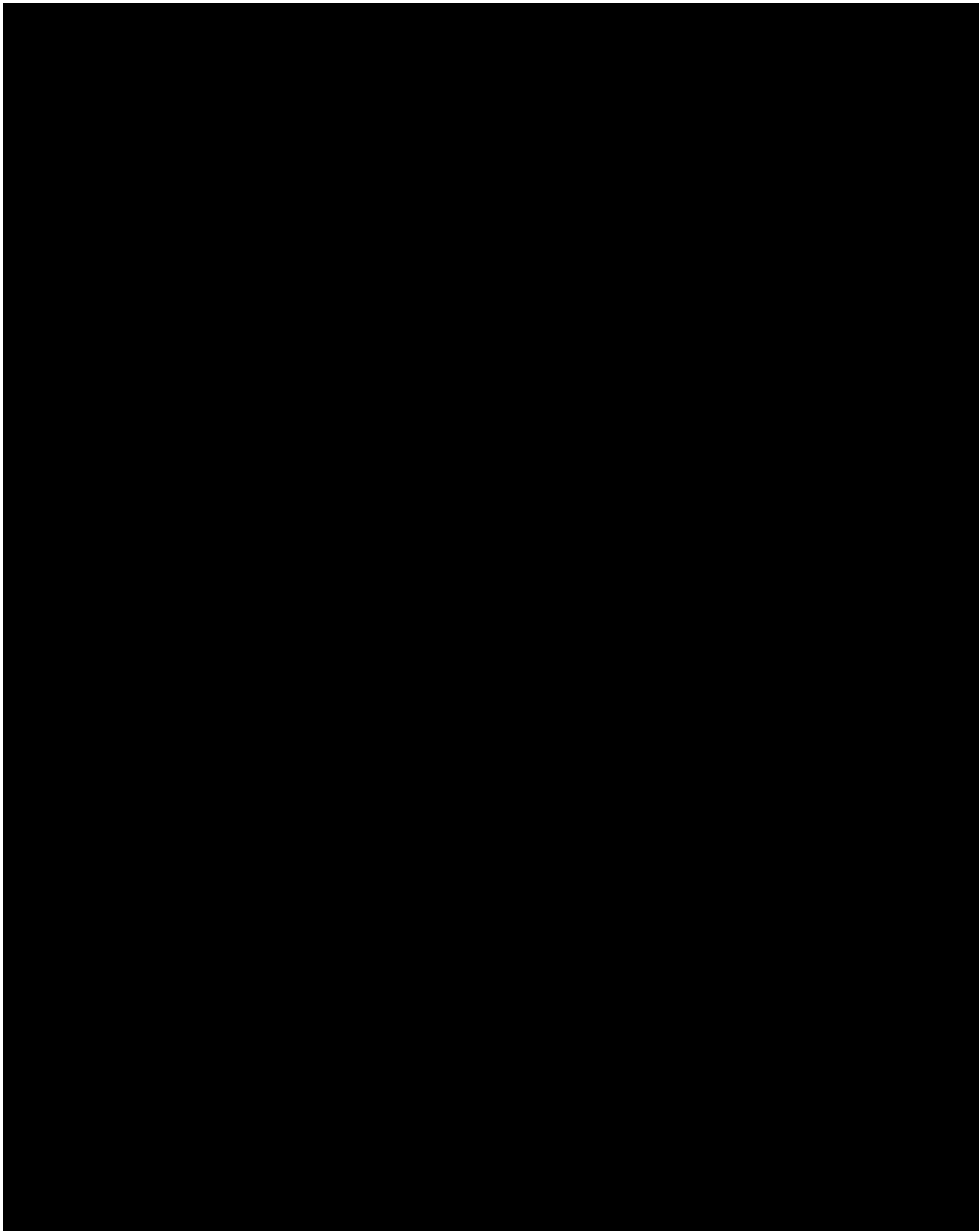
Figure 21 depicts the same PKI architecture with the addition of a KDC for securing IEC 61850 traffic. When using IEC 61850 protocols internally in an organisation, for transmitting control and monitoring data, a KDC is required to distribute keys to devices to encrypt and authenticate messages at the application layer. The KDC uses Group Domain of Interpretation (GDOI) protocol to establish a security association between KDC and group members (e.g. controllers) and distribute symmetric keys to the group members that have authenticated. Authentication is handled using X.509 certificates managed by the organisations PKI. Certificates are installed on the group members and the KDC is granted access to the PKI, allowing the KDC to verify the entity attempting to join the group.

IEC 61850-8-1 GOOSE (for control) and IEC 61850-9-2 SV (for measurements) are both layer 2 multicast protocols, hence are not routable and only operate over local area networks. Controllers utilise the Internet Group Management Protocol (IGMP) to exchange multicast data between group members over LAN. IEC 61850-90-5 R-GOOSE (for control) and IEC 61850-90-5 R-SV (for

measurements) are the extensible protocols allowing GOOSE and SV data to be routed over a wide area network. After IGMP forwards the data to the local multicast router within the LAN, a multicast routing protocol (e.g. Protocol Independent Multicast or PIM)

As discussed in the Distributed ReStart Requirements Report, the use of symmetric keys is not feasible between organisations, so IEC 61850 protocols are only used internally to organisations. However, controllers can receive 61850 data and convert to IEC 60870-5-104 or DNP3, allowing the data to be transmitted between organisations as above.





5 Desktop Study – Penetration Techniques for Designs

The following section presents a desktop study of the penetration testing techniques for the communications designs for Distributed ReStart. The design was reviewed from a security point of view using the following attack methods:

5.1 Network Attacks

The following network attacks could be exploited against the networks used to host and carry data for Distributed ReStart systems:

- **Computer Virus / Worm**

Computer viruses are one of the most common network security attacks that can cause sizeable damage to your data on network.

Computer worms are nothing but a malicious type of software that spreads from one infected device to the other by duplicating the virus. Their objectives by exploiting network vulnerabilities and gain access to devices.

- **Man-in-the-middle**

MIM (man-in-the-middle) attacks are a type of cyberattack, black hats hijack the private communication intended between two parties. By intercepting the communication, the attacker tries to monitor and control their messages to either disrupt files, steal confidential data.

- **Packet Injection Attack**

A packet injection attack is a common attack vector that hackers use to inject data into the packets on a network. This would allow attackers to change data while it is being transmitted to the devices.

- **DoS (Denial of Service) and DDoS Attacks**

The difference between DoS and DDoS attacks is that hackers launch DoS attacks through one host network. DDoS attacks are more sophisticated, and attackers can use several computers to exploit targeted systems. Since the attack is launched from several compromised systems, it's hard to detect and protect from DDoS threats.

5.2 Protocols Attacks

The following protocol attacks could be exploited against the protocols used by Distributed ReStart systems:

- **Man-in-the-middle**

MIM (man-in-the-middle) attacks are a type of cyberattack where black hats hijack the private communications intended between two parties. By intercepting the communication, the attacker tries to monitor and control their messages to either disrupt files or steal confidential data.

- **Packet Injection Attack**

A packet injection attack is a common attack vector that hackers use to inject data into the packets on a network. This would allow attackers to change data while it is being transmitted to the devices.

6 Design Strategies for Cyber Security

The following section summarizes the security design choices and associates the protection mechanisms with the desktop study in the previous section, highlighting how each attack is mitigated using the strategies in the designs.

