Energy Security Board

Interoperability Policy for Consultation

Directions Paper

October 2022

Submission from John R. Markwell

email: john@markwell.net

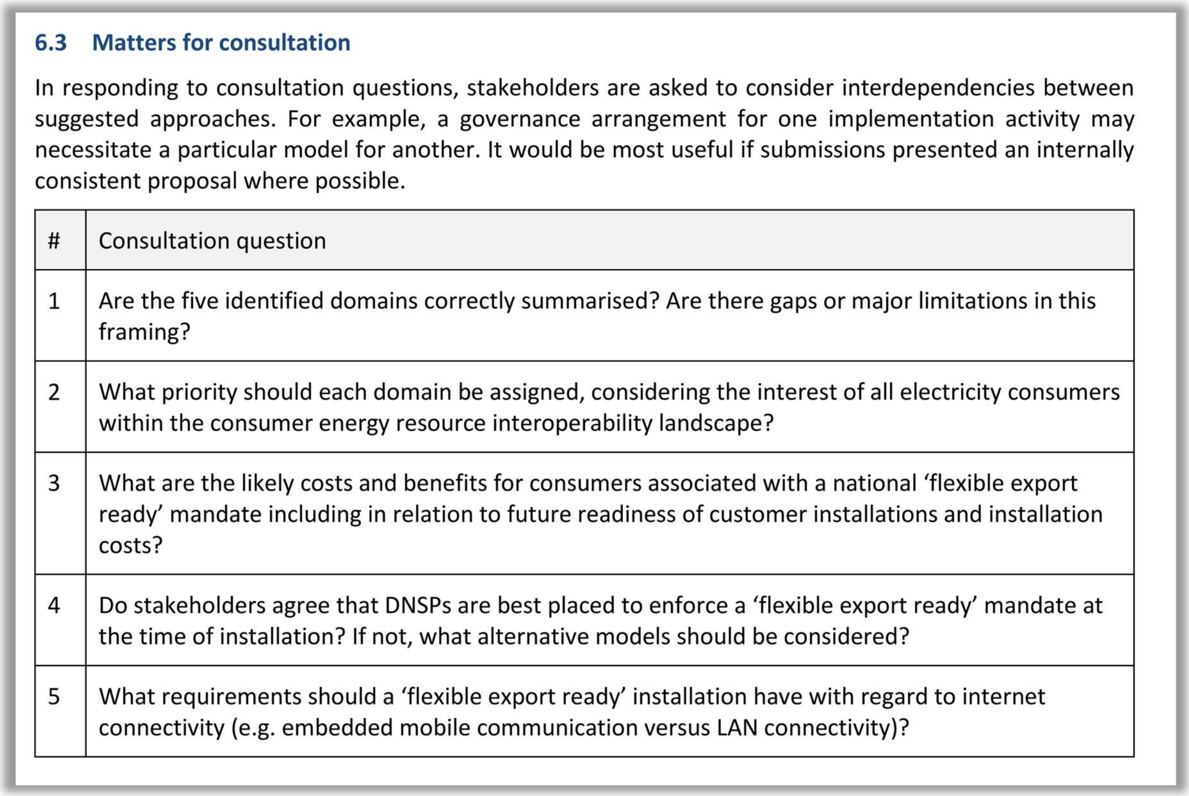
10 November 2022

Objective of my submission.

Attempt to add value to the consultation process by drawing on my experience in robust and trustworthy, mission critical complex systems, spanning the architecture, design, implementation, and operation over decade long periods, of standards compliant networks impacted by evolving technology and by evolving customer behaviour.
Although my experience is not in the energy sector, there are many parallels across all such networks, including legacy systems transitioning requirements, standards adoption, application specific adaptation, and cyber-security essentials.
My experience as an early adopter of domestic PV and EV, and recreational marine balanced system design and implementation, employing PV, wind generator, and tow generator power sources, with comprehensive consumption and battery monitoring, contributes to my end-user customer perspective.

Matters for consultation.

There are many demands, involving inter-related topics across several domains, involved in the consultation questions. In isolation, each question is a difficult one to answer, but with a notional top-down view of the strategic intent and a modern network architecture, suggested answers are much easier to propose.
I will start at the top and then move on to more specific detail.



