GE Digital

Distributed ReStart
Lot 2 – Requirements Phase

Final Report

Author:	**Conan Malone, Sean Norris, Roger Jefferiss, Douglas Wilson, Andreas Glatz, Tony Nutley**
Reference:	**GE-D_RESTART-DRZC_CYBER_REQUIREMENTS**
Version:	**3**
Date:	**09/09/2021**

imagination at work

Contents

Figures

Tables

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
MITS	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 addresses the requirements for cyber security and resiliency within the Distributed ReStart project as part of Lot 2. There is a parallel workstream in Lot 1 that addresses the functional design specification which details the processes and interactions between the components of the system and the interactions with operators and field equipment. This report focuses on the security between the components, networks, users and organisations.

The report initially analyses the current infrastructure in place at the different partner levels, from ESO to TO, down to DNO and DER levels. The analysis highlights what communications channels, data and systems are currently in place that may be utilised for a BlackStart. Baseline security requirements are also highlighted to provide the partners with a delta between the current infrastructure and an adequately secure infrastructure. The requirements are expanded with best practice for communications, networks, protocols, and system configurations. By following the best practice guidance, the design stage of the project shall utilise these recommendations to develop a secure architecture that aligns with the functional design specification. Options for recovering from catastrophic events (such as loss of critical systems or cyber-attacks) are also highlighted in this report, where options shall be discussed in workshops and taken forward into the design phase.

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 Initial Architecture Design

While this report focuses on the analysis of the communications systems in place and requirements and best practice for a generic DRZC model, it is useful to describe the initial proposals for the architecture and components required for context. This was used to direct the analysis for this report and therefore is an important starting point. The draft architecture shown in Figure 1 was based on a system around the Chapelcross area, however this can be adopted to the appropriate network areas. The following description of components and their locations and functions was extracted from the detailed designed specification being created under lot 1 of this project. The same components would be applicable to other study sites, but locations would change. Again, the purpose of this is to highlight the components required/involved in the BlackStart scheme by which to inform the communication analysis.

Table 1: Draft sample initial component and function proposal

Component	Location	Function
Phasor Measurement Units (PMU)	Main Interconnected Transmission System (MITS) Stevens Croft Anchor, Load Bank, BESS1 Chapelcross GSP T1 33&132kV Chapelcross GSP T2 33&132kV	V&I phasors + frequency at 50FPS, streamed to main DRZC controller (Chapelcross 33kV SS) and central WAMS server. Data is streamed in real-time across the network as defined by UDP IEEE.C37.118 protocol. PMUs configured as P-class for low latency
Remote Terminal Units (RTU)	Minsca WF / BESS2 Ewe Hill WF Chapelcross 33kV feeders	RTU data is sufficient at Secondary Balancing Control sites.
DRZC	DNO Control Centre Stevens Croft Minsca WF / BESS2 Ewe Hill WF Chapelcross GSP	Chapelcross controller may host the main DRZC scheme. Control signals are relayed to resources via a range of protocols depending on latency requirements. The DRZC can also act as a PDC to forward measurements to the DNO and can be shared from there to the transmission owner and/or operator as required. All controller locations handle encryption and protocol conversion etc. as per cybersecurity requirements outlined in Section 5.
PTP Source	Chapelcross Grid SS	Provides PTP signals to synchronise range of DRZC devices, based on IEEE-1588 protocol
Resource Interface	Resource locations	Interface to resource control systems (within resource control system) that defines communications protocol
TO-DO link		Communications channel between DNO and TO/TSO to share PMU and DRZC data over IEEE.C37.118 2011 (rev 2014) protocol
DMS	DNO Control Centre	Primary monitoring tool for overall ReStart process and sequences. Data point sent via

		DRZC and WAMS over IEC 60870-5-104, with ADMS as the Master.
EMS †	TSO Control Centre	NGESO monitoring. Information exchanged between DMS and EMS to be defined based on organisational model
NTP	DNO Control Centre	Provide NTP source for WAMS/control monitoring
WAMS/control monitoring server (PDC + Applications)	DNO Control Centre	Store PMU data and DRZC control status to enable DRZC scheme to be audited. Both TCP IEEE.C37.118 and UDP IEEE.C37.118 streams can be configured with data observed via the workbench UI. Relevant data can be streamed to DMS over IEC-60870-104
Workbench UI	DNO Control Centre	JWS UI linked to WAMS server over TCP HTTPS.
DRZC Admin	DNO Control Centre	DRZC controller admin to manage settings and thresholds
Other DRZC	Other DRZ islands	Potential to link multiple DRZC's under one DNO region for possible distribution resynchronisation before transmission connection

2.1 Architecture

The draft architecture is shown in Figure 1**Error! Reference source not found.** and comprises the key components which make up the Restart control scheme:

- ESO EMS
- DNO ADMS
- DRZC Controller
- PMUs at resynchronisation boundaries
- Slow balancing resources (wind farms)
- Fast balancing resource (Load Bank/Battery)
- Anchor Generator

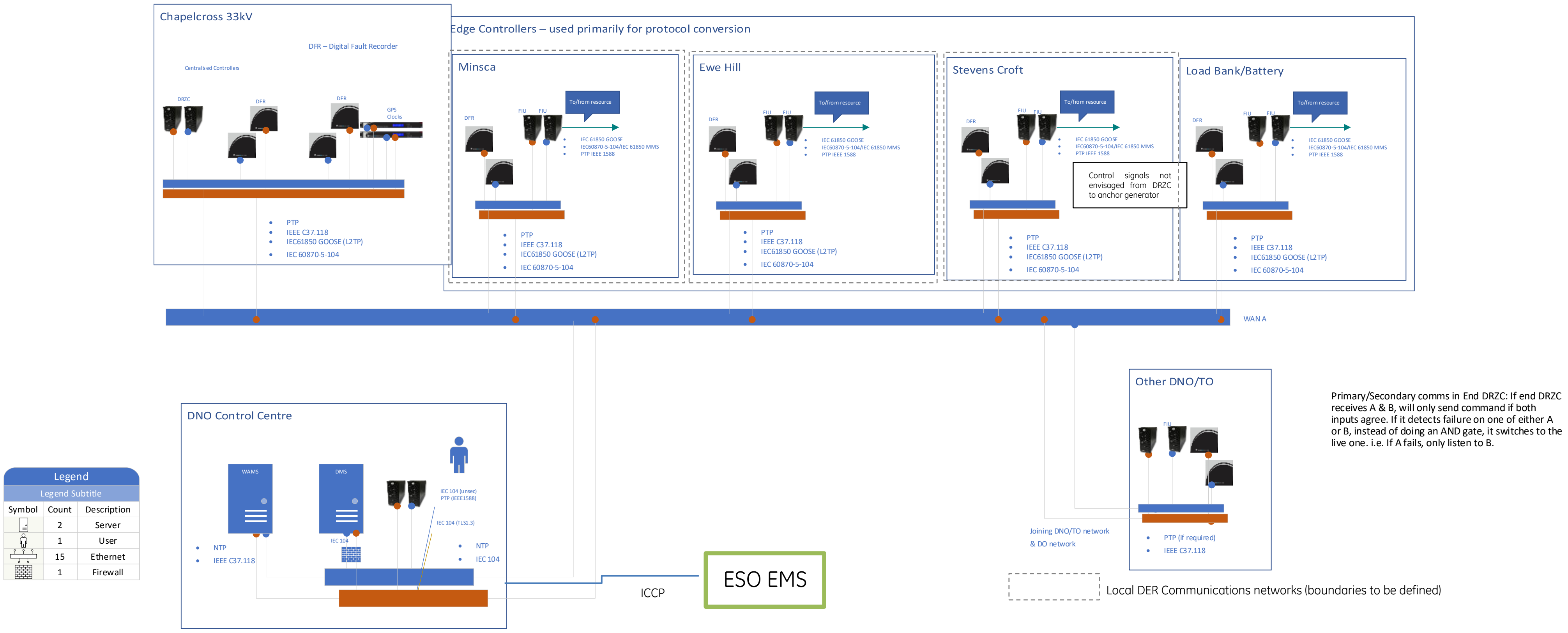
For this analysis, workshops were held with key stakeholders who would be owners/operators of these key components. The following mapping was deduced from these workshops:

Table 2: Roles and asset mapping

Owner/Operator	Assets/Roles
NG ESO	ESO EMS
TO	PMUs
DNO	ADMS DRZC RTUs

	PMUs Fast balancing resources*
Generator sites	Anchor Generator Fast balancing resource*
DERs (e.g. SPR)	Slow balancing resources Fast balancing resources*

*Fast balancing resources may not be fixed to a single operator, and therefore could be owned by any of DNO, generator or DER sites.

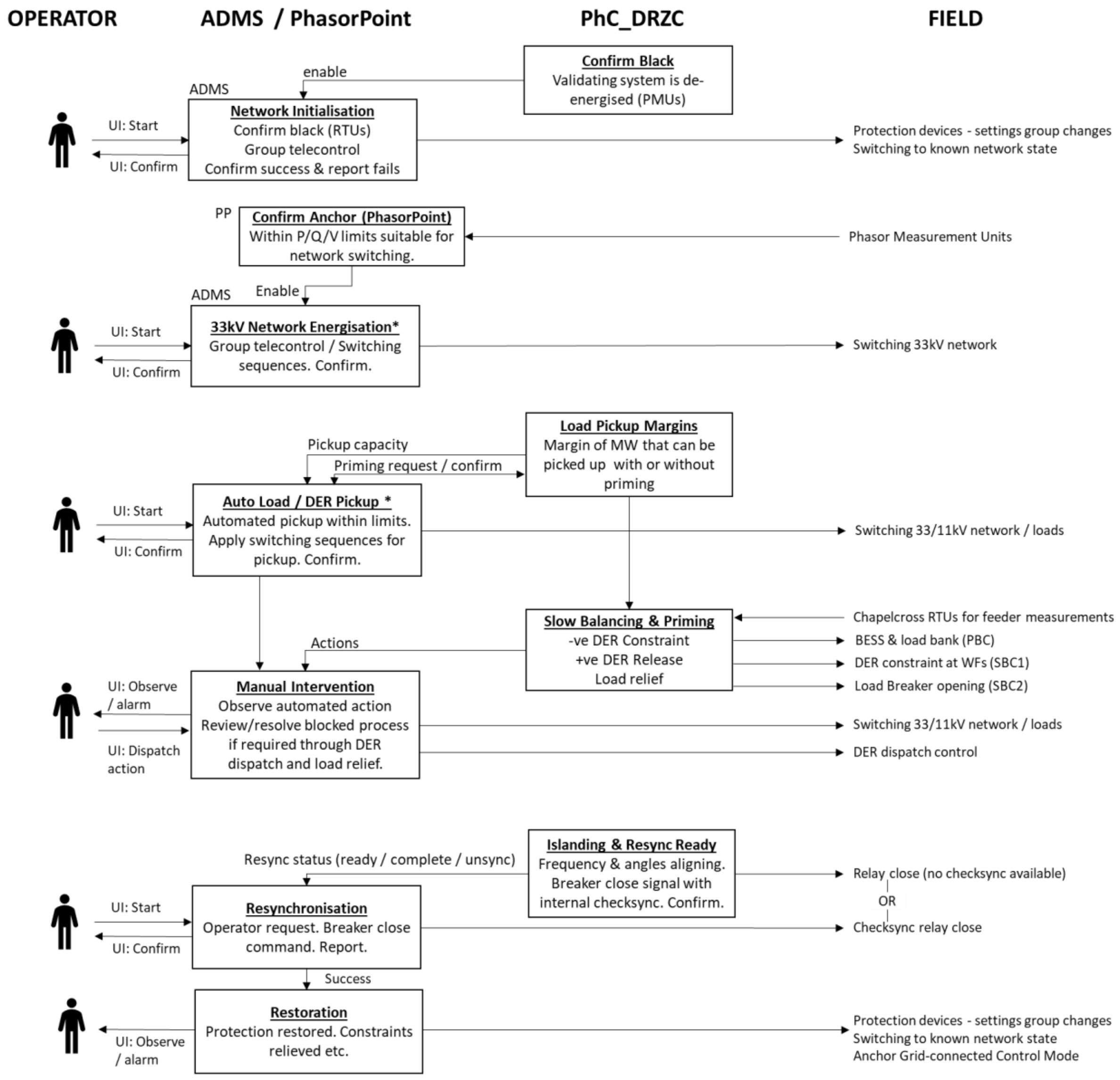


Primary/Secondary comms in End DRZC: If end DRZC receives A & B, will only send command if both inputs agree. If it detects failure on one of either A or B, instead of doing an AND gate, it switches to the live one. i.e. If A fails, only listen to B.

Figure 1 Draft Architecture for Restart Control Scheme prior to requirements refinement

2.2 Process diagram

The process of using the DRZC function from the operational perspective is described in which was based on the Lot 1 detailed design specification. The roles of operator, ADMS, DRZC and field are shown and additional breakdown between DNO and DER has been added to the field components based on likely ownership (e.g. a DER will control their own resources while a DNO will control their own field devices). This diagram can be used to further show the interaction between the various components in the full sequence. This chart was used again to steer the analysis of the various parties that would be involved in the BlackStart scheme to further define the boundaries of responsibilities. For example, anchor generators are not currently envisaged to need control signals from the DRZC while DER sites would have this requirement.


OPERATOR
ADMS / PhasorPoint
PhC_DRZC
FIELD
Confirm Black
Validating system is de-energised (PMUs)
enable
ADMS
UI: Start
UI: Confirm
Network Initialisation
Confirm black (RTUs)
Group telecontrol
Confirm success & report fails
Protection devices - settings group changes
Switching to known network state
PP
Confirm Anchor (PhasorPoint)
Within P/Q/V limits suitable for network switching.
Phasor Measurement Units
ADMS
Enable
UI: Start
UI: Confirm
33kV Network Energisation*
Group telecontrol / Switching sequences. Confirm.
Switching 33kV network
Load Pickup Margins
Margin of MW that can be picked up with or without priming
Pickup capacity
Priming request / confirm
UI: Start
UI: Confirm
Auto Load / DER Pickup *
Automated pickup within limits. Apply switching sequences for pickup. Confirm.
Switching 33/11kV network / loads
Slow Balancing & Priming
-ve DER Constraint
+ve DER Release
Load relief
Chapelcross RTUs for feeder measurements
BESS & load bank (PBC)
DER constraint at WFs (SBC1)
Load Breaker opening (SBC2)
Actions
UI: Observe / alarm
UI: Dispatch action
Manual Intervention
Observe automated action
Review/resolve blocked process if required through DER dispatch and load relief.
Switching 33/11kV network / loads
DER dispatch control
Islanding & Resync Ready
Frequency & angles aligning. Breaker close signal with internal checksync. Confirm.
Resync status (ready / complete / unsync)
Relay close (no checksync available)
OR
Checksync relay close
UI: Start
UI: Confirm
Resynchronisation
Operator request. Breaker close command. Report.
Success
UI: Observe / alarm
Restoration
Protection restored. Constraints relieved etc.
Protection devices - settings group changes
Switching to known network state
Anchor Grid-connected Control Mode

* Operator will initiate a sequence and check for success. Sequence may include one or more staggered events to minimise disturbance, checked at each stage to ensure that the action can be taken within performance limits. The ADMS will automatically choose if priming is needed for a load pickup and instruct PhC_DRZC if required. If a sequence cannot be completed, ADMS will report as a warning and proceed to the next stage until full procedure is complete. Operators then have opportunity to resolve issues manually.

Figure 2 Operational perspective on the distributed restart process

2.3 BlackStart Sequence

According to the staged process (SPEN), the DRZC is mainly used for control in Stages 3 through 6. The anchor generator start-up is monitored with phasor measurements, and once the anchor generator is established and operating in frequency regulation mode, the control processes are enabled and operate through the network energisation, load pickup and island running stages, as well as supervising the resynchronisation.

Stage 1 The network is reconfigured for Black start using switching sequences and protection settings groups deployed from the ADMS. There is no DRZC involvement in Stage 1.

Stage 2 The anchor generator is started by a local process determined by the generator operator, monitored using phasor measurements using WAMS or control monitoring to observe the stability in the start-up process. WAMS provides a status indicator to ADMS that is required for ADMS to allow the operator to proceed to the next stage. DRZC control functions of fast and slow balancing are initiated at the end of Stage 2.

Stage 3a Network energisation is observed using the phasor measurement infrastructure. Voltage control for network energising is achieved with local control without control intervention. However, there is a risk of unplanned load or generation trips in the island during network energisation and the DRZC will maintain the power balance and control margins to maintain frequency stability through such events.

Stage 3b Automated load and generation pickup sequences are initiated by the operator. The DRZC triggers Primary Balancing Control (load bank/BESS) using the Fast-Balancing approach in order to keep RoCoF and frequency within acceptable limits. Slow Balancing will follow up actions and redispatch between Secondary Balancing Control and the Primary Balancing Control to ensure control margin is maintained. Proportional Regulation margins are maintained indirectly through Slow Balancing control.

Stage 4 Island running requires frequency management processes to maintain a stable frequency and to ensure that sufficient regulating margin is available. During island running, load drift and renewable generation output change the balance of the island, resulting in the Proportional Regulation governor function at the anchor generator to change output. If the anchor generator output approaches the limits of its regulating capability, a rebalancing action is be taken to adjust Primary Balancing Control (the load bank) if there is headroom, or Secondary Balancing Control (preferably DER dispatch; load trip if necessary). If a disturbance occurs during Stage 4, Fast Balancing can also be triggered if the event is severe, followed by Slow Balancing.

Stage 5 Resynchronisation requires angle and frequency differences to be measured at PMUs on each side of the resynchronisation boundary. An indicator is provided to the operator to show when the frequency and angle difference values are within the pre-set limits. Once the frequency difference is within limits, the operator can arm the synchrocheck relay. The operator can then observe whether the resynchronisation was successful or not, and if not, there is immediate feedback to improve the conditions for another attempt.

Stage 6 Once continued successful grid-connected operation is confirmed by DRZC (typically within around 10-15s), the anchor generator governor can be switched to constant power and fast and slow balancing processes can be disabled. Any other changes such as restoration of grid-connected protection and earthing can be initiated by the ADMS once the successful synchronisation check is received.

Stage 7 The zone control may transition to Virtual Power Plant (VPP) mode to provide further services for the wider grid restoration process.

2.4 Requirements for data and assumptions

The following have been gathered from the detailed design specification and outline the background to what type of data is currently assumed to be required for the BlackStart scheme. The data described below will be expected to go via the communications systems that will be designed as part of this project.

Table 3: Data requirements and assumptions

Assumption	Description
DRZ protection settings updated via ADMS with DRZC control settings activated	The DRZC requires thresholds and settings to operate. DRZC based on G99 (ENA) settings with additional margins. The actual island protection settings will be less restrictive compared to the DRZC, to allow the DRZC to manage island frequency with protection operation activating as a last resort. Generation-based RoCoF and frequency protection settings are not changed, noting that more recent 1Hz/s RoCoF loss of mains settings are assumed. Network protection settings such as overcurrent can be changed with SCADA commands to select between protection settings groups between islanded and grid connected. The DRZC system does not manage individual protection settings. The protection settings themselves are out of scope of this project.
Anchor generator as grid-forming source	A synchronous generator is the grid forming source to enable load and DER to be connected. Power electronic converted generation may be used as grid-forming in the future but is assumed to be grid-following in this design
DER capability	The capability of the resource should be available via direct measurement and thresholding or directly from the resource where appropriate i.e. windfarm power available. Information should be provided on the interfacing to the resources i.e. ability of the resource to take a trigger signal and a MW setpoint value
DER power response	The DER power response should closely follow DRZC setpoints sent. Back-up control can be specified in future to take further action if the selected resource fails to deliver the requested response but is not included in this phase of the design

DER Availability	Anchor generation and load bank will be available at a minimum. Certain DRZC functions (slow balancing) will only be activated if DER and sheddable load is available.
DER Power Available Measure	For intermittent resources that participate in control, it is assumed that a Power Available signal will be available over SCADA, indicating how much power can be available if requested.
Max number of resources	The DRZC can manage up to 24 separate resources per zone, comprising 6 Proportional Regulation (PR) including the anchor generator and other frequency proportional generation, 6 Primary Balancing Controls, 6 Secondary Balancing Control Type 1 (SBC1, normally dispatchable renewable generation) and 6 Secondary Balancing Control Type 2 (SBC2, normally sheddable loads).
DRZC only manages frequency-based constraints	The DRZC will only manage frequency-based constraints in the DRZ. Voltage and oscillation-related issues are not seen as a concern in the Chapelcross simulations, with voltage control being local. Additional constraints and control may be added in future if required.
DER operation in very low system strength and inertia systems	Enough system strength is available to enable DER to be connected. In future, the system strength and inertia could be estimated and compared against the DER requirements. DER control modes could be adapted to manage very low system strength conditions.
Maximum sustainable load and generation loss should be specified.	The DRZC will report load pickup capability before each load block, which can be compared to the maximum sustainable load and generation loss
PMU locations	PMU measurements are required at locations outlined in the detailed design specification. It is currently expected that PMUs will be installed on the DNO side of the systems and therefore IEEE C37,118 data is not expected across the DER/DNO boundaries.

2.5 Information Exchange for scheme

The following table was based on the testing setup being designed for the Detailed Designed Specification which is based around an Opal RT for the power system model. As the test system was designed to be representative of a realistic setup, many of the components are common between the test and roll out designs.

In the table below, a device called a “FIU” is mentioned. This is a “Field Interface Unit” and is based on the DRZC platform. Its main role is to act as a gateway for encryption of data, e.g. where IEC

104 TLS is required, or as a method to secure the IEEE C37,118. Therefore, it will be used to secure the endpoints of the system.

