Meeting Participants:

Aruna Yahampath <Aruna.Yahampath@endeavourenergy.com.au>; Sumith Withanage <Sumith.Withanage@powerwater.com.au>; Victor Tan <victor@vtanconsulting.com>; Fernandez, Rohan (ENet) <Fernandez.Rohan@electranet.com.au>; Aardenburg, Brenton (ENet) <Aardenburg.Brenton@electranet.com.au>; ahmad.taufiq@originenergy.com.au, Tony Myatt <Tony.Myatt@sapowernetworks.com.au>, louise.watts@sapowernetworks.com.au

Section	Issue raised	Questions	Comments – Cigre AU D2 Panel Response
	SCOPE AND APPLICATION OF THE STANDARD		
3.1.1	Data to be provided - Standard needs to be more definitive on the range of measurements that need to be provided as there is significant uncertainty as to what will actually be required for new connections.	Does the Standard need to be more specific on the range of data covered by the Standard? If so why and what level of detail is considered necessary?	The standard needs to be more specific on emerging connections, for example the standards specifically for generators or DNSPs, and how these differ (if they do) from exiting connections. The standard should remain broad so that it doesn't create adverse limitations based on technology changes. A guideline document that outlines how the standard applies to a specific DCPs with some example scenarios for different types and levels of DCPs would provide greater clarification for consumers of the standard.
3.1.1	Definition of power system data - with the growth of embedded generation and the need for AEMO to monitor power flows in distribution systems which impact on the security of the transmission network, this definition needs to be expanded.	Does the definition of power system data need to be extended? If so why and what would be a more appropriate definition?	Seek better clarification as to whether both conditions need to be true to be identified as a Power System Data or whether it is an and/or. Are DNSPs that connect to AEMO covered by this standard even if less than the voltage stipulated? Are small generators that connect to AEMO either via DNSPs or directly also covered by this standard even if they don't meet the definition for a Power System? Are Virtual Power Plants covered by this standard? All require clarification in the standard.
3.1.1	Definition of Control Commands - this definition is inadequate as it does not cover the full range of control commands sent out from AEMO NEM Control Centres.	Does the definition of control commands need to be extended? If so why and what would be a more appropriate definition?	We wouldn't want to lock ourselves into specific commands here either.
3.1.1	Definition of RCE and RME - this definition in no longer adequate in context of new technology for data acquisition.	Do the definitions of RCE and RME need to be extended? If so why and what would be a more appropriate definition?	Very broad – consider clarification. Consider including overview of the functions of the equipment.
3.1.1	Participants in the data communications process - the Standard in Section 1.1 does not include the full range of participants involved in the data communications process.	Other than the changes required to accommodate additional participant categories identified in clause 4.11.1 of the NER, does the Standard need to extend or specify other participants or sub-groups within a category. If so, how and why?	The ancillary service providers cover this. These groups are sufficient.
	GENERAL ISSUES		
3.1.2	The requirements set under the Standard for different classes of data need to take into account the use of the data and its criticality.	Should requirements under the Standard be varied according to how critical the data is? If so, what criteria should be used to determine the requirements particular data needs to meet?	No. Data applicability as per power system data definition.
3.1.2	The standard is not consistent with more stringent requirements in some areas (e.g. Market Ancillary Service Specification).	Are there examples where AEMO has specified requirements beyond those set in the Standard, and how can any potential inconsistencies best be reconciled?	
3.1.2	The standard seems to assume that all participants in the data communications process operate data centres.	Are there examples where the Standard has not kept pace with developments in data communications technology?	The drawing in section 1.3 implies that an intervening data centre is available and that all connections require primary and backup communications. The drawing is just one example of how DCPs connect to AEMO. Either a guidelines document with examples of different configurations is required and/or the drawing in the document needs to be updated to include more information on the architecture requirements based on current specs. It is confusing as to what redundancy is required within the DCP e.g. from Data Concentrator to RME/RCE, does this require redundancy of only the comms link, redundancy of both the comms link and the RME/RCE – or does the standard need to only define the link to AEMO and the reliability and availability standards are used by the DCPs to make their own decisions on this.

			e.g. It is unclear if dual RTUs is required by all parties (e.g. a small generator).
3.1.2	There is an opportunity to design vulnerability out and design security in, as opposed to putting in place processes to manage the emergence of security issues. It might be possible for the Standard to encourage enhancement of resilience through design.	Is there an opportunity for the standard to encourage enhancement of resilience through design? If so, how might this be done?	
3.1.2	The Standard to be clear on the consequences for a participant failing to meet the requirements of the Standard.	Should the Standard set out the consequences for a participant failing to meet its requirements?	This should be outlined in the regulations. A guideline document could be useful here – reference to point DCPs in the right direction to get more information on what happens if the requirements are not met.