6.3 Matters for consultation

In responding to consultation questions, stakeholders are asked to consider interdependencies between suggested approaches. For example, a governance arrangement for one implementation activity may necessitate a particular model for another. It would be most useful if submissions presented an internally consistent proposal where possible.

#	Consultation question
1	Are the five identified domains correctly summarised? Are there gaps or major limitations in this framing?
2	What priority should each domain be assigned, considering the interest of all electricity consumers within the consumer energy resource interoperability landscape?
3	What are the likely costs and benefits for consumers associated with a national 'flexible export ready' mandate including in relation to future readiness of customer installations and installation costs?
4	Do stakeholders agree that DNSPs are best placed to enforce a 'flexible export ready' mandate at the time of installation? If not, what alternative models should be considered?
5	What requirements should a 'flexible export ready' installation have with regard to internet connectivity (e.g. embedded mobile communication versus LAN connectivity)?

Regarding governance arrangements and internal consistency.

There appears to be a compelling need to integrate and clarify the strategic elements of this overall exercise in a clear and precise Statement of Strategic Intent (SSI).

DER implementation planning work is, in essence, a Strategic Road Map supporting an implied Strategic Intent.

There are many viewpoints on what may constitute a good Statement of SI.
A good SSI defines a general stretch-goal with timeframes and comprehensive metrics that all stakeholders can readily grasp. Once defined, an SSI continues to serve as a solid point-of-reference for much lower-level decision making.

e.g., Does the outcome flowing from a particular decision:
support the SI? is neutral but necessary? or does it work against the SI?
If it works against the SI, then try something else!

I am certainly in no position to flesh out a detailed SSI for the parties involved, but I can attempt an illustrative template: -

A Statement of Strategic Intent for Australia's Distributed Energy Resources

- By 2030 Australia will have a world class Distributed Energy Resources (DER) network that is striving for carbon neutrality, is effectively and efficiently managed, is cost-effective in its delivery of energy to consumers, is profitable for appropriate generators, and for appropriate value-added service providers, and is a network that leverages natural renewable resources for energy driven prosperity, and international competitive advantage.
- Competitive open market forces, and technological change, will drive innovation within a disciplined managed framework of evolving, nationally adopted, open standards for interoperability of all mission critical components.
- The DER network will be reliable in its delivery of energy, robust in its architecture and detailed design, yet flexible and not rigidly coupled in its evolving application, secure in its overall integrity and ongoing management, and accountable and transparent in its regulatory and operational aspects.
- Control mechanisms to sustain continuous improvements and quality standards, will be adopted and maintained.
- Metrics must be developed for all elements of the Statement of Strategic Intent to place additional measurable outcomes into the Strategic Road Map/Top level DER implementation plan.
  The metrics may be financial, non-financial, or statistically derived, but they must be there to serve as milestones or yardsticks for management review of progress in satisfying the Strategic Intent.

  ___

The objectives and timelines in the DER Implementation Plan are generally well presented in a succinct, comprehensive, and clear manner.

Change management

The hierarchical nature of the grid as it is/was, and the distributed network of the near- and longer-term future is inherently, architecturally, conflicted. The new DER network must successfully envelop the old, and then itself evolve in sometimes unforeseen ways. Backwards and forwards compatibility is a necessary network attribute.
To be successful, the change management process needs to push hard at all levels, from the top down via the Strategic Intent and governance arrangements as existing or evolving; from the middle up and down via power generation and grid service providers including TNSP, DNSP, MASP etc., and via a well co-ordinated and on-going education program delivered to the end-user consumers. Better educated consumers will help facilitate the transformational change, rather than resist it. The recent National Energy Performance Strategy **(NEPS): have your say** looks set to tackle this issue but it also lacks an up-front SSI before diving into the detail. I intend to review the NEPS in detail, in the near term.

The SSI should be understood by this entire set of stakeholders so that change is accretive due to its many components remaining focussed on the intended outcome and timeframe.