Currently IEC 61850 GOOSE is proposed for the test system as the real time simulators typically utilise the GOOSE protocol for control inputs. However, for the trial or demonstration sites, it is currently expected that this would be IEC 104 instead of IEC 61850.

The following table defines the data sources and sinks, protocols and the types of data being transferred.

Table 4: Data information exchange for BlackStart scheme

From	To	Protocol	Data transferred
PMUs	FIU	IEEE C37.118 (LAN)	Synchrophasor measurements
RTU	FIU	IEC 104 (LAN)	RTU measurement data (V, P, Q, breaker status)
FIU	DER	IEC 104 (or GOOSE roadmap) (LAN)	Setpoints for generator, BESS and load bank(s) Breaker open/close commands for loads
DRZC	FIU	Encrypted IEC 104 (WAN)	Setpoints for generator(s) with slow control
DRZC	FIU	Encrypted IEC 104 † (IEC 61850-90-5 R-GOOSE roadmap) (WAN)	Setpoints for BESS & load bank with fast control
FIU	DRZC	IEEE C37.118 with TLS (WAN)	Synchrophasor measurements
FIU	PDC	IEEE C37.118 with TLS (WAN)	Synchrophasor measurements
FIU	FEP	IEC 104 (WAN)	RTU measurement data (V, P, Q, breaker status)
FEP	FIU	IEC 104 (WAN)	Breaker control
DRZC	FEP	IEC 104 (WAN)	Load pickup capability values Operator warning/alarms Information/status of actions taken for display and logging
DRZC	PDC	IEEE C37.118 with TLS (WAN)	Key analogue values and digital status relating to actions.
WAMS	FEP	IEC 104 (WAN)	Zone black validation
FEP	Protection Devices	IEC 104 (WAN)	Protection settings group changes

2.6 Roles and Responsibilities

The functional roles are shown in Figure 3 with ESO at the top. The process would start with ESO communication to DNO which is understood to be via a dedicated phone channel. The ESO will not have direct control to the BlackStart systems within the DNO networks. It will be a requirement however to obtain visibility from the scheme from a set of the DNO assets (including the DRZC). This can be done using the existing communications.

The DNO will have the main operational role in the scheme via the ADMS and DRZC. They will receive data from across their network from their own assets and data from the DERs where required for the purposes of BlackStart. They will also issue control signals to both their own assets and to DERs via the DRZC. There are expected to be resources such as load banks or batteries in the system to act as fast balancing resources. The ownership of such assets may be under the DNO or the DER, but these assets are critical components in maintaining stability of the network and will therefore have more stringent requirements for communications.

Finally, the DERs are responsible for provision of the service through active/reactive power balancing. The DERs will need to provide the BlackStart scheme with information regarding the state of the asset and metrics associated with their capability. They will also be required to receive commands from the BlackStart system to adjust outputs of generation (or load/battery if DER owned).

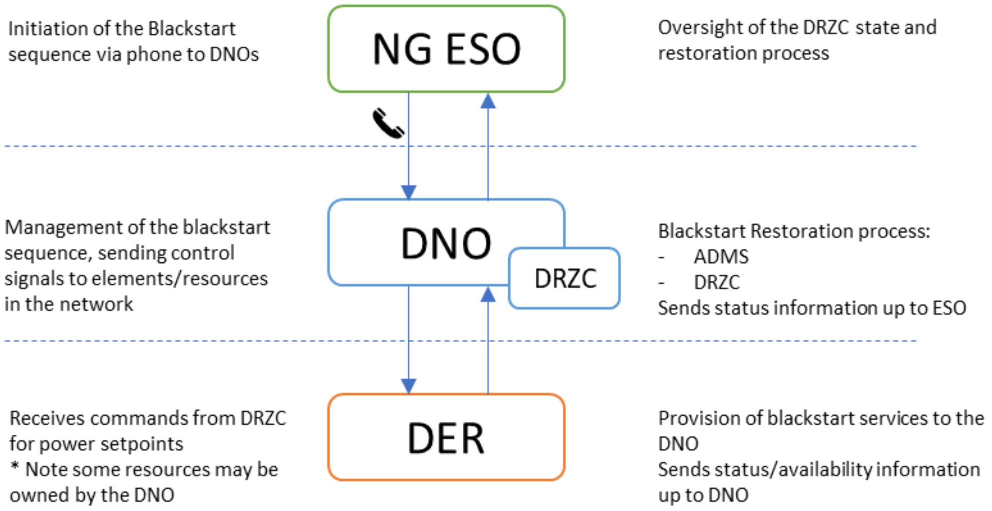

Initiation of the Blackstart sequence via phone to DNOs
NG ESO
Oversight of the DRZC state and restoration process
Management of the blackstart sequence, sending control signals to elements/resources in the network
DNO
DRZC
Blackstart Restoration process:
- ADMS
- DRZC
Sends status information up to ESO
Receives commands from DRZC for power setpoints
* Note some resources may be owned by the DNO
DER
Provision of blackstart services to the DNO
Sends status/availability information up to DNO

Figure 3 High level overview of functional roles and boundaries

Like the above, Figure 4 shows the same flow of data and separation of roles however this time from a security perspective. Since the ESO have a direct voice communications channel to the DNOs to initiate BlackStart – the first line of defense should look at real-time monitoring of the network and staff training to combat social engineering. Voice lines can be hijacked and a wrongful initiation of BlackStart may lead to some disruption of the network.

At the DNO level, network security is fundamental. The DRZ controller sits on the DNO network and interacts with DNO control rooms and DER sites. Ensuring that the data retains its integrity over wide area communications, comes from a reputable source and is safe from snooping is essential for the secure delivery of BlackStart. As the DNO will be interfacing with multiple participants and partners, protection mechanisms at the boundaries of the DNO networks and ESO/DER networks help minimise the attack surface as the entry attack vectors begins to increase.

From small to large scale DER sites, physical security is important when secluded locations with potentially unmanned facilities are a key player in the delivery of an automated BlackStart restoration phase. Should there be a lack of physical security mechanisms, on site devices and security controls may be breached at a key time in the BlackStart process. As above, boundary protection between DNO networks also serves as a key part in the secure design of the automated DNO model.

Power resilient communications at each level is a core principle in the secure design for DRZC schemes. If there is a loss of communications at any level between participants, this can affect the outcome of a BlackStart.

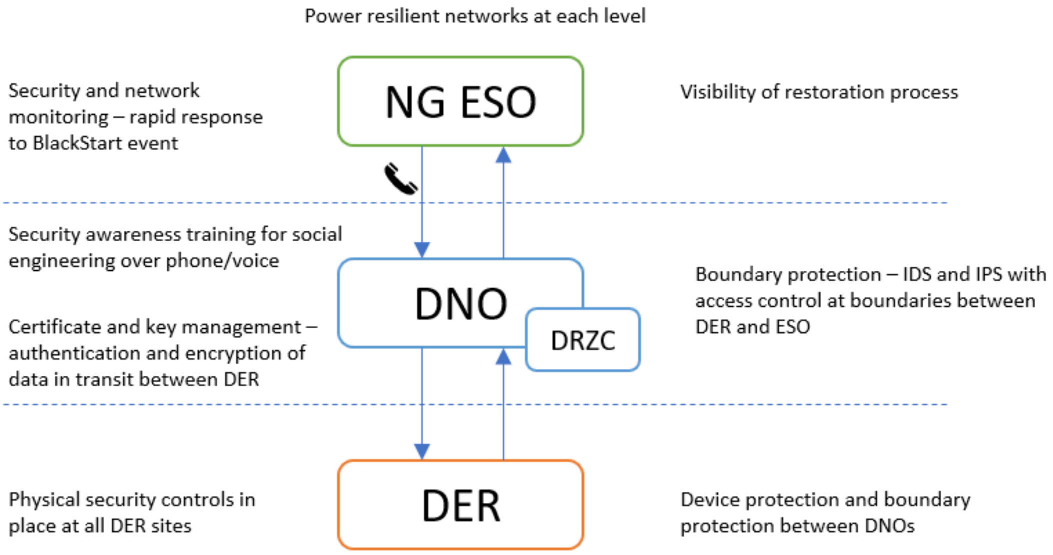

Power resilient networks at each level
Security and network monitoring – rapid response to BlackStart event
NG ESO
Visibility of restoration process
Security awareness training for social engineering over phone/voice
DNO
DRZC
Boundary protection – IDS and IPS with access control at boundaries between DER and ESO
Certificate and key management – authentication and encryption of data in transit between DER
Physical security controls in place at all DER sites
DER
Device protection and boundary protection between DNOs

Figure 4 High level overview of security protection and boundaries

3 Overview of Current Infrastructure

This section provides and overview of the existing communications technologies, power resiliency, data available and interconnections between participants of BlackStart. The section is broken down by each Partner level and splits the different focus areas into sub sections which is then compared in Section 4. Information within the following sections has been collected from workshops between BlackStart Partners, where direct questions and discussions aided in the retrieval of information needed to complete this analysis.

3.1 National Grid Electricity System Operator (NGESO)

3.1.1 Communications technologies

The main network for providing the secure connectivity of substations and control centres in England and Wales is the National Grid Operational Telecommunications (OpTel) network. The network consists of 10000km pairs of optical fibre and interconnects with the DNOs and Scottish TOs to provide secure transmission of control, telephony, and SCADA data. The network also provides leased circuits to third parties locations.

3.1.2 Protocols

- ICCP link with DNOs for visibility of distribution networks
- IEC 60870-5-101 to site from IEMS
- IEC 60870-5-104 for interaction with third parties
- IEEE C37.118 for Synchrophasor data

3.1.3 Power resiliency

The network is highly resilient with no single point of failure; a key factor in the event of a BlackStart. It utilizes SDH protocols to transfer digital information over the physical optical fibre lines, allowing for automatic switching to alternative paths in the event of a channel failure. In the event of a primary channel failure, the SDH network switches to the secondary alternative path resulting in a loss of resiliency but no loss of service. Service Level Agreements are in place to fix any physical faults in the network, which is discussed further in Section 5.

In the event of a BlackStart – sites are separated from the transmission network and continue operation using backup power supplies. Auto start generators with fuel reserves of 168 hours at key sites, 52 hours at other sites and at least 5 days at control centres are employed.

3.1.4 Control centres and sites

The OpTel network interconnects some 300+ substations and multiple control centres, giving the network the ability to securely transmit data and voice between DNOs and TOs. The network connects to power resilient Multiplexers on site, which are dual fed from battery systems to achieve the resiliency. Typically, 2 independent fibre routes will feed into substations, and 3 independent fibre routers into the control centres.

The OpTel network carries the NGESO telephony network or 'control telephone' which is used for normal operations and BlackStart voice communications between NGESO and other BlackStart participants (such as the Scottish TO and UK DNOs). The dedicated network offers priority calling and utilises 2 different voice channels, the 'green telephones' for normal operations and 'black telephones' for BlackStart communications. The voice link for BlackStart takes priority over the normal operations link.

3.1.5 Interconnections with the DNOs

The NGESO IEMS interfaces with the UK distribution network operators including SPEN and WPD. The connection is established via ICCP link between the IEMS and the DNOs ADMS/DMS and exchanges real-time data between the systems. The ICCP link provides NGESO with visibility of the distribution networks in the event of a BlackStart. ESO do not currently have ICCP links with all DNOs, however, this is planned and is assumed in place for DRZC project. It is currently a requirement to have ESO visibility of some of the DNO assets including DRZC switching but will not extend to control. The detailed list of this visibility will be included in later design stages, but for this exercise, the purpose is to identify the channels by which to transfer such data from DNO to ESO.

In the proposed DRZC scheme, the DRZC must interface with the DMS on the distribution networks to exchange data for control, for example the DRZC will tell the DMS if loads are ready to be switched. (Refer to 3 for the roles and interactions). Due to this, NGESO cannot control the distribution networks without a mirrored DMS system for each DNO (which is out of scope for the DRZC scheme) and instead will only receive visibility of the networks from the DRZC/DMS systems.

3.2 Distribution Network Operators

The proposed DRZC controller architecture relies on the communications and networks of the DNOs to coordinate with the independent DER sites to build power islands and bring generation into the distributed resource zones to re-energise the Distribution and Transmission High Voltage Networks. Analysis of the distribution networks and how they communicate with the DER sites is key in understanding the requirements needed for the central controller to interact with the DER sites. This report analyses two independent DNOs to form a more accurate representation of the different networks and intercommunications in place with the DER sites.

3.2.1 Scottish Power Energy Networks (SPEN)

3.2.1.1 Communications technologies

SPEN operates multiple networks for the transfer of data, voice, and protection. The core network is a fully routed layer 3 network that is provisioned for the use of telephony and SCADA data. The underlying hardware for the communications utilises a series of optical fibres lines from the central, north, and south of Scotland and extends to the intermediate sites in the network. Several BT EADs are also included in the network which operate the IP networked services. BT EAD provides point-to-point connectivity and is certified under the CESG Assured Service (CAS) scheme (Telecoms) (CAS(T)). SPEN also maintain copper cabling to the smallest sites in the network.

Along with the IP network, SPEN also still maintain a PDH network for carrying data for legacy systems. PDH networks are still operable as cost effective solutions for point-to-point connectivity, however they are typically being replaced by more modern standards such as SDH. Details of SPENs IP and PDH networks bandwidth and latencies are provided in Section 4.

3.2.1.2 Protocols

- VoIP for telephony/voice
- IEC 60870-5-101 for SCADA data between ADMS and RTUs
- IEC 60870-104 for SCADA data between ADMS and RTUs
- ICCP link between ADMS and NGESO EMS
- DNP3.0

3.2.1.3 Power resiliency

The core network ensures high resiliency by adopting common techniques outlined in IACS Recommendation for Cyber Resilience. The network is fully resilient with no single point of failure, with dual switches and routers at boundary points and gateways and provisioned dual lines to core and intermediate sites. Smaller sites may only utilize a single line. For sites with dual entry points, there is a 5-metre separation of lines to account for environmental damage to the communications.

3.2.1.4 Control centres and sites

The main control centre is located at SPEN HQ in Glasgow which hosts the GE ADMS. The ADMS provides capabilities for managing and control the distribution power system by interfacing with RTUs on site which control substation resources. The ADMS also provides real-time visualisation of the distribution grid.

Currently SPEN do not interface directly with any of the DER sites and rather their communication path is interfaced at a breakpoint. The only data that is received from DER sites into SPENs network is analogs and digitals.

3.2.1.5 Timing/Synchronisation

Accurate clock synchronisation is provided by NTP and PTP carried over the IP network which are synchronised at source with a reference clock – SPEN incorporate primary, secondary and tertiary reference clocks to ensure redundancy of clock synchronisation within the network.

3.2.2 Western Power Distribution (WPD)

3.2.2.1 Communications technologies

WPD operate a primary communications link that comprises of a mixture of technologies to reach the various substations that are owned or managed by WPD. The technologies used are a fixed link microwave transmission for point-to-point communications along with a series of optical fibres, BT EADs, and VSAT satellite systems for locations where cabling presents a challenge.

3.2.2.2 Protocols

- IEC 60870-5-101 for SCADA data between ADMS and RTUs
- IEC 60870-5-104 for SCADA data between ADMS and RTUs
- ICCP link between ADMS and NGESO IEMS

3.2.2.3 Power Resiliency

Currently there is no power resiliency on the primary communications link that WPD uses for transfer of data. If there is a break/fault in the physical communications, that channel will be inactive until it is physically repaired by onsite engineers. This presents a problem in the event of a BlackStart as a loss of key communications channels between DRZC and DNO control centre (or DER sites) could inhibit the successful delivery of automated restoration of the networks.

In the event of a communications failure, WPD use a direct voice line (typically using public GSM or CDMA via mobile phones over PSTN) to communicate with engineers to provide details of failure location. This communication is the typical route to get an engineer onsite to fix the failure, however, in the event of BlackStart this public voice channel will likely be unavailable for WPD to use. In the unlikely event that, primary communications are down at the time of a BlackStart event – it may not be possible to communicate with engineers to fix the problem.

The need for power resilient communications for a BlackStart system is fundamental and these requirements are highlighted in Section 5.10.

3.2.2.4 Control centres and sites

Limitations of workshops with Partners rendered this section incomplete (see Section 1.2)

3.2.2.5 Timing/Synchronisation

Limitations of workshops with Partners rendered this section incomplete (see Section 1.2)

3.3 Distributed Energy Resources

The DERs are a key component in the BlackStart system as they are providing the power by which to re-energise the network. There will exist several different roles such as fast balancing for stability, or slow balancing to allow fast balancing resources to recover. Additionally, there will be a key resource in each network called the anchor generator for which the key purpose of the DRZC is to keep this generator online.

One open question remains as to the ownership of the fast-balancing resources, such as load banks and batteries, as for some BlackStart generators, they may own the assets. Where this is the case, control of the anchor generator from the DRZC is not required, but control of the load bank would be. Therefore, this must be considered for each of the anchor generator sites.

DERs differ in the way they communicate with the distribution networks. They also vary in the components and protocols used on site to interact with the site's resources. This report uses information gathered from two independent DER sites compare the differences and find similarities in their infrastructures.

3.3.1 Ewe Hill Windfarm

3.3.1.1 Communications technologies

Ewe Hill is an onshore wind farm located in Lockerbie that consists of 6 Siemens SWT-2.3-93 turbines capable of generating 2.3MW of power. The site is owned and managed by Scottish Power. The primary communications channel uses a MPLS microwave radio link for point-to-point communications between sites, this network is owned and managed by Vodafone. For secondary backup communications, all wide area networks have access to VSAT links in the event of a loss of service within the core MPLS network. Optical fibre links may exist to some sites, although this is yet to be confirmed.

3.3.1.2 Protocols

- OPC Data Access (OPCDA) for local connection between SCADA and PLCs
- IEC 61850 MMS for control and monitor on site from SCADA
- MODBUS
- IEC 60870-5-104

3.3.1.3 Power Resiliency

Ewe Hill WF provides power resiliency to the primary communications using backup generators on site which are connected to the communications channels and critical equipment.

3.3.1.4 Control centres and sites

The network extends to each site where an in-house SCADA system interacts directly with the sites PLCs. Each SCADA system feeds data back to dual SCADA systems located in the main and backup control centres.

3.3.1.5 Timing/Synchronisation

Limitations of workshops with Partners rendered this section incomplete (see Section 1.2)

3.3.2 Glenlee Hydro

Limitations of workshops with Partners rendered this section incomplete (see Section 1.2)

3.3.3 Interconnections with DNOs

From the sample of DNOs and DER sites that were analysed it was found that there is no data exchange between the DNO networks and DER networks.

The DRZC scheme requires data transfer between the DNO and DER networks as the DRZC is situated on the DNO network and measurements such as voltage and current from the DER sites needs to be available to the DRZC. This requirement is highlighted in the end-to-end system architecture requirements within Section 5.

3.4 Resynchronisation Points

There is an ongoing discussion on the topic of resynchronisation points. It has become clear in the analysis that synchrocheck relays will not exist at each GSP. Therefore, a resynchronisation function can be added to the DRZC itself and it can compare measurements from each side of the resynchronisation point and provide a signal (to operators or a relay) on when to close the breaker and resynchronise.

The requirements for this function will be added to the requirements document as the analysis has shown that:

- Synchrocheck relays don't exist in all places in the system
- PMU measurements could be used, but a PMU would need to be placed on both side of GSP

There is therefore a requirement to get this PMU data to the DRZC which would require PMU data from a TO level which cannot be via the conventional ICCP links.

The OpTel network described in this report is shared by between NGET and ESO. NGET currently operate a PDC which is used to send PMU data to the ESO. There is also a data link which provides PMU data from the SPEN network to the ESO. A previous NIC project: VISOR looked at the GB WAMS system and a further project looking at real time inertia measurement has required PMU data at the ESO. A similar infrastructure could be utilised for this purpose with some reconfiguration as explained later.

The OpTel network has fibre connections to DNO control centres which means provision of PMU data for the purpose of resynchronisation should be possible.

Under this arrangement, data from PMUs for the purposes of resynchronisation could be made available either directly from NGET to DNOs via the OpTel network and then to the DZRC via the DNO network, or via the ESO where data is currently available from NGET. For DNOs in Scotland, there would not be a requirement to get data via NG ESO if there are no GSPs to the NGET systems and data could be made available from SPEN TO directly. (Similar for SSE area).

The decision on whether to go via the ESO, or TOs directly would be largely dictated by latencies observed in the existing systems.