	ARCHITECTUAL REQUIREMENTS		
3.1.3	The requirements specified for DNSPs may be unclear in a number of areas. Possible examples are: • • Current standard does not reflect topology that applies for DNSP (e.g. diagram in Section 1.3 and tables 4 and 5). • • Standard needs to state whether or not DNSP can have direct connection with AEMO rather than going through TNSP • • Standard needs to account for diversity in comms between TNSP/DNSP to AEMO. • • Standard should include situation where there are two intervening facilities and perhaps more.	What changes to the current Standard are required to clarify the requirements for DNSPs?	It is unclear whether a generator needs to connect via a DNSP / directly with AEMO / or via another means. There are no standards between the generator and DNSP listed. No definitions of lines of responsibility. Who is responsible for upgrade of equipment as required and standards around obsolescence? The performance and the reliability sections should drive this. Is this implied through these sections? If not, it should be more well defined. Agree, the diagram in Section 1.3 does not reflect topologies for DNSP and other. The architecture needs to be more well defined and updated. Agreed – extend the architecture to account for the possibility of more than 1 intervening facility.
3.1.3	The current structure is making it difficult for new connections.	Are there specific examples where the current data communications structure is making it difficult for new connections or embedded participants? If so what changes in the Standard would be required to address these issues?	New connections from DNSPs – finding it difficult. Challenges around resourcing, no experience connecting in this way and there is no consistent messaging from AEMO around how to connect. This could be more defined in the standard or appropriate guideline document.
3.1.3	It is reported that wholesale demand response providers are finding it very difficult to be connected for data communications under current arrangements.	What difficulties are wholesale demand response providers finding to be connected for data communications under current arrangements?	Clarification of where the connection should come from- is it to DNSP, straight to AEMO, to TNSP? Is this dependant on the capacity? If so this delineation between DCPs connecting to AEMO should be defined. Unclear if there are different arrangements for different types of DCPs.
3.1.3	New embedded scheduled and semi-scheduled generators have obligations under the rules and Generator Performance Standards (GPS) to participate in Automatic Generation Control (AGC). However, some stakeholders have indicated that this is not possible through some DNSP SCADA systems.	What difficulties do DNSPs have in communicating AGC control signals?	May be a legacy equipment / system issue.

	DATA PROTOCOLS		
3.1.4	The current standard specifies ICCP IEC60870-6 TASE.2 and its extensions as a secure ICCP protocol. A stakeholder has questioned whether this can actually be considered as a secure protocol	Is the current ICCP Protocol specified in the current Standard still appropriate?	ICCP is for inter-control centre by design. Distributed energy systems need faster communications (DNP3/MODBUS/MMS). This should also be covered in emerging technologies section. The security architecture should be considered as a whole, rather than protocol specific.

3.1.4	The Standard in Section 5.1 should be more specific on protocols used when AEMO WAN is connected to another party's data Communications Facility	What protocols should apply for connections to AEMO WAN?	We are not sure what more could be listed here. It is likely more of a matter of being unclear on how that connection is made and the architecture not being defined fully.

	INTERFACING		
3.1.5	The Standard should provide more clarity on the boundary of both operational and financial responsibility between · Generator and NSP · DNSP and TNSP · AEMO and TNSP	What additional detail is required in the Standard to provide more clarity on boundary of both operational and financial responsibilities?	More clarity of the responsibilities of each party. E.g. one party could be forced by a second party to maintain legacy equipment. This might be a regulation issue rather than in the standard. This section 3.1.5 is most important for Generator / NSP.
3.1.5	The standard should make clear the obligation of parties to work together to resolve any problems to ensure a requirement is met.	Should an obligation for parties to work together be added to the Standard?	There is implicit obligation to meet reliability and availability requirements. However could still be disagreements – need to have a mechanism to resolve. This could be via state based regulator?
3.1.5	The Standard needs to be clear that connections are required to both AEMO control room sites.	Does the Standard need to clarify that connection is required to both AEMO control room sites?	Covered in reliability and availability.