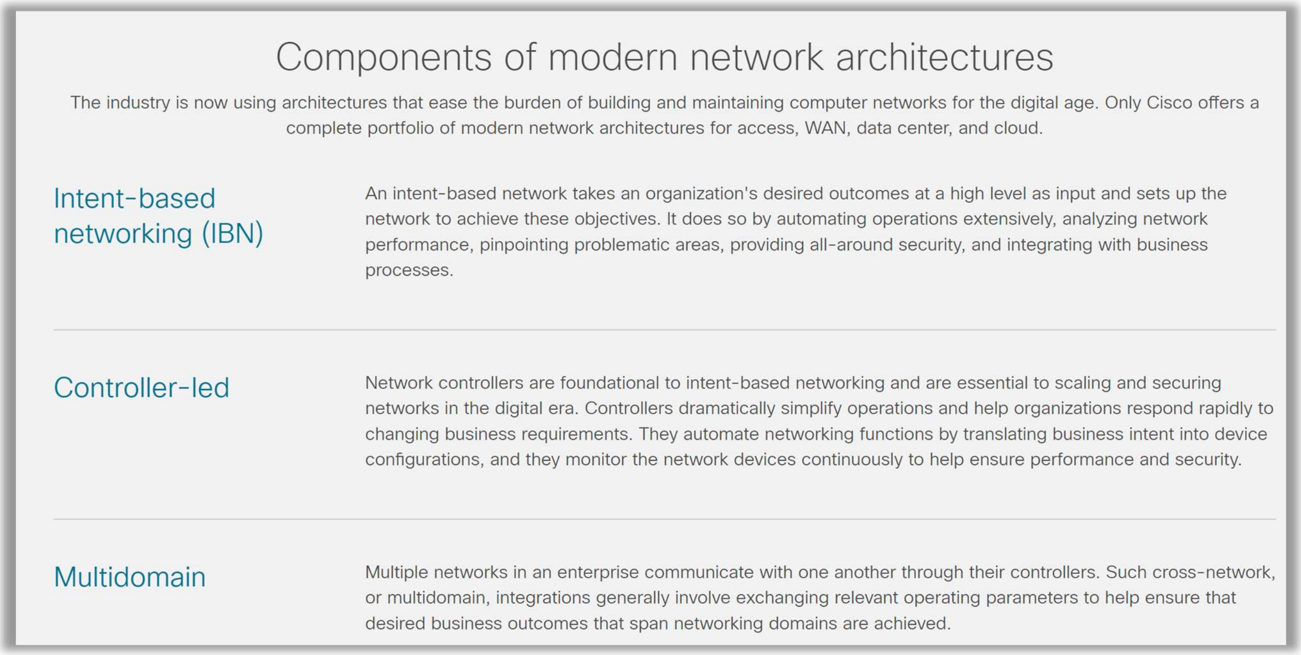
Network Architecture

The CISCO view (below) of the key characteristics supporting a **modern network architecture**, appears eminently sensible to me, especially in the present context.
Despite suggesting this model, I am not proposing any CISCO involvement.
The attributes and reasoning given in the description appear to be a very good fit to my way of thinking about the big-picture framework, within which the answers to the Board's various questions might be found.

1) **Intent based networking** … driven by a good Statement of Strategic **Intent**.

2) **Controller-Led**; feeds directly into any discussion around CSIP, HEMS, IEEE 2030.5, cyber-security, transport layer protocols and such like, and subsequently to where the governance/management responsibilities might be best positioned.

3) **Multidomain**. Exactly what is required.



Components of modern network architectures

The industry is now using architectures that ease the burden of building and maintaining computer networks for the digital age. Only Cisco offers a complete portfolio of modern network architectures for access, WAN, data center, and cloud.

Intent-based networking (IBN)

An intent-based network takes an organization's desired outcomes at a high level as input and sets up the network to achieve these objectives. It does so by automating operations extensively, analyzing network performance, pinpointing problematic areas, providing all-around security, and integrating with business processes.

Controller-led

Network controllers are foundational to intent-based networking and are essential to scaling and securing networks in the digital era. Controllers dramatically simplify operations and help organizations respond rapidly to changing business requirements. They automate networking functions by translating business intent into device configurations, and they monitor the network devices continuously to help ensure performance and security.

Multidomain

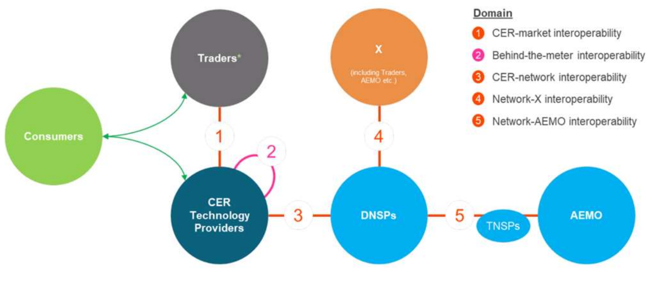
Multiple networks in an enterprise communicate with one another through their controllers. Such cross-network, or multidomain, integrations generally involve exchanging relevant operating parameters to help ensure that desired business outcomes that span networking domains are achieved.

