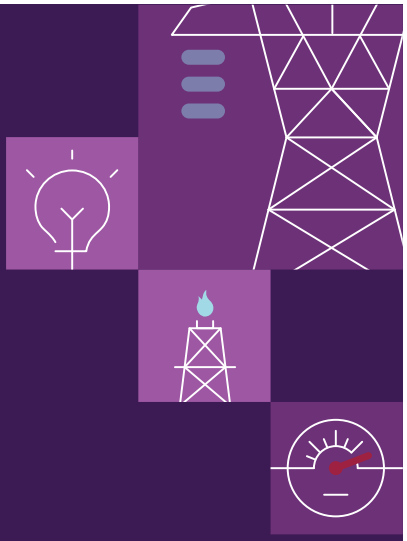


Power System Data Communication Standard

National Electricity Market

~~National Electricity Market~~

Prepared by:	AEMO ~~Systems Capability~~Operations
Version:	~~2~~3.0
Effective date:	~~1 December 2017~~3 April 2023
Status:	FINAL

Approved for distribution and use by:

Approved ~~for distribution and use~~ by:	Michael Gatt
~~APPROVED BY~~Title:	Executive General Manager Operations
~~TITLE~~Date:	24 / 11 / 2022

~~DATE:~~

Inserted Cells

Contents

Current version release details 3

1. Introduction 4
1.1. Purpose and scope 4
1.2. Definitions and interpretation 5
1.3. Related documents 9
1.4. Requirement to provide Intervening Facilities 9
1.5. Overview of Data Communication Facilities 10
1.6. Interdependence and cooperation 11
1.7. Content overview and application 12

2. Performance 13
2.1. Capability to transmit and receive Operational Data 13
2.2. Representation of data 14
2.3. Age of data 15
2.4. Control command delay 16
2.5. Data accuracy 16

3. Reliability 18
3.1. Reliability requirements 18
3.2. Redundant elements 19

4. Security 19
4.1. Standard applies in parallel with SOCI Act 20
4.2. Security risk management plans 20
4.3. Security incident reporting 20
4.4. Physical security and computer network security 21

5. Interfacing 22
5.1. Physical and logical interfaces with AEMO co-ordinating centres 22
5.2. Communication protocols 23

6. Maintenance, planning and testing 24
6.1. Governance and reporting on availability 24
6.2. Response to failures 24
6.3. Planned outage co-ordination 25
6.4. Data management and co-ordination 25
6.5. Testing to confirm compliance 26

7. Near real time data from PMU and HSM devices 27

8. Management of non-compliance 27
8.1. Consequences of non-compliance 27
8.2. Reporting and remediation 27

9. Transitional arrangements for 2023 Standard Update 28
9.1. Definitions, application and maximum timeframes 28
9.2. Transition plan 29
9.3. Deemed compliance between effective date and transition date 29

Version release history 31

Tables

Table 1 Resolution required for analogue values 14
Table 2 End to end time for data to be available for transmission to AEMO 15
Table 3 Deadband for transmission of analogue values 15
Table 3A Data accuracy tolerance 17
Table 4 Maximum critical outages for RME and RCE 19
Table 5 Maximum critical outages for intervening facilities over a 12-month period 19

Figures

Figure 1 General structure of DCF 11

Current version release details

Version	Effective date	Summary of changes
3.0	3 April 2023	Revised following complete review

Note: There is a full version history at the end of this document.

1. Introduction

1.1. Purpose and scope

This is the Power System Data Communication Standard (**Standard**) made under clause 4.11.2(c) of the National Electricity Rules (**NER**). It incorporates the standards and protocols referred to in ~~clause~~NER 4.11.1 and ~~related provisions of the National Electricity Rules (NER).~~

(a) 4.11.2. This Standard has effect only for the purposes set out in the NER. The NER and the National Electricity Law prevail over this Standard to the extent of any inconsistency.

~~The purpose of this document is to set~~This Standard sets out the standards ~~with which Data Communication Providers (DCPs) must comply when transmitting data to~~ and ~~from AEMO.~~

~~DCPs must apply this Standard when providing and maintaining communications facilities[1] that transmit data to and from AEMO~~protocols applicable to the recording, transmission or receipt of telemetered data required for ~~use in AEMO control centres.~~

(b) ~~DCP's Data Communication Facilities (DCF) which are used to enable AEMO to discharge its market~~the purposes of monitoring and managing *central dispatch* and *power system security* ~~functions as set out in Chapters 3~~and reliability (**Operational Data**) (including indications, signals and ~~4 of the NER must be~~ instructions) by:

remote monitoring equipment (RME) and *remote control equipment* (RCE) installed and maintained ~~to this Standard (other DCFs at DCP sites are not captured by this Standard).~~

~~In this Standard, the term DCPs refers to *Network Service Providers*, Generators, Customers, Market Network Services, and Ancillary Services Providers.~~

~~The Standard applies to:~~

~~(b) *Network Service Providers* (NSP)~~by *Registered Participants* who are required to do so under ~~clause 4.11.2(a) of the~~ NER~~;~~

~~(c) *Generators* under clauses~~ 4.11.1~~(a)~~ and S5.2.6 ~~of the NER;~~

~~(d) *Customers* (in respect of *substations*) under clauses 4~~.1~~.1(a) and S5.3.9 of the NER;~~

(i) ~~*Market Network Service Providers* under clauses 4.1.1(a);~~ and ~~S5.3a.4 of the NER; and~~

~~(e) *Ancillary Service Providers* under clause 4.11.1(b) of the NER.~~

(ii) primary and back-up communications facilities maintained by *Network Service Providers* (NSPs) for the transmission of data between RME and RCE and AEMO's *control centres*, as required under NER 4.11.2, and by other *Registered Participants* who may provide such facilities in some cases.

~~[1] Including back-up facilities~~

1.2. Definitions and interpretation

1.2.1. Glossary

Terms defined in the National Electricity Law and the NER have the same meanings in ~~these Procedures unless otherwise specified in this clause~~this Standard unless otherwise specified in the table below. Terms defined in the NER are intended to be identified in this Standard by italicising them, but failure to italicise a defined term does not affect its meaning.

~~Terms defined in the NER are intended to be identified in these Procedures by italicising them, but failure to italicise a defined term does not affect its meaning. For ease of reference, some of the more frequently used NER terms are replicated in this glossary.~~

~~In addition,~~ The words, phrases and abbreviations in the table below have the meanings set out opposite them when used in ~~these Procedures~~this Standard.

Term	Definition
Analogue Value	~~Digital~~Numeric representation of a continuous value (for example, a power flow)
Communication Protocol	A communication protocol that is approved by AEMO for transmission of Operational Data between Intervening Facilities and *AEMO co-ordinating centres*, in accordance with section 5.2.
Control Command	~~A representation of an~~An electronic instruction to perform a defined action (for example a *generation* increase). In the ICCP it is a special data type that is different from a standard Analogue Value or Discrete Value type, and usually requires an acknowledgement of receipt to be sent back.
Critical Outage	For an RME or RCE: A loss ~~for more than 60 seconds~~ of the ability to transmit Operational Data of Good Quality to AEMO or receive Control Commands from AEMO exceeding 60 seconds, but ~~not where the loss arises from a:~~ ~~1. Force Majeure.~~ ~~Failure, or~~excluding an outage~~, of equipment~~ that ~~does not form part of the DCF.~~: • ~~Failure or outage of equipment that~~ affects less than 5% of all Operational Data items of that RME or RCE~~.~~; • ~~*Scheduled generating unit, semi-*~~only affects the transmission of Operational Data relating to scheduled ~~*generating unit, scheduled network service or scheduled load*~~plant that is not available ~~for~~ to participate in *central dispatch*~~.~~; • ~~*Power system*~~ relates to a period when the *plant* ~~that~~associated with the RME or RCE is not in service and ~~the *control centre*~~AEMO has ~~be~~been notified of that ~~*outage*~~.fact; • ~~Outage~~is planned for work to upgrade ~~DCFs to comply with this Standard and *control centre*~~the RME or RCE, where AEMO has been notified in advance~~.~~; or • ~~Loss of DCFs~~is caused solely by an outage of an Intervening Facility. For an Intervening Facility: A loss ~~for more than 3 minutes~~ of the ability to transmit Operational Data of Good Quality to AEMO or receive Control Commands from AEMO~~, but not where the loss arises from a~~ exceeding 3 minutes, but excluding an outage that: ~~1. Force Majeure.~~ ~~2. Failure, or outage, of equipment that does not form part of the DCF.~~ • ~~Loss of~~lasts less than 10 minutes ~~that~~and does not affect the transmission of Dispatch Data~~.~~; or • ~~Loss affecting no more than one *dispatch interval* (or as otherwise agreed with AEMO) arising from~~ is planned for a test of: – DCFs at a disaster recovery site~~, for which the *control centre* has been given at least 24 hours' notice.~~; or – ~~Loss affecting no more than one *dispatch interval* (or as otherwise agreed with AEMO) arising from a test of~~ a major upgrade of an Intervening Facility, ~~3.~~ for which ~~the *control centre*~~AEMO has been given at least 24 hours' notice~~.~~ ~~Loss arising from a loss of DCFs of a Data Concentrator, RME or RCE.~~ and which affects no more than one *trading interval* (or a longer period agreed with AEMO in advance).