6.1 Comms Strategies

Control Centre to DRZC Site

This comms requires power resiliency for the DRZC to send critical RTU measurements, breaker statuses, load pickup values and alarms to the ADMS. The ADMS is also required to send some breaker controls to the DRZC. Low latency is not fundamental for this comms as there is no requirement for fast response control.

This means the following communications mediums are viable options:

- Fibre
- Microwave Radio
- 5G
- 4G
- 3G
- VSAT

DRZC Site to Proportional Regulation Site[s]

This comms requires power resiliency for the DRZC to send setpoints and breaker control to the Field Interface Units located at PR sites. PR sites are required to send RTU measurements and breaker statuses to the DRZC. Low latency is fundamental for this comms as PBC resources may be co-located with the anchor generator and would require fast-balancing responses. However, where PR sites do not have PBC resources co-located, critical measurements from PMUs are still required by the DRZC, so there is still a need for low latency.

This means the following communications mediums are viable options:

- Fibre
- Microwave Radio
- 5G

DRZC Site to Primary Balancing Control Site[s]

This comms requires power resiliency for the DRZC to send setpoints and breaker control to the Field Interface Units located at PBC sites. PBC sites are required to send RTU measurements and breaker statuses to the DRZC. Low latency is fundamental for this comms as there the site contains fast-balancing resources that require fast response times for control.

This means the following communications mediums are viable options:

- Fibre
- Microwave Radio
- 5G

DRZC Site to Secondary Balancing Control Site[s]

This comms requires power resiliency for the DRZC to send setpoints and breaker control to the Field Interface Units located at SBC sites. SBC sites are required to send RTU measurements and breaker statuses to the DRZC. Low latency is not fundamental for this comms as there is no fast-balancing resources and instead bring slow dispatch loads into the DRZC power island.

This means the following communications mediums are viable options:

- Fibre
- Microwave Radio
- 5G
- 4G
- VSAT
- 3G

6.2 Network Strategies

The network designs highlighted in Section 3 includes protection against the attacks shown in the network and protocol attacks sections.

Firewalls and Segregation

The firewalls will have Internal, External and Demilitarised Zone (DMZ), this is protecting the access to the different areas across Distributed ReStart solution as shown in the design. Ingress can limit the number of packets received in a time range to protect against DoS/DDoS attacks while also blocking requests from unknown hosts. An external attack will be required to traverse through multiple layers of firewalls and security zones to reach the designated target. This also helps limit the spread of viruses.

Jump Servers with Strong Authentication

Protects from unauthorised access to the Distributed ReStart and critical control systems. Jump servers should be located in secure locations like a DMZ, giving the firewalls the ability to restrict access. Strong authentication protects against unauthorised access by attackers to the systems and the use of strong authentication (e.g. multi-factor authentication) protects the systems from password cracking attacks and entry into the systems.

Anti-Virus/Anti-Malware

Detection of viruses before they are deployed is one of the most effective ways to protect the networks. Malware and viruses are the most commonly used attack vector in ICS environments, so anti-virus/malware software is essential. Scanning all traffic within the Distributed ReStart networks and systems ensures that viruses are captured and can be contained before causing disruption to normal operation. Anti-virus/malware require internet access to update with new virus signatures, so a DMZ should be used to restrict the traffic flow to the OT network, and signatures can be pushed to offline AV servers for up-to-date scanning of the critical Distributed ReStart systems.

IP/MAC/CA whitelisting

The devices used on the Distributed ReStart network will use IP/MAC/CA whitelisting, this will ensure only the devices that are approved on the network are allowed to access. For critical systems, CA whitelisting should be used to mitigate against IP and MAC spoofing attacks. Any form of whitelisting will protect the networks from attackers deploying unauthorised devices to either mimic control devices, flood the network or perform local hacks that otherwise cannot be exploited remotely. These are especially important for unmanned sites (e.g. DER sites or DNO substations) where physical access to the network equipment is more likely.

Sandboxing Environments

Sandboxing environments help with protecting against viruses or malicious code entering a live environment and spreading to Distributed ReStart and critical systems when applying patches, updates or changing configurations. Patches for software may be susceptible to MiTM attacks where an attacker changes the patch to contain malicious code that is used to infect a network or system when applied. While checksums and hashes can protect against these types of attacks, the use of sandboxing environments act as a last defence mechanism to ensure that malicious code or viruses do not enter production/live environments. This should be used for all Distributed ReStart system patches, updates, training and configuration changes.

Network Isolation

Network isolation mechanisms are typically built into Next Gen Firewalls and can automatically restrict the flow of data between zones, essentially isolating a network or system from the rest of the infrastructure. This aids in reducing the spread of viruses; when a system is compromised and the anti-virus detects unusual activity, it can send signals to the NGFW to isolate the network to contain the virus. Manual intervention is typically required to re-join networks once the compromised system/network is fixed.

Mutual TLS

Mutual TLS not only verifies the authenticity of the host, but also the authenticity of the client. Just as standard TLS, the public keys of the host are used to encrypt data in transit which the host can decrypt with their private key. This encryption protects against sniffing attacks and packet injection attacks. The addition of the client and server authentication using their digital certificates allows each connecting party to prove their identity, protecting the systems from Man-in-The-Middle attacks or unauthorised users trying to communicate with Distributed ReStart systems.

6.3 Protocol Strategies

The following protocols have security built in by design:

- IEC 61850-90-5 R-SV
- IEC 61850-90-5 R-GOOSE

The security mechanisms provided by IEC 61850-90-5 R-GOOSE/R-SV enable each message to be encrypted and authenticated between hosts, protecting every message from sniffing, packet injection and MiTM attacks.

The following protocols do have security built in by design and will be encrypted using Mutual Transport Layer Security (mTLS), ensuring the data does not get tampered with between devices:

- IEC 60870-5-104
- DNP3
- C37.118

Mutual TLS as described in the previous section protects against sniffing, packet injection and MiTM attacks. Therefore, due to the lack of inherent security controls developed into the protocols, this is required for these protocols to protect the data while in transit between Distributed ReStart systems and networks.

Certificates

As some of the protocols do not support end to end encryption, mTLS encryption will be used between devices using an internal certificate authority to generate client certificates to ensure the communication is encrypted on the network.

7 Change Impact Analysis

The following section is a change impact analysis for the newly proposed Distributed ReStart system highlighted in the functional design report and earlier sections of this report delivered as part of the Lot 1 and Lot 2 workstreams. This section is based on information gathered in the requirements and design phase and expands on the OST workstream 'Operating a Distribution Restoration Zone – September 2021' report issued by National Grid, in partnership with SP Energy Networks and TNEI.

The following sections are broken down into the four different parties involved in the Distributed ReStart restoration process (ESO, TO, DNO and DER) and covers the different organisation changes required for each party. This includes changes to:

- Interfaces
- Systems
- Telecommunications
- Training
- Staff
- External Factors
- Security

Each section describes in detail the change to either process or procedure and the impact this has on the organisation based on time and complexity to implement.