Source: https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-network-architecture.html#~q-a

Consultation Questions

CQ1: Are the five identified domains correctly summarised? Are there gaps or major limitations in this framing?

Figure 5: consumer energy resource interoperability domains (incorporating the dynamic export limits use-case)


Consumers
Traders*
X
(including Traders, AEMO etc.)
CER Technology Providers
DNSPs
TNSPs
AEMO
1
2
3
4
5
Domain
1 CER-market interoperability
2 Behind-the-meter interoperability
3 CER-network interoperability
4 Network-X interoperability
5 Network-AEMO interoperability

Regarding Figure 5; The detailed discussion in the three sections is good;
-CER-market interoperability (1)
-Behind-the-meter (CER-CER) interoperability (2)
-CER-DNSP interoperability (3)

Despite the good discussion detail, I cannot readily grasp the implications of the interoperability pathways, in particular #2, without additional context.

The NEM governance direction for the electricity market appears to be heading towards a more flexible two-sided market with emphasis on services and value streams, rather than the presented domains in Fig. 5.
The big-picture of future **services interoperability** is probably clearer than the future interoperability of organizational domains as there is a lot of transformational change underway.

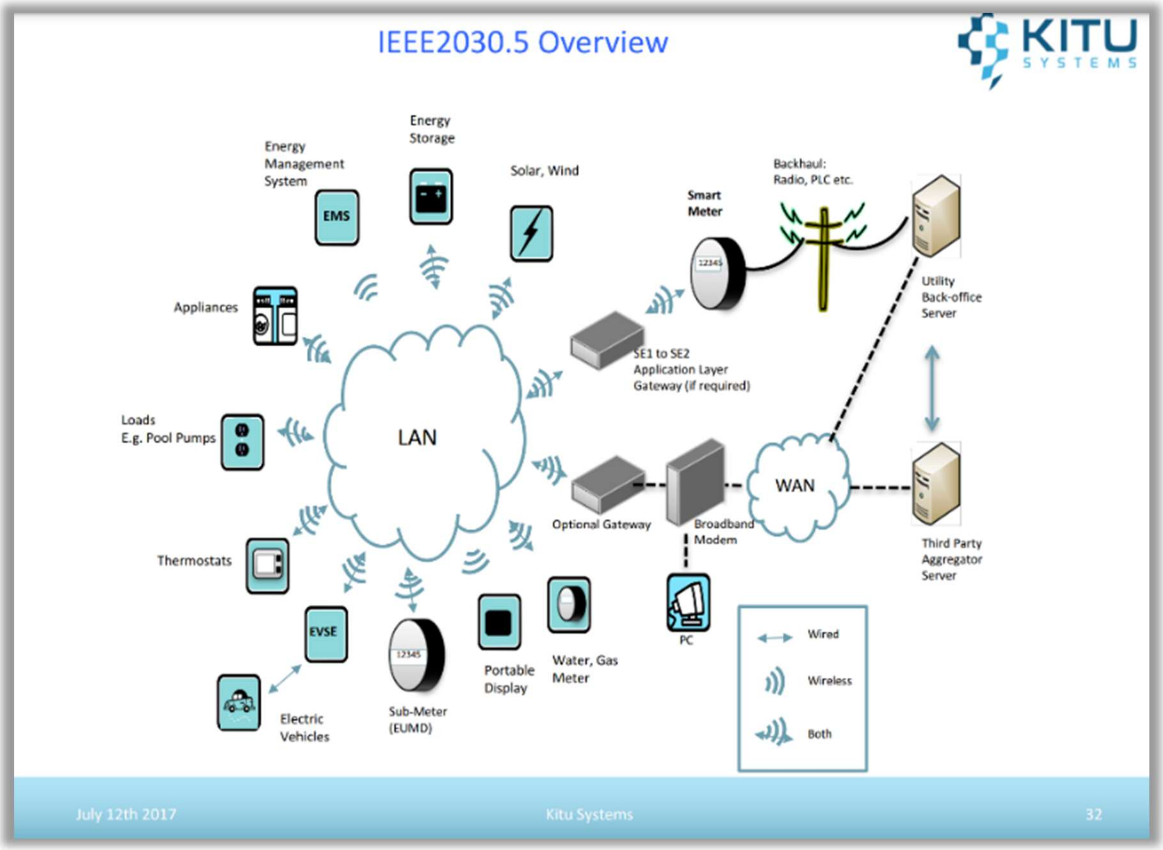
CQ2: What priority should each domain be assigned, considering the interest of all electricity consumers within the consumer energy resource interoperability landscape?

