POWER SYSTEM DATA COMMUNICATION STANDARD

National Electricity Market

PREPARED BY: AEMO Systems Capability
VERSION: [3.0]
EFFECTIVE DATE: [3 April 2023]
STATUS: DRAFT DETERMINATION VERSION – SEPTEMBER 2022

Approved for distribution and use by:
APPROVED BY:
TITLE:

DATE:

CONTENTS

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

1. INTRODUCTION

1.1. Purpose and scope

(a) 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 NER 4.11.1 and 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.

(b) This Standard sets out the standards and protocols applicable to the recording, transmission or receipt of telemetered data required for the purposes of monitoring and managing *central dispatch* and *power system security* and reliability (**Operational Data**) (including indications, signals and instructions) by:

(i) *remote monitoring equipment* (RME) and *remote control equipment* (RCE) installed and maintained by *Registered Participants* who are required to do so under NER 4.11.1 and S5.2.6.1; and

(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.

1.2. Definitions and interpretation

1.2.1. Glossary

Terms defined in the National Electricity Law and the NER have the same meanings in 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.

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

Term	Definition
Analogue Value	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 *control centres*, in accordance with section 5.2.
Control Command	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.

Term	Definition
Critical Outage	**For an RME or RCE:** A loss of the ability to transmit Operational Data of Good Quality to AEMO or receive Control Commands from AEMO exceeding 60 seconds, but excluding an outage that: • affects less than 5% of all Operational Data items of that RME or RCE; • only affects the transmission of Operational Data relating to scheduled *plant* that is not available to participate in *central dispatch*; • relates to a period when the *plant* associated with the RME or RCE is not in service and AEMO has been notified of that fact; • is planned for work to upgrade the RME or RCE, where AEMO has been notified in advance; or • is caused solely by an outage of an Intervening Facility. **For an Intervening Facility:** A loss of the ability to transmit Operational Data of Good Quality to AEMO or receive Control Commands from AEMO exceeding 3 minutes, but excluding an outage that: • lasts less than 10 minutes and does not affect the transmission of Dispatch Data; or • is planned for a test of: – DCFs at a disaster recovery site; or – a major upgrade of an Intervening Facility, for which AEMO has been given at least 24 hours' notice and which affects no more than one *trading interval* (or a longer period agreed with AEMO in advance).
Data Communication Provider (DCP)	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. • power supply equipment for the above equipment.
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 may be necessary to prevent repeated transmission of data when it has not changed materially.
Discrete Value	A numeric representation of one of a limited set of values (for example a *transformer tap position*).

Term	Definition
Dispatch Data	Telemetered data that is required for the operation of the 5-minute *central dispatch* process, representing any of the following: • the operational status and measurement of the production, consumption or flow of *scheduled plant* or a *wholesale demand response unit*[1], including aggregated data for *plant* or services that are *dispatched* in aggregate; . • measurements of *interconnector* flow; • the *enablement* status or 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 *control centre*; or • transmission of a command from an AEMO control centre and receipt of the command at RCE.
Force Majeure	An event or circumstance that directly affects the ability of a DCF to transmit or receive Operational Data, to the extent that: • the occurrence of the event or circumstance is 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, and either mitigated or prevented, by the 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	Data measured and transmitted to AEMO in near real time by devices with GPS clock synchronisation 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 • data measured by PMU and HSM devices for real time operations.
HSM	High Speed Monitor
ICCP	Inter-Control Center Communications Protocol - IEC 60870-6 TASE.2 and its extensions[2]
Intervening Facility	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 *control 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 *control centre*.