Term	Definition
Data Communication ~~Protocol~~Provider (DCP)	~~ICCP IEC60870-6 TASE.2 and its extensions secure ICCP~~Any: • *Registered Participant* required to install and maintain RCE and RME in accordance with NER 4.11.1; and • *Network Service Provider* required to provide and maintain communications facilities in accordance with NER 4.11.2.
Data Communications Facility (DCF)	A generic term used to denote any part of equipment used to transmit Operational Data from one site to another, and includes: • the part of RME and RCE providing analogue to digital conversion functions~~.~~; • the part of RME and RCE providing data communication functions. • the parts of an Intervening Facility providing data communications functions • telecommunications equipment and media. ~~1. Any Data Concentrator.~~ • power supply equipment for ~~items 1 to 4~~the above equipment.
~~Data Communication Providers (DCPs)~~	~~**In this Standard, the term Data Communication Providers refers to:**~~ ~~1. *Network Service Providers*~~ ~~2. *Generators*~~ ~~3. *Customers*~~ ~~4. *Market Network Service Providers*~~ ~~5. *Ancillary Service Providers*,~~ ~~**in connection with their respective obligations under the NER as indicated in clause 1.2 of the Standard.**~~
~~Data Concentrator~~	~~A DCF that:~~ ~~1. Communicates with an Intervening Facility.~~ ~~2. Collects data from multiple RMEs.~~ ~~3. Relays Control Commands to RCE.~~
Deadband	**A deadband is a region of values where a change in the value of data will not result in activation of data transmission. A deadband ~~is~~may be necessary to prevent repeated transmission of data when it has not changed ~~significantly~~materially.**
Discrete Value	A ~~digital~~numeric representation of one of a limited set of values (for example a *transformer tap position*).
Dispatch Data	Telemetered data that ~~represents:~~ ~~The~~is required for the operation of the 5-minute *central dispatch* ~~of scheduled generating units, semi-scheduled units, scheduled network services or scheduled loads.~~process, representing any of the following: • ~~An~~the operational status and measurement of the production, consumption or flow of *scheduled plant* or a *wholesale demand response unit*[2], including aggregated data for *plant* or services that are *dispatched* in aggregate; . • measurements of *interconnector* flow~~.~~; • the *enablement* status~~.~~ or ~~the~~ amount, of a *market ancillary service*~~.~~, *non-market ancillary service, system strength service, inertia network service* or *inertia support activity*; • a *dispatch instruction* or other Control Command. • indications and measurements for, and instructions from, the VAR dispatch system (VDS)
DNP3	Distributed Network Protocol 3 version SAv5 or later.
End to end time (latency)	End to end time means time between: • detection of an event or change in value at RME and receipt of the associated data at an *AEMO co-ordinating centre*; or • transmission of a command from an *AEMO co-ordinating centre* and receipt of the command at RCE.
Force Majeure	An event or ~~effect which~~circumstance that directly affects the ability of a DCF to transmit or receive Operational Data, to the extent that:

[2] From 3 June 2024, *scheduled plant* and *wholesale demand response units* will be referred to by the umbrella term 'scheduled resources'.

Deadband	A deadband is a region of values where a change in the value of data will not result in activation of data transmission. A deadband ~~is~~may be necessary to prevent repeated transmission of data when it has not changed ~~significantly~~materially.
	• the occurrence of the event or circumstance is ~~neither~~not within the reasonable control of the relevant DCP, its related bodies corporate or its service providers or subcontractors; and • the impact of the event or circumstance could not reasonably have been anticipated, ~~nor controllable~~and either mitigated or prevented, by the ~~affected parties including acts of nature, governmental interventions and acts of war.~~relevant DCP, its related bodies corporate, service providers or subcontactors.
Good Quality	Data that is a true representation of the equipment state, quantity or other indication being measured. It is not replaced or modified, other than for the purpose of conversion to the agreed unit of measure, and is indicated by data quality flags in accordance with section 2.2.
High Resolution Data	~~Measurements of the following types of data:~~ Data measured and transmitted to AEMO in near real time by devices with GPS clock synchronisation (or equivalent technology) and a typical sample rate of 20 millisecond intervals, allowing for accurate representation of power system behaviour, including during transient events, including: • measurements of system *frequency*~~.~~ and electrical time; and • ~~Electrical Time.~~data measured by PMU and HSM devices that is transmitted for real time operation purposes, but excluding Dispatch Data.
HSM	High Speed Monitor
ICCP	Inter-Control ~~Centre~~Center Communications Protocol - IEC 60870-6 TASE.2 and its extensions[3]
Intervening Facility	~~A DCF that:~~ ~~1. Receives polls from a *control centre*.~~ ~~2. Collects data from RME and relays that data to *control centre*.~~ ~~3. Relays Control Commands from *control centre* to RCE.~~ An NSP Intervening Facility or a Non-NSP Intervening Facility, being a DCF that is required or permitted to transmit Operational Data directly to and from an *AEMO co-ordinating centre* under this Standard. For clarity, an Intervening Facility does not include any facility or service provided by AEMO. for communication between an Intervening Facility and an *AEMO co-ordinating centre*.
NER	National Electricity Rules. A reference to NER followed by a number is to the corresponding rule or clause of the NER.
~~Other Data~~Non-NSP Intervening Facility	~~Data~~A DCF that ~~represents~~: ~~1. Status Indications~~ ~~2. Discrete Values~~ ~~3. Analogue Value~~ • is not an asset of, or provided by, an NSP; • receives Polls directly from *AEMO co-ordinating centres*; • collects data from an RME (whether directly or via an aggregation facility) and relays that data to *AEMO co-ordinating centres*; and 4. relays Control Commands 5. ~~*Power system* Data from plant that operates at nominal voltage of less than 220 kV~~ • ~~Any other data which is not dispatch data, high resolution data or system data~~ from *control centre* to RCE.
NSP (TNSP, DNSP)	*Network Service Provider* (including a *Transmission Network Service Provider*, and a *Distribution Network Service Provider*, but excluding a *Market Network Service Provider*)
NSP Intervening Facility	A DCF that: • is provided and maintained by an NSP; • receives Polls either directly from an *AEMO co-ordinating centre* or (where this Standard permits) via another NSP Intervening Facility;

[3] International Electrotechnical Commission (IEC), available for purchase https://webstore.iec.ch/publication