3.4.1 Analysis

[redacted]

[redacted]

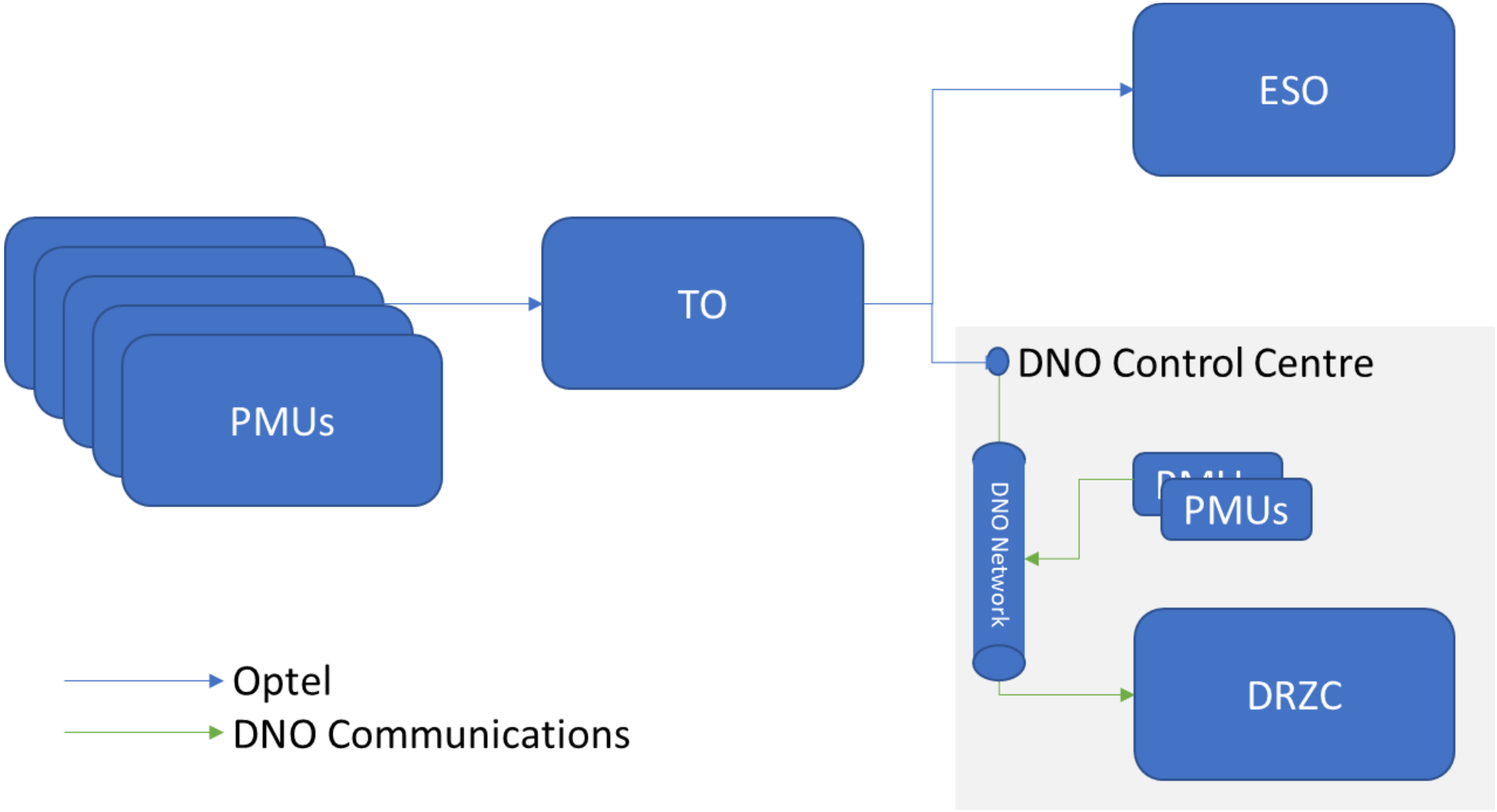


Figure 5 proposed PDC routing from PMU data for the purposes of resynchronisation for Restart

3 Overview of Current Infrastru

4 Telecommunications and Network Analysis

4.1 Technologies

Analysis of the sample of potential BlackStart participants shows there is a varying level of resiliency and technologies available within the UKs different energy licensees. Challenges when designing a DRZC scheme arise when there are multiple different physical communications technologies in place as each technology offers different bandwidths, latencies, and availability.

The DRZ controller requires fast response times from load banks and batteries to maintain stability of the network, e.g. when a new load is switched online, there may be rapid deviations in frequency which could cause loss of the anchor generator. The fast balancing offered by battery/load banks is designed to counteract this behaviour. If the physical communications path the data is transmitted over adds additional latency to the round trip of the packets, the controller may not send/receive a request/response quick enough to act accordingly and lose the current load, bringing the system back to its initial state.

The DRZC scheme also uses C37.118 Synchrophasor Data to receive voltage and current measurements from on-site PMUs. Since C37.118 data is sampled at 50Hz, the volume of data may require large bandwidths to successfully transfer the data. However, the number of different PMUs sending C37.118 data to a DRZ controller is likely to be small. Typical bandwidth requirements for C37.118 data are highlighted in Section 5.10.

The following communications technologies are currently in use:

Table 6: Overview of communication technologies

Technology	Comments
Optical Fibre	High bandwidth and low latency solution. Point to point communications. Requires lengthy and costly amounts of cabling to connect all sites to network.
Microwave Radio	Point to point communications link that utilizes a line of sight between sites. Narrow beam on wavelength spectrum and typically provides high bandwidth and low latency.
Copper	Low bandwidth and high latency however a more cost-effective solution. Current trends are moving away from older copper technology and replacing with fibre or microwave.
VSAT	Typically used as a secondary or backup communications strategy. Used in remote areas where cabling is challenging. Higher latencies and lower bandwidths than other communications methods.

Private 4G	Custom networks built on private LTE spectrums allowing organisations to reduce latencies and enhance power resiliency over public channels.
Ethernet Access Direct (EAD)	Openreach provided communications technology utilizing point to point communications link over dedicated fibre channel.

The following protocols are currently in use:

Table 7: Overview of power system protocols

Protocol	Comments
IEC 60870-5-101	Serial protocol used between RTUs and EMS/DMS systems – used for control and information. Used by NGET over OpTel.
IEC 60870-5-104	IP protocol used between RTUs and EMS/DMS systems – used for control and information. Latest versions of 104 include TLS encryption but not available on all assets
IEC 61850 MMS	IP protocol for messaging and reporting
DNP3.0	IP protocol used between RTUS and EMS/DMS systems - used for control and information
ICCP	Real time application later based protocol used for data exchange and transfer, monitoring and control. Typically, interconnecting control centres at distribution and transmission levels
VoIP	Voice over IP, exists between ESO, DNOs and DERs
MODBUS	Serial or IP based protocol for control/information

4.2 Bandwidths

[redacted]

[redacted]

4.3 Latencies

High level latency information from the sample participants presents potential challenges for the DRZC scheme where the exchange of fast-acting protocols requires response times within a timeframe. The following latency information from the BlackStart participants is highlighted below:

Table 8: Latency statistics for Partner organisations

Network	Latency
[redacted]	[redacted]

For comparison, the maximum latency requirements are set out in Requirements DRZC-RN-3 and DRZC-RN-4.

5 BlackStart Cyber Security Requirements

The following section defines the baseline security requirements for Distributed ReStart. The requirements align with standards outlined in Section 1.3 and are mapped in their corresponding tables to each Annex. Recommendations for each requirement are made based on best practice and ability to deliver a successful BlackStart. Some requirements are purely architectural and are only defined by the functional and design specification for the Distributed ReStart project Lot 1 and Lot 2 work.

5.1 Risk and Asset Management

Risk and asset management in the context of DRZC BlackStart involves highlighting the key components to the solution – in terms of assets this may be information, physical, systems or even people. Once the organisation has highlighted the assets and components, a risk profile for each should be created to understand the risks of the system. Risks are based on the concept of threat likelihood and vulnerability impact.

The likelihood of a threat may depend on different criteria such as the exposure of a system or the motivational drive behind the theat. The impact dictates what level of damage an exploited vulnerability would cause.

These risk assessments will be explored in later reports when the solution architecture of the DRZC scheme is finalised. Once a clear understanding of the different components, networks and data is achieved, organisations can collaborate to build threat models and identify potential risks. Risk assessments for the generic DRZC model have been carried out by third party to initially identify the risks.

Table 9: Risk and asset management requirements

ID	Requirement	Recommendation	Reference
DRZC-RAM-1	Organisations shall build risk profiles for each component within the OT environment	Organisations should begin by building an asset register for OT environments – containing all systems and devices. Highlight critical systems – this should include systems that allow continuous operation and systems containing confidential information. Build the risk profiles for each component and highlight any high-risk systems – review and discuss mitigation strategies to reduce risks	NIST800-53 3.16 ISO27001 Annex A.8 IEC 62443-3-2 CAF A.2/A.3
DRZC-RAM-2	Organisations shall build risk profiles for each component within the IT environment	Organisations should begin by building an asset register for IT environments – containing all servers, systems, network devices, workstations etc. For organisations maintaining or working towards ISO27001 certification, this is done as part of the process.	NIST800-53 3.16 ISO27001 Annex A.8 IEC 62443-3-2

		Highlight critical systems – this should include systems that allow continuous operation and systems containing confidential information. Build the risk profiles for each component and highlight any high-risk systems – review and discuss mitigation strategies to reduce risks	CAF A.2/A.3
DRZC-RAM-3	Organisations shall identify and document protected assets within the DRZC solution.	ADMS, central DRZ and local controllers, WAMS, IEMS, network devices – these will be highlighted in the design phase where assets can begin to be documented.	NIST800-53 3.16 ISO27001 Annex A.8 IEC 62443-3-2 CAF A.2/A.3
DRZC-RAM-4	Organisations shall build a risk assessment of complete DRZC solution.	During the design phase, threat models will help build risk profiles for the DRZC scheme once the architecture has been highlighted (as above) and will allow organisations to highlight the risks. Risks can then go under review and mitigation strategies implemented.	NIST800-53 3.16 ISO27001 Annex A.8 IEC 62443-3-2 CAF A.2/A.3

5.2 Supply Chain Management

Organisations need to understand and manage the security risks which may arise from external suppliers. Organisations need to effectively control the supply chain and ensure that any third-party solution that is deployed within an organisation's environment has been developed and maintained with security as a primary focus. Communication is crucial when setting the requirements with suppliers to ensure that they meet the organisations expected delivery for security. Both supplier and organisation should be transparent with their security policies to efficiently align and ensure a smooth yet secure deployment of any solution.

Organisations may choose to work with supplier who only possess government approved certifications that provide organisations with the confidence that the supplier adheres to strict guidelines when handling data and developing software. Certifications and schemes such as ISO27001 or Cyber Essentials help give organisations confidence that the supplier is maintaining the highest level of security.

It should be the organisations responsibility to communicate their security needs with the supplier to ensure both parties agree on the security requirements. This may include agreeing on patch requirements, ensuring the software development lifecycle is followed with security in mind or transparent vulnerability disclosure for effective management of risks.

Table 10: Supply chain management requirements

ID	Requirement	Recommendation	Reference
DRZC-SCM-1	Organisations shall communicate their security needs and agree on requirements with suppliers.	This may include: • Regular penetration testing reports from suppliers on software • Vulnerability disclosure • Patch management • Right to audit clauses • SDLC security information • Assurance certifications such as Cyber Essentials or ISO27001	NIST800-53 3.20 IEC 62443-2-4 CAF A.4
DRZC-SCM-2	Organisations and supplier shall work collaboratively to continuously improve and update security requirements and practices	Organisations should raise concerns about security and work together with their suppliers to meet their needs.	NIST800-53 3.20 IEC 62443-2-4 CAF A.4

5.3 Access Control

Access control defines the level of permissions a user (organisational or non-organisational) and/or a device has when accessing a protected resource. An organisation needs to define the different user accounts and permissions available for each system to limit the capabilities of any individual user accessing a system. This will prevent an attacker from compromising an unprivileged account and performing elevated tasks that require additional permissions.

Granularity when defining access control lists can be important to ensure a user performing a typical task does not accidentally change a configuration or remove a file. Administrative accounts should also be limited to administrative tasks only.

5.3.1 Roles and Responsibilities

Table 11: Access control requirements

ID	Requirement	Recommendation	Reference
DRZC-AC-1	Systems shall provide the capability to enforce role-based access control to support	All systems part of the DRZC architecture should provide varying levels of access control for users accessing the system.	IEC 62351-8 NIST800-53 3.1

	the segregation of duties.	DRZC controller, ADMS and WAMS systems, as well as network devices and protection devices should support role-to-right mappings where a user can have 1 or multiple rights assigned to their account. Appendix A highlights typical role and right mappings in accordance with IEC 62351-8, however, these systems may present different rights to suit their use case. Appendix B highlights the requirements for DRZC controller roles and rights. Role to right mappings can be managed via external LDAP/AD group policies if this is enabled – some applications do not offer this feature and should be managed using internal mechanisms in the software.	ISO27001 Annex A.9 CAF B.2
DRZC-AC-2	Systems and users shall follow the principle of least privilege when accessing protected resources.	Users should use unprivileged accounts when performing unprivileged tasks e.g. don't use the Linux 'root' account for updating Apache settings. Services and processes should run as specific users i.e. don't run every service as 'root' or 'Administrator'	IEC 62351-8 NIST800-53 3.1 ISO27001 Annex A.9 CAF B.2
DRZC-AC-2	Fail-safe emergency admin account shall be available in event RBAC fails to gain access to systems. Account shall not be password-based or static.	Strong local authentication should be used for emergency admin access. Access should only be used in the event of emergency where service accounts are unavailable. Servers hosting critical systems can have smartcard or OTP based login (e.g. YubiKeys) enabled and enforced, both supported by Windows and Linux.	IEC 62351-8 NIST800-53 3.1 ISO27001 Annex A.9 CAF B.2

5.4 Authentication and Identification

5.4.1 Organisational User Authentication

A user that the organisation defines as an individual of employee status or equivalent possesses unique identification as such the organisation and organisational systems can identify the individual. Authentication is used for protecting the organisations resources from unauthorized access; organisational users use their unique identifiers to access such resources.

This can include access control cards for physical access to secure locations, passwords for access to user workstations and strong authentication mechanisms like MFA or certificates for accessing mission critical systems.

Unified and centralised account management allows organisations to manage user authentication more efficiently. Integration with SSO or AD services brings flexibility to user authentication where access control (see Section 5.3) and group policies can permit and forbid a user from accessing select resources. For example, policies can define an on-site engineer having the ability to access systems contained in site A and not site B where the business justification for the engineer accessing a site only requires said engineer to access site A.

Table 12: Organisational user authentication requirements

ID	Requirement	Recommendation	Reference
DRZC-AI-O-1	Systems and locations containing information that must be protected from public disclosure shall support unique user authentication within the organisation.	Organisational users requiring access to secure locations are issued uniquely identifiable access control cards or keys to gain access. Organisational users requiring access to systems containing protected resources are issued uniquely identifiable credentials to gain access.	NIST800-53 3.7 CAF B.2 IEC 62443-4-2

5.4.2 Non-Organisational User Authentication

Any user that the organisation defines as an individual not of employee status or equivalent is deemed as a non-organisational user. For various business and security rationale, the organisation may require a non-organisational user to access a protected resource. For example, a security auditor on site or a contractor accessing a system.

Assuming that a detailed background vetting process has been carried out prior to any non-organisational user accessing a system hosting protected resources, the non-organisational user uses a temporary unique identifier that is valid for only the minimum time required to access a protected resource. For physical access, visitor badges are used to visibly identify a non-organisational user on premise within the organisation. Personal escorts are used to ensure non-organisational users do not attempt to access locations that they are not permitted to.

Table 13: Non-organisational user authentication requirements

ID	Requirement	Recommendation	Reference
DRZC-AI-NO-1	Systems and locations containing information that must be protected from public	For non-secure locations, non-organisational users should use visitor badges to be visibly identifiable.	NIST800-53 3.7 CAF B.2

	disclosure shall support unique user authentication for non-organisational users where the business need is justifiable.	For secure locations, non-organisational users must always be escorted. For non-organisational users who have a business or security justification for accessing a protected resource, temporary unique identifiers should be issued.	IEC 62443-4-2

5.4.3 Device Authentication

Device authentication is a method of building trust between devices in trusted or untrusted networks. When a connection between devices is established, the devices share identity information for the opposing parties to verify and maintain a trust relationship. Common methods for device authentication include X.509 certificates, symmetric keys, or Kerberos.

An attacker may introduce an untrusted device into the system and begin communicating with other trusted devices. This could lead to an attacker leveraging the untrusted device to send control signals around the network and/or take control of the system. By using device authentication, any traffic from untrusted devices is ignored. It should be noted that logging and reporting of any traffic from untrusted devices is essential for the analysis of potential security events in an ICS.

Organisations can restrict device authentication to a limited number of mission-critical devices due to the challenges of implementing device authentication on a large scale (management of cryptographic keys, auditing overhead).

Table 14: Device authentication requirements

ID	Requirement	Recommendation	Reference
DRZC-AI-D-1	Mission critical devices and/or devices not owned by the organisation shall support device authentication.	Devices connecting over a wide area network should use authentication to verify their identity before establishing a connection. Third party devices attached to the organisations network should use authentication to verify their identity before establishing a connection.	NIST800-53 3.7 CAF B.2 IEC 62443-4-2

5.4.4 Multi-Factor Authentication

Multi-factor authentication (MFA) utilizes two or more authentication mechanisms to gain access to a protected resource. MFA methodology typically follows three different authentication mechanisms:

- Something you know i.e. password or PIN
- Something you have i.e. SMS to smartphone or hardware-based token
- Something you are i.e. biometric fingerprints

MFA provides an additional layer of security when authenticating a user and protects the resource from brute force password attacks or sniffing attacks. Critical control systems in ICS benefit from the use of MFA when a user requires access to the system, however, it should be noted that many legacy systems do not support MFA.

Table 15: Strong authentication requirements

ID	Requirement	Recommendation	Reference
DRZC-AI-MFA-1	Where applicable, critical control systems shall support multi-factor authentication for user authentication.	Users requiring access to critical control systems are issued with two independent authentication mechanisms. Systems with multi-factor authentication support should enabled and policy changed to force users to use MFA. The design stages of the DRZC architecture will highlight the systems capable of using MFA.	NIST800-53 3.7 CAF B.2 IEC 62443-4-2

5.5 Configuration Management

5.5.1 Change Control

Configuration change control allows organisations to track changes made to system and service configurations. It provides organisations with a systematic approach for proposal, justification, reviewal, implementation, testing and post-reviewal of configuration changes. This includes any changes to baseline configurations (see Section 5.5.2), current configurations, upgrades of physical servers or version upgrades of BlackStart systems (EMS, DMS, WAMS). For DRZC controllers this may include changes to the logic schemes, patching firmware versions or networking changes.

Table 16: Change control requirements

ID	Requirement	Recommendation	Reference
DRZC-CM-CC-1	Changes to system and/or device configurations that deviate from the existing configuration or baseline configuration shall be proposed and reviewed by the organisation and/or supplier.	Any changes to critical systems must first be proposed and reviewed with a clear plan outlined to decrease the likelihood of accidental misconfigurations to the system.	NIST800-53 3.5 IEC 62443-4-1 CAF B.4

DRZC-CM-CC-2	Changes to system and/or configurations that deviate from the existing configuration or baseline configuration shall be recorded and logged for security auditing purposes.	A record of all changes to critical system configurations should be kept in accordance to the organisations cyber security configuration management for security auditing and potential rollback in the event of a disruption to normal operation.	NIST800-53 3.5 IEC 62443-4-1 CAF B.4

5.5.2 Baseline Configuration

Baseline configurations are documented and reviewed configurations of systems and/or components that provide a basis for consistent and secure platforms across the organisation. Baseline configurations can include OS level system hardening and application-level system configuration, for example, a SCADA system deployed on a Linux server may be deployed on a 'hardened' baseline Linux image and deployed with a baseline secure configuration.

Baseline configurations and images should be kept secure and safe from interference without a justified reviewal and update process between the applicable parties. An example of a justifiable update of baseline configurations may be increasing the security by moving from a less secure hashing algorithm to a more secure hashing algorithm.

Table 17: Baseline configuration requirements

ID	Requirement	Recommendation	Reference
DRZC-CM-BC-1	Organisations shall keep secure baseline configurations of server operation system images for deploying systems.	Hardened Linux and Windows OS images used to deploy a server hosting any BlackStart service. Image to follow System Hardening requirements and meet appropriate CIS benchmark level.	NIST800-53 3.5 IEC 62443-4-1 CAF B.4
DRZC-CM-BC-2	Organisations shall keep secure baseline configurations of client operation system images for organisational users accessing resources.	Hardened Linux and Windows OS images used to deploy on organisational users' workstations that may interact with systems hosting BlackStart services. Image to follow System Hardening requirements and meet appropriate CIS benchmark level.	NIST800-53 3.5 IEC 62443-4-1 CAF B.4

DRZC-CM-BC-3	Organisations shall keep secure baseline configurations of applications and systems critical to the BlackStart architecture	DRZC/local controller baseline images for scalable and secure rollout to DNO networks and DER sites.	NIST800-53 3.5 IEC 62443-4-1 CAF B.4

5.5.3 Patch Management

Software, applications and operating systems may present vulnerabilities within source code which can lead to exploitation and potential breach of a system. Suppliers release patches for any critical or high impact security vulnerabilities discovered within the software; how an organisation defines its policies for managing these patches is critical for maintaining a holistically secure system.

Validation of patches is essential to avoid disruption to operation. Typically, third party suppliers release patch reports ensuring applying a patch (OS level patch or application level) does not inhibit the application from performing as normal. Organisations typically use test systems to further validate.

Application upgrade and patching plans will be provided as part of the design of DRZC scheme, including ADMS, WAMS and DRZ controller elements. Support may also be provided by third parties – this will be highlighted in the final design phase report.