7.1 Electricity System Operator

7.1.1 Interfaces

Change	Description	Impact
The ESO is required to interface with the DNOs	The ESO currently interfaces with the TO for SCADA/EMS and WAMS measurements into the ESO WAMS systems and applications. The ESO will now require further visualization of DNO level systems and therefore links into the ADMS systems. It's not expected that WAMS data from the DNO level would be required at the ESO level.	Low impact

Table 18 ESO change impact analysis to interfaces

7.1.2 Systems

Change	Description	Impact
Changes to IEMS to integrate ICCP link with DNOs	Creation of bi-lateral table to define the point names and tags which are to be exchanged for the visualisation of the DNO networks over ICCP. Tools are available for defining the ICCP connection.	Low Impact

Table 19 ESO change impact analysis to systems

7.1.3 Telecommunications

Change	Description	Impact
Communications network extended to DNO network for exchange of visualisation data of DRZ and DNO network	Currently the existing OpTel network extends to each DNO. The additional bandwidth as a result of the ICCP data exchange is minimal as data points are reported by exception (i.e. when a value or quality changes).	Low Impact

Table 20 ESO change impact analysis to telecommunications

7.1.4 Training

Change	Description	Impact
Functional DRZC training	<p>With the addition of DRZC scheme into the DNO networks and the interaction between ESO and DNO, required for awareness of the DRZC, training for ESO operators is required.</p> <p>Training shall include:</p> <ul style="list-style-type: none"> • ICCP integration • Concepts and effects of DRZC on ESO • IEMS visualisation and restoration procedures 	Medium Impact

	Training frequency shall be yearly.	
Distribution network-based training	<p>The new requirement for visualisation and awareness of the distribution networks requires the exchange of knowledge and training between the different parties, who's skillset is based within their own domain.</p> <p>Joint sessions with ESO, TO and DNO for knowledge transfer and training shall include:</p> <ul style="list-style-type: none"> • Distribution network visualisation • Restoration sequence between parties • Simulated BlackStart between parties • ESO operator requirements for BlackStart <p>Training frequency shall be yearly.</p>	Medium Impact

Table 21 ESO change impact analysis to training

7.1.5 Staff

Change	Description	Impact
None	No change to staffing requirements	No impact

Table 22 ESO change impact analysis to staff

7.1.6 External Factors

Change	Description	Impact
Support for new systems from third party suppliers	Support for critical system (IEMS) by third party to ensure continuous operation and defect mitigation through support teams/channels.	Low impact

Table 23 ESO change impact analysis to external factors

7.1.7 Security

Change	Description	Impact
Increased security awareness among operators	<p>Security awareness should be a fundamental part of every party and/or individual who interacts with the entire DRZC system. For ESO, social engineering (i.e. a spoofed voice call from apparent DNO operator) or malware infection (via email, cascading down ICCP link to distribution network) could result in a breach of the system.</p> <p>This may be achieved via regular awareness sessions, training, team meetings.</p>	Low impact
Security testing of ICCP links	<p>The addition of a new interface between ESO and 6 DNOs increases the attack surface, where a direct ICCP connection from ESO can cascade down into the DRZC system. Sufficient security testing of these links should be included into the ESOs current procedures.</p>	Medium impact

Table 24 ESO change impact analysis to security

7.2 Transmission Operator

7.2.1 Interfaces

Change	Description	Impact
No change	The TOs currently interface with both ESO and the DNOs.	No impact

Table 25 TO change impact analysis to interfaces

7.2.2 Systems

Change	Description	Impact
--------	-------------	--------

<p>Addition of Phasor Data Concentrator (PDC) into transmission network</p>	<p>A newly installed PDC is required into the TOs network where resynchronisation measurement is required for the DNO. PDC is configured to receive synchrophasor data from field measurement devices (PMUs) and forward the data to the DNOs own PDC. Synchrophasor data sent over WAN must be encrypted and authenticated.</p> <p>This will require detailed network design to ensure connectivity to the DNO.</p>	<p>Low impact</p>
<p>Addition of PMU devices into key transmission substations</p>	<p>Synchrophasor measurement devices (PMUs) are required in transmission-side substations where the DNO requires data to provide resynchronisation functionality with the transmission network.</p> <p>This will require detailed network design within substation.</p>	<p>Medium impact</p>

Table 26 TO change impact analysis to systems

7.2.3 Telecommunications

Change	Description	Impact
<p>Increase in bandwidth for the telecommunications between TO and DNO to accommodate synchrophasor data.</p>	<p>Synchrophasor data containing measurements from the transmission network is required to be sent to DNO for resynchronisation between distribution and transmission network. The additional bandwidth on the communications link between TO and DNO is max [REDACTED] per GSP in region.</p>	<p>Medium impact</p>

Table 27 TO change impact analysis to telecommunications

7.2.4 Training

Change	Description	Impact
Functional DRZC training	<p>With the addition of DRZC scheme into the DNO networks and the interaction between TO and DNO, required for awareness of the DRZC, training for ESO operators is required.</p> <p>Training shall include:</p> <ul style="list-style-type: none"> • ICCP integration • Concepts and effects of DRZC on TO • IEMS visualisation and restoration procedures <p>Training frequency shall be yearly.</p>	Medium Impact
Distribution network-based training	<p>The new requirement for visualisation and awareness of the distribution networks requires the exchange of knowledge and training between the different parties, who's skillset is based within their own domain.</p> <p>Joint sessions with ESO, TO and DNO for knowledge transfer and training shall include:</p> <ul style="list-style-type: none"> • Distribution network visualisation • Restoration sequence between parties • Simulated BlackStart between parties • TO operator requirements for BlackStart <p>Training frequency shall be yearly.</p>	Medium Impact
WAMS admin training	The addition of a PDC in TO for exchanging synchrophasor	Low impact

	<p>from transmission network to distribution network may require some additional administrative training.</p> <p>Training shall include:</p> <ul style="list-style-type: none"> • Synchrophasor input and output stream configuration • TLS configuration • LDAP integration • Backups and restores • Disaster recovery <p>Training frequency shall be one-off, with follow up sessions available if necessary</p>	
--	---	--

Table 28 TO change impact analysis to training

7.2.5 Staff

Change	Description	Impact
No change	No change to staffing requirements	No impact

Table 29 TO change impact analysis to staff

7.2.6 External Factors

Change	Description	Impact
Support for new systems from third party suppliers	Support for critical system (WAMS) by third party to ensure continuous operation and defect mitigation through support teams/channels.	Low Impact

Table 30 TO change impact analysis to external factors

7.2.7 Security

Change	Description	Impact
Increased security awareness among operators	Security awareness should be a fundamental part of every party and/or individual who interacts with the entire DRZC system. For TO, social engineering (i.e. a spoofed	Low impact

	<p>voice call from apparent DNO operator) or malware infection (via email, cascading down PDC link to distribution network) could result in a breach of the system.</p> <p>This may be achieved via regular awareness sessions, training, team meetings.</p>	
<p>PKI for generating certificates to secure synchrophasor data in transit between TO and DNO</p>	<p>TLS requires server-side certificates for the client to verify the identity of the server. MTLS also requires client-side certificates for the server to verify the identity of the client. This provides two-way or mutual authentication between the connecting parties.</p> <p>Synchrophasor data must be encrypted between TO PDC and DNO PDC, with each instance providing trusted certificates to verify their identity to each other.</p> <p>This requires an infrastructure to generate and distribute certificates to the TO PDC, along with a means of exchanging client certificates with the DNO.</p> <p>The challenging aspect is the chain of trust derived from the root certificate authority (CA), where each organisation will sign the generated certificates with their own CA.</p> <p>A shared or 'bridge' CA can be used to generate root certificates for the independent organisations own root CA, or access to the other parties CA certificate are viable options. Security,</p>	<p>Medium Impact</p>

	network design and cost should be accounted for with both options.	
KDC for generating and managing key lifecycles to secure IEC 61850 measurement protocols	<p>For IEC 61850 protocols, symmetric keys are used to encrypt and authenticate messages. A shared key is distributed among group members, allowing each member in the group to transmit encrypted and authenticated control and monitoring data.</p> <p>A KDC is used to automatically generated and distribute keys to group members, this requires detailed network design to ensure each group member has connectivity to the KDC.</p>	Medium Impact

