Battery Storage and Grid Integration Program

An initiative of The Australian National University

Evolve Project

Knowledge Sharing Report

Milestone 5

DER Impacts on Operational Technology

Mar 2021

Document Control

Change History

Version No.	Issue Date	Authors	Description
1.0	10-Mar-2020	WRT, LB, KG, AF	Initial Version

References

This document is to be read in conjunction with and may directly reference the following documents.

Ref	Document	Version	Date	Author
[1]	Advancing Renewables Program Funding Agreement 2018/ARP154	2.0	April 2019	ARENA/Zepben
[2]	Evolve consortium agreement	1.0	Feb 2019	Zepben
[3]	Evolve Design Blueprint	1.0	August 2019	Zepben/ANU
[4]	Evolve knowledge report #1 - Using the IEC Common Information Model (CIM) for Electrical Network Model Exchange	1.1	Feb 2020	Zepben

Contents

Glossary of terms

Term	Definition
AEMO	Australian Energy Market Operator
ADMS	A term that has arisen recently and used in the industry to describe an Advanced DMS. The ADMS is the most significant operational technology used by DNSPs
Aggregator	An Aggregator is an organisation that provides an integration point and control mechanisms for a large number of DER assets
ANU	The Australian National University
BAU	Business as Usual.
CIM	Common Information Model, a standard for data exchange for network models, based on the IEC 61970, 61968 and 62325 family of standards.
DER	Distributed Energy Resource. Disruptive technologies being connected to distribution networks, including PV, EV, demand response solutions, storage and wind farms.
Distribution Substation	A location where one or more transformers are located. The transformer(s) change the voltage level from HV to LV. The distribution transformers are typically rated from 10kVA to 1500kVA
DMS	Distribution Management System. A computer system which is used to control an electrical distribution network. See also ADMS.
DNSP	Distribution Network Service Provider. These are the organisations that own and operate electricity distribution network infrastructure.
DSO	Distribution System Operator; this term refers to the functions of Distribution Level coordination and optimisation of multiple DER aggregators in multiple markets, and connecting at the distribution network level.
EHV	Extra High Voltage – higher than 66kv. Sometimes also referred to as transmission. These are typical voltages used by transmission networks. This network forms part of the TNSP asset base.
EMS	Energy Management System. A computer system which is used to control an electrical transmission network.
EPRI	Electric Power Research Institute. https://www.epri.com/#/about/epri?lang=en-US
EV	Electric Vehicle.
GIS	Geographic Information System. A computer system that incorporates geographical features with tabular data in order to help manage the assets in an electrical network.
HV	High Voltage – 6.6kV to 66kv. Sometimes also referred to as MV. These are typical voltages used by distribution network to transport. This network forms part of the DNSP asset base.

IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers. https://www.ieee.org/about/index.html
LV	Low Voltage – 400 V phase to phase. This is used for the last km of electricity reticulation in Australia. This network forms part of the DNSP asset base.
MV	Medium Voltage - 6.6kV to 66kv. Sometimes also referred to as HV. This network forms part of the DNSP asset base.
PKI	Public Key Infrastructure; a set of roles, policies and procedures to manage digital certificates and public key encryption.
Prosumer	A prosumer is an electricity using individual who both consumes and produces energy. The term is a portmanteau of the words producer and consumer.
PV	Photovoltaic – refers to solar generation.
SCADA System	Supervisory Control and Data Acquisition System – a sub-system of the ADMS that is used for monitoring and controlling plant and equipment from a central location.
SDLC	Software Development Life Cycle
TNSP	Transmission Network Service Provider. These are the organisations that own and operate electricity transmission network infrastructure.

Acknowledgement and Disclaimer

This Project received funding from ARENA as part of ARENA's Advancing Renewables Program and from the NSW Government. The views expressed herein are not necessarily the views of the Australian or NSW Governments, and the Australian or NSW Governments do not accept responsibility for any information or advice contained herein.