Table 18: Patch management requirements

ID	Requirement	Recommendation	Reference
DRZC-CM-PM-1	Third party patches shall be validated using a checksum issued by the supplier to ensure the integrity of the patch	Patches should be issued with a checksum such as a SHA256 hash or GPG that can verify the patch remained unchanged during transit.	IEC 62443-2-3 NIST800-53 3.19 CAF B.4
DRZC-CM-PM-2	Patches shall be validated offline on test systems either by the organisation or supplier to ensure the system remains operational after the patch is applied	Suppliers may issue regular reports providing information of latest patches tested against the software. Organisations may use test environments to ensure patches can be applied without causing a disrupt to normal operation before applying to live systems.	IEC 62443-2-3 NIST800-53 3.19 CAF B.4

DRZC-CM-PM-3	Centralised and unified remote patch management mechanisms shall be used by organisations to manage the distribution of patches	Remote patching mechanisms which utilize a secure channel help address scalability and resource issues when patching DRZC and local controllers. Provides better management and accountability for patching systems that are distributed as part of the BlackStart environment Due to the nature of uncertainty around remote patching – test systems should also be incorporated into the remote patching mechanism (as above) For critical operational equipment, where the organisation deems a failure in a system can cause a disruption to normal operation, manual patching with onsite support for rollback can be used if the risk to impact ratio raises concern. Systems part of remote patching should have rollback options available in the event of a failure in the new patch.	IEC 62443-2-3 NIST800-53 3.19 CAF B.4

5.5.4 Backups and Restores

Backup and restore procedures are used in the event of a disaster in which a system or systems become corrupt or unable to operate as normal (potentially due to hardware faults or cyber-attacks). Regular backups are used to quickly restore the working configuration of a system back to normal operation. Backups located in different locations (onsite and offsite, or clustered backup servers) help protect against site-wide disasters where the primary backup files are partially destroyed – leading to a more extensive disaster recovery process.

Further disaster recovery options are highlighted and explored in Section 11.

Table 19: Backup and restore requirements

ID	Requirement	Recommendation	Reference
DRZC-CM-BR-1	All systems shall take a backup of critical configurations at regular intervals	Organisation's policies and procedures should document exactly what systems are backed up and how often they are backed up.	IEC 62443-3-3 NIST800-53 3.6 ISO27001 Annex A.12.3

DRZC-CM-BR-2	Procedures for restoring backups shall be documented and tested at regular intervals	Organisations should document the process for restoring the backup to a test system. This process should be tested every quarter to ensure backups work and process is accurate.	IEC 62443-3-3 NIST800-53 3.6 ISO27001 Annex A.12.3
DRZC-CM-BR-3	On-site critical devices shall incorporate regular offsite backups using an automated and configurable mechanism.	DRZ and local controllers whose configuration is dynamic should perform regular automated backups and transfer backups offsite to secure repositories managed by the organisation.	IEC 62443-3-3 NIST800-53 3.6 ISO27001 Annex A.12.3

5.6 Staff Awareness and Training

Staff who operate and manage critical systems, whether this is control room operators or on-site engineers, have direct access to IT and OT systems within an ICS and should be classified as a potential attack entry point. Accidental misconfigurations or lack of awareness relating to cyber security can ultimately lead to a breach of any system within the organisation.

Organisations must ensure that staff are provided with the knowledge and information to effectively operate systems day-to-day and ensure that they can identify anything that may present as malicious within their typical tasks. Regular role-based training and desktop exercises help prepare staff for different real-life scenarios and is fundamental for BlackStart. With the introduction of DNO lead automated models for delivering a distributed BlackStart, new skillsets, roles and responsibilities with the various systems is required. Well documented knowledge bases for existing systems (i.e. operating ADMS) and continuous training to account for future changes within the organisation and software should also be adopted.

Organisations who maintain an ISO27001:2013 certification frequently provide mandatory security awareness programmes to ingrain the ability to protect the organisations assets and allow staff to understand the risks around cyber security. Overall, developing a cyber security focused culture within an organisation may take years to be fully adapted. However, this awareness has a significant impact in the overall strength of security within the organisation.

5.6.1 Role Based Training

Table 20: Role based training requirements

ID	Requirement	Recommendation	Reference

DRZC-ST-RB-1	Organisations shall develop, maintain, update and deliver training programmes to highlight the duties, roles and responsibilities within manual and automated BlackStart models.	All participants in the BlackStart model should host regular training sessions that make use of desktop exercises to highlight the individual users' roles and responsibilities and define the duties within a BlackStart event. Introduction of automated DNO lead DRZC architecture may require additional skillsets, or new roles and duties by teams to deliver successful BlackStart. Training programmes should be updated on regular basis to accommodate the changing environments.	NIST800-53 B.2 CAF B.6
DRZC-ST-RB-2	Organisations shall ensure users of systems critical to BlackStart are given regular system-based training and/or desktop exercises.	Users of ADMS/DMS, WAMS, DRZC, IEMS systems should be provided with regular training relating to the automated DNO led DRZC model. Skillsets for new systems and adopting to more automation driven processes require staff to posses the knowledge for operating and monitoring. Social engineering training for staff whose role requires the use of voice communications to deliver a successful BlackStart. This should include control room staff and DER on-site staff.	NIST800-53 B.2 CAF B.6

5.6.2 Security Awareness

Table 21: Security awareness requirements

ID	Requirement	Recommendation	Reference
DRZC-ST-SA-1	Organisations shall develop, maintain and deliver a staff security awareness and training programme at regular intervals	Security awareness programme should include phishing awareness. Organisations can adopt fake phishing email schemes within their mail domain to capture statistics and train staff to identify these attacks. General social engineering training to protect staff from sharing confidential information such as passwords. General physical security awareness training that includes ensuring secure areas are locked, not leaving confidential documents on desks and awareness when in secure locations.	NIST800-53 B.2 CAF B.6

		Use of strong passwords – this should be enforced as part of the organisations password policies for systems. Awareness when using removeable media – this should be blocked as part of the organisations device and system protection policies (Requirement DRZC-SC-CC-DP-1)	

5.7 Audit and Accountability

Cyber incidents present themselves in a variety of manners and the ability to identify a potential incident before it causes any significant impact to an organisation is a vital step in an organisation's approach to cyber security. Audit trails can be used to investigate any unexpected behaviour in systems and allow analysts to trace the information and find the root cause. These make for a fundamental tool in post-incident investigations to build timelines and determine where improvements in the systems are needed.

By using detailed security audit logging from all systems, a real-time (when logs are actively collected and collated) analysis within a SIEM environment can quickly identify any potential threat against the system. This critical information containing key security related events on the system, each marked with an exact timestamp, can help build a timeline of events post-threat for organisations to create an investigation in the recovery process of a cyber-attack.

Unrelated to cyber-attacks, the general health of systems and devices should also be proactively monitored to capture statistics that may indicate a fault in the system/device. Statistics may include CPU and RAM usage, disk I/O and power consumption. Thresholds for statistics can be used to raise alarms or alerts in the event of a hardware failure or memory leak and could allow organisations to mitigate the issue before it causes disruption to normal operation.

5.7.1 Security Auditing

Table 22: Security auditing requirements

ID	Requirement	Recommendation	Reference
DRZC-AA-SA-1	All systems critical to BlackStart shall provide security-based audit trails for real-time and offline analysis.	Audit logs should be collected from each system which highlight successful and unsuccessful logins, changes to models/configurations, system reboots and key processor crashes. DRZ and local controllers, ADMS systems and WAMS systems should allow option to off load logs to SIEM, SOAR and/or log management servers for real-time/offline analysis.	NIST800-53 3.3 CAF C.1 ISO27001 Annex A.12.4

DRZC-AA-SA-2	All systems critical to BlackStart shall be time synchronised with a network time source to ensure security-based audit trails are accurate and are evidential	All entries in audit logs must be timestamped. Timestamps must be accurate to ensure security teams can build offline timelines of any cyber events.	NIST800-53 3.3 CAF C.1 ISO27001 Annex A.12.4

5.7.2 Monitoring

Table 23: Security monitoring requirements

ID	Requirement	Recommendation	Reference
DRZC-AA-M-1	Unified and centralised security monitoring of all systems relevant to BlackStart shall be operated by organisations 24 hours a day, 7 days a week.	Organisations should enable and centrally collect syslog, rsyslog, syslog-ng [or equivalent] logs from all systems in BlackStart. Systems should include DRZ and local controllers, ADMS/DMS, WAMS, firewalls/routers/switches and protection and control devices.	NIST800-53 3.3 CAF C.1 ISO27001 Annex A.12.4

5.8 Security Assessment

Each component and system that comprise the DRZC architecture must be security assessed. Taking both an independent view of the systems and the components that are used within the systems, along with a holistic view of the solution is crucial to build a complete assessment of the degree of security offered.

As part of the secure software development lifecycle (SDLC), security assessment relates closely with the organisations risk and asset management (Section 5.1) and supply chain management (Section 5.2). The outcome of security assessments may raise vulnerabilities within the software or solution and should be managed accordingly to mitigate the risks associated with the vulnerabilities. By managing the supply chain effectively, organisations can ensure software and solutions are delivered and supported with security as a focus. Collaboration with third party suppliers who possess information security standards/certifications and suppliers who proactively assess and implement security from the beginning of SDLC gives organisations assurance of security.

While management of suppliers can help identify risks within third party software or solutions, organisations should action their own security assessments of solutions to identify risks in a more holistic view.

5.8.1 Vulnerability Management

Table 24: Vulnerability management requirements

ID	Requirement	Recommendation	Reference
DRZC-SA-VM-1	Organisations shall perform regular vulnerability scans of the networks. Scans shall be performed in such a way to not disrupt the normal operation and/or availability of the networks.	To avoid disruption of the live systems – scan should be performed against test systems to ensure there is no issue with configuration and/or software. This information should then be used to build a risk profile of the live system.	NIST800-53 3.4 CAF B.4 IEC 62443-3-2 ISO27001 Annex A.12.6
DRZC-SA-VM-2	All software, firmware and operating system shall be in active support, this may include extended support, to receive patch updates for vulnerabilities in third party software/firmware.	All servers should be running OS that is supported and still receiving security updates. All End-Of-Life OS should have a migration plan to move to supported versions and should be isolated from the operational networks.	NIST800-53 3.4 CAF B.4 IEC 62443-3-2 ISO27001 Annex A.12.6
DRZC-SA-VM-3	New applications shall have thorough security assessments conducted before implementation to the organisation's networks, and hereafter have regular security assessments conducted.	Third party applications or software suites should be independently security assessed either by the third party or the organisation. This should include a full penetration test. Full penetration tests should be carried out on major code changes and/or yearly intervals. Third parties should provide release notes showing the vulnerabilities mitigated at each release. Full library patching list on major releases and delta library patching list on minor.	NIST800-53 3.4 CAF B.4 IEC 62443-3-2 ISO27001 Annex A.12.6

5.9 Systems and Communications Protection

5.9.1 Cryptographic Controls

5.9.1.1 Device Protection and Encryption

Devices critical to BlackStart such as DRZ and local controllers, network devices, relays need to have levels of security built into their configuration or hardware to add additional layered security to protect against attacks. Following the layered security approach, in the event a segment or zone within a network is compromised at the network level, device level protection helps minimise the attack surface and can potentially limit a cyber-attack. For example, if a network firewall is compromised but the device persists a local firewall to restrict traffic, an attacker may not be able to progress an attack into control of devices/operation.

Malware may enter a network via an enabled USB port that can then traverse the network connected to the port, or attackers can physically attempt to remove hard drives from devices to obtain key information such as secret keys to perform a more sophisticated attack.

Table 25: Device protection and encryption requirements

ID	Requirement	Recommendation	Reference
DRZC-SC-CC-DP-1	All unused ports or interfaces on devices, systems and workstations interacting or part of BlackStart architecture shall be disabled	USB ports should be disabled where possible to prevent malware entry via USB. Firewall ports should be closed when not used. MAC filtering can be used to restrict the physical access to the local area network on port-by-port basis.	CAF B.4 NIST800-53 3.18
DRZC-SC-CC-DP-2	Devices, servers, systems and workstations shall restrict traffic using built-in local firewall protection.	DRZ controller should support and enable deny-by-default firewall to restrict services and access to device. Server's hosting ADMS and WAMS systems should support and enable deny-by-default firewall to restrict services and access to servers. Firewall rules on local servers/devices should be restricted to minimum required without disrupting normal operation. Workstations acting as clients for BlackStart systems should have built-in firewall enabled i.e. Windows Firewall Defender.	CAF B.4 NIST800-53 3.18
DRZC-SC-	Disk level encryption shall be enabled on DRZC devices and	DRZ and local controllers should fully encrypt the filesystem and partitions on disk to ensure a stolen	CAF B.4 NIST800-53 3.18

CC-DP-3	systems in physically less secure areas.	device cannot be used to retrieve protected information or data. Server's hosting WAMS/ADMS may encrypt disks, although due to the location of servers and level of physical security, this is not required. This may also impact performance.	

5.9.1.2 Transport Layer Security

TLS is a set of cryptographic protocols operating between the transport and applications layers to provide additional security controls over a computer network. TLS provides both confidentiality and integrity of data over networks, typically used over wide area networks to protect data in transit from tampering or eavesdropping.

TLS offers encryption of data via public and private key pairs, along with digital certificates that clients and servers can use to verify their identity when communicating over a network.

TLS versions before 1.2 are widely accepted as insecure and current guidance advises against using any TLS version before 1.2. However, TLS version 1.2 has been found to contain vulnerabilities such as POODLE (ref. *https://docs.digicert.com/certificate-tools/discovery-user-guide/tlsssl-endpoint-vulnerabilities/poodle-tls/*) and Racoon (ref. *https://raccoon-attack.com/*) that can allow attackers to gain shared session keys via man-in-the-middle attacks. TLS version 1.3 should be prioritised for critical BlackStart systems.

Table 26: Transport layer security requirements

ID	Requirement	Recommendation	Reference
DRZC-SC-CC-TLS-1	All systems using Transport Layer Security (TLS) for encryption or authentication shall use TLS v1.2 as a minimum requirement. Systems shall prioritize TLS v1.3 where applicable.	Deprecate the use of TLS versions prior to version 1.2 on all systems to mitigate the risk of various TLS attacks. Ensure newer components and/or mission critical systems provide TLS v1.3 support (e.g. DRZC controllers)	CAF B.3 NIST800-53 3.18 SC-13 ISO27001 Annex A.10
DRZC-SC-CC-TLS-2	All systems using Transport Layer Security (TLS) for encryption and authentication shall disable any weaker	Systems should prioritise the most secure available cipher suites available during the TLS negotiation. Appendix C highlights the current standard secure cipher suites that should be used – priority in descending order.	CAF B.3 NIST800-53 3.18 SC-13 ISO27001 Annex A.10

	cipher suites and force	Any systems using cipher suites containing 3DES, RC4 or MD5 should have these cipher suites disabled.	
DRZC-SC-CC-TLS-3	All IEC 104, DNP3 and C37.118 data transmitted over a wide area network between controllers shall be encrypted using TLS.	IEC 104/DNP3 and C37.118 data sent between central DRZ controller and local controllers should use TLS for encryption of traffic. Protocol converter controllers should be deployed in control centres which receive unencrypted 104/DNP3 traffic from ADMS over the local network. These devices add TLS encryption to 104/DNP3 data and communicate with DRZ and local controllers over wide area. Likewise, the converters receive encrypted 104/DNP3 data from DRZ and local controllers and convert to unencrypted 104/DNP3 to send to ADMS. Controllers should use TLS when sending C37.118 data to PDC in control centre.	DRZC Architecture CAF B.3 NIST800-53 3.18 SC-13 ISO27001 Annex A.10 IEC 62351-5
DRZC-SC-CC-TLS-4	TLS certificates used for the encryption of data or authentication of parties shall only be valid a maximum of 365 days	With automated certificate management solutions, certificates can be rotated at more frequent intervals. Smaller certificate validity periods increase the security by minimising the exposure of compromised certificates Overhead of maintaining a CA and issuing certificates regularly should be considered. Automated TLS certificate and key management solutions explored in the design phase of this project.	CAF B.3 NIST800-53 3.18 SC-13 ISO27001 Annex A.10

5.9.1.3 Virtual Private Networks

VPNs provide a mechanism for extending a private network over public networks allowing a secure control method of connecting from, between or to untrusted zones. VPNs can provide site-to-site connections and are typically used for third parties connecting to an organisations network.

VPNs provide authentication and encryption between two or more parties and may be utilised for DNO to DER connections that converge over untrusted wide area communications paths. Third parties may also use VPNs to connect to an organisations corporate network to provide support – it should be assumed that any third party corresponds to requirements set out in Section 5.2 for accessing protected resources or handling organisational data.

Table 27: Virtual private network requirements

ID	Requirement	Recommendation	Reference

DRZC-SC-CC-VPN-1	Third party connections to DNO/DER networks and sites shall prioritize IPsec VPNs where applicable.	Use IPsec VPNs for site-to-site connections to DER sites with sufficiently reliable communications channels. Use SSL/TLS VPNs where multiple VPN clients are used to connect to a single site. This may be uncommon in the ICS scenario.	DRZC Architecture CAF B.3
DRZC-SC-CC-VPN-2	All IEC 104/DNP3 data sent over wide area networks where the systems do not support TLS shall utilize site-to-site VPNs to encrypt the traffic on the network layer	104/DNP3 data from ADMS to protection devices and/or legacy RTUs currently do not support TLS encryption via protocol extensions in software. Instead, site-to-site VPNs should be used to protect the integrity of data by utilizing encryption on the network layer and sending data across the secure connections.	DRZC Architecture CAF B.3

5.9.1.4 Key Distribution (IEC 61850)

KDCs help automate the generation and distribution of symmetric keys to on-site devices to allow the devices to use a particular service. In the case of BlackStart, this service may include granting the ability of central DRZC controllers to communicate with local controllers on site at a DER. By building a network of trust, the controllers can utilize the use of a KDC to share a temporary symmetric key to all parties and allow the secure communications between all parties.

Any party within the network that requires to communicate with other trusted parties first uses an authentication mechanism (such as TLS client certificate authentication) to establish a line of trust between the KDC and party. In a zero-trust network, by issuing each client or device with a TLS certificate generated by the organisations CA and imported to the KDC, the client can initially authenticate with the KDC and start receiving symmetric keys to communicate with the other clients in the network. Best practice for using IEC 61850 protocols with KDCs is highlighted in Section 6 – where the use of KDCs between single-party and multi-party organisations is explored.

IEC 62351-9 defines the requirements of a KDC when using IEC61850 protocols (such as R-GOOSE, R-SV or MMS) to provide encryption and authentication of 61850 protocols over a wide area network.

Table 28: IEC 61850 key distribution requirements

ID	Requirement	Recommendation	Reference
DRZC-SC-CC-KDC-1	Where the secure transmission of IEC 61850 protocols over wide area networks is required, the organisation shall utilize a Key	Central DRZC controllers and local controllers make use of symmetric keys to securely exchange control and data signals. Controllers receive keys from KDC once trust relationship is built using TLS certificate authentication/verification.	IEC 62351-9

	Distribution Centre for management and distribution of cryptographic keys to secure 61850 protocols.		
DRZC-SC-CC-KDC-2	Any client requiring access to the KDC shall first authenticate using a strong authentication mechanism.	Controllers and other systems utilizing a KDC should use X.509 certificates issued by organisations trusted CA root/intermediate certificate to authenticate with KDC. KDC contains a list of client X.509 certificates for authentication. KDC operates a 'zero trust' security model.	IEC 62351-9
DRZC-SC-CC-KDC-3	KDC shall support both PUSH and PULL mechanisms for distribution of symmetric keys.	PUSH allows for greater scalability as it utilizes synchronous key distribution i.e. all keys are pushed simultaneously to client devices. PULL allows clients to reconnect with the system quickly on device/system reboot.	IEC 62351-9
DRZC-SC-CC-KDC-4	KDC shall support Key Delivery Assurance (KDA) and shall account for availability of devices in network.	Clients should send confirmation to KDC that key PUSH/PULL was successful. Shared key only becomes active when >98% and < 100% of clients in network send confirmation – to account for potential device failures. KDA typically set to less than 100% to account for device failures.	IEC 62351-9
DRZC-SC-CC-KDC-5	KDC shall manage symmetric key lifecycles in accordance with the requirements set out by the organisations cyber security policies.	KDC cycles new keys to trusted clients after previous key is no longer valid. KDC allows organisation to set validity of key to specific time frame – rotation every 1 day.	IEC 62351-9
DRZC-SC-CC-KDC-6	Any KDC used by the organisation shall be made highly available with no single point of failure.	KDC should be clustered over 3 or more servers to ensure no single point of failure. Dual power sources to each physical server hosting the KDC. Complete communications loss to KDC results in trusted parties using last-known key until the network can again communicate with KDC.	IEC 62351-9

5.9.2 Network Segregation and Security Zones

Network segregations and the use of different security zones and conduits within industrial control systems help reduce the attack surface by restricting the access and data flows to mission critical systems from less secure networks. Typical network segregation models such as the Purdue Model define the different levels (or layers) of segregation between process, control, operational and corporate/enterprise networks. Bridging the gap and converging between the traditional IT networks and the OT networks is becoming more prevalent as the need for bidirectional data flows increases with the increase in demand for automation. However, unidirectional data flows between zones provides a greater degree of security as the attack surface is decreased.

Additional security controls such as firewalls and proxies can be included within a DMZ which typically sits between the IT network and the OT network to air gap the two zones. Boundary protection and security controls are used at each layer to restrict the data flows and add an additional security layer between zones (see Boundary Protection).