Table 31 TO change impact analysis to security

7.3 Distribution Network Operator

7.3.1 Interfaces

Change	Description	Impact
The DNO is required to interface with the ESO	The DNO currently interfaces to the TO typically at the GSP where each owner may have a breaker by which to disconnect. The DNOs will now require more high-frequency monitoring from a TO level for automated resynchronization across GSPs. DNO is required to interface with the ESO to provide visualisation of DNO level systems and network.	Low Impact
The DNO is required to interface with at least 1 Proportional Regulation DER site (Anchor Generator)	The DNO is required to interface with a DER site containing an anchor generator, this is the key	Medium Impact

	inertia provision for the BlackStart restoration	
The DNO is required to interface with at least 1 Primary Balancing Control DER site (where PBC is not co-located with PR)	The DNO is required to interface with a DER site containing a fast resource such as a load bank. PBC resources may be co-located with anchor generators	Medium Impact
The DNO is required to interface with at least 1 Secondary Balancing Control DER site	The DNO is required to interface with a DER site that provides slow dispatch loads into the DRZC power island (e.g. wind farms)	Medium Impact

Table 32 DNO change impact analysis to interfaces

7.3.2 Systems

Change	Description	Impact
SCADA configuration changes to ADMS	This requires mapping of RTU and IO points in the ADMS. The ADMS will communicate to DRZC via IEC-60870-5-104. This can be done either manually via the SCADA configuration interface or via internal tool for bulk load of data (plant file loader).	Medium Impact
Network visualisation configuration for ADMS	A new display will be created in the Network Diagram to show the status of Restart stages and will allow the ADMS user to control the progress of such stages.	Low Impact
New automation sequences configured for ADMS	Group Telecontrol (GTC) allows the creation of predefined ordered list of tele-controllable devices and a set of telecontrol operations which are applied to that list. Automation Manager allows the creation of automation scripts, with the ability to check and write real time values, issue a scan	Medium Impact

	<p>command, issue a telecontrol and a GTC, raise an alarm, write into the system log. Both GTCs and automation programs will be created for this GTCs will be created for certain Restart stages.</p>	
<p>Addition of new Distribution Restoration Zone Controller (DRZC)</p>	<p>A newly installed DRZC is required for the Distributed ReStart project as the core component of the automated DNO lead BlackStart restoration process. The DRZC consists of 2 redundant embedded devices that interface with the network using protocols such as IEC 104, DNP3 or IEC 61850-90-5 over Ethernet.</p> <p>The location of the DRZC is fundamental to the design – the requirements for location are as follows:</p> <ul style="list-style-type: none"> • Power resilient communication channels (addressed in Section 2) • Power resilient site (72-hour backup power integrating into redundant controllers) • Redundancy of network within site (redundant network equipment and wiring) <p>Detailed network design is required for the DRZC site to incorporate the devices into the network in a secure and safe manner. Security controls must be applied.</p>	<p>Medium impact</p>
<p>Addition of distribution-level Wide Area Monitoring System (WAMS)</p>	<p>A newly installed WAM system is a required component as part of the DRZ model for Distributed ReStart. For the</p>	<p>Medium Impact</p>

	<p>DNO, the WAMS consists of 2 services:</p> <ul style="list-style-type: none"> • Phasor Data Concentrator (PDC) – for aggregating synchrophasor data. Provides TLS connection between TO and DNO for transmission-side measurements required for resynchronisation. • WAMS server – for real-time visualisation of data, events and alarming. Offline historical analysis of data. Critical function for WAMS is IEC 104 signal to ADMS to inform operators that anchor generators and load banks are within operational limits. <p>Detailed network design is required for both elements of the WAMS component to ensure connectivity to TO, ADMS and DRZC. Security controls must be applied.</p> <p>Configuration includes:</p> <ul style="list-style-type: none"> • Input and output streams • PMU and measurement mapping • IEC 104 points for ADMS 	
<p>Addition of PMUs into key distribution substations</p>	<p>Newly installed PMU devices may be required in key substations where the DRZC needs measurement data for the restoration process.</p> <p>Detailed network design is required for the sites to incorporate the PMUs into the network and power system in</p>	<p>Medium Impact</p>

	a secure and safe manner. Security controls must be applied.	
Addition of replica DRZC solution to existing SCADA test environment (or isolated HIL environment)	<p>A replica testing environment is required for each DNO. The testing environment is used for the following:</p> <ul style="list-style-type: none"> • Testing configuration changes before applying to live environment • Testing patches before applying to live environment • Testing upgrades before upgrading on live environment • Training • Disaster recovery simulations • Pen testing 	Low Impact

Table 33 DNO change impact analysis to systems

7.3.3 Telecommunications

Change	Description	Impact
Power resilient communications network extending from DNO control centre to DRZC site	Currently the existing distribution comms network should extend to a potential DRZC site. The additional bandwidth as a result of the control and measurement data exchange will be [REDACTED]. This should be factored into the impact.	Medium Impact
Power resilient communications network extending from DRZC site to at least 1 Proportional Regulation DER site (Anchor Generator)	The distribution comms network is required to extend to an interface point at a DER PR site (e.g. anchor generator). The additional bandwidth as a result of the control and measurement data exchange will be [REDACTED]. This should be factored into the impact.	High Impact

Power resilient communications network extending from DRZC site to at least 1 Primary Balancing Control DER site (where PBC is not co-located with PR)	The distribution comms network is required to extend to an interface point at a DER PBC site (e.g. a site containing a load bank or BESS). The additional bandwidth as a result of the control and measurement data exchange will be [REDACTED]. This should be factored into the impact.	High Impact
Power resilient communications network extending from DRZC site to at least 1 Secondary Balancing Control DER site	The distribution comms network is required to extend to an interface point at a DER SBC site (e.g. wind farm or slow dispatch hydro plant). The additional bandwidth as a result of the control and measurement data exchange will be [REDACTED]. This should be factored into the impact.	High Impact

Table 34 DNO change impact analysis to telecommunications

7.3.4 Training

Change	Description	Impact
Regular DRZC operational training to be carried out	Regular training on test DRZC environment with a focus on the operational functionality of the DRZC scheme. Training should include: <ul style="list-style-type: none"> • Creating and applying PLC logic schemes • Interfacing DRZC with resources and ADMS • IEC 60870-5-104 integration • DNP3 integration • IEC 61850 integration • Administrator training • Synchrophasor management 	High Impact
DRZC security training to be carried out	Regular training on test DRZC environment with a focus on cyber security. Training should include:	Medium Impact

	<ul style="list-style-type: none"> • Identification of security threats through monitoring tools • Certificate management process training • Security best practice training when accessing critical systems • Network security best practice and training 	
Disaster recovery training for DRZC included in organisations training processes.	<p>Regular training on test DRZC environment simulating different disaster recovery scenarios to prepare staff for emergencies. Training should include:</p> <ul style="list-style-type: none"> • Simulated loss of power to DRZC, WAMS, ADMS • Simulated loss of comms between critical systems • Simulated Denial of Service (DoS) attacks • Simulated hardware or software corruption • Simulated malware infection to workstations connecting to critical systems • Simulated malware infection to critical system <p>Training exercise frequency shall be carried out at least yearly or for new staff members.</p>	High Impact
WAMS admin training	The addition of a WAMS in DNO environment for visualisation and offline analysis of synchrophasor data will require administrative training.	Low impact