Deadband	A deadband is a region of values where a change in the value of data will not result in activation of data transmission. A deadband ismay be necessary to prevent repeated transmission of data when it has not changed significantlymaterially.
	• collects data from RME or another NSP Intervening Facility and relays that data to an *AEMO co-ordinating centre* or (where this Standard permits) another NSP Intervening Facility; and • relays Control Commands from an *AEMO co-ordinating centre* to RCE or another NSP Intervening Facility.
Operational Data	~~All data - Dispatch data, high resolution data, *power system* data, and other data~~An umbrella term for all data required to be transmitted to or from *AEMO co-ordinating centres* using RME, RCE and the Intervening Facilities for AEMO's *market* and *power system security* functions. Unless otherwise specified, Operational Data includes Dispatch Data, High Resolution Data, System Security Primary Data and System Security Secondary Data.
PMU	Phasor Measurement Unit
Poll	An electronic request sent from a *control centre* or an Intervening Facility to ~~a *power station or substation*~~RME to request Status Indications, Discrete Values or Analogue Values.
System Security Primary Data	Telemetered data relating to: • all *transmission network* assets and *dual function assets*; and • *plant* that is directly *connected* to such *network* assets, but excluding Dispatch Data.
RCE	*Remote control equipment* as defined in the NER, but not limited to *power stations* and *substations* - Equipment used to control the operation of elements of a ~~*power station*~~*facility* or ~~substation~~the provision of a service from a *control centre*.
Resilient Network	A communication network which has back-up power supplies sufficient to sustain operation for at least 10 hours following loss of external AC (alternating current) supply.
RME	*Remote monitoring equipment* as defined in the NER - Equipment installed to enable monitoring of a *facility* from a *control centre*.
Scale Range	The range of measurements for an Analogue Value that can be represented by a ~~digital~~numeric value.
System Security Secondary Data	Telemetered data required for effective *market* operation and *power system security* that is not Dispatch Data, High Resolution Data or System Security Primary Data . Examples include data required for: • inputs to short term forecasting systems; and • inputs to dynamic rating systems.
Secure Network	A communication network which is not accessible to third parties and meets the cyber security requirements outlined in section 4.4.2(b) to (d).
SOCI Act	The *Security of Critical Infrastructure Act 2018* (Cth).
Status Indication	The state of a device that has a finite number of discrete states. It includes switching and control indications and alarm conditions.
Telecommunication Carrier ~~***Power system* Data~~	~~Data concerning all *plant* within:~~ ~~A Substation containing *plant* that operates at a nominal *voltage* of at least 220 kV.~~ ~~A Substation having at least four sources of *supply*, including *power station* sources.~~A carrier as defined in the *Telecommunications Act 1997* (Cth).
~~**Substation**~~**True Value**	~~As defined in the NER, and for purposes of this Standard, a *facility* with one or more *transmission lines*.~~True value of a measurement is a perfect measurement in an ideal world. It assumes zero measurement error in the measurement process, from the sensor to the measurement instrument.
WAN ~~**Telecommunication Carrier**~~	Wide area network~~A carrier as defined in the Telecommunications Act 1997.~~

1.2.2. Interpretation

~~The following principles of interpretation apply to these Procedures unless otherwise expressly indicated.~~

These Procedures are subject to the principles of interpretation set out in Schedule 2 of the National Electricity Law.

~~(a) References to time are references to Australian Eastern Standard Time.~~

1.3. Related documents

Title	Location
Australian Energy Sector Cyber Security Framework	https://aemo.com.au/initiatives/major-programs/cyber-security/aescsf-framework-and-resources
Australian Signals Directorate Information Security Manual, Guidelines for Cryptography	https://www.cyber.gov.au/acsc/view-all-content/advice/guidelines-cryptography
Communication System Failure Guidelines	https://aemo.com.au/energy-systems/electricity/national-electricity-market-nem/participate-in-the-market/network-connections/victorian-transmission-connections/stage-6-completion
Market Ancillary Service Specification	https://aemo.com.au/en/energy-systems/electricity/national-electricity-market-nem/system-operations/ancillary-services/market-ancillary-services-specification-and-fcas-verification-tool
AEMO Policy 020113: Electricity Market Management Systems Access Policy and Procedure	https://www.aemo.com.au/-/media/files/electricity/nem/it-systems-and-change/2016/electricity-market-management-systems-access-policy-and-procedure.pdf?la=en&hash=60D050E074048EB08563BB60906FD4A7

1.4. Requirement to provide Intervening Facilities

1.4.1. NSP obligations

(a) Each TNSP and DNSP must maintain one or more DCFs, called **NSP Intervening Facilities**, to receive Operational Data from RME, HSMs and PMUs connected to its *network* (subject to section 1.4.2), and transmit Control Commands to RCE or, where applicable, to another NSP Intervening Facility[4].

(b) For the purpose of the transmission and receipt of Operational Data between its Intervening Facilities and an *AEMO co-ordinating centre*, a DNSP must either:

(i) establish a direct connection to both *AEMO co-ordinating centres*[5];

(ii) establish a connection to the Intervening Facility maintained by its *regional* TNSP; or

(iii) with the consent of the TNSP and AEMO, establish a direct connection to one *AEMO co-ordinating centres* and a second connection to the Intervening Facility maintained by its *regional* TNSP, so that the TNSP's Intervening Facility then retransmits the relevant Operational Data to and from *AEMO co-ordinating centres*,

[4] Data transmission between RME/RCE and Intervening Facilities can occur via one or more other aggregating facilities, which are not specifically addressed in this Standard.

[5] This does not affect any obligations of a DNSP under its connection and operating arrangements to provide the same or similar data to a TNSP.

provided that the DNSP must select a communication path that allows all applicable requirements of this Standard to be met.

(c) Each TNSP must:

(i) for the purpose of the transmission and receipt of Operational Data between its Intervening Facilities and an *AEMO co-ordinating centre*, establish a direct connection to both *AEMO co-ordinating centres*; and

(ii) cooperate with any DNSP in its *region* as reasonably required to establish a connection between the TNSP and DNSP Intervening Facilities.

(d) AEMO provides a WAN connection for NSP Intervening Facilities, and physical or logical interfaces are to be established in accordance with section 5.

1.4.2. Other participants

~~1.4.~~ Some *Registered Participants* (for example aggregators) may be required by the NER to transmit and receive Operational Data to and from AEMO that is not also required by the NSP for its operational purposes. In such cases, where the use of an NSP Intervening Facility for the relevant data is not provided for in a *connection agreement* or other arrangement, the *Registered Participant* may establish a Non-NSP Intervening Facility for direct connection to the *AEMO co-ordinating centres* in accordance with section 5.1~~General structure of DCFs~~

.

1.5. Overview of Data Communication Facilities

The ~~following~~ diagram in Figure 1 illustrates the relationships between:

- *AEMO* ~~control~~*co-ordinating centres*~~.~~ (Control Centres 1 and 2).
- NSP Intervening Facilities.
- Non-NSP Intervening Facilities.
- RME and RCE.

This conceptual schematic represents a number of possible configurations including:

- DNSP Intervening Facility (IF2) connects directly to a TNSP Intervening Facility (IF1) which in turn provides the DNSP data to AEMO via IF1's direct connections to both *AEMO co-ordinating centres*;

- DNSP Intervening Facility (IF4) connects directly to one *AEMO co-ordinating centre* and also connects directly to a TNSP Intervening Facility (IF3) which in turn provides the DNSP data to AEMO via the TNSP's direct connections to the other *AEMO co-ordinating centre*[6];
- DNSP or Non-NSP Intervening Facility connects directly to both *AEMO co-ordinating centres* (IF5).