Table 29: Network segregation and security zone requirements

ID	Requirement	Recommendation	Reference
DRZC-SC-NSSZ-1	Organisations shall segregate networks and systems according to their cyber security policies either logically or physically.	Mission critical systems should be isolated to their own secure network or zone with adequate boundary protection and restricted data flows. Corporate network should not be in the same physical or logical zone as DRZC controllers and DMS/ADMS or SCADA systems.	IEC 62443-3-2 CAF B.5 NIST800-53 3.18 ISO27001 Annex A.13
DRZC-SC-NSSZ-2	Organisations who require access to OT networks from IT or corporate networks shall use a DMZ to separate the zones and apply security controls.	Network convergence of OT and IT should ensure an extra level of security within a dedicated zone (DMZ) is used to bridge the gap. Typically, with dual firewalls between boundary zones to restrict traffic. Jump servers should be used within a DMZ where remote access is required.	IEC 62443-3-2 CAF B.5 NIST800-53 3.18 ISO27001 Annex A.13
DRZC-SC-NSSZ-3	Unidirectional data flows shall be used where possible to minimise the attack surface between networks and security boundaries.	Data flows within the DRZC architecture will determine the possibility of unidirectional flow. This will be highlighted in the later design stages of the project.	IEC 62443-3-2 CAF B.5 NIST800-53 3.18 ISO27001 Annex A.13

DRZC-SC-NSSZ-4	Organisations requiring access to third party OT networks shall utilise a zero-trust environment and apply managed boundary protection for their own trust zones.	Organisations should manage their own boundary deny-by-default firewall. Risk assessment and business justification shall dictate the level of access between organisations. Trust zones for each organisation should stop at the boundary firewall. Additional security controls should manage the untrusted territory between gateways e.g. physical security.	IEC 62443-3-2 CAF B.5 NIST800-53 3.18 ISO27001 Annex A.13

5.9.3 Boundary Protection

Boundary protection restricts the data flows between logical or physical networks and provides additional layers of security on the boundary of each permitter or zone – acting as the first, second or third line of defence against attackers trying to penetrate the system.

Firewalls allow organisations to restrict the data flows between zones by blocking traffic with unknown source IP addresses or a particular protocol not used within the system. Whitelisting and blacklisting are methods for allowing or denying traffic by default.

Table 30: Boundary protection requirements

ID	Requirement	Recommendation	Reference
DRZC-SC-BP-1	Organisations shall utilize whitelisting policies for boundary protection of networks and incorporate a deny-by-default policy to restrict traffic between networks.	Deny-by-default should be used for all boundary firewalls to deny all traffic (unidirectional and bidirectional) between zones unless a business need and justification permits it.	NIST800-53 3.18 CAF B.4
DRZC-SC-BP-2	Organisations shall include IPS and IDS mechanisms at boundaries between networks – physical and logical.	While it is important to prevent the access of unauthorized traffic through a boundary and into a network, it is equally as important to identify and report any unauthorized traffic trying to gain access. By utilizing deny-by-default method, any traffic that is not part of the typical operation and not defined in the IDS/IPS should be blocked and reported for investigation.	NIST800-53 3.18 CAF B.4

5.9.4 Anti-Virus and Anti-Malware Protection

Malware, ransomware and computer viruses are becoming more widespread within computer networks, where attackers use malicious software designed to cause damage to data and systems. Not only is this becoming a problem within IT networks but has been seen within industrial control system environments in recent years.

By monitoring for the presence of malware, within IT and OT environments, systems can be quickly isolated from the rest of networks to incapacitate the malware from infecting further systems and leading to more serious disruption. The move to convergence of IT and OT networks could allow malware to enter via IT networks and infiltrate OT networks – leading to potential control of devices connected to generators or breakers.

Table 31: Anti-virus and anti-virus requirements

ID	Requirement	Recommendation	Reference
DRZC-SC-AV-1	Mission critical systems with sufficient performance capabilities shall deploy real-time anti-virus/anti-malware scanning.	Physical servers running services critical to BlackStart i.e. ADMS/DMS, WAMS, EMS; use real-time scanning for anti-virus and anti-malware. For ADMS, scanning on peripheral servers e.g. Calltaker, FEPs and clients should be as above. Main ADMS and database nodes should have hardware requirements and exclusions considered. For WAMS, as above. Endpoint protection on client devices that interact with systems.	CAF B.4 ISO27001 Annex A.12.2 IEC 62443-2-4 DRZC Architecture
DRZC-SC-AV-2	Mission critical systems with limited performance capabilities shall deploy ad-hoc anti-virus/anti-malware scanning.	Components with limited CPU and RAM reservations such as DRZC and local controllers should not use real-time scanning. If device CPU is fully utilized with anti-virus/anti-malware scanning, mission critical BlackStart functions may not work. Incorporate scheduled maintenance scans as part of the organisations policies and procedures.	CAF B.4 ISO27001 Annex A.12.2 IEC 62443-2-4 DRZC Architecture

5.9.5 System Hardening

An additional layer of security involves 'hardening' or ensuring that a systems configuration and/or settings have been securely implemented following commonly available and standardised guidelines. Common techniques for hardening include but are not limited to:

- Limiting user accounts

- Limiting permission of user accounts
- Setting secure permissions on files (no execute on specific folders, use of sticky bits)
- SSH keys favoured over passwords
- Local firewall and intrusion detection
- Immutable filesystems

Table 32: System hardening requirements

ID	Requirements	Recommendations	Reference
DRZC-SC-SH-1	Organisations shall harden hosted systems in accordance with Center for Internet Security (CIS) benchmarking standards.	CIS benchmarks are available for different flavours of operating systems, giving recommendations for system hardening to provide another layer of defence in security. For Linux, topics such as SELinux, SSH configuration, filesystem permissions and limitation of installed packages should be explored. For Windows, topics such as user accounts, permissions, access and service disabling should be explored.	CIS Benchmarks

5.10 Resilient Networks and Systems

Due to the nature of the automated DRZC scheme, which requires data transfer between key sites, resilient and redundant communications channels are essential to deliver a successful BlackStart. As a minimum requirement, resilient communications are required for the locations that are necessary for the power island to start, run and resynchronise.

Different sites within the DRZC architecture may require different levels of physical communications in place depending on their control function, with routes that carry fast-balancing protocols requiring a lower latency than routes carrying slow-balancing protocols.

The different control functions for the DRZC scheme contain:

- Proportional Regulation (PR) sites, which act as anchor generators or any other generators with frequency droop control – these send measurements only, but they do require low[er] latency communications since the data is used in the DRZC. PMU measurements from PR sites are fed into the DRZC, so latencies greater than the controller wait time would result in a loss of data to the controller.
- Primary Balancing Control (PBC) sites, which may be a load bank or BESS – these require fast balancing control signals and low[er] latency communications
- Secondary Balancing Control (SBC) sites, which may be constrained generation with slow dispatch control or sheddable loads – these use slow-balancing control signals so do not require the low[er] latency communications.

In general, the controlled locations (PR, PBC, SBC) should be power resilient to ensure that the load is restored in the zone as far as possible given the available resources. Exceptions can be made for some SBC resources, as this would not prevent the anchor from starting and the PBC from providing fast response, however failure of SBC communications could result in reduced capacity of the zone to connect load and energise the external network.

The GSP substation(s) is an important location and requires resilient communications. The primary substation loads will be energised from the GSP, and the DRZC will normally be located at the GSP. The resynchronisation boundary is also normally at the GSP transformers.

The requirement for the low[er] latency communications is defined in Requirement DRZC-RN-3.

Table 33: Resilient networks and system requirements

ID	Requirement	Recommendation	Reference
DRZC-RN-1	All participants critical to the successful delivery of BlackStart shall provide a power resilient primary and/or secondary communications channel	Power resilient comms are required for - DNO must ensure power resilient comms between ADMS and central DRZC. - DRZC to all sites designated Primary Balancing Control, i.e. batteries and load banks used for fast response - DRZC to all sites designated Proportional Regulation, i.e. anchor generator and other frequency proportional resources - ADMS and the Grid Supply Point(s) feeding the primary substation loads to be picked up. Primary substations need not have power resilient comms unless a high priority load is connected, such as a hospital.	DRZC Architecture CAF B.5
DRZC-RN-2	A power resilient voice channel between DNO and DER site personnel (especially at anchor generators) shall be used where voice communications are required for co-ordination.	For DER sites that are involved in the BlackStart process and do not have a power resilient voice communications channel, it is recommended to utilize battery powered satellite phones for a communications line between DNO control centre and DER site staff. One phone located in DNO control centre and multiple phones provided to DER 'on call' engineers. Phones should be periodically tested; frequency of testing should be defined within the organisations own policies. Some sites may maintain power resilient voice communications and can co-ordinate using this channel; however, satellite phones should still be	DRZC Architecture

		used as a secondary backup option in these cases.	
DRZC-RN-3	Communications channels between central DRZC and PBC sites shall have a maximum latency of **200ms.**	These links are for the fast-balancing protocols which require low response times. **100ms** latency where possible to ensure adequate time to respond	DRZC Architecture
DRZC-RN-4	Communications channels between central DRZC and PR or SBC sites shall have a maximum latency of **2s**	These links are for the slow-balancing protocols with higher response times. Less than **1s** where possible	DRZC Architecture
DRZC-RN-5	Communications channels between central DRZC and PR, PBC or SBC sites shall allow for an additional [redacted]	[redacted]	[redacted]

		Calculation for bandwidth shown in Appendix D	
DRZC-RN-6	Additional bandwidth shall be available on networks used to connect to controllers and receive security logs	It is not yet known the amount of additional bandwidth required for log traffic received from controllers (i.e. syslog back to SIEM). This figure will be highlighted during the security testing within the design phase of this project. As part of the testing, this will also include traffic capturing during key events (simulated cyber attacks, poor data quality etc.) to understand the maximum possible bandwidth requirements for logging and security related tasks.	DRZC Architecture

5.11 Physical Security

While remote and network-based attacks are predominantly used by cyber criminals to attack organisations, physical attacks in an ICS environment can be disastrous. As availability is the key factor in ICS, an attack such as simply gaining access to a remote location and damaging equipment is typically far more consequential that stealing personal information from the IT environment (however, in a financial sector for example, confidentially of personal data remains the top priority). The need for physical security and the ability to protect control devices from malicious damage (or accidental) is essential for continuous normal operation of the system.

Simple security measures such as locked doors and cabinets protecting critical equipment, security perimeters and security controls including CCTV and alarms provide a good base level of security. These security controls need to be included in the backup resiliency as a loss of power in the BlackStart scenario means a loss of security.

Table 34: Physical security requirements

ID	Requirement	Recommendation	Reference
DRZC-PS-1	All industrial control systems shall be contained within a physical security perimeter, with entry and exit points identified and secured.	Physical perimeters vary depending on size of site, location, criticality. Anti-climb fences for large sites that are deemed critical. Secure buildings for smaller sites deemed critical. Highly critical sites may have guards on perimeter.	ISO 27001 Annex A.11 NIST800-53 3.11 IEC 62443-2-1
DRZC-PS-2	Entry and exit points within physical security perimeters shall be protected with security controls. Controls shall include	Entry and exit points to secure locations should be protected with at least one layer of physical security (depending on criticality may introduce more). Doors should be locked with either key/access cards. CCTV and alarms at critical locations – these security mechanisms should be included in the	ISO 27001 Annex A.11 NIST800-53 3.11

	locks/access card points, CCTV and alarms.	resilient power. A loss of power would mean a loss of security if these protection schemes are not included.	IEC 62443-2-1
DRZC-PS-3	Critical systems and devices shall be physically secured within lockable casings to prevent tampering.	Redundant systems should be self-contained in separate casings or cabinets – this includes DRZ and local controllers. Casings or cabinets should be protected from unauthorized access via key or access control cards.	ISO 27001 Annex A.11 NIST800-53 3.11 IEC 62443-2-1
DRZC-PS-4	Physical access shall be audited, stored, and maintained.	Logbooks or electronic key access points should contain an audit trail of entry and exist along with timestamps.	ISO 27001 Annex A.11 NIST800-53 3.11 IEC 62443-2-1
DRZC-PS-5	Uninterruptible power supplies (UPS) shall be installed on site to protect equipment from loss of primary and/or secondary power source.	Core control equipment must be included for the continuous operation of BlackStart. Security controls should be included to ensure site is still secure in the event of power loss. DRZC and local controllers should be included in this scope.	ISO 27001 Annex A.11 NIST800-53 3.11 IEC 62443-2-1
DRZC-PS-6	Environmental protection shall be implemented on sites to protect against fire, floods and extreme weather.	It is assumed that sites critical to the delivery of BlackStart have been built with environmental protection in place. Additional actions can be taken by organisations to further mitigate the risk of environmental threats – i.e. raised equipment for flooding or 'no flammable material' policies within secure areas.	ISO 27001 Annex A.11 NIST800-53 3.11 IEC 62443-2-1

5.12 Incident Response

Identification and detection of cyber-attacks utilize real-time security auditing and monitoring of components and systems as discussed in Section 5.7. Prevention and protection are achieved using various layers of security and protection mechanisms within systems and data. Response and recovery happen in the critical moments after the cyber incident occurs. A cyber incident can range from an accidental configuration of a system to a targeted attack by a malicious actor. All incidents should be dealt with rapidly and effectively to reduce the exposure within the networks and systems.

The key to incident response is planning. A well-documented plan should be a collaboration of different individuals to best apply operational and cyber response in the event of an incident. Continuous improvement from feedback on scheduled rehearsals can better equip and prepare the organisation for a real-world incident.

Table 35: Incident response requirements

ID	Requirement	Recommendation	Reference
DRZC-IR-1	Organisations shall implement, document and maintain a detailed incident response and recovery plan highlighting roles, responsibilities, risks, impact, assets and next steps.	Plan should include: The different scenarios and situations that can occur (see Section 10). The roles and responsibilities for each staff member (and potentially third party) The first steps after the moment an incident is discovered – including communications. Next steps in mitigating/minimising – for example isolating affected systems or networks. More detailed response and recovery options are highlighted in Section 11.	CAF D.1 NIST800-53 3.8 ISO27001 Annex A.16
DRZC-IR-2	Organisations shall conduct regular business continuity or operational continuity rehearsals to ensure staff are aware of roles and responsibilities in the event of a cyber incident.	Security-based simulations of cyber events should be carried out at regular intervals (yearly at most) for incident response team to ensure rapid response to potential cyber-attacks. Simulations/rehearsals should also consult the incident response plan. Lessons learned should be captured and improved on for each session – this should be documented and used for improvement of plans.	CAF D.1 NIST800-53 3.8 ISO27001 Annex A.16
DRZC-IR-3	Organisations shall conduct post-incident root cause analysis after any cyber incident.	Comprehensive analysis using data collected during an incident (real or simulated) should be undertaken by the necessary teams/third parties. Investigating the root cause of an incident is essential for building more secure systems or processes going forward. Any areas for improvement should be highlighted and actioned to prevent repeated mistakes and/or to deal with certain aspects more efficiently in the future.	CAF D.1 NIST800-53 3.8 ISO27001 Annex A.16

5.13 Data and Architecture

In addition to the cyber security requirements highlighted from Sections 5.1 to 5.12 – there is also some data requirements for the successful delivery of the DRZC BlackStart scheme. The following set of requirements and recommendations are applicable to all Participants within the DRZC BlackStart scheme.

Table 36: Data and architecture requirements

ID	Requirement	Recommendation	Reference
DRZC-DA-1	Fast Voltage, current and frequency measurements	Synchrophasors (IEEE C37.118 or IEC 61850-90-5 R-SV)	DRZC Architecture
DRZC-DA-2	Slower Voltage, power and reactive power, breaker status	From RTUs via IEC 60870-5-104, DNP3.0 or IEC 61850 MMS (encryption where possible and may require additional devices)	DRZC Architecture
DRZC-DA-3	Generator Setpoints from controller (Slow)	From DRZC to generators via and IEC 60870-5-104, DNP3.0 or IEC 61850 MMS protocol (see previous note)	DRZC Architecture
DRZC-DA-4	Fast resource (BESS/Load bank) setpoints from controller	From DRZC to resource, fast protocol, IEC 61850-90-5 R-GOOSE, or IEC 60870-5-104/DNP3.0 if latency can be kept sufficiently low. Note previous comment on encryption.	DRZC Architecture
DRZC-DA-5	Breaker control data (From ADMS)	Using the existing SCADA infrastructure	DRZC Architecture
DRZC-DA-6	Commands from DRZC to ADMS	Utilising SCADA based protocol such as IEC 60870-104, DNP3.0 or IEC 61850 MMS, used for load pickup capability values, alarms, information/status	DRZC Architecture
DRZC-DA-7	High resolution data capture for archive	Synchrophasor data (selected data from the DRZC to the central WAMS archive) IEEE C37.118 or IEC 61850-90-5 R-SV	DRZC Architecture
DRZC-DA-8	Zone black validation	Signal to the ADMS to verify that zone is black prior to starting sequence	DRZC Architecture
DRZC-DA-9	Protection setting group change	From ADMS to protection devices	DRZC Architecture
DRZC-DA-10	Oversight data to ESO	Selected data from process (DRZC/ADMS) to ESO system (likely the EMS or similar monitoring platform) via encrypted ICCP like (or other suitable alternative)	DRZC Architecture

DRZC-DA-11	Data from Resynchronisation (fast measurements of frequency/voltage)	Synchrophasor data from transmission operator (TO) levels at GSPs to allow DNO area to resync back to TO area	DRZC Architecture
DRZC-DA-12	System ready data	For manned stations, dedicated encrypted voice channel to ensure all parties are ready. For unmanned stations, must be a suitable connection to a manned control centre. Backup encrypted voice system for unmanned locations recommended in case of failure of comms to remote centre where person could be sent to site to initiate equipment for BlackStart purposes (assuming comms are operational for BlackStart)	DRZC Architecture

6 Communications – Best Practice

6.1 Networks

Network security is fundamental for the overall security of a BlackStart system. Networks carry data and act as entry points and couriers for attackers. Breaking networks down into multiple zones and applying different security controls depending on the criticality of the systems (or data) inside the network ensures that attacks can be contained and recovered from easily. There are many best practice guidelines for securing networks, including NIST800-53, IEC62443 standards and guidance from NCSC and CISA government organisations.

The following is a list of common threats and attacks on networks:

- Computer virus
- Rogue security software
- Trojan horse
- Adware and spyware
- Computer worm
- DOS and DDOS attack
- Phishing
- Rootkit
- MITM attacks

Physical segregation of networks utilises the lowest layer of the OSI model – the physical layer. Physically containing a network within the boundaries of an array of cables and network devices will ensure traffic is segregated from other networks. Networks are connected using boundary devices such as routers and firewalls and traffic converging networks is limited and restricted.

When physically segregating a network, the following best practice should be followed:

- Principle of least privilege – systems should only have access to resources that are necessary to complete their intended function. Administrative tasks should not be carried out by unprivileged users. Privilege bracketing should be used for critical functions to limit the time a superuser account is accessible.
- Security controls across all networks – boundary protection over conduits including firewalls or VPNs. IDS and IPS for traffic inspection and security-based monitoring for identification of unusual behaviour of traffic.
- Separate networks based on security requirements – Business and IT networks separate from OT networks, split networks into zones of varying levels of criticality. Define trust boundaries of networks and apply boundary protection.
- Security zones and conduits – network segments should be categorised into varying levels of criticality, each with different cyber security requirements. Lower security zones should not be able to initiate a connection with higher security zones, instead, higher security zones should initiate the connection and restrict ingress traffic from the lower zones.
- IT and OT network separation and protection – back-to-back firewalls should be deployed to isolate a DMZ between IT and OT networks. IT firewall controls all traffic between IT network and DMZ, OT firewall controls all traffic between OT network and DMZ. Using different vendor firewalls mitigates duplicate vulnerabilities on firewalls. For

management, different parties should manage each firewall. Separating duties for managing firewalls limit's ability for one party to compromise both firewalls.

Best practice guidelines for interconnecting the firewalls of different organisations OT networks are scarce – this is likely due to how uncommon this architecture is an ICS environment. From the initial analysis of ESO, TO, DNO and DER networks, it was found that currently none of the DER sites have an interconnection with DNO/TOs. Following the same guidelines for IT and OT convergence is a plausible solution, where one firewall is operated by DNO and another by DER – with agreement on using different vendor firewalls. However, operating a DMZ between the firewalls results in one organisation taking responsibility for securing and applying cyber security controls to another organisation's assets. Instead, a 'no man's land' approach can be taken where the organisations firewalls are connected by a single cable, and data between the boundaries is not owned by any party.

Industry stakeholders have been working over the last few years to create several DER security recommendations, best practices, and reference solutions that can be codified by standards development organizations and reference solutions that can be codified by standards development organizations (SDOs). This work is challenging because there are multiple entities within this ecosystem with varying roles and responsibilities and they need differing levels of access to DER data and/or DER control modes. For example, DER vendors and aggregators monitor production to advise maintenance schedules, DER owners track their solar generation, and grid operators track production and push control setpoints to the equipment for DER-based grid services. With so many users needing access to the equipment control settings or data, there is a need to establish robust access control security policies and technologies.

Data connections run from several users and roles to DER equipment, DER gateways, DER site controllers, aggregators, DER vendors, etc. and each of these endpoints must support the AC mechanisms. Additionally, the diversity in device endpoints (utility owned DER, residential systems, commercial DER with site controllers, etc.) and interfaces (each have their own operating constraints.

An DER AC security policy needs to be established to select the AC model and build the rules into hardware and software (via security mechanisms).

Within the DER Cybersecurity Workgroup, utility participants indicated they would not like to be the owner of the identity server and did not want to be responsible for the cybersecurity of assets that they did not own. Therefore, there are a couple potential implementation options for access control when the utility is communicating IEEE 2030.5. In these cases, the utility may communicate directly to the DER equipment or to DER service providers (or a combination). (ref: Johnson, Jay Tillay. Recommendations for Distributed Energy Resource Access Control https://www.osti.gov/biblio/1765273)

Logical segregation uses the same design principles as physical segregation; however, no additional hardware is required. Instead, managed infrastructure and existing technologies are used to virtually separate network traffic over the same physical communications.