	<p>Training shall include:</p> <ul style="list-style-type: none"> • Synchrophasor input and output stream configuration • PMU mapping and configuration • IEC 104 integration • TLS configuration • LDAP integration • Backups and restores • Disaster recovery <p>Training frequency shall be one-off, with follow up sessions available if necessary</p>	
ADMS training	<p>The addition of new ADMS configurations may require refresher training for control operators, along with expanding skillsets within organisations.</p> <p>Training may include:</p> <ul style="list-style-type: none"> • General functionality • Control engineering • System configuration • Network Display (Diagram) management • Symbol configuration • RT system configuration • System administration • SCADA tools and configuration • Disaster recovery <p>Training frequency shall be one-off, with follow up sessions available if necessary</p>	Low Impact

Table 35 DNO change impact analysis to training

7.3.5 Staff

Change	Description	Impact
No change	No change to staffing requirements	No impact

Table 36 DNO change impact analysis to staff

7.3.6 External Factors

Change	Description	Impact
Support for new systems from third party suppliers	Support for critical system (DRZC/ADMS/WAMS) by third party to ensure continuous operation and defect mitigation through support teams/channels.	Low impact
New VPN connection between third party support and organisation	To provide remote support for the critical BlackStart systems, a VPN connection from third party to organisation should be set up. This should include jump servers and user accounts as security controls	Low impact

Table 37 DNO change impact analysis to external factors

7.3.7 Security

Change	Description	Impact
Increased security awareness among operators	Security awareness should be a fundamental part of every party and/or individual who interacts with the entire DRZC system. For DNO, social engineering (i.e. a spoofed voice call from apparent DER/ESO operator) or malware infection (via email, cascading down from HMI workstation to DRZC) could result in a breach of the system. This may be achieved via regular awareness sessions, training, team meetings.	Low Impact
Integration of DRZC with security monitoring and event management	The DRZC is required to have the capability to securely transmit the following information:	Low/Medium Impact

	<ul style="list-style-type: none"> • Security event logs • Audit logs • System logs <p>For real-time alerting and offline analysis, these logs are required to be captured, visualised and stored in a SIEM or SOC environment</p>	
Integration of ADMS with security monitoring and event management	<p>The ADMS is required to have the capability to securely transmit the following information:</p> <ul style="list-style-type: none"> • Security event logs • Audit logs • System logs <p>For real-time alerting and offline analysis, these logs are required to be captured, visualised and stored in a SIEM or SOC environment</p>	Low/Medium Impact
Integration of WAMS with security monitoring and event management	<p>The WAMS is required to have the capability to securely transmit the following information:</p> <ul style="list-style-type: none"> • Security event logs • Audit logs • System logs <p>For real-time alerting and offline analysis, these logs are required to be captured, visualised and stored in a SIEM or SOC environment</p>	Low/Medium Impact
Additional certificate management to accommodate addition of DRZC and controller encryption	<p>As per the design documents, the requirement for selected protocols is encryption and authentication in transit. This is achieved (with the exception of IEC 61850) with TLS and/or VPNs. Digital certificates are required to be generated, distributed, renewed and revoked within the DRZC solution.</p>	Medium/High Impact

	<p>This requires an infrastructure to generate and distribute certificates to the DRZC, along with a means of exchanging client certificates with the TO and DER sites.</p> <p>The challenging aspect is the chain of trust derived from the root certificate authority (CA), where each organisation will sign the generated certificates with their own CA.</p> <p>A shared or 'bridge' CA can be used to generate root certificates for the independent organisations own root CA, or access to the other parties CA certificate are viable options. Security, network design and cost should be accounted for with both options.</p>	
<p>Updates to current disaster recovery strategies to account for DRZC solution</p>	<p>The introduction of new critical systems as part of the Distributed ReStart project requires new processes for the DNOs disaster recovery strategy. Business continuity planning with the organisations cyber security team is required to ensure the ongoing operation of DRZC and the ability to recover from a disaster. This includes detailed step-by-step procedures for different scenarios, yearly business continuity rehearsals with key stakeholders and yearly training for operational staff to ensure readiness.</p>	<p>Medium Impact</p>
<p>Changes to existing patch management processes to accommodate for additional</p>	<p>DRZC and field controllers require on-site patch updates with rollback procedures available. Patches must first</p>	<p>Medium/High Impact</p>

systems introduced as part of the DRZC	<p>be tested on a replica environment to ensure compatibility.</p> <p>Patches should be released for critical, high and medium security issues. Patches should be made available within 8 weeks if within the 3rd party's scope.</p>	
New key management processes with the addition of Key Distribution Centres design and implementation to accommodate IEC 61850 protocol usage	<p>As per the design documents, the requirement for selected protocols is encryption and authentication in transit. For IEC 61850 protocols, this is achieved using symmetric keys generated and distributed from a KDC.</p> <p>A KDC is used to automatically generate and distribute keys to group members, this requires detailed network design to ensure each group member has connectivity to the KDC.</p>	Medium/High Impact
Increase in data backup storage capacity to accommodate for additional systems introduced as part of the DRZC	<p>For WAMS, an additional 650GB is required in storage for configuration and 6 months full resolution data (backups on weekly basis)</p> <p>For DRZC, an additional 500MB (excluding PMU data for backfilling) is required in storage (backups on weekly basis)</p> <p>For PMU data on DRZC, the repository size is configurable and typically set between 1 - 5GB</p>	Low Impact
Addition of DRZC to organisations existing penetration testing scope	New critical system containing DRZC, ADMS and WAMS with unique configurations requires regular penetration testing to discover vulnerabilities at	Low Impact

	early stages. This testing should be carried out on the isolated testing environment in order to not disrupt normal operation. Testing environment should be replica of live.	
Increase of physical security measures in DRZC site	Site specific – the site hosting the DRZC is required to be physically secure to prevent unauthorised access.	Medium/High Impact

Table 38 DNO change impact analysis to security

7.4 Distributed Energy Resource

7.4.1 Interfaces

Change	Description	Impact
The DER site is required to interface with the DNO	Currently there is limited interfaces between DER sites and DNOs, however the DRZC brings a new requirement for DER sites to exchange data and voice with DNOs.	Medium Impact

Table 39 DER change impact analysis to interfaces

7.4.2 Systems

Change	Description	Impact
Addition of Field Interface Unit (FIU) controller into DER site	<p>A newly installed FIU is required for the Distributed ReStart project as a key component for interfacing the DER site with the DRZC. The FIU consists of either 1 independent or 2 redundant embedded devices that interface with the network using protocols such as IEC 104, DNP3 or IEC 61850-90-5 over Ethernet.</p> <p>Redundancy is determined by the availability of resources</p>	Medium Impact

	<p>(i.e. if two or more SBC sites are available in a zone, the requirement is for 1 independent FIU at each site, as redundancy is provided at a site level).</p> <p>The location of the FIU is fundamental to the design – the requirements for location are as follows:</p> <ul style="list-style-type: none"> • Power resilient communication channels (addressed in Section 5.3) • Power resilient site (72-hour backup power integrating into redundant controllers) <p>Detailed network design is required for the DER site to incorporate the devices into the network in a secure and safe manner. Security controls must be applied.</p>	
<p>Addition of PMU devices into DER site</p>	<p>Newly installed PMU devices may be required in key DER sites where the DRZC needs measurement data for the restoration process.</p> <p>For example, a Proportional Regulation (PR) site that does not have a co-located PBC resource (e.g. load bank) on site, requires exchanging measurement data only with the DRZC.</p> <p>Detailed network design is required for the sites to incorporate the PMUs into the network and power system in a secure and safe manner. Security controls must be applied.</p>	<p>Medium Impact</p>