Figure 1 General structure of DCF

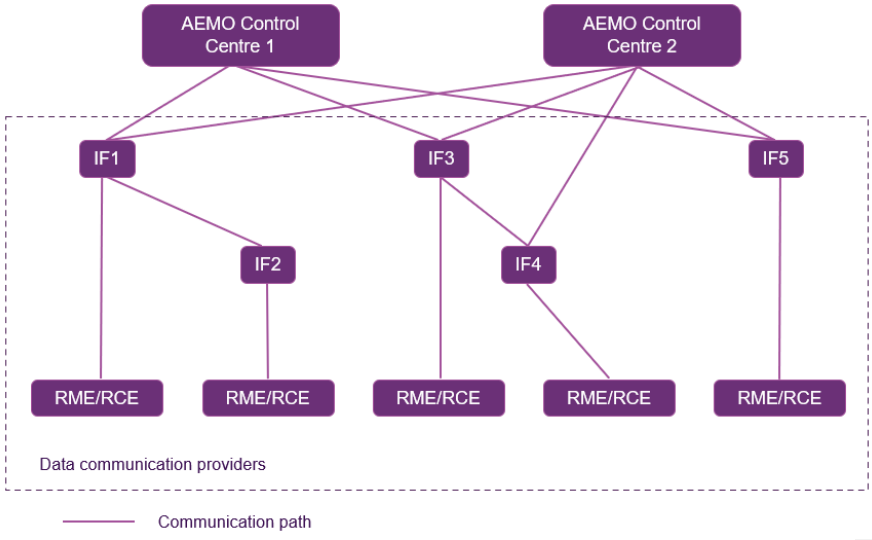


Figure 1 is only intended to be a conceptual schematic showing potential connection paths of various facilities. It is not a conceptual/solution architecture design for a DCP to install their infrastructure; a DCP is expected to design its infrastructure and communication services to meet the requirements of the Standard.

1.6. Interdependence and cooperation

(a) As illustrated in sections 1.4 and 1.5, the transmission of Operational Data from *power system* equipment in the field or dispatch aggregators to *AEMO co-ordinating centres* and vice versa in accordance with the requirements of this Standard often relies on satisfactory performance by multiple DCFs.

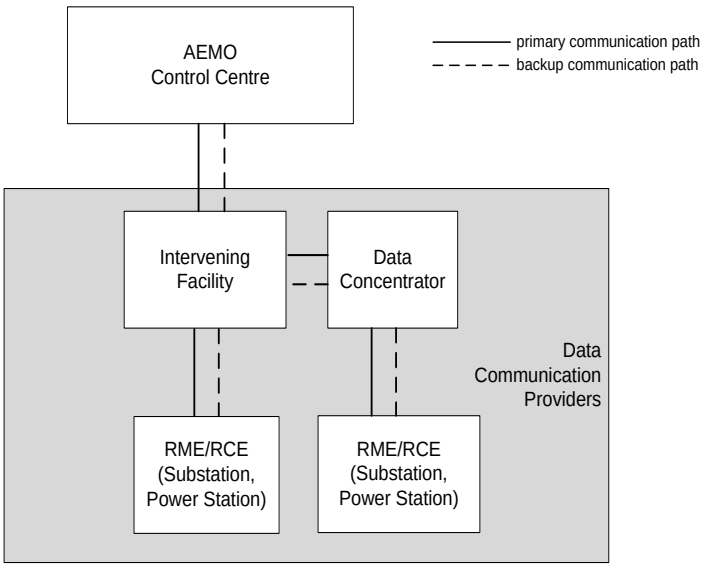
(b) Each DCP should cooperate with, and provide reasonable assistance to, other relevant DCPs to facilitate the overall achievement of the Standard. In doing so, a DCP is not expected to exceed any individual performance requirement for its own DCFs.

[6] If practical and agreed to by all relevant parties.

1.7. Content overview and application

The following sections of the Standard are structured as follows:

- Section 2 specifies performance requirements for DCFs, either generally or by reference to the type of Operational Data being transmitted. These requirements do not apply to High Resolution Data from PMUs and HSMs unless specified in accordance with section 7.
- Section 3 specifies reliability requirements for DCFs. These requirements do not apply to the provision of High Resolution Data from PMUs and HSMs unless specified in accordance with section 7.
- Section 4 specifies the cyber, physical and network security requirements applicable to all DCFs (including all PMUs and HSMs) and associated communication paths.
- Section 5 deals with interfaces between DCFs and *AEMO co-ordinating centres*. Section 5.1 applies to PMUs and HSMs providing High Resolution Data- but section 5.2 does not, unless specified in accordance with section 7.
- Section 6 deals with DCF maintenance, planning and testing, including coordination. These requirements do not apply to PMUs and HSMs providing High Resolution Data unless specified in accordance with section 7.
- Section 7 explains how performance requirements for High Resolution Data from PMUs and HSMs are determined for the purpose of this Standard.
- Section 8 explains the framework for non-compliance with this Standard, by reference to the NER.
- Section 9~~Data Concentrators.~~
- ~~*Remote monitoring equipment* (RME)/*Remote control equipment* (RCE).~~



- covers transitional arrangements for compliance with additional requirements introduced by version 3.0 of this Standard.

2. Performance

The purpose of this section is to ensure that DCFs perform effectively.

~~2.1. Quantity of data~~

2.1. Capability to transmit and receive Operational Data

~~(a)~~ DCFs must be capable of transmitting ~~all~~and receiving the types and quantities of Operational Data required by AEMO ~~and includes all data that:~~

~~(i) was in use at the~~ for its *market* and *power system security* functions from time ~~this Standard came into effect;~~

~~(ii) has been requested in writing by AEMO; and~~

~~(iii) has not been subsequently rejected in writing by AEMO.~~

(a) ~~The transmission of additional Operational Data beyond that required by AEMO~~to time under the NER, including, for example:

~~**Explanatory note:** Chapters 4 and 5 of the NER allow AEMO to request data that it requires to discharge its *market* and *power system security* functions. This Standard sets out requirements that apply to data that AEMO already receives and to data that AEMO might require in the~~

(i) quantities and signals approved in respect of *plant* or ~~any~~a service on registration and classification under NER Chapter 2;

(ii) RME quantities requested under a *performance standard* for NER S5.2.6.1 or S5.3a.4.1;

(iii) requirements for performance data from RME specified under NER 4.11.1(d);

(iv) requirements for AGC signals specified under NER 4.11.1(g);

(v) requirements specified in an agreement ~~between AEMO and a DCP does not diminish~~or supporting arrangements for the *dispatch* and monitoring of *non-market ancillary services*, *network support*, *system strength services* or *inertia services*;

(vi) quantities and signals required for *market ancillary services* under the MASS.

(b) Additional quantities and types of data may be transmitted beyond AEMO's requirements, but this does not limit a DCP's obligations ~~of the DCP~~ to comply with this Standard~~.~~ in respect of Operational Data.

(c) As noted in section 1.7, the references to Operational Data and High Resolution Data in this section 2 do not apply to High Resolution Data from PMUs and HSMs. Requirements for those devices are set under section 7.

2.2. Representation of data

(a) DCFs must transmit Operational Data to and from AEMO in accordance with this section 2.2~~2.2.~~.

(b) Analogue ~~Data~~Values must be transmitted:

(i) with the sign convention nominated by the DCP from which the data originates~~;~~ (see paragraph (c); and

(ii) with the resolutions specified in Table 1.

Table 1 Resolution required for analogue ~~Data~~values

Category of Analogue ~~Data~~Value	Resolution (Max % of Scale Range)
Dispatch Data and High Resolution Data[7]	0.1
~~*Power system* Data~~System Security Primary Data System Security Primary Data	0.2
~~Other~~System Security Secondary Data	1.0

(c) DCPs must notify AEMO of their sign convention when applying to AEMO for registration as a Registered Participant. To change the sign convention, DCPs must give 60 business days' notice to AEMO. This notice period does not apply to the correction of sign convention issues remediated as part of regular maintenance, which are to be updated in accordance with normal database procedures.

~~(c)~~(d) Analogue Values, Status Indications and Discrete Values must be transmitted with a data quality in accordance with the Communication Protocol.

~~(d)~~(e) Control Commands must be transmitted in accordance with the Communication Protocol.