When logically segregating a network, the following best practice should be followed:

- Use of Virtual Local Area Networks (VLANs) – Broadcast domains that are isolated within a network at the data link layer (layer 2 of OSI).

- Use of Virtual Routing and Forwarding (VRF) – VRF is a technology that allows multiple routing tables to exist simultaneously on a single router.
- Use of Virtual Private Networks (VPNs) – technology to securely extend private networks by tunnelling across public or other private networks.

Safeguarding network devices with secure configurations adds an additional layer of security to the networks they operate. Governments and vendors provide guidelines and benchmarks for best practice when security hardening devices and servers.

For secure configuration of network devices, the following best practice should be followed:

- Access Control Lists (ACLs) – use AD or group policies to restrict systems access to resources. Implement fail safe privileged account in the event of loss of ACL servers.
- Strong authentication where possible – modern network devices provide strong authentication mechanisms for accessing interfaces (e.g. MFA). Use robust password policies where strong authentication is not possible.
- Disable unnecessary services – mail transport agents, NFS, HTTP, RDP, print spooler etc.
- Disable unencrypted admin services – File Transfer Protocol (FTP), Telnet. Use secure options instead e.g. SFTP and SSH.
- Back up configurations – regular onsite and offsite backups of systems, updated OS and patches.
- Physically secure devices – Restrict access to routers, firewalls and switches with cabinets, secure access points and tamper proof ethernet cables.
- Protect configurations with encryption and authentication – use latest TLS versions and strongest keys available, prioritise more secure algorithms. Ensure all devices are authenticated.
- Use SNMPv3 – do not use versions prior to v3.

6.1.1 Example of Best Practice for BlackStart Architecture

Network segregation to reduce the attack surface:

- TO, DNO and DER networks physically separated with back-to-back firewalls.
- DRZC logically separated from control network.
- Field controllers logically separated from control network.
- ADMS physically separated from DRZC i.e. from site control network.
- ADMS physically separated from IEMS.
- Control monitoring logically separate from ADMS.
- OT network physically separated from IT networks with back-to-back firewalls and OT owned DMZ in place.

Secure configuration to protect against unauthorised access and vulnerabilities:

- Jump servers and/or proxy servers secured access with MFA when connecting from IT to OT remote devices and role-based access control.

- DRZC and field controller interfaces secured access using MFA and role-based access control.
- ADMS secured access using MFA and role-based access control.
- All additional critical server secured using MFA and role-based access control.
- Fail safe administrative access on critical servers/devices using dynamic authentication mechanism (e.g. smart cards). No static password-based authentication for 'recovery' account.
- Administrative access on dedicated management network or encrypted and authenticated over communications channels (i.e. no HTTP admin interfaces).
- Security, audit and system logs collated and parsed for security threats from all systems as part of the functional and security design.
- Local intrusion detection on all systems, hash function used as a file integrity check to monitor filesystem changes

Network security to protect against malware, unauthorised access and reduce attack surface:

- Single firewalls/VLAN switch at each conduit where logical separation is applied.
- Single firewall at each conduit internal to organisation and existing within OT environment.
- Back-to-back firewalls and DMZ between organisations IT and OT networks.
- Back-to-back firewalls and no trust zone between different organisations OT networks.
- IDS at each conduit, security monitoring and logging between each boundary. Network isolation capabilities at each boundary.
- Sufficient access control for systems and networks – ensure only authorised systems can traverse network zones. Ensure authorised user can only access role-specific resources. Enable CA or MAC based access control on boundary protection devices (e.g. firewalls).
- Dedicated security monitoring of all networks and security controls to isolate compromised networks. By situating each critical system on separate networks (physical and logical), any compromised component can be isolated and recovered in a secure manner.

Anti-virus and patching to protect against malware and vulnerabilities:

- Anti-virus installed on every machine in organisations networks.
- Middleware anti-virus server installed in DMZ between IT and OT networks – virus signatures pushed from IT to DMZ to OT.
- Real-time anti-virus scanning on servers hosting ADMS, IEMS, control monitoring, SCADA, and client workstations.
- Proactive anti-virus scanning on DRZC and field controllers.
- Passive monitoring for vulnerabilities relating to OT assets – automatic checking against national vulnerability database to identify vulnerabilities within software deployed on OT systems.
- Virus signatures and security patches deployed on pre-production (testing/development) environment prior to deploy on production environment.

- Rollback plan for all patches on OT systems – tested backups, engineer on site when patching (or restoring) critical systems to ensure local access to system is still achievable in the event network/remote access fails.
- Change management policies for deploying virus signatures and patches should be implemented and adhered to.

Remote access to critical systems:

- Remote access to OT environments should not be done via a corporate device with access to mail or internet services. Instead, a dedicated remote access device with security hardening and locked down services and ports should be used.
- Remote access to OT environments should use multi-factor authentication and least privilege policy
- Use a Privileged Access Workstation (PAWs) to access jump servers when administrative tasks are required.
- For third party support – use dedicated VPN with time-based access and MFA (e.g. smart cards or TOTP)

6.2 Protocols

The following section describes the best practices of the protocols that may be used as part of the Distributed ReStart DRZC architecture. Each protocol is reviewed to determine the threats and risks associated, with best practice guidelines and mitigation techniques highlighted for each. These protocols are:

- IEEE C37.118
- IEC 61850-9-2 SV
- IEC 61850-90-5 R-SV
- IEC 61850-8-1 GOOSE
- IEC 61850-90-5 R-GOOSE
- IEC 61850 MMS
- IEC 60870-5-104
- DNP3
- PTP
- NTP

6.2.1 IEEE C37.118

The IEEE C37.118 protocol (C37.118) is used to transfer real-time synchrophasor data between Power Systems. Data is collected by devices such as phasor measurement units (PMU), with each measurement time-stamped from a precise time source such as GPS. This data can be aggregated by phasor data concentrators (PDC) for transmission to other systems. The protocol uses TCP/IP (TCP) as the transport protocol and has five frame types:

- Data frame (binary)
- Two configuration frames (binary)
- Header frame (ASCII)
- Command frame (binary)

The C37.118 standard does not specify any requirement for a cryptographic signature or encryption of the data, this renders the plain text data in the network packets susceptible to interception, modification, or spoofing. This results in the protocol being vulnerable to the following attacks:

- Replay Attacks
- Man-in-the-Middle Attack
- Denial of Service (DoS)

Recommendations to ensure best practice

The best practice guidelines for securing IEEE C37.118 with respect to Confidentiality, Integrity and Availability of data are outlined below.

Table 37: Confidentiality, Integrity and Availability best practice for IEEE C37.118

Confidentiality	Integrity	Availability
The IEEE C37.118 standard does not specify any requirement for a cryptographic signature or encryption of data.	The IEEE C37.118 standard incorporates a cyclic redundancy check (CRC) against CHK bits within C37.118 packets to protect against modification.	The IEEE C37.118 standard does not specify any mechanism to protect the availability of data.

Synchrophasor systems frequently require communication to pass over insecure networks, as there is no facility within C37.118 with which to implement secure communications, this must be provided by the communications network used to transport the synchrophasor data. Although the mechanisms for encryption and end-to-end secure transport of TCP are ubiquitous, careful analysis is required to ensure that the networks, components and any connectivity or use unrelated to the synchrophasor system does not compromise the system security. Table X outlines the generic steps required.

Table 38: Security risk assessment and system design for IEEE C37.118

Task	Description	Output
Identify network components	This stage ensures that there is a comprehensive understanding of all the assets connected to the synchrophasor network. This should be all connected components, including those that play no functional part in the synchrophasor system.	Detailed asset list
Identify communication paths and connected networks	For the synchrophasor network, identify internal and external connections, within and between sites. Routes, locations, ownership, third-party management and access should be determined.	Network diagram, location map, inventory of inter-site links and providers
Vulnerability assessment	Assess the vulnerability of assets and networks, e.g. carry out penetration testing of network components.	Vulnerabilities
Create model, define security zones and conduits	Using the information from the above tasks, identify security zones and conduits. Trusted conduits crossing	Documentation identifying zone boundaries and detailing security levels

	zone boundaries need to use an end-to-end secure process, for example a VPN	
Assess the risks and consequences of attack	With an understanding of vulnerabilities and interconnectivity, assess the risks from attack vectors and actors. Where communication is via a 3rd party network, or a network accessible and managed by 3rd parties, it is recommended that these networks are assessed as untrusted, as the supply chain presents an unknow risk.	Target security level requirement for zones and conduits
Mitigated Design	Produce system architecture to meet target security levels, to include detailed specification and requirements for controls, configuration and connectivity.	Network diagram, specification, and requirements

6.2.2 IEC 61850-9-2 SV

IEC 61850-9-2 Sampled Values (SV) is a layer 2 protocol for the intended use of sending measurements within a local area network (e.g. substation). Measurements are received from Instrument Transformers (which sample analog signals to digital) or Merging Units (MU) which collate analog signals (e.g. voltage and current) from CT/VTs and format the data as a digital representation. The standard specifies that the sampling rate for these values is 4000 samples/sec for 50Hz systems and 4800 samples/sec for 60Hz systems. Compared to C37.118 data, which has a sampling rate of 30-60 samples/sec.

Recommendations to ensure best practice

The best practice guidelines for securing IEC 61850-9-2 (SV) with respect to Confidentiality, Integrity and Availability of data are outlined below.

Table 39: Confidentiality, Integrity and Availability best practice for IEC 61850-9-2 SV

Confidentiality	Integrity	Availability

The IEC 62351-6 (Security for 61850) standard specifies IEC 61850-9-2 SV applications requiring 4ms response time, multicast and low CPU overhead should not use encryption. IEC 61850-9-2 SV is restricted to logical substation LANs and confidentially shall be protected by the network.	The IEC 62351-6 standard specifies the use of a Hash-based Message Authentication Code (HMAC) within the extended PDU of the SV application protocol.	Neither IEC 61850-9-2 nor IEC 62351-6 standards specify any mechanism to protect the availability of data.

Table 40: Security risk assessment and system design for IEC 61850-9-2 SV

Task	Description	Output
Identify network components	This stage ensures that there is a comprehensive understanding of all the assets connected to the synchrophasor network. This should be all connected components, including those that play no functional part in the synchrophasor system.	Detailed asset list
Identify communication paths and connected networks	For the synchrophasor network, identify internal and external connections, within and between sites. Routes, locations, ownership, third-party management and access should be determined.	Network diagram, location map, inventory of inter-site links and providers
Vulnerability assessment	Assess the vulnerability of assets and networks, e.g. carry out penetration testing of network components.	Vulnerabilities
Create model, define security zones and conduits	Using the information from the above tasks, identify security zones and conduits. Trusted conduits crossing zone boundaries need to use an end-to-end secure process, for example a VPN	Documentation identifying zone boundaries and detailing security levels
Assess the risks and consequences of attack	With an understanding of vulnerabilities and interconnectivity, assess the	Target security level requirement for zones and conduits

	risks from attack vectors and actors. Where communication is via a 3rd party network, or a network accessible and managed by 3rd parties, it is recommended that these networks are assessed as untrusted, as the supply chain presents an unknow risk.	
Mitigated Design	Produce system architecture to meet target security levels, to include detailed specification and requirements for controls, configuration and connectivity.	Network diagram, specification, and requirements

6.2.3 IEC 61850-90-5 R-SV

As IEC 61850-9-2 (SV) is a layer 2 protocol, it is only confined to local area networks (i.e. communications within a substation). With the interoperability of networks and the requirement for data exchange between substations rather than inside, this presents a problem for the non-routable 61850-9-2 SV standard. IEC 61850-90-5 (R-SV) addresses this problem by encapsulating the 61850-9-2 SV application message within a transport layer protocol, allowing the data to be routed over a wide area network. IEC 61850-90-5 specifies a new profile for SV messaging over an IP-Multicast network using UDP/IP.

Additional security measures were required for the standard, as the confidentiality and integrity of the data was at risk traversing over an untrusted wide area network. These features include encryption and authentication based on cryptographic keys.

Recommendations to ensure best practice

The best practice guidelines for securing IEC 61850-90-5 (R-SV) with respect to Confidentiality, Integrity and Availability of data are outlined below.

Table 41: Confidentiality, Integrity and Availability best practice for IEC 61850-90-5 R-SV

Confidentiality	Integrity	Availability
The IEC 61850-90-5 standard specifies encryption of data, perfect forward secrecy (PFS) using symmetric keys distributed by a KDC to publishers and subscribers.	The IEC 61850-90-5 standard specifies cryptographic signatures for authentication to ensure integrity of data.	The IEC 61850-90-5 standard does not specify any mechanism to protect the availability of data.

Table 42: Security risk assessment and system design for IEC 61850-90-5 R-SV

Task	Description	Output
Identify network components	This stage ensures that there is a comprehensive understanding of all the assets connected to the synchrophasor network. This should be all connected components, including those that play no functional part in the synchrophasor system.	Detailed asset list
Identify communication paths and connected networks	For the synchrophasor network, identify internal and external connections, within and between sites. Routes, locations, ownership, third-party management and access should be determined.	Network diagram, location map, inventory of inter-site links and providers
Vulnerability assessment	Assess the vulnerability of assets and networks, e.g. carry out penetration testing of network components.	Vulnerabilities
Create model, define security zones and conduits	Using the information from the above tasks, identify security zones and conduits. Trusted conduits crossing zone boundaries need to use an end-to-end secure process, for example a VPN	Documentation identifying zone boundaries and detailing security levels
Assess the risks and consequences of attack	With an understanding of vulnerabilities and interconnectivity, assess the risks from attack vectors and actors. Where communication is via a 3rd party network, or a network accessible and managed by 3rd parties, it is recommended that these networks are assessed as untrusted, as the supply chain presents an unknow risk.	Target security level requirement for zones and conduits

Mitigated Design	Produce system architecture to meet target security levels, to include detailed specification and requirements for controls, configuration and connectivity.	Network diagram, specification, and requirements

6.2.4 IEC 61850-8-1 GOOSE

The IEC 61850-8-1 (GOOSE) protocol can be used to relay Control signals to the DRZC.

IEC 61050 Generic Object-Oriented Substation Events (GOOSE) is designed to provide reliable and fast transmission of electrical substation events over the local area network using layer 2 multicast or broadcast packets in a publish-subscribe scenario.

The end-to-end latency requirements of GOOSE, (4ms for 60hz systems), and limited resources available in substation intelligent electronic devices (IED), mean in practical terms, that it is not feasible to implement end-to-end encryption of data. Security measures specified in IEC 62351-6 recommend the use of the asymmetric cryptography-based Hash Message Authentication Code (HMAC) using an RSA digital signature, although many implementations of the GOOSE protocol do not have this implemented and remain vulnerable to attack.

The following vulnerabilities that attacker could do against the IEC 61850 protocol:

- Man-in-the-middle attack
- Replay attack
- Injection attack
- Spoofing
- Eavesdropping
- Denial of Service (DoS)

Note: some attacks may be mitigated by the IEC 62351-6 HAMC, however research suggest that the protocol is still vulnerable to attack, (ref: Reda, H.T., et al. Vulnerability and Impact Analysis of the IEC 61850 GOOSE Protocol in the Smart Grid. Sensors 2021, 21, 1554. https://doi.org/10.3390/s21041554).

Recommendations to ensure best practice

The best practice guidelines for securing IEC 61850-8-1 (GOOSE) with respect to Confidentiality, Integrity and Availability of data are outlined below.

Table 43: Confidentiality, Integrity and Availability best practice for IEC 61850-8-1 GOOSE

Confidentiality	Integrity	Availability

The IEC 62351-6 (Security for 61850) standard specifies IEC 61850-8-1 GOOSE applications requiring 4ms response time, multicast and low CPU overhead should not use encryption. IEC 61850-8-1 GOOSE is restricted to logical substation LANs and confidentially shall be protected by the network.	The IEC 62351-6 standard specifies the use of a Hash-based Message Authentication Code (HMAC) within the extended PDU of the GOOSE application protocol.	Neither IEC 61850-8-1 nor IEC 62351-6 standards specify any mechanism to protect the availability of data.

The GOOSE protocol does not encrypt data in transit but may digitally sign messages, given the broadcast nature of the protocol it is still vulnerable to attack from a malicious actor who is locally connected or has connectivity to a compromised locally connected system.

Table 44: Security risk assessment and system design for IEC 61850-8-1 GOOSE

Task	Description	Output
Identify network components	This stage ensures that there is a comprehensive understanding of all the assets connected to the same layer 2 network as GOOSE IED's. This should be all connected components, including those that are connected to, but unrelated to the GOOSE systems.	Detailed asset list
Identify communication paths and connected networks	The layer 2 GOOSE protocol is restricted to the Ethernet broadcast domain containing the IED's connected by the protocol. Although not routable, this may be connected to other physical locations using direct layer 2 connections or tunnelled over layer 3 networks using layer 2 tunnelling protocol (L2TP), this should be considered when assessing the network attack surface. For any external connections identified, within and between	Network diagram, location map, inventory of inter-site links and providers

	sites, routes, locations, ownership, third-party management, and access should be determined.	
Vulnerability assessment	Assess the vulnerability of assets and networks, e.g. carry out penetration testing of network components / IED's.	Vulnerabilities
Create model, define security zones and conduits	Using the information from the above tasks, identify security zones and conduits. Trusted conduits crossing zone boundaries need to use an end-to-end secure process, for example a VPN	Documentation identifying zone boundaries and detailing security levels
Assess the risks and consequences of attack	With an understanding of vulnerabilities and interconnectivity, assess the risks from attack vectors and actors. Where communication is via a 3rd party network, or a network accessible and managed by 3rd parties, it is recommended that these networks are assessed as untrusted, as the supply chain presents an unknow risk.	Target security level requirement for zones and conduits
Mitigated Design	Produce system architecture to meet target security levels, to include detailed specification and requirements for controls, configuration and connectivity.	Network diagram, specification, and requirements

6.2.5 IEC 61850-90-5 R-GOOSE

As IEC 61850-8-1 (GOOSE) is a layer 2 protocol, it is only confined to local area networks (i.e. communications within a substation). With the interoperability of networks and the requirement for data exchange between substations rather than inside, this presents a problem for the non-routable 61850-8-1 GOOSE standard. IEC 61850-90-5 (R-GOOSE) addresses this problem by encapsulating the 61850-8-1 GOOSE application message within a transport layer protocol, allowing the data to be routed over a wide area network. IEC 61850-90-5 specifies a new profile for GOOSE messaging over an IP-Multicast network using UDP/IP.

Additional security measures were required for the standard, as the confidentiality and integrity of the data was at risk traversing over an untrusted wide area network. These features include encryption and authentication based on cryptographic keys.

The following vulnerabilities that attacker could do against the IEC 61850-90-5 (R-GOOSE) protocol:

- Man-in-the-middle attack
- Packet injector attacker
- Replay attack
- Denial of Service (DoS

Recommendations to ensure best practice

The best practice guidelines for securing IEC 61850-90-5 (R-GOOSE) with respect to Confidentiality, Integrity and Availability of data are outlined below.

Table 45: Confidentiality, Integrity and Availability best practice for IEC 61850-90-5 R-GOOSE

Confidentiality	Integrity	Availability
The IEC 61850-90-5 standard specifies encryption of data, perfect forward secrecy (PFS) using symmetric keys distributed by a KDC to publishers and subscribers.	The IEC 61850-90-5 standard specifies cryptographic signatures for authentication to ensure integrity of data.	The IEC 61850-90-5 standard does not specify any mechanism to protect the availability of data.

The R-GOOSE protocol uses certificates are required for key negotiation and update, the key negotiation between devices and Key Distribution Centre (KDC) and most popular encryption algorithms like AES-CBC or 3DES-CB.

Table 46: Security risk assessment and system design for IEC 61850-90-5 R-GOOSE

Task	Description	Output
Identify network components	This stage ensures that there is a comprehensive understanding of all the assets connected to the same layer 3 network as R-GOOSE.	Detailed asset list
Identify communication paths and connected networks	The layer 3 R-GOOSE protocol is restricted to the Ethernet multicast and broadcast containing the connected by the protocol.	Network diagram, location map, inventory of inter-site links and providers

Vulnerability assessment	Assess the vulnerability of assets and networks, e.g. carry out penetration testing of network devices	Vulnerabilities
Create model, define security zones and conduits	Using the information from the above tasks, identify security zones and conduits. Trusted conduits crossing zone boundaries need to use an end-to-end secure process, for example a VPN	Documentation identifying zone boundaries and detailing security levels
Assess the risks and consequences of attack	With an understanding of vulnerabilities and interconnectivity, assess the risks from attack vectors and actors. Where communication is via a 3rd party network, or a network accessible and managed by 3rd parties, it is recommended that these networks are assessed as untrusted, as the supply chain presents an unknow risk.	Target security level requirement for zones and conduits
Mitigated Design	Produce system architecture to meet target security levels, to include detailed specification and requirements for controls, configuration, and connectivity.	Network diagram, specification, and requirements

6.2.6 IEC 61850-8-1 MMS

The IEC 61850-8-1 MMS (Manufacturing Message Specification) protocol is a client or server-based protocol for communications between IEDs.

The following vulnerabilities that attacker could do against the IEC 61850 MMS protocol:

- Man-in-the-middle attack
- Packet injector attacker

Recommendations to ensure best practice

The best practice guidelines for securing IEC 61850-8-1 MMS with respect to Confidentiality, Integrity and Availability of data are outlined below.

Table 47: Confidentiality, Integrity and Availability best practice for IEC 61850-8-1 MMS

Confidentiality	Integrity	Availability
The IEC 62351-4 (Security for MMS) standard specifies TLS for encryption of data.	The IEC 62351-4 (Security for MMS) standard specifies application layer authentication via the exchange of Association Control Service Element (ACSE) AARQ and AARE protocol data units (PDU)s.	Neither IEC 61850-8-1 nor IEC 62351-4 standards specify any mechanism to protect the availability of data.