Table 40 DER change impact analysis to systems

7.4.3 Telecommunications

Change	Description	Impact
Power resilient communications network on-site extending to the interface point of the DNO communications network. Critical DER systems and resource connections included on communications.	<p>The requirement for the DRZC is to extend the DNO communications networks to DER sites for data and voice exchange. However, up to and terminating at the DNO interface point, the DER is required to provide power resilient communications where a site is deemed critical for a successful BlackStart restoration sequence.</p> <p>This includes at least 1 PR site, 1 PBC site and 1 SBC site per distributed restoration zone.</p> <p>The additional bandwidth in the site as a result of the control and measurement data exchange will be [REDACTED]. This should be factored into the impact.</p>	High Impact

Table 41 DER change impact analysis to telecommunications

7.4.4 Training

Change	Description	Impact
DRZC operational training to be carried out	<p>Scheduled training from third party supplier with a focus on the operational functionality of the DRZC scheme. Training should include:</p> <ul style="list-style-type: none"> • Creating and applying PLC logic schemes • Interfacing DRZC with resources and ADMS • IEC 60870-5-104 integration • DNP3 integration • IEC 61850 integration • Administrator training 	Medium Impact

	<ul style="list-style-type: none"> • Synchrophasor management 	
DRZC security training to be carried out	<p>Scheduled training from third party supplier with a focus on cyber security. Training should include:</p> <ul style="list-style-type: none"> • Identification of security threats through monitoring tools • Certificate management process training • Security best practice training when accessing critical systems • Network security best practice and training 	Medium Impact

Table 42 DER change impact analysis to training

7.4.5 Staff

Change	Description	Impact
New staff may be required to facilitate the BlackStart restoration process	Due to the variability of DERs, additional staff may be required to co-ordinate the restoration procedure with the DNO. Additional security personnel may also be required to help protect the resources.	Medium Impact

Table 43 DER change impact analysis to staff

7.4.6 External Factors

Change	Description	Impact
Support for new systems from third party suppliers	Support for critical system (FIU) by third party to ensure continuous operation and defect mitigation through support teams/channels.	Low Impact

Table 44 DER change impact analysis to external factors

7.4.7 Security

Change	Description	Impact
Increased security awareness among operators	<p>Security awareness should be a fundamental part of every party and/or individual who interacts with the entire DRZC system. For DER, social engineering (i.e. a spoofed voice call from apparent DNO operator) or malware infection (via email, cascading down HMI workstation to FIU, and through to DRZC) could result in a breach of the system.</p> <p>This may be achieved via regular awareness sessions, training, team meetings.</p>	Low Impact
Integration of FIU with security monitoring and event management	<p>The FIU is required to have the capability to securely transmit the following information:</p> <ul style="list-style-type: none"> • Security event logs • Audit logs • System logs <p>For real-time alerting and offline analysis, these logs are required to be captured, visualised and stored in a SIEM or SOC environment</p>	Low/Medium Impact
Additional certificate management to accommodate addition of FIU and controller encryption	<p>As per the design documents, the requirement for selected protocols is encryption and authentication in transit. This is achieved (with the exception of IEC 61850) with TLS and/or VPNs. Digital certificates are required to be generated, distributed, renewed and revoked within the DRZC solution.</p> <p>This requires an infrastructure to generate and distribute certificates to the FIU controllers, along with a</p>	Medium/High Impact

	<p>means of exchanging client certificates with the DNO.</p> <p>The challenging aspect is the chain of trust derived from the root certificate authority (CA), where each organisation will sign the generated certificates with their own CA.</p> <p>A shared or 'bridge' CA can be used to generate root certificates for the independent organisations own root CA, or access to the other parties CA certificate are viable options. Security, network design and cost should be accounted for with both options.</p>	
<p>Changes to existing patch management processes to accommodate for additional systems introduced as part of the DRZC</p>	<p>DRZC and field controllers require on-site patch updates with rollback procedures available. Patches must first be tested on a replica system to ensure compatibility.</p> <p>Patches should be released for critical, high and medium security issues. Patches should be made available within 8 weeks if within the 3rd party's scope.</p>	<p>Medium/High Impact</p>
<p>New key management processes with the addition of Key Distribution Centres design and implementation to accommodate IEC 61850 protocol usage</p>	<p>As per the design documents, the requirement for selected protocols is encryption and authentication in transit. For IEC 61850 protocols, this is achieved using symmetric keys generated and distributed from a KDC.</p> <p>A KDC is used to automatically generated and distribute keys to group members, this requires detailed network design to ensure each group</p>	<p>Medium/High Impact</p>

	member has connectivity to the KDC.	
Increase in data backup storage capacity to accommodate for new FIU controller system	For FIUs, an additional 500MB (excluding PMU data for backfilling) is required in storage (backups on weekly basis) For PMU data, the repository size is configurable and typically set between 1 - 5GB	Low Impact
Increase of physical security measures in DER site	Site specific – the site hosting the FIU is required to be physically secure to prevent unauthorised access.	Medium/High Impact

Table 45 DER change impact analysis to security

8 Future Operating Service Models

8.1 Vulnerability Management

After initial implementation of the live and test environments for Distributed ReStart, it is essential to incorporate the systems into the organisations vulnerability management process. The test environment should be a replica of the live, housing the same operating system versions, patch versions, software versions and hardware specifications for each system. As discussed later in Section 3, once a software patch is made available the organisation should deploy and perform validation tests on the replica environment before applying to the live. Each step and change should be fully documented to ensure consistency between the environments.

Organisations should implement automated vulnerability scanning on the Distributed ReStart testing environment. Scans detect open ports within a system and perform service analysis which can be compared with a database of CVEs to determine whether a service contains a vulnerability, these vulnerabilities might be present within the libraries of the service. Scans will return a list of vulnerabilities with a severity scoring, typically based on the Common Vulnerability Scoring System v3 (CVSSv3), ordered by low, medium, high and critical. The severity is based on a number of factors, for example whether a vulnerability can be exploited remotely or only with physical access, if the vulnerability will breach the confidentiality, integrity or availability of the system (or a mixture of all three) or if it requires elevated privileges or not. The Centre for Internet Security (CIS) recommends weekly automated vulnerability scans (or more frequent).

Some common vulnerability scanners include Nessus or Nexpose. Scanners typically also provide some basic remediation advice to allow organisations to mitigate quickly against any vulnerabilities identified.

Once identified, organisations should assess the risk of each vulnerability, prioritising those deemed high and critical. Where possible, and to minimise the risk in a timely manner, the remediation advice from a scanner should be tested and validated on the test environment for high and critical findings. Assuming the fix does not impact the functionality of the systems, ensure a new scan is manually launched to verify the remediation advice for the vulnerability has been successful and the scan no longer reports the finding. After validation testing, apply the mitigation to the live environment.

Suppliers should be notified of any vulnerability found during scanning, this should be done through the supplier's support channels to allow the supplier to raise a defect and issue a patch for remediation. Suppliers may also provide remediation advice to mitigate against vulnerabilities. If no immediate remediation is available, the risk should be understood by the organisation and supplier until a patch is released. By understanding the attack surface and the potential threat the vulnerability poses, systems can be closely monitored to identify the initial signs of a breach.