EXECUTIVE SUMMARY

The proliferation of Distributed Energy Resources (DERs) and the ongoing displacement of fossil fuel generation with renewables is a transformative change currently being experienced by the electricity system.

The software systems used to operate electricity distribution networks form part of a collection of systems known as operational technologies, which will become a key enabler of the transformation. This report shares insights, gathered through the implementation of the Evolve project across four Australian distribution network service providers (DNSPs), into the challenges and opportunities for DNSP operational technologies over the coming years.

DNSPs have historically designed and operated their networks assuming certain, non-controllable patterns of customer load and a one-way flow of power from the network to the consumer. With limited ability to actively change customer behaviour, the low voltage networks, which are the final leg in the distribution network's "supply chain", have been designed for set-and-forget operation.

Existing control room operational technologies have been developed to suit this set-and-forget paradigm – they support the work involved in restoring the local electricity supply when assets fail or are damaged and in providing access to the network for planned work, including automation of some of these processes. They allow requests from the transmission network service provider (TNSP) to shed or restore blocks of load during system level events to be rapidly actioned, and allow rapid removal of power from electrical assets via remote control when needed for safety reasons.

These existing operational technology solutions are well secured and relatively mature.

DER creates challenges for the DNSPs as it changes the basic assumptions about customer load patterns and the one-way flow of power that historically underpinned the electrical network and operational technology design. In the short to medium term, new operational technologies can be developed that help the existing network infrastructure host increasing amounts of DER, through techniques such as publishing operating envelopes to individual DER assets to avoid the local electrical network operating outside its design parameters.

In the longer term, the design of the network infrastructure itself will change because of changing customer behaviour enabled through DER. The new operational technologies will need to be further developed and integrated with existing systems in tandem with these changes to the network infrastructure to suit active management of the DER at the edge of the grid, rather than set-and-forget operation.

It has become apparent through the Evolve project that transitioning to these new ways of operating will be challenging. The transition must be achieved while maintaining the current high levels of reliability in the networks and the overall electricity system, and ensuring the operational technologies remain secured from cyber-attack.

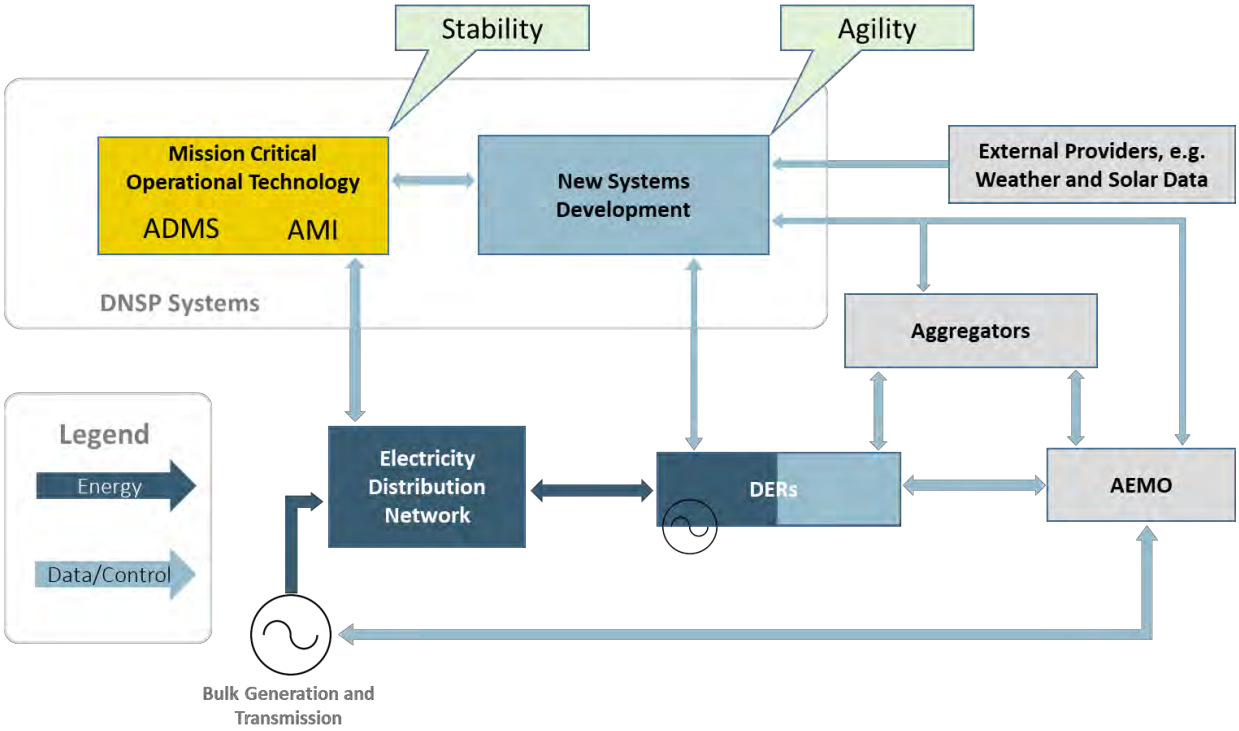
All DNSPs working on the Evolve project have identified a need for these new operational capabilities that must be developed alongside existing systems as they move away from set-and-forget operation to active management of DER.