The certificate-based security mechanism in IEC 61850 MMS messages is used prevent unwanted access to the substation or spoofing by using the certificate of the devices.

Table 48: Security risk assessment and system design for IEC 61850-8-1 MMS

Task	Description	Output
Identify network components	This stage ensures that there is a comprehensive understanding of all the assets connected to the same network as IEC 61850 MMS.	Detailed asset list
Identify communication paths and connected networks	The IEC 61850 MMS protocol is restricted to the Ethernet domain containing the devices connected by this protocol.	Network diagram, location map, inventory of inter-site links and providers
Vulnerability assessment	Assess the vulnerability of assets and networks, e.g. carry out penetration testing of devices	Vulnerabilities
Create model, define security zones and conduits	Using the information from the above tasks, identify security zones and conduits. Trusted conduits crossing zone boundaries need to use an end-to-end secure process, for example a VPN	Documentation identifying zone boundaries and detailing security levels
Assess the risks and consequences of attack	With an understanding of vulnerabilities and interconnectivity, assess the risks from attack vectors and actors. Where communication is via a 3rd party network, or a	Target security level requirement for zones and conduits

	network accessible and managed by 3rd parties, it is recommended that these networks are assessed as untrusted, as the supply chain presents an unknow risk.	
Mitigated Design	Produce system architecture to meet target security levels, to include detailed specification and requirements for controls, configuration, and connectivity.	Network diagram, specification, and requirements

6.2.7 IEC 60870-5-104

The IEC 60870-5-104 protocol is companion standard of IEC 60870-5, this standard defines the use of an open TCP/IP-interface to transport data and an extension of IEC 101 protocol with the changes in transport, network, link, and physical layer services to suit the network access.

The following vulnerabilities that attacker could do against the IEC 60870-5-104 protocol:

- Man-in-the-middle attack
- Packet injector attacker
- Replay attack
- Denial of Service (DoS)

Recommendations to ensure best practice

The best practice guidelines for securing IEC 60870-5-104 with respect to Confidentiality, Integrity and Availability of data are outlined below.

Table 49: Confidentiality, Integrity and Availability best practice for IEC 60870-5-104

Confidentiality	Integrity	Availability
The IEC 60870-5-7 (Security extensions to IEC 60870-5-101 and IEC 60870-5-104) specifies TLS for encryption of data with accordance to IEC 62351-3.	The IEC 60870-5-7 (Security extensions to IEC 60870-5-101 and IEC 60870-5-104) specifies application layer authentication using Message Authentication Codes (MAC) with accordance to IEC 62351-5	Neither IEC 60870-5-104, IEC 60870-5-7 or IEC 62351-5 specifies any mechanism to protect the availability of data.

Recommendation for IEC 60870-5-104 protocol is that vendor examine the behaviour of the protocol messages, via checking the field lengths are used that do not match with the actual length should be in the protocol specification. The first three bytes of an IEC-104 message are received, these bytes can already be parsed to identify which message format was received on the device. If the message received is a U-format or S-format type, it will have a length field of four. If the field is greater than four the message is faulty, the device should recognise these messages as faulty and drop them to ensure the device is less prone to denial-of-service attacks.

To ensure the integrity of the IEC 60870-5-104 protocol, authentication needs to take place before IEC-104 messages can be sent to the device and this can be accomplished by implementing standards like IEC 62351, which provides end-to-end encryption.

Table 50: Security risk assessment and system design for IEC 60870-5-104

Task	Description	Output
Identify network components	This stage ensures that there is a comprehensive understanding of all the assets connected to the same network layer as devices using IEC 60870-5-104 protocol.	Detailed asset list
Identify communication paths and connected networks	The IEC 60870-5-104 (IEC 104) protocol is an extension of the IEC 101 protocol, this including the transport, network, link, and physical layer extensions to enable a full network access	Network diagram, location map, inventory of inter-site links and providers
Vulnerability assessment	Assess the vulnerability of assets and networks, e.g. carry out penetration testing of network components.	Vulnerabilities
Create model, define security zones and conduits	Using the information from the above tasks, identify security zones and conduits. Trusted conduits crossing zone boundaries need to use an end-to-end secure process, for example a VPN	Documentation identifying zone boundaries and detailing security levels
Assess the risks and consequences of attack	With an understanding of vulnerabilities and interconnectivity, assess the risks from attack vectors and actors. Where communication is via a 3rd party network, or a network accessible and managed by 3rd parties, it is recommended that these	Target security level requirement for zones and conduits

	networks are assessed as untrusted, as the supply chain presents an unknow risk.	
Mitigated Design	Produce system architecture to meet target security levels, to include detailed specification and requirements for controls, configuration, and connectivity.	Network diagram, specification, and requirements

6.2.8 DNP3

The DNP3 protocol was developed for the intended use to communicate data outside substations, allowing interoperability between control centres and substation systems over a wide area network. It was developed as an open standard based on IEC 60870-5-101/104 to provide a scalable and reliable option for exchanging SCADA data. Unlike IEC 104, which polls data at the same frequency (1Hz), DNP3 provides 3 data priority classes enabling it to poll data at different frequencies. This is an advantage over IEC 104 in networks where bandwidth is limited. DNP3 also operates at higher baud rates, allowing it to transmit data faster through a network.

The following vulnerabilities an attacker could exploit against the DNP3 protocol are:

- Man-in-the-middle attack
- Packets drops attack
- Dropping attack DNP3 packets modification and injection attacks
- Denial of Service (DoS) attack

Recommendations to ensure best practice

The best practice guidelines for securing DNP3 with respect to Confidentiality, Integrity and Availability of data are outlined below.

Table 51: Confidentiality, Integrity and Availability best practice for DNP3

Confidentiality	Integrity	Availability
The IEEE 1815-2019 standard does not specify any requirement for encryption of data.	The IEEE 1815-2019 standard specifies application layer authentication using Message Authentication Codes (MAC). This specification is based on IEC 62351-5.	The IEEE 1815-2019 standard does not specify any mechanism to protect the availability of data.

Table 52: Security risk assessment and system design for DNP3

Task	Description	Output
Identify network components	This stage ensures that there is a comprehensive understanding of all the assets connected to the same network layer as devices using DNP3 protocol.	Detailed asset list
Identify communication paths and connected networks	The DNP3 is based on IEC 60870-5-104 (IEC 104) protocol, which is also an extension of the IEC 101 protocol, this including the transport, network, link, and physical layer extensions to enable a full network access	Network diagram, location map, inventory of inter-site links and providers
Vulnerability assessment	Assess the vulnerability of assets and networks, e.g. carry out penetration testing of network components.	Vulnerabilities
Create model, define security zones and conduits	Using the information from the above tasks, identify security zones and conduits. Trusted conduits crossing zone boundaries need to use an end-to-end secure process, for example a VPN	Documentation identifying zone boundaries and detailing security levels
Assess the risks and consequences of attack	With an understanding of vulnerabilities and interconnectivity, assess the risks from attack vectors and actors. Where communication is via a 3rd party network, or a network accessible and managed by 3rd parties, it is recommended that these networks are assessed as untrusted, as the supply chain presents an unknow risk.	Target security level requirement for zones and conduits
Mitigated Design	Produce system architecture to meet target security levels, to include detailed specification and requirements for controls,	Network diagram, specification, and requirements

	configuration, and connectivity.	

6.2.9 Precision Time Protocol (PTP)

The Precision Time protocol (PTP) protocol is used for synchronizing clocks throughout the network

The following vulnerabilities that attacker could do against the PTP protocol:

- Man-in-the-middle attack
- Packet injector attacker
- Replay attack
- Denial of Service (DoS)

Recommendations to ensure best practice

The best practice guidelines for securing IEEE 1588 PTP with respect to Confidentiality, Integrity and Availability of data are outlined below.

Table 53: Confidentiality, Integrity and Availability best practice for IEEE 1588 PTP

Confidentiality	Integrity	Availability
Confidentiality of time protocol data is not protected as the information is not confidential (i.e. the current time)	The IEEE 1588-2019 standard specifies an authentication type-length-value (TLV), which appends a cryptographic integrity check to each PTP message. The mechanism uses symmetric keys for signing.	The IEEE 1588-2019 standard specifies authentication for master clocks to prevent denial of service to intermediate clocks. This is on the application layer and only protects from specific DoS attacks. Layer 2 and 3 DoS attacks are still vulnerable.

The Precision Time protocol (PTP) protocol makes use of an Authentication Type-Length-Value (TLV) and this verification approach, an associated key management protocol. The Authentication TLV in this case is used to carry security related information necessary for calculating an ICV to provide integrity and authenticity

Table 54: Security risk assessment and system design for IEEE 1588 PTP

Task	Description	Output
Identify network components	This stage ensures that there is a comprehensive understanding of all the assets connected to the same network layer as devices using Precision Time protocol (PTP) protocol.	Detailed asset list

Identify communication paths and connected networks	The Precision Time protocol (PTP) protocol is used a synchronize clocks throughout the network	Network diagram, location map, inventory of inter-site links and providers
Vulnerability assessment	Assess the vulnerability of assets and networks, e.g. carry out penetration testing of network components.	Vulnerabilities
Create model, define security zones and conduits	Using the information from the above tasks, identify security zones and conduits. Trusted conduits crossing zone boundaries need to use an end-to-end secure process, for example a VPN	Documentation identifying zone boundaries and detailing security levels
Assess the risks and consequences of attack	With an understanding of vulnerabilities and interconnectivity, assess the risks from attack vectors and actors. Where communication is via a 3rd party network, or a network accessible and managed by 3rd parties, it is recommended that these networks are assessed as untrusted, as the supply chain presents an unknow risk.	Target security level requirement for zones and conduits
Mitigated Design	Produce system architecture to meet target security levels, to include detailed specification and requirements for controls, configuration, and connectivity.	Network diagram, specification, and requirements

6.2.10 Network Time Protocol (NTP)

The NTP (Network Time Protocol) protocol is used for synchronizing the time of a system between client and server.

The following vulnerabilities that attackers can exploit against the NTP services are:

- Denial of Service (DoS)
- Information Leakage on the services

Recommendations to ensure best practice

The best practice guidelines for securing NTP with respect to Confidentiality, Integrity and Availability of data are outlined below.

Table 55: Confidentiality, Integrity and Availability best practice for NTP

Confidentiality	Integrity	Availability
Confidentiality of time protocol data is not protected as the information is not confidential (i.e. the current time)	RFC5906 specifies an asymmetric key mechanism for authentication of NTP v4, however, this was discovered to be insecure. There is currently a mechanism Network Time Security (NTS) in development however it is not yet standardised. NTS looks to add a secure authentication mechanism to NTP.	NTP does not use an application layer mechanism to protect the availability of data.

The following best practices are used to secure the NTP services on an appliance or server:

- Enable access control list to only allow specific IP addresses to synchronize with
- Restrict the commands that can be used on the NTP services.
- Do not allow queries of the NTP services.
- Only allow known networks/devices to communicate with their respective NTP services.
- Enabling NTP Encryption
- Monitor Restarts of the NTP service

Table 56: Security risk assessment and system design for NTP

Task	Description	Output
Identify network components	This stage ensures that there is a comprehensive understanding of all the assets connected to the same network layer as devices using Network Time Protocol (NTP) protocol.	Detailed asset list
Identify communication paths and connected networks	The Network Time Protocol (NTP) protocol is used to	Network diagram, location map, inventory of inter-site links and providers

	synchronize time between client and server.	
Vulnerability assessment	Assess the vulnerability of assets and networks, e.g. carry out penetration testing of network components.	Vulnerabilities
Create model, define security zones and conduits	Using the information from the above tasks, identify security zones and conduits. Trusted conduits crossing zone boundaries need to use an end-to-end secure process, for example a VPN	Documentation identifying zone boundaries and detailing security levels
Assess the risks and consequences of attack	With an understanding of vulnerabilities and interconnectivity, assess the risks from attack vectors and actors. Where communication is via a 3rd party network, or a network accessible and managed by 3rd parties, it is recommended that these networks are assessed as untrusted, as the supply chain presents an unknown risk.	Target security level requirement for zones and conduits
Mitigated Design	Produce system architecture to meet target security levels, to include detailed specification and requirements for controls, configuration, and connectivity.	Network diagram, specification, and requirements

6.3 Data and Protocol Comparison

The following section looks at the main data exchanges for delivering BlackStart and the comparison of potential protocols that may be used to complete each function, with a focus and discussion around the security provided (or applied) to each.

6.3.1 Synchrophasor Data

Both IEEE C37.118 and IEC 61850-90-5 R-SV have the capability to carry synchrophasor data over a wide area network. This is required as part of the DRZC architecture to send measurements from

DER sites and substations to the central DRZ controller, and control centres for offline monitoring. Below is a comparison of the two protocols (from Section 2.2).

Table 57: Comparison of protocols capable of carrying synchrophasor data

Protocol	Confidentiality	Integrity	Availability
IEEE C37.118	The IEEE C37.118 standard does not specify any requirement for a cryptographic signature or encryption of data.	The IEEE C37.118 standard incorporates a cyclic redundancy check (CRC) against CHK bits within C37.118 packets to protect against modification.	The IEEE C37.118 standard does not specify any mechanism to protect the availability of data.
IEC 61850-90-5 R-SV	The IEC 61850-90-5 standard specifies encryption of data, perfect forward secrecy (PFS) using symmetric keys distributed by a KDC to publishers and subscribers.	The IEC 61850-90-5 standard specifies cryptographic signatures for authentication to ensure integrity of data.	The IEC 61850-90-5 standard does not specify any mechanism to protect the availability of data.

IEEE C37.118 does not specify encryption or authentication for confidentiality and integrity of data, however it is recommended to use IEEE C37.118 (over TCP) with TLS in accordance with IEC 62351-3. Client certificate authentication using digital certificates should also be used to verify the identity of the publisher and subscriber and provide additional data integrity protection.

Alternatively, a secure VPN can be established between the substation gateway and control centre gateway

IEC 61850-90-5 R-SV specifies encryption and authentication using symmetric keys issued from a KDC (specified in IEC 62351-6/62351-9). Symmetric keys are a single key shared among parties used for encrypting and decrypting data. DRZC BlackStart utilises the data from multiple parties and information is exchanged via interconnected networks. Granting another party access to an organisations KDC highlights some security implications. The third-party would be responsible for the security controls for protecting the organisations private keys, which would require additional security requirements and risk assessments. On the other hand, the organisation would require allowing the third-party access to the KDC, increasing the attack surface of compromising private keys cross-party.

Additional security implications when utilising a central KDC within an ICS environment are due to the different security zones. Synchrophasor data crosses different trust boundaries and zones, where the higher criticality security zones will not allow ingress connections – resulting in the KDC being situated in the least secure zone.

Due to the implications of utilising a KDC in a multi-party environment, it is recommended to use IEEE C37.118 with TLS for transmitting synchrophasor data in the BlackStart DRZC architecture between **third parties**. IEC 61850-90-5 for communications between single party sites can be utilised with connections to an organisation's KDC.

6.3.2 Fast-Balancing Data

There are multiple protocols that have the capability of carrying control data over a wide area network, many of which are widely used within ICS environments. For the functional specification of the BlackStart scheme, some of these protocols (the fast-balancing protocols) need to have a very low response time, typically in the 100s of milliseconds. Below is a comparison of the different protocols (from Section 2.2).

Table 58: Comparison of protocols capable of carrying fast response control data

Protocol	Confidentiality	Integrity	Availability
IEC 61850-90-5 R-GOOSE	The IEC 61850-90-5 standard specifies encryption of data, perfect forward secrecy (PFS) using symmetric keys distributed by a KDC to publishers and subscribers.	The IEC 61850-90-5 standard specifies cryptographic signatures for authentication to ensure integrity of data.	The IEC 61850-90-5 standard does not specify any mechanism to protect the availability of data.
IEC 60870-5-104	The IEC 60870-5-7 (Security extensions to IEC 60870-5-101 and IEC 60870-5-104) standard specifies TLS for encryption of data with accordance to IEC 62351-3.	The IEC 60870-5-7 (Security extensions to IEC 60870-5-101 and IEC 60870-5-104) standard specifies application layer authentication using Message Authentication Codes (MAC) with accordance to IEC 62351-5	Neither IEC 60870-5-104, IEC 60870-5-7 or IEC 62351-5 standards specify any mechanism to protect the availability of data.
DNP3	The IEEE 1815-2012 standard does not specify any requirement for encryption of data.	The IEEE 1815-2012 standard specifies application layer authentication using Message Authentication Codes (MAC). This specification is based on IEC 62351-5.	The IEEE 1815-2012 standard does not specify any mechanism to protect the availability of data.

IEC 61850-90-5 R-GOOSE specifies encryption and authentication using symmetric keys issued from a KDC (specified in IEC 62351-6/62351-9). Symmetric keys are a single key shared among parties used for encrypting and decrypting data. DRZC BlackStart utilises the data from multiple parties and information is exchanged via interconnected networks. Granting another party access to an organisations KDC highlights some security implications. The third-party would be responsible for the security controls for protecting the organisations private keys, which would require additional security requirements and risk assessments. On the other hand, the organisation would require allowing the third-party access to the KDC, increasing the attack surface of compromising private keys cross-party.

IEC 62351-3 specifies the requirements for TLS with IEC 60870-5-104 for encryption of data, with regards to cipher suites, key size, certificate lifecycle and management. IEC 62351-5 specifies the use of message authentication codes and extending the IEC 60870-5-104 Application Service Data Unit (ASDU) to include authentication of messages to protect their integrity in transit.

The IEEE 1815-2012 does not specify encryption for confidentiality for data, however it is recommended to use DNP3 with TLS in accordance with IEC 62351-3. IEEE 1815-2012 specifies the use of application layer authentication, known as DNP3 Secure Authentication (DNP3-SA) which adds an additional layer using MAC authentication to verify the integrity of messages.

Due to the implications of utilising a KDC in a multi-party environment, it is recommended to use either IEC 60870-5-104 with TLS or DNP3-SA with TLS for transmitting fast-balancing data in the BlackStart DRZC architecture between **third parties**. Analysis on the additional latency overheads when using TLS with the fast-balancing protocols should be considered when designing the BlackStart architecture. IEC 61850-90-5 for communications between single party sites can be utilised with connections to an organisation's KDC.

6.3.3 Slow-Balancing Data

In addition to carrying fast acting data, there is a requirement for data with slower response times for bringing generation into the DRZC. Due to this data not requiring fast response times, the options for protocols are greater and less dependant on the performance of the protocol.

Table 59: Comparison of protocols capable of carrying slow response control data

Protocol	Confidentiality	Integrity	Availability
IEC 61850-90-5 R-GOOSE	The IEC 61850-90-5 standard specifies encryption of data, perfect forward secrecy (PFS) using symmetric keys distributed by a KDC to publishers and subscribers.	The IEC 61850-90-5 standard specifies cryptographic signatures for authentication to ensure integrity of data.	The IEC 61850-90-5 standard does not specify any mechanism to protect the availability of data.
IEC 60870-5-104	The IEC 60870-5-7 (Security extensions to IEC 60870-5-101 and IEC 60870-5-104)	The IEC 60870-5-7 (Security extensions to IEC 60870-5-101 and IEC 60870-5-104)	Neither IEC 60870-5-104, IEC 60870-5-7 or IEC 62351-5 standards specify any

	standard specifies TLS for encryption of data with accordance to IEC 62351-3.	standard specifies application layer authentication using Message Authentication Codes (MAC) with accordance to IEC 62351-5	mechanism to protect the availability of data.
DNP3	The IEEE 1815-2012 standard does not specify any requirement for encryption of data.	The IEEE 1815-2012 standard specifies application layer authentication using Message Authentication Codes (MAC). This specification is based on IEC 62351-5.	The IEEE 1815-2012 standard does not specify any mechanism to protect the availability of data.
IEC 61850-8-1 MMS	The IEC 62351-4 (Security for MMS) standard specifies TLS for encryption of data.	The IEC 62351-4 (Security for MMS) standard specifies application layer authentication via the exchange of Association Control Service Element (ACSE) AARQ and AARE protocol data units (PDU)s.	Neither IEC 61850-8-1 nor IEC 62351-4 standards specify any mechanism to protect the availability of data.

See Section 2.3.2 for overview of IEC 61850-90-5 R-GOOSE, IEC 60870-5-104 and DNP3.

IEC 62351-4 specifies the requirements for TLS with IEC 61850-8-1 MMS for encryption of data, with regards to cipher suits, key size, certificate lifecycle and management. IEC 62351-4 specifies the use of peer authentication on the application layer where ACSE AARQ and AARE PDUs carry the calling-authentication-value and responding-authentication-value used for authenticating the messages (i.e. the client passes an authentication string with each message, which is verified by the server). The authentication string is sent as plaintext.

Due to the implications of utilising a KDC in a multi-party environment, it is recommended to use either IEC 60870-5-104 with TLS or DNP3-SA with TLS for transmitting slow-balancing data in the BlackStart DRZC architecture between **third parties**. The additional latency overhead when using TLS with the slow-balancing protocols is likely to be redundant due to the higher margin for error in the slower response times. IEC 61850-90-5 for communications between single party sites can be utilised with connections to an organisation's KDC.