~~(e)~~(f) Subject to paragraph (g), quality of data indicators (multi-state data quality flags) must be transmitted with each data point and must indicate:

(i) whether there is a sustained communication failure (lasting 30 seconds or more) between an Intervening Facility and RME ~~(including failure of a relevant Data Concentrator);~~; and

(ii) whether a value has been overridden at any RME~~, Data Concentrator~~ or Intervening Facility~~.~~.

~~(f) DCPs must notify AEMO of their sign convention when applying to AEMO for registration as a Registered Participant. To change the sign convention, DCPs must give 60 business days' notice to AEMO.~~

~~(g) A sustained communications failure is a failure lasting 30 seconds or more. A transient communication failure is one that lasts less than 30 seconds.~~

and if no conditions described in (i) or (ii) apply then the data quality flag(s) must indicate that the data is of good quality.

(g) In respect of data from an RME device installed prior to 7 September 2022 that does not support the use of data quality flags, the DCP must artificially set the quality flag to good.

[7] Excludes High Resolution Data from PMUs and HSMs unless specifically applied under section 7.

2.3. Age of data

2.3.1. General requirements

~~(h)~~(a) Subject to section 2.3.2, Operational Data must be available for transmission to AEMO in response to a Poll within the time intervals specified in Table 2. The time interval is ~~calculated~~measured from the instant the data first gets converted to digital form and includes any time within an Intervening Facility.

Table 2 ~~Time intervals~~End to end time for data ~~to be available for~~ transmission to AEMO

Category	Data Type	~~Time Interval (seconds)~~	Maximum Time Interval via Data
High Resolution Data[8]	Analogue Value		2
Dispatch Data	Status Indication		~~6~~3
	Analogue Value		6
	Discrete Value		6
~~Power~~ System Security Primary Data	Status Indication		~~8~~3
	Analogue Value		14
	Discrete Value		14
~~Other~~System Security Secondary Data	Status Indication		12
	Analogue Value		22
	Discrete Value		22

Deleted Cells

Deleted Cells

~~(i)~~(b) A Status Indication is considered converted to digital form when the digital signal representing it is carried by circuits that are not used solely for that Status Indication.

~~(j)~~(c) Status Indications and Discrete Values do not have to be re-transmitted for up to ~~five~~5 minutes if the relevant data has not changed since the last transmission.

~~(k)~~(d) Analogue Values do not have to be re-transmitted for up to ~~five~~5 minutes if the relevant data has not changed by the relevant deadband amount shown in Table 3.

Table 3 Deadband for ~~analogue data~~ transmission of analogue values

Category of Analogue ~~Data~~Value	Deadband (% of Scale Range)
Dispatch Data and High Resolution Data[9]	0.2
~~*Power system*~~System Security Primary Data	0.5
~~Other~~System Security Secondary Data	0.5

~~(l)~~(e) An Intervening Facility must respond to Polls once per second with the relevant data.

[8] Excludes High Resolution Data from PMUs and HSMs unless specifically applied under section 7.

[9] Excludes High Resolution Data from PMUs and HSMs unless specifically applied under section 7.

2.3.2. Limited exceptions

(a) A DCP may request AEMO to approve an extended maximum time interval for end-to-end transmission than is specified in Table 2, in respect of Status Indications for:

(i) Dispatch Data; or

(ii) System Security Primary Data.

(b) AEMO may grant or refuse the request at its discretion or subject to conditions, and will have regard to:

(i) the significance of the type of Status Indication for the reliable operation of AEMO's state estimator application; and

(ii) whether it is reasonably practicable for the DCP to achieve the time specified in Table 2 for the relevant Status Indication,

and the DCP must provide information reasonably required by AEMO to consider the DCP's request.

(c) Subject to any applicable conditions of approval, if AEMO approves a request under this section the DCP must meet a maximum time interval for transmission of the relevant Status Indications of:

(i) 7 seconds in respect of Dispatch Data; or

(ii) 9 seconds in respect of System Security Primary Data.

2.4. Control command delay

DCPs must relay Control Commands ~~to relevant RCE within three seconds of receiving a Control Commands~~such that commands from *AEMO* *co-ordinating centres* to RCE or ~~within four seconds if~~ responses from RCE to *AEMO co-ordinating centres* will not have a delay of more than 2 seconds.

2.5. Data accuracy

(a) All Analogue Values received at *AEMO co-ordinating centres* and transmitted ~~via~~ from data points that come into service on or after 1 January 2024 must be accurate within a ~~Data Concentrator~~tolerance set out in Table 3A below. The absolute value of the difference between the measured value and the True Value is not to exceed the amount determined under the table for the relevant category of Operational Data.

Table 3A Data accuracy tolerance

Data Category	True Value less than 25% of Scale Range	True Value 25-80% of Scale Range	True Value greater than 80% of Scale Range
High Resolution Data[10]	0.25% of Scale Range	1 % of true value	1% of Scale Range
Dispatch Data	0.25% of Scale Range	1 % of true value	1% of Scale Range
System Security Primary Data	0.5% of Scale Range	2% of true value	2% of Scale Range
System Security Secondary Data	1.25% of Scale Range	5% of true value	5% of Scale Range

(a) For data points in service prior to 1 January 2024:

(i) by 31 January 2024, the relevant DCP must advise AEMO of the current accuracy of those data points[11]; and

(ii) if AEMO identifies that the inaccuracy of a particular data point is causing or materially contributing to operational issues impacting the reliability of the state estimator application, AEMO may request the relevant DCP to meet the accuracy requirement in paragraph (a), and the DCP must comply with that request by the date that is six months after the date of the request or any later date for compliance determined under the process described in paragraph (c).

(b) If AEMO makes a request under paragraph (b)(ii), the following process applies:

(i) The relevant DCP and AEMO must use reasonable endeavours to agree an implementation plan within one month of the request date or such longer period as AEMO reasonably allows, and for this purpose the relevant DCP must promptly provide AEMO with the information it reasonably requests about the nature and cost of meeting the relevant accuracy requirement, the timeframes in which this can be completed, resourcing requirements and limitations, and any dependencies on third parties or (where the cost is material) regulatory approval.

(ii) The implementation plan must describe the work to be undertaken and a schedule for completing it, including any interim milestones and the date for compliance, having regard to:

(A) the likely implications of not meeting the increased requirement for AEMO's *market* and *power system security* functions;

(B) the work required to address the issue by all relevant parties (including other DCPs or *Registered Participants* if applicable); and

(C) the relevant DCP's reasonable cost and resourcing constraints.

(iii) The relevant DCP is expected to work diligently to achieve the transition plan, including interim milestones, and must report on progress:

(A) on completion of any interim milestone; and

(B) if it appears to the DCP that the date for compliance is unlikely to be met.

[10] Excludes High Resolution Data from PMUs and HSMs unless specifically applied under section 7

[11] If AEMO has specified a format for the provision of this advice, the DCP should provide its advice in that format.

~~(i)~~(iv) If it appears to AEMO or the relevant DCP that the transition plan is not being met, either of them can request negotiation of suitable amendments to meet the increased requirement, and both are expected to negotiate in good faith.

3. Reliability

The purpose of this section is to ensure the reliability of data transmitted to AEMO.

3.1. Reliability requirements

(a) For the RME or RCE relating to any given *plant* or aggregation of *plant* for which Operational Data[12] must be transmitted to or from an *AEMO co-ordinating centre*:

(i) the total ~~period~~aggregate duration of Critical Outages ~~for a RME and RCE~~ in ~~a~~any rolling 12-month ~~assessment~~ period; and

(ii) the duration of any individual Critical Outage,

must ~~be no greater than those~~not exceed the relevant limit indicated in Table 4.

(b) For an Intervening Facility:

(i) the total ~~period~~aggregate duration of Critical Outages of an Intervening Facility over a rolling 12-month ~~assessment~~ period; and

(ii) the duration of any individual Critical Outage,

must ~~be no greater than those~~not exceed the relevant limit indicated in Table 5.

(c) An Intervening Facility must have back-up power supplies sufficient to sustain operation for at least 10 hours following loss of external AC (alternating current) supply, unless AEMO approves a shorter period for a specified Non-NSP Intervening Facility.