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

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

Term	Definition
NER	National Electricity Rules. A reference to NER followed by a number is to the corresponding rule or clause of the NER.
Non- NSP Intervening Facility	A DCF that: • is not an asset of, or provided by, an NSP; • receives Polls directly from AEMO *control centres*; • collects data from an RME (whether directly or via an aggregation facility) and relays that data to AEMO *control centres*; and • relays Control Commands 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 *control centre* or (where this Standard permits) via another NSP Intervening Facility; • collects data from RME or another NSP Intervening Facility and relays that data to an AEMO *control centre* or (where this Standard permits) another NSP Intervening Facility; and • relays Control Commands from an AEMO *control centre* to RCE or another NSP Intervening Facility.
Operational Data	An umbrella term for all data required to be transmitted to or from AEMO *control centres* using RME, RCE and the Intervening Facilities for AEMO's *market* and *power system security* functions – includes Dispatch Data, High Resolution Data, Primary System Security Data and Secondary System Security Data.
PMU	Phasor Measurement Unit
Poll	An electronic request sent from a *control centre* or an Intervening Facility to RME to request Status Indications, Discrete Values or Analogue Values.
Primary System Security Data	Telemetered data relating to: • all *network* assets that operate at a nominal *voltage* of at least 220 kV or are *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 *facility* or the provision of a service from a *control centre*.
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 numeric value.
Secondary System Security Data	Telemetered data required for effective *market* operation and *power system security* that is not Dispatch Data, High Resolution Data or Primary System Security Data. Examples include data required for: • inputs to short term forecasting systems; and • inputs to dynamic rating systems.
Secure Private Network	A communication network which; • is not accessible to third parties; and • has back-up power supplies sufficient to sustain operation for at least 10 hours following loss of external AC (alternating current) supply.

Term	Definition
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	A carrier as defined in the Telecommunications Act 1997.
True Value	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	Wide area network

1.2.2. Interpretation

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

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[3].

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

(i) establish a direct connection to both AEMO *control centres*[4];

(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 *control centre* and a second connection to the Intervening Facility maintained by its *regional* 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 *control centre*, establish a direct connection to both AEMO *control 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

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 *control centres* in accordance with section 5.1.

1.5. Overview of Data Communication Facilities

The following diagram illustrates the relationships between:

- AEMO *control centres*.
- NSP Intervening Facilities (in the diagram Intervening Facility 1 represents a TNSP facility and Intervening Facility 2 represents a potential connection configuration of a DNSP Facility).
- Non-NSP Intervening Facilities.
- RME and RCE.

[3] 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

[4] 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.