The priority should be to 'intercept' a version of the relevant standards IEEE 2030.5/CSIP and adapt it with the minimum of change to establish CSIP-Aus in a **Controller-Led** implementation.

The minimum of change is necessary as base standards will be updated from time-to-time and CSIP-Aus will need to evolve in a very agile manner. E.g., the upcoming Sunspec Alliance DER Conference in December is focussing on cyber-security and DER asset protection.

One could ask the question; why are we so different that significant standards adaptation is necessary? This leads to other questions such as: How will compliance and certification be managed? Will existing certification and testing organizations be interested in providing such services for CSIP-Aus? Will IEEE 2030.5 or CSIP-CA evolve faster than CSIP-Aus?
Given Australia's rapid uptake of PV and a likely rapid catch-up in electrification of transport, CSIP-Aus may well set the pace.

A Controller-Led (data communications) network architecture could look somewhat like an extended version of the network illustrated below, with the **addition** of a higher-level supervisory layer; i.e. at the level of market operator/regulator(s).
The servers in the illustration are IEEE 2030.5 (substitute with CSIP-Aus) compliant and the Gateway would offer sufficient CSIP-Aus functionality to handle well defined and controlled flexible export requirements along with any other necessary network management and CER management information needs.



IEEE2030.5 Overview

Source: IEEE 2030.5/CA Rule 21 Foundational Workshop June 12, 2017 download from Sunspec Alliance https://sunspec.org/

Despite the CSIP nomenclature, a dedicated CSIP-Aus compliant gateway co-located with, and operating in concert with Smart Metering, may offer a better and more secure, and sustainable, approach to interfacing CER to service providers, than locating such functions in smart inverters.

The Smart Inverter and/or HEMS and other equipment and systems on premises may then implement any necessary client level protocols to communicate with the **'CER Gateway.'** In conjunction with a smartphone/tablet/desktop/laptop app, a CER Gateway would immediately be useful to consumers by providing tariff and consumption analysis, and meter reading.

Supporting the argument for a dedicated CER Gateway are some findings outlined in a Sandia National Labs Report (SAND2019-1490) - Recommendations for Trust and Encryption in DER Interoperability Standards; Page 22, paragraph 4 (my **bold** emphasis):-

“GAP ANALYSIS
*The security features in IEEE 2030.5 are commonly used in computing platforms, however, there are still questions of how well the technologies will scale in highly-distributed, **computationally limited DER environments**.*
In this section, potential security gaps are identified.
These include:
• No Certificate Policy defining security procedures, policies and practices for the ecosystem
• Non-expiring certificates and no certificate revocation methods
• No method to update the cryptographic algorithms for the lifetime of the DER devices
• Possibly weak or poorly implemented TLS interception techniques
• No physical security requirements
• Unclear requirements for aggregator IEEE 2030.5 servers”

Source URL: Recommendations for Trust and Encryption in DER Interoperability Standards (sunspec.org)

https://sunspec.org/wp-content/uploads/2020/01/Recommendations-for-Trust-and-

In my experience, any secure system implemented today uses today’s hardware. However; it must cope with potential criminal activity for the lifetime of the weakest network components, and those attacking the network will always have the latest hardware and tools available to do so.

A dedicated CER Gateway can resolve: -

- Physical security requirements
- Computational limitations of, Smart Inverters, HEMS etc. that are designed for other tasks. (When quantum computing arrives, the cryptographic security scene will most certainly be impacted.)
- Can be software upgraded (patched) under central control to move forward as network standards evolve and this, in time, will also improve certificate handling and TLS issues etc.
- Could provide for significant hardware augmentation in future if such expansion interfaces are built-in to the basic unit.
- Could provide a level of internal redundancy, fallback and recovery.
- Could implement default templates (of rules) for local control of flexible export in the event of temporary network outages
- Could handle local system diagnostics and power supply event journals of interest.
- Could help simplify AS 4777.2 implementation going forward by uncoupling the physical electrical network safety and other functionality from the increasingly more complex data communications requirements.