~~(a)~~(d) AEMO will actively monitor and report on the ~~Intervening Facility~~ performance~~.~~ of Intervening Facilities against the Critical Outage limits.

(e) If, in any rolling 12-month ~~assessment~~ period, the total ~~period~~aggregate duration of Critical Outages for a DCF exceeds ~~those~~a relevant limit indicated in Tables 4 and 5, the responsible ~~DCPs~~DCP and the DCP for any relevant connecting DCF must jointly take reasonable corrective action to bring those times within the ~~times~~applicable limits.

(f) A DCP will not be taken to breach the Critical Outage limits to the extent that a Critical Outage is caused or prolonged by:

(i) Force Majeure; or

~~(i)~~(ii) loss of external AC power supply to a network or equipment that lasts longer than the duration for which the DCP is required ~~by section 3.1(a) or (b) (as applicable).~~to ensure availability of back up power supplies under this Standard or an applicable *performance standard*,

[12] Excluding High Resolution Data from PMUs or HSMs.

Total period ofprovided that the DCP must take any reasonable steps within its control to mitigate the ongoing impact of the Force Majeure or loss of supply on the extent and duration of the outage.

Table 4 Maximum critical outages ofor RME and RCE over a 12-month period

Category of RME and RCEOperational Data	Max aggregate in 12 month period	Total period ofMax per Critical Outages Outage
Dispatch Data where there is no agreed substitute data	6 hours	6 hours
Dispatch Data where there is agreed substitute data	12 hours	12 hours
RCESystem Security Primary Data and System Security Secondary Data	24 hours	24 hours

Inserted Cells

Inserted Cells

Table 5 Total period ofMaximum critical outages of Intervening Facilityfor intervening facilities over a 12-month period

Category of Intervening FacilityOperational Data	Period per Critical OutageMax aggregate in 12 month period	Total Period ofMax per Critical Outages Outage
Dispatch Data	2 hours30 minutes	30 minutes2 hours
*Power system*System Security Primary Data and other dataSystem Security Secondary Data	6 hours1 hour	1 hour6 hours

3.2. Redundant elements

DCFs must have sufficient redundant elements to reasonably satisfy the reliability requirements set out in section 3.13.1., taking into account:

(a) the likely failure rate of their elements;

(b) the likely time to repair of their elements; and

(c) the likely need for planned outages of their elements.

4. Security

The purpose of this section is to ensure that cyber, physical and network security considerations are appropriately addressed by all parties. DCPs and AEMO must have, including through robust programs in placeand reporting frameworks to adequately and continuously manage cyber security risks that could adversely impact power system communications and supporting systems and infrastructure.

These cyber security programs should use reasonable endeavours to address the following functions:

Table 6 Cyber security functions

Function	Definition	Categories
Identify	An understanding of cyber security risks to systems, assets, data, and capabilities and how to manage these.	Asset management Business environment Governance Risk assessment Risk management strategy

Function	Definition	Categories
Protect	The controls and safeguards necessary to protect or deter cybersecurity threats	Access control Awareness and training Data security Data protection processes Maintenance Protective technologies
Detect	Continuous monitoring to provide proactive and real-time alerts of cybersecurity-related events	Anomalies and events Continuous monitoring Detection processes
Respond	Incident response activities	Response planning Communications Analysis Mitigation Improvements
Recover	Business continuity plans to maintain resilience and recover capabilities after a cyber breach	Recovery planning Improvements Communications

4.1. Standard applies in parallel with SOCI Act

(a) All DCPs that are responsible entities for critical infrastructure assets under the SOCI Act must comply with their obligations under that Act. This Standard does not limit the SOCI Act obligations in any way.

(b) This Standard may:

(i) extend requirements corresponding with the SOCI Act to DCPs that are not responsible entities or otherwise subject to the SOCI Act; or

(ii) apply additional requirements to responsible entities in relation to security risks relating to the transmission of Operational Data.

4.2. Security risk management plans

All DCPs must have in place a risk management program that identifies and manages material security risks. For these purposes, DCPs should, at a minimum, meet the requirements of Security Profile 1 (SP-1) as outlined in the Australian Energy Sector Cyber Security Framework[13] and be able to attest to this requirement being satisfied.

4.3. Security incident reporting

(a) NER 4.8.1 is a broad risk reporting obligation for all *Registered Participants*, which covers relevant cyber security risks, as follows:

Registered Participants' advice

[13] AESCSH framework and resources available on AEMO's website at: https://aemo.com.au/initiatives/major-programs/cyber-security/aescsf-framework-and-resources

A Registered Participant must promptly advise AEMO or a relevant System Operator at the time that the Registered Participant becomes aware, of any circumstance which could be expected to adversely affect the secure operation of the power system or any equipment owned or under the control of the Registered Participant or a Network Service Provider.

(b) *Registered Participants* should report identified or potential cyber security incidents under NER 4.8.1 to AEMO's Cyber Duty Manager. The conditions and timeframes for reporting cyber security incidents should be consistent with both NER 4.8.1 and Part 2B of the SOCI Act.

(c) In accordance with AEMO Policy 020113: Electricity Market Management Systems Access Policy And Procedure[14], *Registered Participants* must provide and maintain up to date contact details of a nominated cyber security contact. This contact should be reachable by AEMO 24/7 to coordinate any critical cyber security matters that may arise.

~~4.1.~~4.4. Physical security and computer network security

4.4.1. General obligations

DCPs should use reasonable endeavours to:

(a) prevent unauthorised access to DCF sites, and to DCFs and Operational Data, via computer networks;

(b) prevent unauthorised access to, or use of, AEMO's ~~wide area network (~~WAN~~)~~ via computer networks;

(c) prevent the ingress and distribution of malicious software into DCFs or AEMO's WAN;

(d) keep access information, including computer network address information, confidential[15];

(e) consult with AEMO on any matter that could reasonably be expected to adversely impact the security of DCFs or AEMO's WAN; and

(f) ensure that adequate procedures and training are provided to persons who are authorised to have access to DCFs and AEMO's WAN.

4.4.2. Communications between RME/RCE and Intervening Facilities

(a) The digital communications service between a DCP's RME/RCE and an Intervening Facility, where that service is used for the transmission of Dispatch Data or System Security Primary Data, must be provided by means of:

(i) a Secure Network; and

(ii) A Resilient Network, unless an exemption under section (d)5.1(d) applies to the relevant Intervening Facility.

[14] Made under NER 3.19

[15] See NER glossary for definition of *confidential information*: In relation to a *Registered Participant* or AEMO, information which is or has been provided to that *Registered Participant* or AEMO under or in connection with the Rules and which is stated under the Rules, or by AEMO, the AER or the AEMC, to be *confidential information* or is otherwise confidential or commercially sensitive. It also includes any information which is derived from such information.

(b) DCPs must implement protection of communications with field devices against threats as outlined in IEC 62351 Power systems management and associated information exchange – Data and communications security, that:

(i) authenticates communications and implement integrity measures to prevent message tampering, replay or spoofing, person-in-the-middle and masquerade attacks; and

(ii) where implementation is operationally and economically feasible, that the confidentiality of communications is protected using encryption.

(c) Priority should be given to implementing security protections at the application layer, and should also be implemented at the transport or network layer as an additional layer of defence or when it is infeasible to implement at the application layer.

(d) The protocols and algorithms used by these security protections should preference recommendations for approved protocols and algorithms from the Australian Signals Directorate's Guidelines for Cryptography[16].

5. Interfacing

The purpose of this section is to ensure appropriate interfaces between ~~DCFs~~Intervening Facilities and AEMO systems.

5.1. Physical and logical interfaces with AEMO co-ordinating centres

(a) Where AEMO agrees to extend its WAN to ~~DCP DCFs, each~~an Intervening Facility, the relevant DCP must establish a physical connection to an AEMO-designated port on an AEMO router for each *AEMO co-ordinating centre*, and it must use Ethernet and TCP/IP protocols.