	DATA QUALITY		
3.1.6	The Standard needs a specific requirement that data sent is of good quality. It is possible for a connection to be available and the data to be unusable due to quality.	Should the Standard include a specific requirement that data sent should be of good quality? If so, what would be implications for stakeholders?	
3.1.6	Some remote metering equipment does not provide quality flags.	Should all data be sent with quality flags? If so, what would be implications for stakeholders?	

	DATA ACCURACY		
3.1.7	The Standard does not have an effective requirement to ensure the accuracy of data in particular to ensure that RME remains calibrated. Monitoring and remediation may be problematic (e.g. kv measurements at some stations can vary by over 10kV).	Should the Standard include a more specific requirement regarding data accuracy? If so, what would be implications for stakeholders?	
3.1.7	All semi-scheduled units being clamped in SCADA (at the AEMO end) such that telemetered MW values could not be negative is undesirable, noting that participants are responsible for providing accurate data and separate metering of auxiliary loads.	How material is the issue regarding clamping of values for semi-scheduled units? If the standard were to be changed as suggested, what would be the implications for participants?	

	DATA LATENCY		
3.1.8	The Standard is not clear on requirements for data latency or end-to-end response times. There is current no minimum requirement for data latency.	Should the Standard include a specific requirement regarding data latency? If so, what would be implications for stakeholders?	

3.1.8	Significant timing difference can exist particularly for the RME equipment that uses UTC time and the conversion of this to AEST. There should be greater clarity on the requirements for calibration, testing, validation, and maintenance of the timing stamp quality.	How material is the issue regarding timing differences due to RME? If the standard were to be changed to address this, what would be the implications for participants?	
3.1.8	Monitoring end-to end update times is difficult post commissioning	Should an additional requirement be included in the Standard to allow ongoing monitoring of end-to-end response times? If so, what would be the implications of such a change?	

	CONTROL COMMANDS		
3.1.9	AGC is showing performance issues which suggest that a more responsive control loop is needed. With the current 4 second AGC cycle, updates at a minimum of less than 2 seconds may be required. There have been incidents where AGC used to control a battery is stale (20s old) resulting in unwarranted discharge and charge cycles and at times oscillations. This is mainly because the communications delay is more than 97% of the response delay time.	What would the implications be if the specification of maximum delay for control commands was tightened to 2 seconds? What are the implications if control command delays remain at current levels?	
3.1.9	There should be increased use of dispatch signals via SCADA through the NSP as AEMO's Market Portal may be unreliable and any failure to meet dispatch requirement increases system risk.	Is there a material issue associated with reliability of the connection to AEMO's market portal?	
3.1.9	The specification of maximum delays may not adequately take into account the number of intervening facilities through which the command signal needs to be relayed.	Should the specification of control command delays in the Standard take into account the number of intervening facilities? If so, how should these be accounted for and what would the implications be?	

	SECURITY		
3.1.10	The current standard is not clear on obligations of the parties to the security of the data (physical, personnel and cyber) and of control protocols at the level required for critical infrastructure.	What specific obligations regarding maintenance of security should be included in the Standard, and what would be the implications of this?	The security section needs to be in alignment with AESCSF or reference AESCSF – it could also reference a particular Maturity Level – though there would need to be time allowed for DCPs to get to this level. Also noting that smaller companies may not have the resources to fully comply.
3.1.10	Alignment between this data communications standard and these current and proposed regulations requires consideration.	Does the legislation adequately cover security obligations and requirements or is there a need for more detailed obligations in the Standard?	
3.1.10	The Standard should include an obligation for participants to advise AEMO of any known relevant cyber security issues or when abnormal risks to cyber security arise.	What would be the implications of including a specific obligation to advise on cyber security risks?	Does this exist in regulations? If not, then this should be included in the standard.
3.1.10	There are questions about ownership and control and rights to data, and when. While not specifically related to the Standard, the standard should nonetheless fully support and enable these requirements.	Should the Standard be enhanced to better identify and support the protection of the confidentiality of data? If so what type of enhancement is required?	Specific to generation. There should be clarification of who has the rights to and owns the data.