6.3.4 Time Synchronisation Data

Table 60: Comparison of protocols capable of carrying time synchronisation

Protocol	Confidentiality	Integrity	Availability
IEEE 1588 PTP	Confidentiality of time protocol data is not protected as the information is not confidential (i.e. the current time)	The IEEE 1588-2019 standard specifies an authentication type-length-value (TLV), which appends a cryptographic integrity check to each PTP message. The mechanism uses symmetric keys for signing.	The IEEE 1588-2019 standard specifies authentication for master clocks to prevent denial of service to intermediate clocks. This is on the application layer and only protects from specific DoS attacks. Layer 2 and 3 DoS attacks are still vulnerable.
NTP	Confidentiality of time protocol data is not protected as the information is not confidential (i.e. the current time)	RFC5906 specifies an asymmetric key mechanism for authentication of NTP v4, however, this was discovered to be insecure. There is currently a mechanism Network Time Security (NTS) in development however it is not yet standardised. NTS looks to add a secure authentication mechanism to NTP.	NTP does not use an application layer mechanism to protect the availability of data.

IEEE 1518 PTP is the recommended approach for time synchronisation within wide area networks. PTP offers additional security features (as NTS is still in development) and provides a more accurate time reference.

Due to the current lack of security and less accurate timing of NTP, it is recommended to use IEEE 1518 PTP for time synchronisation in the DRZC BlackStart architecture.

7 System Hardening – Best Practice

7.1 Hardware

Hardware security is an often-overlooked discipline when designing a secure system. It is essential to include this extra line of defense when following a layered approach to security. Physical attacks are becoming more of a threat within ICS environments with the increase in controllers, IEDs, relays and RTUs – many of which are situated in remote areas and are at an increased risk of being accessible by a malicious actor.

Many devices utilise cryptographic keys for encrypting data – if these keys are stored on hardware chips that are vulnerable to physical tampering, the keys can be extracted and used to decrypt the protected resources. Unused ports without proper security measures could also be used to gain access to the device.

The following is a list of common hardware attacks:

- Manufacturing backdoors
- Exploitation of debugging ports including JTAG interfaces and serial consoles
- Bypass of firmware signature and encryption protection
- Decryption and analysis of outgoing communication
- Exploitation of network interfaces
- Access to unencrypted storage on the device
- Outdated and excessive software and services
- Hardcoded credentials

To protect against these common hardware attacks, the following best practices should be followed to ensure a greater level of security within ICS devices:

- Disable unused hardware interfaces – Universal Asynchronous Receiver-Transmitters (UARTs) for serial communications, NIC interfaces (e.g. Ethernet ports or wireless) and JTAG ports used for communicating directly with on-board chips.
- Hardware-based encryption – hard drives, external flash drives, DRAM
- External physical security – anti-tampering casing, potting electronics to make circuits and chips difficult to access.
- Secure key storage – secure elements protect against tampering and key extraction
- Secure authenticators – Mutual authentication between devices to prevent device spoofing
- Key wiping techniques – Key loaded into chip which is wiped if device is opened or tampered with, environment triggers (such as temperature or light) can also be used as a trigger to automatically wipe keys

7.2 Software

7.2.1 Linux Distributions

Filesystem security

- Disable filesystem mounting for uncommon filesystem types (cramfs, hfs, freevxfs etc.)
- Manage partitions and permissions for folders (/home, /var, /usr)
- Disable USB and media storage
- Configure automatic updates (yum, apt-get)
- Enable filesystem integrity checking (AIDE)
- Enable secure boot
- Configure SELinux and set to enforcing
- Enable sticky bits on world-readable directories

Service security

- Disable unnecessary services (rsh, telnet, NFS, HTTP/Apache/NGINX, SNMP, POP3, FTP etc.)
- Configure accurate time synchronisation (chrony, ntp)

Network security

- Configure IPv4/IPv6 firewall and default deny policy (iptables)
- Configure rules for all open ports (iptables)
- Disable IP forwarding

Logging

- Configure data retention
- Configure syslog/rsyslog/syslog-ng
- Configure journald

Authentication and Authorisation

- Configure PAM – configure password polices, lockout and strong authentication
- Configure user accounts - ensure correct permissions, configure sudo, disable root login
- Configure SSH - disable password login, disable root login

7.2.2 Windows Distributions

User accounts

- Enable and enforce password policies
- Enable and enforce account lockouts and session timeouts
- Disable guest accounts and Microsoft accounts
- Disable anonymous enumeration of SAM accounts and shares
- Remove unused accounts
- Disable anonymous SID/name translation

Local policies

- Allow local system to use computer identity for NTLM
- Disable Local System NULL session fallback
- Lock down local file/folder permissions

Security

- Configure and enable Windows Firewall
- Configure rules for Domain, Private and Public
- Default incoming to block
- Restrict RDP
- Lock down PowerShell and SSH
- Set RDP encryption to high

- Enable Encrypting File System (EFS) with NTFS/Bit locker

Services

- Remove unnecessary services (SMB, ftp, Telnet, ncacn_ip_tcp, NetBIOS)
- Configure accurate time synchronisation (use a third party NTP/PTP client)

Registry settings

- Set MaxCachedSockets to 0
- Set AutoShareServer to 0
- Set AutoShareWks to 0
- Delete all value data inside the NullSessionPipes key
- Delete all value data inside the NullSessionShares key

For more extensive lists for both Linux and Windows, along with an array of other operating systems and technologies, utilise the best practice guidelines set out by the Center for Internet Security (CIS) benchmarks (https://www.cisecurity.org/cis-benchmarks/).

8 Cyber Resilience – Best Practice

8.1 Introduction

Cyber resilience for multi-party Power Systems and Industrial control is the ability to prepare for, respond to and recover from a cyber-attack- against the environment and system.

The standard cyber resilience framework is made up of five key points:

- **Identify** critical assets, systems and data flows. The Power Systems and Industrial control must understand the resources that support all critical functions within the DRZC BlackStart architecture.
- **Protect** critical infrastructure services running DRZC BlackStart. In this step, the Power Systems and Industrial control systems have a set of security programs that will limit or contain the impact of any potential threat.
- **Detect** strange events and suspected breaches or data leaks before major damage occurs. This step demands constant security monitoring of the DRZC BlackStart architecture.
- **Respond** to a detected security breach or failure within the DRZC BlackStart architecture. This function involves an end-to-end incident response plan to ensure business runs as usual in the face of a cyberattack.
- **Recover** to restore any affected DRZC BlackStart infrastructure and services that were compromised during a cybersecurity incident. This step focuses on making a timely return to normal service.

8.2 Cyber Resilience

The following details the five steps that should be followed as part of the cyber resilience:

8.2.1 Identify

The objective of identify is to develop an organisation-wide understanding of managing cybersecurity risks to systems, assets, data, people, and capabilities. This function proves that understanding the context and cybersecurity risks allows DRZC BlackStart architecture to be focused and reliable with its needs and risk management. This includes risk management strategy, risk assessment, governance, business environment, and asset management.

- **Risk management strategy**. This is the development of DRZC architecture priorities, risk tolerances, and restrictions.
- **Risk assessment**. The assessment involves an understanding of the cyber risks in all operations, individuals, and assets in DRZC architecture.
- **Governance**. This is to manage and monitor an DRZC architecture operational, environmental, regulatory, risk, and legal requirements.
- **Business Environment**. The classification of the DRZC architecture objectives, stakeholders, and activities.
- **Asset Management**. This is to identification of facilities, systems, services and data used to accomplish the DRZC architecture.

8.2.2 Protect

This involves developing and implementing suitable safeguards to make sure that the transport of critical services is effective. The limitation and control of secure access to critical physical and digital assets and systems to prevent a breach. Protect has six key categories that include protective technology, maintenance, information protection processes and procedures, data security, awareness and training, and identity management and access control.

- **Protective technology.** This category covers the technical solutions for security and the implementation, review, documentation of log and audit records.
- **Maintenance**. The remote maintenance should be done carefully to prevent unauthorized access. This also promotes maintenance that is appropriately scheduled and implemented.
- **Information Protection Processes and Procedures**. Security policies are maintained and leveraged in this category. These policies are first established under the Governance category of the Identify function of a framework.
- **Data Security** This category revolves around supporting integrity and confidentiality of data while also making it available.
- **Awareness and Training**. Security education must be given to an organization’s personnel. Training should be carried out to uphold the protection strategies of an organization effectively.
- **Identity Management and Access Control.** This covers the appropriate management of credentials and identities related to its system authorized users. This also involves establishing secure access protection for these authorized users.

8.2.3 Detect

Detect aims to implement and develop suitable activities and actions to identify a cybersecurity risk event. The focus of this function is to recognize suspicious activities and quickly access its effect on an organization. This function has three key categories, which include detection processes, security, continuous monitoring, and anomalies and events.

- **Detection Processes.** This covers the definition of roles and responsibilities involved in the detection and the maintenance of activities detecting anomalous events and protection against cyber risks.
- **Security Continuous Monitoring.** Vulnerability review should be carried out throughout DRZC architecture. This should monitor assets and information technology systems to identify issues in security and measure the risk.
- **Anomalies and Events.** The detect events that are considered anomalous and understand the potential effect of these events.

8.2.4 Respond

The respond are suitable sets of actions to be carried out when a cybersecurity event is detected. This supports the capability of the system to withstand the impact of a potential cyberattack. The Respond function covers five key categories, and they are as follows: response planning, communications, analysis, mitigation, and improvements.

- **Response Planning.** After the Detection function when a cybersecurity incident is discovered, this category begins with the execution of the response procedures. In a timely manner, these response plans should be done either during or after the cybersecurity event.
- **Communications.** After following the response plans, must coordinate response activities, and if needed, they may seek help from outside parties.
- **Analysis.** This revolves around investigation and examination of the detected event. Analysis of the impact of the incident and the ability of the organization to take action should be involved.
- **Mitigation.** This involves taking actions that will prevent the cyberattack from continuing and spreading. Mitigating the potential impact of the threat is of utmost importance.
- **Improvements.** After the cybersecurity event, examine and learn the lessons from the previous response to threats. These findings should be improved to help with future related events.

8.2.5 Recover

The recover aims to implement and develop suitable activities to maintain resilience strategies. This also involves the restoration of any damaged services or capabilities caused by a cybersecurity breach. In a timely manner, the DRZC architecture should recover to normal operations to decrease the effect of cyberattacks. This function has three key categories that include recovery planning, improvements, and communications.

- **Recovery Planning.** Depending on the timeliness of the incident, this category can happen during or after the event has concluded. Recovery plans should be carried out, and in a timely manner, all affected systems should be supported, restored, and addressed.

- **Improvements.** This revolves around the lessons learned during and after the cybersecurity event and how these can be used to improve the security strategies of the DRZC architecture.
- **Communications.** This involves the coordination of efforts to concerned stakeholders. All the recovery plans and strategies should be communicated among the involved individuals, may it be internal and external, to reduce the damage and protect the reputation.

9 Threat Modelling

9.1 Introduction

Threat modeling using STRIDE this is an acronym that stands for 6 categories of security risks as shown below:

Table 61: STRIDE overview

	Threat	Property Violated	Threat Definition
S	Spoofing	Authenticity	Pretending to be something or someone other than yourself
T	Tampering	Integrity	Modifying something on disk, network, memory or elsewhere
R	Repudiation	Non-repudiation	Claiming that you didn't do something or were not responsible.
I	Information Disclosure	Confidentiality	Providing Information to someone not authorized to access it
D	Denial of Service	Availability	Exhausting resources needed provide service
E	Elevation of Privileges	Authorization	Allowing someone to do something they are not authorized to do

9.2 Protocol Mapping

As shown below table of protocols used with in the Distributed ReStart DRZC architecture mapped across to the STRIDE Threat modeling:

Table 62: STRIDE protocol mapping

Protocols	S	T	R	I	D	E
IEEE C37.118	X	X	X		X	
IEC 61850-9-2 SV					X	
IEC 61850-90-5 R-SV					X	
IEC 61850-8-1 (GOOSE)	X	X	X		X	
IEC 61850-90-5 (R-GOOSE)	X	X	X		X	
IEC 61850 MMS	X	X	X			
IEC 60870-5-104	X	X	X		X	
DNP3	X	X	X		X	

PTP	X	X	X		X	
NTP	X	X	X		X	

The above table shows all protocols are susceptible to Denial-of-Service attacks. All but two are susceptible to Spoofing, Tampering and Repudiation. Many of the protocols were not developed with security in mind and do not check if the packets have been modified in transit, however there are security controls that can be applied to mitigate against most of the STRIDE attacks.

One method for protecting the protocols is to encapsulate them in an encrypted tunnel between devices or gateways such as a VPN. This allows the protocols to have a dedicated encrypted and authenticated layer 2 communication link to protect the data over a [untrusted] wide are network. There is a high overhead with VPNs, especially using IPsec VPNs for point-to-point connections. The BlackStart architecture may require a substation to communicate with multiple other sites which would require a point-to-point connection for each.

Alternatively, some of the protocols can be secured in the higher layers, including transport and application. This provides a more end-to-end security approach rather than terminating the security controls at the site's boundary gateway.

IEEE C37.118 can be protected using TLS and client certificate authentication as discussed in Section 2.3.1

IEC 61850-8-1 GOOSE has no mechanism for protection against tampering, however spoofing vulnerabilities can be mitigated using HMAC message authentication (see Table 7).

IEC 61850-90-5 R-GOOSE provides mechanisms for encryption and authentication as discussed in Section 2.3.2

IEC 61850 MMS can be protected with TLS and a dedicated authentication mechanism built into the MMS protocol (more information in Section 2.3.3)

IEC 60870-5-104 can be protected with TLS and application layer authentication using Message Authentication Codes as discussed in Section 2.3.2.

DNP3 can be protected with TLS and application layer authentication using Message Authentication Codes as discussed in Section 2.3.2.

PTP provides a cryptographic integrity check for each message as discussed in Section 2.3.4

NTP has an extension in development (NTS) to provide message integrity, this is discussed more in Section 2.3.4.

None of the protocols have mechanisms for protecting against Denial-of-Service attacks – as these types of attacks are typically done to compromise an entire network rather than a single protocol. Therefore, protection for Denial-of-Service attacks across all protocols can be handled using network security controls such as IDS and IPS, along with sufficient security-based network monitoring to identify attacks quickly.

10 Disaster Scenarios

The following section highlights the different disaster scenarios that may occur within the DRZC solution. Each scenario is based on the initial architecture design and accounts for the different systems, data and networks that are in scope for the DRZC architecture. Each asset that is affected by the scenario is highlighted and a risk profile is derived from the impact and likelihood of the scenario.

Note: For the purposes of this report, we are including external malicious actors, insider threats with privileged permissions acting maliciously and accidental changes to configurations or system under the term 'cyber-attack'

10.1 Likelihood and Impact

Likelihood is measured as the probability of a scenario happening. The likelihood rating for the following scenarios has been based on the security controls of the affected systems. For example, an unmanned remote site containing a controller is more likely to be breached than a manned and large site that hosts controllers and anchor generators.

For impact, the rating has been based on the effect the scenario would have to the BlackStart sequence, and to normal operation. For example, loss of the entire ADMS system results in the inability to successfully deliver a BlackStart and the inability to switch breakers in a normal day of operation.

10.2 Loss of data communications

The following scenarios depict a loss of communications between critical systems that are part of the DRZC architecture. Some of the below scenarios are closely linked, for example, a communications channel failure could result in multiple losses due to the location of components (e.g. communications failure between control centre and DER site could result in loss of ADMS to RTU, ADMS to Field Controller, WAMS to Field Controller etc).

Table 63: Loss of communications risk ratings

Description	Potential Cause	Location	Likelihood	Impact	Risk Rating
Loss of communications between PMU and Field Controller (LAN)	Physical damage, Local Denial of Service, Cable pulled out	DER site, substation	High (if remote)	Low	Medium
Loss of communications between RTUs and Field Controller	Physical damage, Local Denial of Service, Cable pulled out	DER site, substation	High (if remote)	Medium	Medium

Loss of communications between DER resource and Field Controller	Physical damage, Local Denial of Service	DER site, substation	High (if remote)	Medium	Medium
Loss of communications between DRZC and Field Controller (PR site)	Physical damage, Denial of Service, Network Flood	Central controller site (may vary) and Anchor Generator – these may be in the same location (LAN)	Low (manned) Medium (unmanned)	High	High
Loss of communications between DRZC and Field Controller (PBC site)	Physical damage, Denial of Service, Network Flood	Central controller site (may vary) and DER site / substation	High (unmanned) Low/Medium (if co-located with anchor generators)	High	High
Loss of communications between DRZC and Field Controller (SBC site)	Physical damage, Denial of Service, Network Flood	Central controller site (may vary) and DER site / substation	High	Medium	Medium
Loss of communications between ADMS and DRZC	Physical damage, Denial of Service, Network Flood	DNO control centres and central controller site (may vary)	Low	High	High
Loss of communications between ADMS and Field Controllers	Physical damage, Denial of Service, Network Flood	DNO control centres and substations / DER sites	Low (may get higher as comms transverses out to remote areas)	Medium	Medium
Loss of communications between ADMS and RTUs	Physical damage, Denial of Service, Network Flood	DNO control centres and substations / DER sites	Low (may get higher as comms transverses out to	High	High

			remote areas)		
Loss of communications between WAMS and DRZC	Physical damage, Denial of Service, Network Flood	DNO control centres and central controller site (may vary)	Low	Medium	Low
Loss of communications between WAMS and Field Controller	Physical damage, Denial of Service, Network Flood	DNO control centres and DER site / substation	Low (may get higher as comms transverses out to remote areas)	Low	Low
Loss of communications between IEMS and ADMS	Physical damage, Denial of Service, Network issues	NGESO control centres and DNO control centres, ICCP link	Low	Medium	Medium

10.3 Loss of voice communications

Table 64: Loss of voice communications risk ratings

Description	Potential Cause	Location	Likelihood	Impact	Risk Rating
Loss of satellite link for voice	Environmental disaster, jamming attack	All sites	Low	Medium	Low
Loss of wired link for voice	Physical damage, loss of power	All sites	Medium	Medium	Medium

10.4 Loss of BlackStart systems

Table 65: Loss of BlackStart systems risk ratings

Description	Potential Cause	Location	Likelihood	Impact	Risk Rating
Loss of DRZC controller	Loss of power, device firmware	DNO central controller site	Medium	High	High

	corruption, hardware failure				
Loss of Field Controller	Loss of power, device firmware corruption, hardware failure	DER site, substation	Medium	High (location dependent)	High
Loss of ADMS	Loss of power, database corruption, hardware failure	DNO control centres	Low	High	High
Loss of IEMS	Loss of power, database corruption, hardware failure	ESO control centres	Low	High	High
Loss of WAMS	Loss of power, database corruption, hardware failure	DNO control centres, ESO control centres	Low	Medium	Medium
Loss of DER control system	Loss of power, database corruption, hardware failure	DER sites	Low	High	High
Loss of DER resource	Mechanical fault, physical damage	DER sites	Low	High	High

10.5 Cyber-attack

Table 66: BlackStart cyber-attack risk ratings

Description	Potential Cause	Location	Likelihood	Impact	Risk Rating
DRZC/Field Controllers infected by malicious software	USB containing malware, transverse of malware from IT networks, insider threat	DNO central controller site, all sites if spread	Low	High	Medium
Server hosting ADMS infected by malicious software	USB containing malware, transverse of malware from	DNO control centres, all sites if spread	Low	High	Medium

	other IT networks, insider threat				
Server hosting WAMS infected by malicious software	USB containing malware, transverse of malware from other IT networks, insider threat	DNO control centres, all sites if spread	Low	High	Medium
Configuration or scheme change in DRZC/Field Controllers	Malicious change from remote attack, disgruntled employee, accidental change	DNO central controller site, may affect other sites depending on logic	Medium	High	High
Configuration change replicated to all ADMS servers	Malicious change from remote attack, disgruntled employee, accidental change	DNO control centres, likely to affect entire network	Medium	High	High
Configuration change replicated to all WAMS servers	Malicious change from remote attack, disgruntled employee, accidental change	DNO control centres	High	High	High
Stealing cryptographic keys or secrets from DRZC/Field Controllers	Physically insecure location, supply chain attack,	All controller sites potentially affected	Medium	High	High
Stolen device reconfigured and attached back to network	Physically insecure location, poor network practices, supply chain attack	All controller sites potentially affected	Medium	High	High

11 Disaster Recovery Options

Using the information collected in the previous section, different options are suggested to help protect and recover from the different disaster scenarios. Options will be discussed and finalised in the later design stages of this project.

11.1 [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

11.1.2.1 [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

11.2.2.2 [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

11.4.2 [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

11.4.2.3 [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

11.4.2.5 [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

12 Appendices

12.1 Appendix A

[redacted]

12.2 Appendix B

[redacted]

12.3 Appendix C

Supported Cipher Suites			
Key Exchange	**Certificate Verification**	**Encryption**	**Hashing**
ECDHE	ECDSA	AES_256_GCM	(HMAC-)SHA-384
ECDHE	ECDSA	CHACHA20_POLY1305	(HMAC-)SHA-256
ECDHE	ECDSA	AES_128_GCM	SHA256
ECDHE	RSA	AES_256_GCM	SHA384
ECDHE	RSA	CHACHA20_POLY1305	SHA256
ECDHE	RSA	AES_128_GCM	SHA256

12.4 Appendix D

[redacted]

[redacted]

[redacted]

12 Appendices

[redacted]

13 Addendums

13.1 [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]		[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]		[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]		[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	

[redacted]

[redacted]

13 Addendums

[redacted]

[redacted]

13 Addendums

[redacted]

[redacted]

[redacted]

[redacted]

13 Addendums

[redacted]

[redacted]

13 Addendums

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

13 Addendums

[redacted]

[redacted]

[redacted]

[redacted]

In addition to the requirements above NG Technology Risk management process shall be followed. A NIST800:37 Risk process is being developed and will be used.