The above also partially answers CQ5, with further discussion below. (CQ3, CQ4 are covered later)

CQ5: What requirements should a 'flexible export ready' installation have with regard to internet connectivity (e.g., embedded mobile communication versus LAN connectivity).

> *"The application layer with TCP/IP providing functions in the transport and Internet layers to enable utility management of the end user energy environment, including demand response, load control, time of day pricing, management of distributed generation, electric vehicles, etc. is defined in this standard.*
>
> *Depending on the physical layer in use (e.g., IEEE 802.15.4™, IEEE 802.11™, IEEE 1901™, IEEE 1901.2™), a variety of lower layer protocols may be involved in providing a complete solution. Generally, lower layer protocols are not discussed in this standard except where there is direct interaction with the application protocol."*
> Source: https://standards.ieee.org/ieee/2030.5/5897/

The IEEE 2030.5 standard is transport layer agnostic so the simple answer is that the CER Gateway should offer a range of commonly used connectivity methods such as Ethernet, RS 422 (a pathway to Modbus), WiFi, Bluetooth, 5G Mobile communication (via expansion module), ZigBee, and for Smart Meter connection, an optical (or wired) port supporting ANSI C12.18, C12.19 for table driven, user specific, function extension.

Unfortunately, this is not quite the end of the inter-operability road as CER devices are usually IoT devices, and cyber-security issues extend right down to the end points.

A robust modern network architecture must encompass end-to-end cyber-security.

While the uppermost sections can rely on IEEE 2030.5 as a basis, secure interoperability standards for the IoT area have only recently emerged.

For example: -

> *"The first **Matter** specification is set for publication by the second half of 2022, but already at CES 2022 there were key Matter product announcements from Amazon, Apple, Google, Samsung, as well as key component and service providers ranging from NXP to Tuya.*
>
> *Even so, the specification sets a host of new demands across connectivity, interoperability, security, and marketing. Some aspects are already detailed while others remain in development. Smart home hardware vendors must assess the value and investment that Matter compliance requires, as well as the strategic impact on their roadmaps and their place in the market."*
>
> Source: https://www.abiresearch.com/press/more-than-55-billion-smart-home-matter-compliant-devices-will-ship-between-2022-and-2030/

It is suggested that the emerging Matter standard from The Connectivity Standards Alliance (previously ZigBee) be monitored for a potential intercept. If and when this standard is widely adopted and sufficiently matured, it could be mandated for CERs interfacing to a CER Gateway.
Once again, computational resources will be required and some CER devices, including inverters, may have severe limitations in responding to evolving connectivity standards. Such limitations threaten to derail the **intent** to implement a secure and **robust and responsive** network of interoperable components, over the longer term.
A suggested metric for service-to-service response time is; 1 second (best case); 2.5 seconds (on average); 5 seconds (worst case)

CQ3: What are the likely costs and benefits for consumers associated with a national 'flexible export ready' mandate including in relation to future readiness of customer installations and installation costs?

Costs

In this CER Gateway led model, the Gateway equipment could be cost effectively bulk purchased with cost recovery from customers through additional, incremental charges in electricity billing, in much the same way as meter and controller costs are recovered over time.

Benefits

A CER Gateway (Controller) provides: -

- A standardized, secure, Smart Meter communications channel with network simplification benefits. The information flow to consumers assists them in optimizing their consumption and export behaviour.
- A one energy resource at-a-time connectivity into the flexible export ready environment is possible.
  For example; with the extreme multi-vendor, multi-model diversification within their CER, customers may choose to go V2G/V2X independently of their inverter/battery arrangements. Flexibility and options benefit consumers.
- Import/export consumption reporting for customers, timely load and tariff analysis, for optimal cost and consumption pattern tuning.
- A billing credit for internet services used by the Gateway. This provides consumer incentive to connect a Gateway and support its internet connectivity. Payment could be a fixed daily amount determined as a percentage of an average basic NBN fee.
- Transmission network services use postage stamp costing models; customers could receive a location/region-based credit determined from transmission services peak capacity savings due to local consumption of their exports. Such a payment could be based on a percentage from the postage stamp determination modelling.
- Customers could receive a billing credit for the capital outlay associated with their network connected and controlled battery costs, be it stationery or mobile.
  Firming power must come from somewhere and dedicated battery storage facilities are capital intensive. If customers participate in providing 'equivalent' services they should be rewarded accordingly.
- On the flip-side of 'flexible export ready', demand response 'flexible import ready', customers should be compensated for their bi-directional networking and demand/price curve flattening contribution. Within a decade, it is quite possible that Australia's EV battery capacity and combined V2G power will rival that of Snowy 2.0.