(b) Where AEMO agrees that a DCP may establish a logical connection ~~to~~between its Intervening Facility and AEMO's WAN, the DCP must do so by engaging a Telecommunications Carrier to provide a digital communications service between the DCP's ~~DCFs~~Intervening Facility and an AEMO-designated network access facility. The communications service must be provided by means of:

(i) a Secure Network; and

(ii) a Resilient Network, unless specifically agreed under paragraph (d).

[16] Information Security Manual, Guidelines for Cryptography, published 16 June 2022 and as amended from time to time. Downloadable from: https://www.cyber.gov.au/acsc/view-all-content/advice/guidelines-cryptography

~~5.2.~~ To ensure resilience in Operational Data communications, all Intervening Facilities must establish a physical or logical connection to both *AEMO co-ordinating centres* unless another connection configuration is established for a DNSP Intervening Facility under section 1.4.1 ~~Data communications protocols~~

(c) .

(d) A DCP wishing to establish a connection to AEMO's WAN from a Non-NSP Intervening Facility may request AEMO to exempt it from the requirement to provide a Resilient Network and instead utilise a public internet service to provide a Secure Network. AEMO may grant or refuse the request at its discretion, and will have regard to:

(i) the capacity and operation of the related *plant*;

(ii) the quantities and significance of Operational Data to be transmitted;

(iii) the aggregate capacity of *plant* in the same *region* for which Operational Data is transmitted via public internet; and

(iv) any other factors AEMO considers relevant.

AEMO may publish guidance from time to time on how AEMO applies these considerations.

5.2. Communication protocols

5.2.1. NSP Intervening Facilities

The Communication Protocol to be used for any communication of Operational Data (other than High Resolution Data from PMUs or HSMs) through a physical or logical interface ~~with AEMO must use the secure~~between an NSP Intervening Facility and an *AEMO co-ordinating centre* is ICCP IEC60870-6 TASE.2 ~~protocol. Legacy non-~~and its extensions (secure ICCP ~~connections will continue to be~~).

5.2.2. Non-NSP Intervening Facilities

(a) The Communication Protocol to be used for any communication of Operational Data (other than High Resolution Data from PMUs or HSMs) through a physical or logical interface between a Non-NSP Intervening Facility and an *AEMO co-ordinating centre* is either:

(i) ICCP IEC60870-6 TASE.2 and its extensions (secure ICCP); or

~~(i)~~(ii) where the Intervening Facility equipment is not suitable for secure ICCP, an alternative secure protocol supported ~~until 1 January 2020.~~by AEMO as specified under paragraph (b).

(b) Alternative secure protocols are:

(i) from a date determined by AEMO and published on its website[17], DNP3; or

(ii) another secure protocol specified by AEMO on its website from time to time for use for Non-NSP Intervening Facilities,

and the configuration of any alternative protocol must be consistent with recommendations for approved protocols and algorithms from the Australian Signals Directorate's Guidelines for Cryptography.

6. Maintenance, planning and testing

The purpose of this section is to ~~ensure that~~minimise the impact of outages of DCFs ~~do not unduly impact~~ on central dispatch or power system security.

6.1. Governance and reporting on availability

(a) AEMO will at regular intervals make available a report on the availability and performance of Intervening Facilities, including:

(i) link up time to *AEMO co-ordinating centres*; and

(ii) data quality measures,

and for the purposes of this reporting a DCP must provide information about its DCFs reasonably requested by AEMO within a reasonable timeframe.

(b) The DCP for each Intervening Facility must maintain current phone and email contacts for communicating outages and data issues.

(c) Routine maintenance activities affecting the transmission of data are to be communicated via email contact at the start and finish of each activity.

~~6.1.~~6.2. Response to failures

In response to a DCF failure, including a failure to transmit Operational Data[18] in accordance with the requirements of this Standard, a DCP must:

(a) rectify the DCF ~~within the timeframes~~promptly, and as far as practicable to ensure Critical Outages do not exceed the limits specified in Tables 4 and 5 in section 3~~.~~;

(b) in respect of inaccurate Operational Data measurements, rectify the inaccuracy within 30 days after the DCP becomes aware of it;

~~(b)~~(c) inform AEMO[19] of the progress of related rectification works, if a failure is causing a Critical Outage~~, and~~ or in relation to data inaccuracy; and

~~(c)~~(d) consult with AEMO about the priority of related rectification works, if a failure is causing or likely to cause a Critical Outage~~.~~; and

[17] https://aemo.com.au/energy-systems/market-it-systems/electricity-system-guides/power-systems

[18] Excludes High Resolution Data from PMUs or HSMs unless specifically applied under section 7.

[19] ~~*Control*~~By telephone to an *AEMO co-ordinating centre*.

(e) provide reasonable assistance to other DCPs in responding to DCF failures.

~~6.2.~~6.3. Planned outage co-ordination

(a) A DCP must give AEMO ~~five~~5 *business days*' notice, subject to ~~section 6.2~~paragraph (d), of a planned outage of any of its DCFs affecting, or likely to affect:

(i) Dispatch Data~~;~~ or High Resolution Data; or

(ii) the majority of ~~Operational~~System Security Primary Data ~~to or from a Substation~~ or ~~*power station*~~System Security Secondary Data transmitted by the DCF.

(b) If 5 *business days*' notice cannot be given, subject to ~~section 6.2~~paragraph (d), AEMO may defer the outage.

(c) AEMO may defer or cancel outages and require DCFs on outage to be returned to service if AEMO considers that a planned outage would:

(i) adversely affect power system security;

(ii) occur when *power system security* is adversely affected by other events; or

(iii) occur when AEMO has issued, or is likely to issue, a *lack of reserve* notice.

(d) If *plant* related to the DCF is out of service at that time, and will not return to service while the DCF is out of service, the outage notice may be reduced to 24 hours.

~~(e) A planned outage of DCFs excludes an outage that does not cause a Critical Outage.~~

~~6.3.~~6.4. Data management and co-ordination

(a) DCPs must keep AEMO informed of planned and unplanned changes to Status Indications, Discrete Values and Analogue Values transmitted to AEMO and Control Commands received from AEMO.

(b) DCPs must notify AEMO of planned changes to DCFs, subject to ~~section 6.3~~paragraph (c), with sufficient details to allow AEMO to implement the corresponding changes to its own *control centre* facilities. AEMO must be notified:

(i) at least 15 *business days* before the planned implementation date for a minor augmentation of an existing ~~*power station* or Substation~~DCF; and

(ii) at least 30 *business days* before the planned implementation date for a new ~~Substation or *power station*~~DCF or major augmentation of an existing ~~*power station* or Substation~~DCF.

(c) The periods of 15 and 30 *business days* in ~~section 6.3~~paragraph (b) may be reduced by agreement between the DCP and AEMO if the DCP:

(i) includes AEMO's corresponding implementation tasks in its project schedules, with task durations agreed with AEMO; and

(ii) provides the major part of the detailed information in an electronic format suitable for AEMO to automatically populate its relevant databases.

(d) For an unplanned change to DCFs the DCP must:

(i) promptly notify AEMO before the change is implemented;

(ii) coordinate with AEMO by phone before the change is implemented; and

(iii) confirm the change in writing within 14 days of the change.

(e) An augmentation is taken as implemented when the relevant primary plant is first electrically connected to the *power system*, or when the relevant secondary plant is commissioned.

(f) Unless AEMO agrees otherwise, a major augmentation includes the installation of:

(i) a *busbar*, *transmission line* or *transformer* intended to operate at more than 100 kV; and

~~(ii) 100 kV; and~~

~~(iii)~~(ii) a scheduled generating unit, semi-scheduled generating unit, scheduled network service or scheduled load.

(g) A minor augmentation is any other project.

(h) A planned change is one that could reasonably have been foreseen in sufficient time to give prior written notice under ~~section 6.3~~paragraph (b).