	RELIABILITY		
3.1.11	There is a need for greater clarity in Section 3.1 of the Standard regarding the specification of reliability requirements. In particular:	What changes would be required to clarify reliability requirements in the Standard?	A guidance document would be good here, how do different DCPs meet the redundancy. Clarify what is required – are multiple RTUs requires at Generator sites and DNSPs- is this covered by this standard?

	• • In table 4 standard term RCE needs to be better defined • • Tables 4 and 5 are not clear. For instance does the 6 hour requirement apply to a single site or all sites? • • Possible inconsistency between table 4 and 5 • • Difficulty in seeing how tables 4 and 5 apply to DNSPs • • Need to better define what is meant by a critical outage in Section 3.1 - i.e. does it refer to total loss of data or simply loss of redundant path?		Agree that the definition of critical outage needs to be defined. Do different data sets require different outage times depending on data criticality? This needs further clarification in the standard.
3.1.11	The Standard should set expectations on the level of monitoring and reporting of reliability required. For instance, this might include a comprehensive heartbeat facility.	Does the Standard need to set enhanced expectations regarding monitoring and reporting of availability and why? What would be reasonable expectations to set? What changes would be required to data communications systems to achieve enhanced monitoring and reporting of availability?	
3.1.11	Frequent and rapid applications of software patches is becoming an increasing requirement for maintaining cyber security. One stakeholder has queried whether new or additional redundancy may be needed at DCFs to allow rapid application of patches without disrupting operations.	Does any lack of redundancy currently restrict the ability of participants to apply software security patches in a timely manner?	This should be implicit from availability and reliability requirements. The redundancy of different types of NSPs needs to be clarified to answer this question. E.g. at multiple comms nodes / firewalls/ rtus required at all sites to allow for software updates.

	MAINTENANCE		
3.1.12	Section 2.2 of the current Standard states that "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". It is not clear whether this requirement applies to small scale changes to correct individual sign conventions or only to a major change following a change in policy.	What change to Section 2.2 of the Standard would be required to clarify the requirement for adequate notice?	

	RESPONSE TO FAILURES		
3.1.13	The Standard has no specific requirements for the times required to return to service following forced outages and in practice failed data can take a long time to rectify. Tables 4 and 5 of the current Standard refer to a reliability requirement rather than a specific response time.	What issues have arisen that would justify including in the Standard a specific requirement regarding response time to forced outages? If so, what would reasonable expectations be?	

	TESTING		
3.1.14	The current testing scope does not include testing of whether the data is correct, but only that data is being communicated. The scope of testing specified under the Standard could also include testing for cyber security; and robust RCE and RME testing, calibration and validation.	What issues have arisen that would justify expanding the scope of testing specified in the Standard? If so, what increases in scope are required? What would be the implications of a change in testing scope?	
3.1.14	The level of testing required for new generators is onerous.	What are examples of testing requirements that are considered too onerous for new generators? Are there opportunities to make these	

		requirements less onerous without materially reducing the effectiveness of the testing programme in demonstrating the necessary capabilities?	
3.1.14	Section 6.4 of the current Standard is not clear on what constitutes an “upgrade”.	What changes to the definition of an “upgrade” is required? What implications would such a change have?	
3.1.14	The requirement under Section 6.4(c) of the current Standard is unclear and that for the sake of efficiency it should encourage the use of standard test procedures.	Should section 6.4(c) of the current Standard be amended to encourage use of standard test procedures?	
3.1.14	Due to the changing nature of the power system the requirements for advice on augmentations under the Standard need to be increased.	What issues have arisen that would justify expanding the scope of augmentations required to be advised under the Standard?	
3.1.14	The Standard needs to require the provision of an appropriate testing environment for data links.	What issues have arisen that would justify the Standard specifying the provision of testing environments for data links? What implications for stakeholders would such a new requirement have?	