"Explanation of demand response effects on a quantity (Q) - price (P) graph. Under inelastic demand (D1) extremely high price (P1) may result on a strained electricity market. If demand response measures are employed the demand becomes more elastic (D2). A much lower price will result in the market (P2). It is estimated[13] that a ***5% lowering of demand would result in a 50% price reduction during the peak hours*** *of the California electricity crisis in 2000/2001. The market also becomes more* ***resilient*** *to intentional withdrawal of offers from the supply side."*
Source: Demand response - Demand response - Wikipedia
https://en.wikipedia.org/wiki/Demand_response#/media/File:Demand_response.png

QC4: Do stakeholders agree that DNSPs are best placed to enforce a 'flexible export ready' mandate at the time of installation? If not, what alternative models should be considered?

In this Controller-led CER Gateway model proposal, the DNSPs are best placed to install such a standardized gateway, and establish its security credentials.
Once installed, the Gateway may be remotely managed by authorized service providers to provide flexible export, and for that matter, flexible import controls for controlled load devices/circuits. (An eventual retirement path for ripple controls would become available.)

The DNSPs are **not** the appropriate entities to intercept, adapt, mandate, certify, maintain, and evolve, the associated suite of implementation standards within an overall Intent-based, Multidomain, Controller-led data communications network architecture.

This role must be handled at the highest practical level within the regulation and governance structure.
In my experience, the long-term scope of standards management resources needs independence from day-to-day operational matters until an intercept of a standard is decided. Adaptation and implementation of a standard certainly needs full stakeholder collaboration.

Cyber-security operations are by necessity, day-to-day, and best situated at a high level, but these resources need to be alongside, and not within, normal operations resources, because internal operational security weaknesses must be a part of the cyber-security remit.

Conclusion

The interoperability big picture is much simpler and easier to manage when a good statement of Strategic Intent is in place, with a modern secure network architecture to support it.

Management of the required standards and cyber-security elements should be within the upper levels of governance structure. Proprietary implementations must be avoided as they likely represent a conflict of intent, unless they offer a path to an open standard.

The required feature sets (**functions**) will be identified and added into standards.
For example; as part of the adoption process in defining SCIP-Aus.

The **purpose** of communications exchanges is to satisfy the strategic intent of the entire interoperability exercise through identified service provider use-cases.

The **implementation priorities** of use-cases within the presently identified domains should be determined by following a path that has a very high probability of success. The likelihood of failure in such a complex environment is high, unless the problem is properly risk-managed and implemented in stages.

It is anticipated that there will be significant implementation timing differences between domains and that **simulators and emulators will be required** in order to build-out the complete network architecture from end-to-end, with otherwise missing or delayed interoperability dependencies.

Implementation of control stages might follow something along the lines listed below.
At each stage, the network management information flow between and across domains will develop and mature: -

- Monitoring and limited network management information flow around the network would appear to be a good initial starting-point.
- Individual or grouped appliance demand-response control, including domestic EV charging. This offers constrained consumer impact, with flexible adoption and roll-out.
- CER stationary battery flexible export control, as the impact is much more limited than that of PV or EV battery control. This stage would provide considerable organizational learning and network consolidation. There has already been a fair amount of inverter to battery interoperability work performed in the marketplace, but it is mostly proprietary in nature and in intent. Interoperability standards and a CER Gateway would build upon and extend such functionality, as the multi-vendor interface basics are there already.
- PV flexible export control; an important intent, once network structures and cyber-security are in-place and tested.
- EV battery flexible export control, would come later as this function is presently immature and needs time to evolve. The ISO 15118 series of standards promises a framework for managing both the charging and export aspects of EVs.
- The collective potential of EV batteries for peak demand power dispatch is quite huge and will be a major consideration in the future DER network.