Figure 1 General Structure of DCF

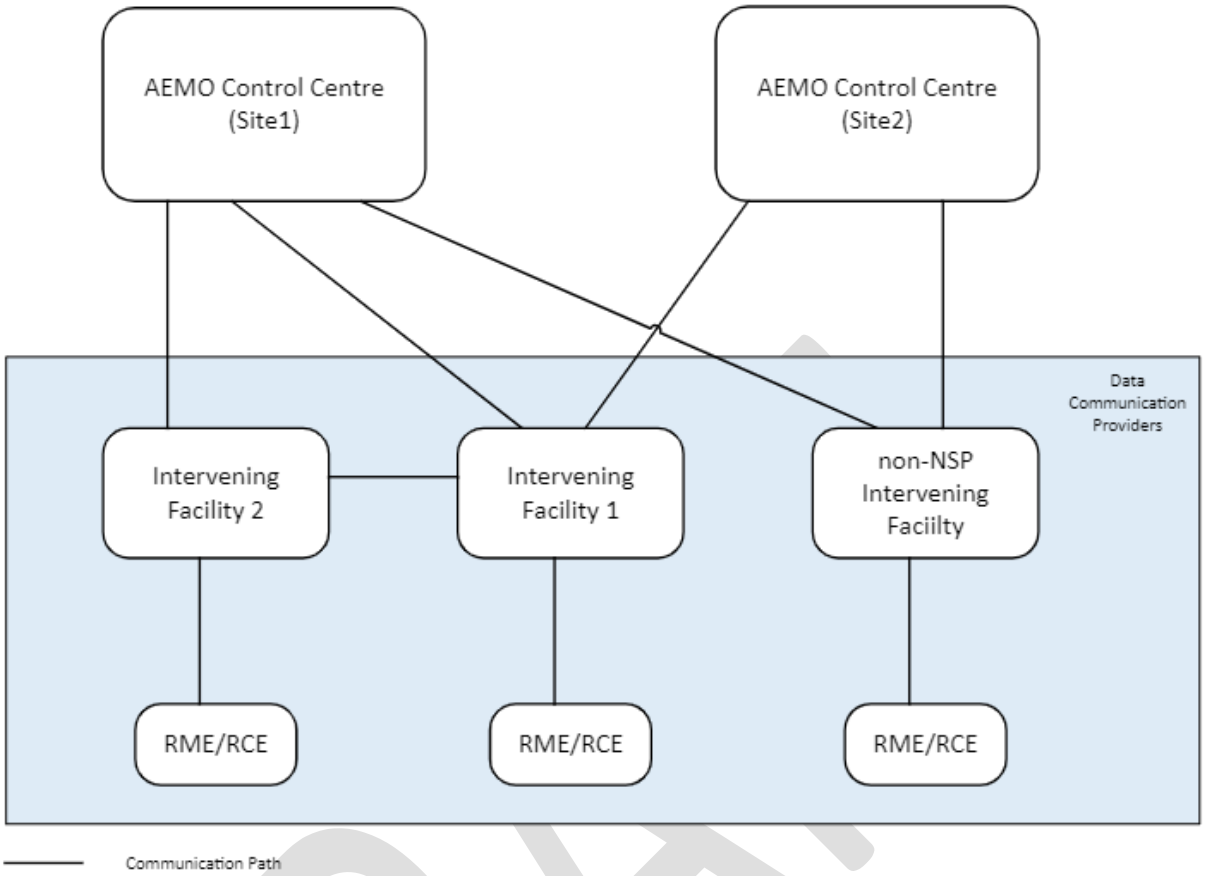

Figure 1 is only intended to be a conceptual schematic showing potential connection paths of various facilities. It is not a conceptual/solution architecture design for a DCP to install their infrastructure; a DCP is expected to design its infrastructure and communication services to meet the requirements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

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 near real-time 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 PMUs and HSMs providing near real-time data 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 *control centres*. Section 5.1 applies to PMUs and HSMs providing near real-time 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 near real-time data unless specified in accordance with section 7.
- Section 7 explains how performance requirements for near real-time 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. These requirements do not apply to PMUs and HSMs providing near real-time data unless specified in accordance with section 7.
- Section 9 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. Capability to transmit and receive Operational Data

(a) DCFs must be capable of transmitting and receiving the types and quantities of Operational Data required by AEMO for its *market* and *power system security* functions from time to time under the NER, including, for example:

(i) quantities and signals approved in respect of *plant* or 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 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 to comply with this Standard in respect of Operational Data.

(c) As noted in section 1.7, the references to High Resolution Data in this section 2 do not apply to near real-time data from PMUs and HSMs. Requirements for those devices are set under section Error! Reference source not found..

2.2. Representation of data

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

(b) Analogue 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 Values

Category of Analogue Value	Resolution (Max % of Scale Range)
Dispatch Data and High Resolution Data	0.1
Primary System Security Data	0.2
Secondary System Security 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.

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

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

(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; and

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

provided that the default state must be set to good, unless interfering actions or failure is detected at any stage between an Intervening Facility and RME.

(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.

2.3. Age of data

(a) 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 measured from the instant the data first gets converted to digital form and includes any time within an Intervening Facility.

Table 2 End to End Time for data to be available for transmission to AEMO

Category	Data Type	Time Interval (seconds)
High Resolution Data	Analogue Value	2
Dispatch Data	Status Indication	3
	Analogue Value	6
	Discrete Value	6
Primary System Security Data	Status Indication	3
	Analogue Value	14
	Discrete Value	14

Category	Data Type	Time Interval (seconds)
Secondary System Security Data	Status Indication	12
	Analogue Value	22
	Discrete Value	22

(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.

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

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

Table 3 Deadband for transmission of Analogue Values

Category of Analogue Value	Deadband (% of Scale Range)
Dispatch Data and High Resolution Data	0.2
Primary System Security Data	0.5
Secondary System Security Data	0.5

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

2.4. Control Command delay

DCPs must relay Control Commands such that commands from AEMO *control centre* to RCE or response from RCE to AEMO *control centre* will not have a delay of more than 2 seconds.

2.5. Data Accuracy

All Analogue Values received at AEMO *control centres* must be within +/- 1 % of the True Value.