8.2 Patch Management

Before policies and procedures are created within an organisation for patch management within the Distributed ReStart solution, inventory and current version lists should be generated and kept up to date. This list should include the core components of the Distributed ReStart system, along with any system that interacts with the network and the network devices themselves.

Once operational, ensure the inventory list contains the following:

- ADMS servers – current version of Linux/Windows, list of all dependencies and versions, list of installed packages
- FEP servers – current version of Linux/Windows, list of all dependencies and versions, list of installed packages
- IEMS servers – current version of Linux/Windows, list of all dependencies and versions, list of installed packages
- WAMS servers – current version of Linux/Windows, list of all dependencies and versions, list of installed packages
- PDC servers – current version of Linux/Windows, list of all dependencies and versions, list of installed packages
- Controllers – current version of OS, list of all dependencies and versions, list of extended libraries included
- PKIs and KDCs – current version of OS, list of all dependencies and versions, list of installed packages
- Firewalls and switches – current version of OS
- Workstation clients – current version of OS

Ensure testing and live environment are aligned.

8.2.1 Secure Patch Retrieval

Linux utilises GnuPrivacyGuard (GPG) to allow package owners to sign their packages and distribute GPG keys into the Linux package manager to verify the authenticity of updates. To ensure a package is not maliciously altered in transit, the package is signed using the GPG private key and tools such as 'rpm' or 'dnf' provide the functionality to verify the signed package using the GPG public key before installing onto the server. This ensures legitimate patches are downloaded and installed without replacements being made to packages that contain malicious code, bugs or backdoors.

Microsoft provide a mechanism for Windows called Authenticode, which is a code signing mechanism that uses various cryptographic techniques to verify software publisher and code integrity. Publishers sign software using a digital certificate provided by a Certificate Authority (CA) that the client can use to verify the authenticity of the publisher, as the root certificate is known by the client and the chain of trust can be verified.

Third party dependencies, such as Java or PostgreSQL, provide patch updates via online portals or directly from repositories. These packages are hashed and provided with a checksum to validate the authenticity of the package. Suppliers should regularly test products against new third party dependency patches to ensure no compatibility issues. Patch reports should be made available to organisations as part of Distributed ReStart running products that require third party dependency patch testing, if requested.

For patches relating to products that provide the core functionality as part of the Distributed ReStart, such as ADMS, Controllers and WAMS, suppliers should provide patches in a secure and timely manner. As above, suppliers should use a code signing mechanism on new patches to ensure the patch can be verified by the customer before applying to the test environment.

Suppliers should use a secure method with authentication to deliver the patch to the customer and provide a checksum (such as a SHA-2 hashed value) of the patch for verification of the integrity.

8.2.2 Patch Frequency

Patches are made available at different times – some are automated, some are manual, and some may be more frequent than others. This should be factored into the organisations patch management policy. The following table outlines an example policy for managing patches.

Patch	Frequency	Manual/Automated	Policy	Recommendations
Microsoft Windows	2 nd Tuesday of each month Ad-hoc for critical patches	Both	Use Windows Server Updates Services (WSUS) to automatically download updates locally. Use TLS to connect clients to WSUS. Perform analysis on updates and determine risks and priority (critical security updates prioritise over feature updates). Apply updates to test environment and test functionality. If successful, schedule downtime on live environment and apply update. Ensure up-to-date backup is available for rollback.	Automate patch testing on test environment and report on new updates. Perform automated validation testing and send report to security/IT team.

Linux	Typically ad-hoc	Both	<p>Ensure Linux machines are updated regularly using the distributions update command (e.g. yum update). Test updates on testing environment either manually or scheduled automatically. Tools like 'cron' can be used to schedule updates on frequent basis. Ensure each package marked for update is logged. Once validated, schedule downtime period and update live environment. Commands offer rollback features if required.</p>	<p>Automate patches on test environment and provide reports on updated packages. Perform automated validation testing with reports sent to security/IT teams. Use 'cron' to schedule on a weekly basis.</p>
Third Party Dependencies	Typically quarterly	Typically Manual (can be made automatic with scripting)	<p>Take two examples of third-party dependencies (Java and PostgreSQL database). Patches are released quarterly to the respective</p>	<p>Create automated patch management system for third party dependencies. Parse dependency repositories on a weekly basis and send an email to the security/IT</p>

			<p>online portals. Patch schedules should be known and downloaded when made available. Testing environment should be used for testing patches. Schedule downtime for live environments once patch has been validated. Ensure up-to-date backups are available for rollback.</p>	<p>team informing of a new patch update. If possible, create automated patch deployment to apply, test and report on patch updates on test environment.</p>
Product (Controllers, ADMS, WAMS)	Ad hoc	Manual	<p>Suppliers should have a matured vulnerability assessment process to identify new vulnerabilities within libraries as part of their secure software development lifecycle. Scans should be performed nightly, and any vulnerabilities should be categorised and added to next minor release. For</p>	<p>Ensure up to date documentation is available for updating patches. Utilise suppliers maintenance and support contracts to provide additional support when updating systems.</p>

			<p>critical security patches, these should be released within [REDACTED]</p> <p>Upgrade paths should be provided and followed on the test environment. Downtime scheduled on live once testing has been validated. Ensure up-to-date backups are available for rollback.</p>	
--	--	--	--	--

The testing environment for Distributed ReStart owned by the distribution network operators should reflect an exact copy of the live environment, with operating system patches and software patches aligned. Once the inventory list and a policy for each component is defined, along with a timescale for potential patch updates and schedules, the testing environment can be utilised to perform patch tests. Once a patch has been applied to the testing environment, organisations should wait a minimum of 48 hours before applying to the live environment, to account for any potential application-level memory leaks caused by updates to libraries.

All patch management policies and procedures should contain a rollback plan to account for unforeseen circumstances when applying new patches. Many products and operating systems will offer this functionality to quickly undo updates (for example, a Linux kernel update may inhibit an application from functioning correctly due to a change in threading, so Linux package manager can allow removal of installed updates). Organisations should check with providers about rollback functionalities, sometimes full backups may be required to be taken before an update if a rollback is needed.

8.3 Software Lifecycles

8.3.1 Operating Systems

Organisations should ensure up-to-date inventory lists include operating system information for each server, client or device in their infrastructure. This list should be used to plan upgrades accordingly before the software reaches the end of its lifecycle, where no further security updates are released, and vulnerabilities may be left open for exploitation.

8.3.1.1 Windows

For servers running Windows, Microsoft typically provide monthly quality updates for organisations or users running supported and licensed versions of their software. Quality updates include bug fixes, feature enhancements and security issue resolutions.

It is assumed the following Windows OS are included in the Distributed ReStart scope:

- Windows Server
- Windows Desktop

For these products, the typical lifecycle is:

Initial Release	End of Mainstream Support	End of Extended Support	Beyond Extended Support
Date the software is released	Date feature enhancement requests end. Security updates still available. Typically ~6 years after initial release.	Date non-paid security updates end. Typically ~11 years after initial release.	Provides paid support for security updates. Typically available for ~3 years after end of extended support.