~~6.4.~~6.5. Testing to confirm compliance

(a) A DCP installing, upgrading or replacing RME or RCE must test a representative sample of ~~Dispatch and *Power system*~~each category of Operational Data ~~of~~ transmitted from or to that RME or RCE. These tests must ~~confirm compliance with the timing requirements set out in section 2.3.~~:

(i) confirm that each sample of Operational Data is correctly identified;

(ii) determine at least 5 measurements (not synchronous with scanning of the data) within a single period of at least 5 minutes;

(iii) verify compliance with each applicable requirement in section 2; and

(iv) identify any issues requiring remediation.

(b) A test under ~~section 6.4~~paragraph (a) must be carried out either prior to, or within 60 *business days* ~~of~~after, the relevant RME or RCE ~~being~~is placed into service, and otherwise in accordance with any applicable *performance standard* compliance assessment or test plan under Chapter 5 of the NER.

(c) Prior to a test, the DCP installing, upgrading or replacing the RME or RCE must:

(i) coordinate with the provider(s) of ~~Data Concentrator(s) and~~ Intervening Facility(ies) relaying the Operational Data to be tested;

(ii) prepare and provide to AEMO the test procedure;

(iii) amend the test procedure if AEMO reasonably considers it inadequate to assess compliance; and

(iv) consult and agree with AEMO with regards to the RME or RCE and the associated Operational Data to be tested.

(d) A DCP that provides an Intervening Facility for another DCP must cooperate with that DCP and AEMO in planning and conducting the tests.

(e) The DCP providing the RME or RCE must submit a report to AEMO within a reasonable time after the test. The report must summarise the results of the test and any remedial action necessary ~~to ensure compliance with section 2.3. For that purpose, a test under section 6.4 must be used to determine at least five measurements (not synchronous with scanning of the data) within a single period of at least five minutes.~~as identified in paragraph (a).

7. Near real time data from PMU and HSM devices

Where AEMO requires High Resolution Data to be transmitted to *AEMO co-ordinating centres* from a PMU or HSM, the minimum requirements to apply to that data for the purposes of this Standard will be:

(a) specified in a notice issued to the relevant *Registered Participant* under NER 4.11.1(d), as may be subsequently amended by agreement between AEMO and the *Registered Participant*; or

(b) recorded in an operational protocol, procedure or similar document agreed or approved by AEMO and the relevant *Registered Participant*.

Unless otherwise specified, those requirements will apply in addition to any provisions in this Standard that are apply to the transmission of High Resolution data from PMU and HSM devices, as indicated in section 1.7.

8. Management of non-compliance

The purpose of this section is to provide information relevant to the reporting and remediation of non-compliances with this Standard, consistent with the NER.

8.1. Consequences of non-compliance

Compliance by a DCP with this Standard is a requirement of NER 4.11 and, to the extent incorporated in a *performance standard*, NER 4.15. Failure to comply, or remedy a non-compliance, with a requirement of the Standard could result in a range of potential consequences for a DCP under the NER, including:

(a) enforcement action by the AER;

(b) in relation to a new facility, a determination by AEMO not to approve an application for registration;

(c) restrictions on output of generating systems; or

(d) incorrect inputs to *dispatch* targets and incorrect measurement of ancillary services.

Compliance by one DCP may rely on the combined efforts of multiple DCPs, who are each expected to perform their obligations in accordance with section 1.6.

8.2. Reporting and remediation

(a) DCPs required to comply with this Standard for the purpose of a *performance standard* are expected to observe the requirements of NER 4.15 in respect of the monitoring,

assurance, reporting and remediation of any failure of a DCF to meet the Standard requirements.

(b) All DCPs are expected to observe any applicable reporting requirements established under NER 8.7.2.

9. Transitional arrangements for 2023 Standard Update

This section provides a mechanism by which DCPs can have additional time to implement any changes to their existing DCFs and related systems, that are necessary to meet any increased requirements introduced in version 3.0 of the Standard (effective from 3 April 2023).

9.1. Definitions, application and maximum timeframes

(a) In this section 9:

effective date means 3 April 2023.

increased requirement means a requirement introduced or amended in section 2 of version 3.0 of this Standard that is applicable to a DCF established prior to 7 September 2022 and is a new or more onerous requirement than any corresponding requirement that applied to the DCF under the old Standard. An increased requirement excludes a requirement that the DCF is obliged to meet under a separate legal requirement (not implemented through the Standard).

implementation changes means the work, upgrades or other changes to a DCF or related systems that are necessary to meet an increased requirement.

old Standard means the version of the Standard in effect immediately prior to the effective date.

relevant DCP means the DCP that has given an advice to AEMO under paragraph (b) in respect of one or more of its DCFs.

transition date means the date agreed for the DCF to achieve compliance with an increased requirement as agreed or amended under section 9.2, which must not be later than:

(i) for a TNSP or a DNSP, 12 months after the start of the first *regulatory control period* for which the *AER* made a final *distribution determination* or *transmission determination* (as applicable) after the effective date; or

(ii) for any other DCP, 2 years after the effective date or, if compliance with the increased requirement depends on implementation of changes by an NSP, 12 months after implementation of those changes.

transition plan means the plan approved for completing and commissioning the implementation changes by the transition date, as approved and amended under section 9.2.

(b) This section applies to a DCP in respect of a DCF if, prior to the effective date, the DCP has advised AEMO in writing that it is not reasonably able to comply with an increased requirement in respect of a DCF by the effective date, and the reasons why.

9.2. Transition plan

(a) A relevant DCP and AEMO must use reasonable endeavours to agree a transition plan within 3 months after the effective date or such longer period as AEMO reasonably allows, and for this purpose the relevant DCP must promptly provide AEMO with the information it reasonably requests about the nature and cost of proposed implementation changes, the timeframes in which they can be completed, resourcing requirements and limitations, and any dependencies on third parties or (where the cost is material) regulatory approval.

(b) A transition plan must describe the implementation changes and set out a schedule for completing them, including any interim milestones and the transition date. The schedule must be set with regard to:

(i) the likely implications of not meeting the increased requirement for AEMO's *market* and *power system security* functions;

(ii) the work required to address the issue by all relevant parties (including other DCPs or *Registered Participants* if applicable); and

(iii) the relevant DCP's reasonable cost and resourcing constraints.

(c) The relevant DCP is expected to work diligently to achieve the transition plan, including interim milestones, and must report on progress:

(i) on completion of any interim milestone;

(ii) when it appears to the DCP that a target date in the transition plan is unlikely to be met; and

(iii) otherwise, at least every 6 months unless AEMO otherwise agrees.

(d) If it appears to AEMO or the relevant DCP that the transition plan is not being met, either of them can request negotiation of suitable amendments to meet the increased requirement, provided that the transition date must not be later than defined in section 9.1(a).

(e) AEMO and the relevant DCP are expected to negotiate in good faith in respect of any amendments requested under paragraph (d).

9.3. Deemed compliance between effective date and transition date

(a) A relevant DCP is taken to be compliant with an increased requirement in respect of its relevant DCF between the effective date and the transition date, if and for as long as the following conditions are satisfied:

(i) all requirements applicable to the DCF under the old Standard are being met;

(ii) the relevant DCP is actively working in a timely manner to establish, implement or negotiate amendments to the transition plan in accordance with section 9.2.

(b) If AEMO considers that those conditions are not being met, AEMO may notify the relevant DCP and the *AER* that the relevant DCP is considered non-compliant with the increased requirement. Where compliance with the increased requirement is part of a *performance standard*, NER 4.15 will apply to the non-compliance.

Version release history

~~Version~~	~~Effective Date~~	~~Summary of Changes~~
Version	Effective date	Summary of changes
3.0	3 April 2023	Revised following complete review
2.0	1 December 2017	Updated following review of the standard
1.2	7 April 2005	Revised to make consistent with National Electricity Rules
1.1	24 June 2004	Revised to correct a typographical error in the definition of data concentrator
1.0	1 January 2004	