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 must be transmitted to or from an AEMO *control centre*:

(i) the total aggregate duration of Critical Outages in any rolling 12-month period; and

(ii) the duration of any individual Critical Outage,

must not exceed the relevant limit indicated in Table 4.

(b) For an Intervening Facility:

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

(ii) the duration of any individual Critical Outage,

must 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.

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

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

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

provided 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 for RME and RCE

Category of Operational Data	Max aggregate in 12 month period	Max per Critical 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
Primary and Secondary System Security Data	24 hours	24 hours

Table 5 Maximum Critical Outages for Intervening Facilities over a 12-month period

Category of Operational Data	Max aggregate in 12 month period	Max per Critical Outage
Dispatch Data	2 hours	30 minutes
Primary and Secondary System Security Data	6 hours	1 hour

3.2. Redundant elements

DCFs must have sufficient redundant elements to reasonably satisfy the reliability requirements set out in section 3.1, 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, including through robust programs and reporting frameworks

to adequately and continuously manage security risks that could adversely impact power system communications and supporting systems and infrastructure.

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[5] 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**
>
> *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[6], *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.

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

[6] Made under NER 3.19

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 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[7];

(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 must be provided by means of a Secure Private Network where that service is used for the transmission of Dispatch Data or Primary System Security Data, unless an exemption under section (d)5.1(d) applies to the relevant Intervening Facility.

(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 possible, protects the confidentiality of communications 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[8].

5. INTERFACING

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

[7] 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.

[8] 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

5.1. Physical and logical interfaces with AEMO control centres

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

(b) Where AEMO agrees that a DCP may establish a logical connection 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 Intervening Facility and an AEMO-designated network access facility. The communications service must be provided by means of a Secure Private Network unless specifically agreed under paragraph (d).

(c) To ensure resilience in Operational Data communications, all Intervening Facilities must establish a physical or logical connection to both AEMO *control centres* unless another connection configuration is established for a DNSP Intervening Facility under section 1.4.1.

(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 Secure Private Network and instead utilise a public internet service. 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 through a physical or logical interface between an NSP Intervening Facility and an AEMO *control centre* is ICCP IEC60870-6 TASE.2 and its extensions (secure ICCP).

5.2.2. Non-NSP Intervening Facilities

(a) The Communication Protocol to be used for any communication of Operational Data through a physical or logical interface between a Non-NSP Intervening Facility and an AEMO *control centre* is either:

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

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

(b) Alternative secure protocols are:

(i) from a date determined by AEMO and published on its website[9], DNP3; or

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

[9] [website location for publication of list and specifications to be inserted]

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 minimise the impact of outages of DCFs 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 *control 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.

6.2. Response to failures

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

(a) rectify the DCF 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;

(c) inform AEMO[10] of the progress of related rectification works, if a failure is causing a Critical Outage or in relation to data inaccuracy; and

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

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

6.3. Planned outage co-ordination

(a) A DCP must give AEMO 5 *business days*' notice, subject to 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 Primary System Security Data or Secondary System Security Data transmitted by the DCF.

[10] By telephone to an AEMO *control centre*

(b) If 5 *business days*' notice cannot be given, subject to 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.

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 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 DCF; and

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

(c) The periods of 15 and 30 *business days* in 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) 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 paragraph (b).

6.5. Testing to confirm compliance

(a) A DCP installing, upgrading or replacing RME or RCE must test a representative sample of each category of Operational Data transmitted from or to that RME or RCE. These tests must:

(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 paragraph (a) must be carried out either prior to, or within 60 *business days* after, the relevant RME or RCE is placed into service.

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

(i) coordinate with the provider(s) of 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 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 *control centres* in near real time, 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 expressed to apply to the transmission of near real time data from PMU and HSM devices.

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.

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 in section Error! Reference source not found. introduced in version 3.0 of the Standard (effective from [1 April 2023].)

9.1. Definitions, application and maximum timeframes

(a) In this section Error! Reference source not found.:

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 next *regulatory control period* after the effective date for which the *AER* had not made a final *distribution determination* or *transmission determination* (as applicable) prior to 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 Error! Reference source not found.(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
3.0	[1 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	