Organisations as part of Distributed ReStart running the following should begin to plan to upgrade to a later (preferably latest supported and stable) version:

- Windows Server 2012 R2
- Windows Server 2008 R2 and earlier
- Windows 10 (SP 1809) and earlier

8.3.1.2 Linux

For servers running Linux distributions, updates are provided by the distribution on a frequent basis which may include updates to the Linux kernel, package updates and security fixes. The following commercially available Linux distributions may be used in the Distributed ReStart scope:

- Red Hat Enterprise Linux (RHEL)
- Ubuntu (Canonical Ltd)
- OpenSUSE (SUSE)

The typical lifecycle for Linux distributions, based off Red Hat Enterprise Linux are:

Initial Release	End of Full Support	End of Maintenance Support	End of Extended Lifecycle Support Add On	Extended Life Phase

<p>Date the software is released</p>	<p>Critical and important security updates. Errata - security, bug and enhancement updates. Typically ~5.5 years after initial release.</p>	<p>Critical and important security updates. Typically ~10 years after initial release.</p>	<p>Critical and important security updates. Typically available for ~2 years after end of extended support.</p>	<p>Access to documentation and limited technical support. No security, bug or enhancement updates. May be terminated at any time.</p>
--------------------------------------	---	--	---	---

For server operating systems, RHEL is likely the most common distribution in use in enterprise environments. Organisations as part of Distributed ReStart running the following should begin to plan to upgrade to a later (preferably latest supported and stable) version:

- RHEL 6 or earlier
- Ubuntu 14 or earlier
- OpenSUSE Leap 15.2 or earlier

8.3.2 Products

For systems running critical functionality for Distributed ReStart, such as Controllers, ADMS or WAMS – lifecycles should be managed between organisation and vendor. It is likely that new updates are released for security patches and new features that are requested by the organisation to further expand the capability of the systems. Furthermore, changes in technologies and cyber security will issue new roadmaps and organisations should ensure they are informed of upcoming roadmap features and work with vendors to provide details around upgrade paths and enhancements.

8.4 Hardware Lifecycles

8.4.1 Controllers

A controller is typically an embedded platform on varying types of hardware, due to the potential degree of variability with hardware, organisations should consult the vendor for information regarding the hardware lifecycles. Controllers are substation-rated hardware platforms, facing potential exposure to extreme environmental conditions and a variety of electromagnetic interference. For this reason, controllers must be able to withstand temperature changes, lightning strikes, radio frequency interference and more. Due to this, it is required that hardware lifecycles for controllers are carefully considered and inventory is maintained for efficient replacement.



[Redacted]

8.4.2 Servers

As a server's lifespan increases, its ability to perform at optimum capacity decreases, causing potential problems for resource-heavy software such as WAMS. Using HPE and Dell as examples, the typical lifecycle for server hardware is:

- Server launch date (date the server is released)
- Retirement date (date the server is discontinued for production)
- End of Life date (date the server is no longer supported)

Typically, companies will keep servers on the marketplace for 3 years before retiring. Once the retirement date is reached, support is usually offered for an additional 5 years. Organisations deploying systems as part of Distributed ReStart should ensure servers procured have their retirement date tracked and are migrated to new hardware before the End-of-Life date. It is recommended to migrate to new hardware every 5 years from initial operation.

8.4.3 Network Devices

Network devices such as firewalls and switches follow a similar hardware lifecycle to servers where typically, a supplier will release a retirement date for the selected product, from there an End-of-Life date is established and proceeding that date the product will no longer be supported for hardware faults. Using Cisco as an example, the supplier shall notify the customer 6 months prior to the retirement date of their product. Once retirement (end of sale) date is reached, support for hardware shall continue for 5 years. Organisations should ensure their network devices are migrated before the End-of-Life date.

8.4.4 PMUs/RTUs

For Phasor Measurement Units (PMUs), the hardware lifecycle varies from device to device. As these devices are substation rated and are connected into the power system network, they are typically more fault tolerant than traditional IT network devices. They consist of no moving parts and are tested in vigorous conditions to ensure electromagnetic interference and certain extreme conditions do not hinder their ability to operate.

[Redacted]

- [Redacted]
- [Redacted]

[Redacted]

[Redacted]

8.5 Changes in Cyber Security

The next 10 years may see a lot of changes in the world of cyber security, especially around the security of industrial control systems. The convergence of IT and OT systems demands an increase in security controls and defence in depth approach to protect the infrastructure that controls the grids around the world. There has been a clear influx in targeted attacks on critical national infrastructure in recent years and with the transition to digital energy this is likely to become more prevalent than ever. Technologies are always evolving and at rapid rates, while this is beneficial for the organisations trying to protect their assets, it also means that attackers are equipped with more sophisticated tools than ever to infiltrate systems and cause the maximum level of destruction.

Below are some areas that should be monitored over the coming years with a focus on a Distributed ReStart system:

- Targets – the main area of focus for Distributed ReStart. The increase in attacks against ICS environments in recent years indicate that cyber criminals are moving from business disruption and financial gain to weaponised attacks with the potential to cause physical harm or disruption to a nation. Attacks by nation-states for political gain on critical national infrastructure may become a huge risk, with Distributed ReStart it is critical that the infrastructure is secure by design to the highest possible capabilities.
- Quantum computing – encryption is a key defence mechanism for protecting the data within Distributed ReStart. The designs show the use of asymmetric encryption to securely transmit data between organisations. However, it is well-known that quantum computing breaks conventional asymmetric encryption and attackers equipped with more sophisticated equipment may have the ability to bypass some of the security controls in place. It is believed that symmetric encryption algorithms (such as AES) are quantum resistant.
- Biometrics – increasingly more popular in today's age (e.g. facial recognition on smartphones to authenticate), biometrics and the use of 'three-factor' authentication may be required when accessing the critical systems in Distributed ReStart, adding more security for users authenticating and accessing resources. Fingerprint and iris scanning, facial and voice recognition are all viable options.
- Artificial intelligence – the use of AI in cyber security is likely to be a massive contributor to the defence of organisations assets. Likewise, it is likely to be a key part of an attacker's arsenal for sophisticated attacks. AI could provide the ability for threat detection and prevention software to rapidly identify new and unknown anomalies in the network in real-time. Learning the behaviour of attackers could be a key factor in the success of new-age IDS and IPS. On the other hand, attackers may use AI to bypass bot and threat detection software by learning and mimicking the behaviour attributes of a system operator when accessing systems. Voice synthesis tools could be used within malware to record and generate speech to bypass biometric defence mechanisms.

8.6 Transition to IEC 61850

The designs for secure network and data flows in the Distributed ReStart system included the following protocols in scope:

- IEC 61850-8-1 GOOSE
- IEC 61850-9-2 SV
- IEC 61850-90-5 R-GOOSE

- IEC 61850-90-5 R-SV

The designs demonstrated the methods for securing these protocols in accordance with IEC 62351, discussing the use of key distribution centres to centrally generate and distribute keys to group members, allowing group members to encrypt and authenticate messages for secure transmission. A key factor for the current implementations for IEC 61850 protocols that hinders the use for Distributed ReStart is the inability to securely transfer data cross-party. Adequate security measures are a challenge when organisations are required to distribute their private keys among different organisation devices or when access is granted to the private KDC across networks.

Another factor to take into consideration is the limited use of IEC 61850 protocols in the current industry, with many power systems and industrial control systems still using the older, more widely compatible protocols for SCADA, control and measurements. Many devices, such as legacy RTUs and PMUs, do not support the use of 61850 and results in a major upgrade plan to begin the transition to their use.

As technology advances and legacy software begins to fade out, the industry may shift towards more abundance with the 61850 protocols, bringing security by design into the protocol stack. Future implementations of 61850 utilising mesh VPNs and more robust technologies may allow for cross-party data exchange, without adding the additional complexity of key management.

9 Appendices