	TRANSITIONAL ARRANGEMENTS		
3.1.15	Any increased requirements in the Standard need to be transitioned to accommodate additional funding requirements to meet such increased requirements.	In what circumstances would transitional provisions be justified for increased requirements in the Standard? If justified, what form of provisions would be needed and for how long?	

	EMERGING ISSUES – SCOPE OF STANDARD		
3.2.1	AEMO NEM Control Centres currently use limited real time data from PMUs. In the near future the level of this real time data from PMUs and High-Speed Monitors (HSMs) will greatly increase and requirements for the communication of these data types may need to be included within the Standard.	Does the Standard need to cover to cover PMU and HSM data? If so why and on what basis should the requirements be set (i.e. appropriate standards on which the requirements could be based)?	
3.2.1	Some stakeholders have noted that the Integrating Energy Storage Systems rule change will enable Small Generation Aggregators (SGAs) to provide FCAS and that the Standard may need to accommodate this change	Does the Standard need to cover SGAs? If so why and on what basis should the requirements be set?	
3.2.1	The Scheduled Lite Visibility Model to provide visibility to AEMO of the output in the form of five-minute data may be required by mid-2022 and this may need to be accommodated in the Standard.	Are changes to Standard required now to accommodate the first stage of the Scheduled Lite Project? If so, what changes are required?	
3.2.1	The Scheduled Lite Dispatchability Model is expected in 2024-25 to enable distribution connected aggregated DER to participate in central dispatch.	What future changes to the Standard are likely to be required to accommodate the second stage of the Scheduled Lite Project?	
3.2.1	In the future there may be a requirement for AEMO to also provide real time data to participants.	Is it likely that future changes to the Standard will be required to also cover provision of real time data from AEMO to participants?	
3.2.1	Whilst provision of real time to NSPs from Generators and others is not within the scope of the Standard, it remains part of the overall data communications process in the NEM. For instance even if, say, a generator was to provide real time data directly to AEMO, there	Regardless of provision of data to AEMO, does the Standard need to incorporate or reference requirements for generators and others to provide real time power system data to their NSPs?	

	may still be a requirement for the generator to provide data separately to its NSP.		
3.2.1	Enhancements to the Standard will bring benefits but also may result in increased costs to the industry and ultimately consumers. It is possible that costs may be disproportionate in the case of enhanced requirements for smaller participants, however the necessity for those requirements may increase as the relative numbers of smaller participants increase.	Are there any specific factors AEMO should take into account in assessing the costs and benefits of a proposed enhancement to the requirements of the Standard?	

	EMERGING ISSUES – ARCHITECTUAL REQUIREMENTS		
3.2.2	In the near future, a growing number of embedded battery generation, aggregated DER and VPP connections will need to be accommodated. Some stakeholders believe that this will mean that the current data communications structure will be no longer fit for purpose.	What changes to the current NEM power system data communications structure are likely to be required? Are there different options for such changes?	Not necessarily changes to structure – consider broadening the definition to include where to connect the DER e.g. to DNSP or TNSP or AEMO and at what size. TNSP still require the data from the generators – if a generator connects direct to AEMO, the standard should ensure that data is still delivered to the TNSP.
3.2.3	Under the current architecture as described in Section 3.2.2, the only communication protocol support for connection to AEMO is the ICCP protocol. If a change in the data communications structure is required, then it may be necessary for the Standard to accommodate alternative protocols for connection to AEMO. The ICCP protocol is designed for data communication between control centres and would not be suitable if a generating unit were to communicate directly with AEMO.	If generators and other participants were permitted to communicate directly with AEMO, then what types of data protocols would be preferred? If for cyber security and other reasons, only a single protocol can be accommodated in addition to secure ICCP, what criteria should AEMO use to determine the most suitable protocol?	There are some discussions on the merit / for / against the current DNP3 plaintext protocol and the use of secure DNP3, which provides integrity only and doesn't really provide confidentiality. Also operational impact on the existing EMS systems in supporting secure DNP3 We would be considering the suite of SCADA protocols (Modbus / MMS / DNP3) as it is hard to change to different protocols from what is natively supported by the existing equipment that connecting parties use. Note that a change to protocols may impact existing security solutions e.g. IPS / application scanning.