The requirement for ongoing stable operations of the ADMS was reported in the DNSP responses to a questionnaire issued to support the compilation of this report, where all DNSPs envisaged an "integrated grid management system", but were unwilling to

destabilise their current operational technology platforms by "experimenting" with operational instances of the system.

From this we can conclude that the new systems development must be effectively partitioned from the current mission critical operational technology during a transitional period, but ultimately it must be integrated or become part of that operational technology.

This is illustrated in the following diagram, in which the mission critical operational technology continues to be managed for stability, and the more speculative systems development needed due to the disruptive changes caused by DER is partitioned to allow an evolutionary development approach.



These new operational technologies will need to work with at least an order of magnitude more sensor devices and network asset data than current systems.

Novel computational techniques to continuously optimise the use of network and DER assets will also be required, as will more complex integrations with external parties, with potentially significant utilisation of the public internet for communications with end devices.

This will require strengthening of cyber-security assurance across multiple actors that collectively will be implementing a distributed "system of systems" in an operational technology context. This will need new levels of co-operation and transparency between these actors. It is not clear what body will oversee these cyber-security assurance mechanisms. There is an opportunity here for policy makers to provide clarity in this space.

Beyond the challenges of developing, transitioning and securing the operational technology, we have observed that the data needed to support the required computations for operating envelopes and other higher order optimisation outcomes is often missing or inaccurate in DNSP source systems. We have concluded this is largely a result of the

historical set-and-forget design approach, where detailed information about assets in the last leg of the electricity network was not needed for operational purposes.

All DNSP partners on the project are implementing programs to improve visibility of both static asset data, as well as dynamic sensor data, to provide insights into the behaviour of the network assets at the edge of the grid.

These programs will improve the data in DNSP systems needed to support both the real time management of the networks, as well as longer term planning horizons under new DER-driven design and operating paradigms.

We have observed significant demand from research institutions, government departments, energy consultants and technology development houses for electrical network asset and measurement data to support the development of policy and to enable better energy forecasting, streamline network connection requests and develop new information technologies, including operational technologies.

Lack of broad level access to this data is an inhibitor of innovation in the sector – lack of clarity in the various legislation and rules the DNSPs must adhere to about what data can and should be shared is creating impediments to the sharing of this data by DNSPs, and there are opportunities for policy makers to address this issue.

1 INTRODUCTION AND OVERVIEW

This report has been prepared as part of the knowledge sharing requirements of the Evolve project, under the ARENA agreement "2018/ARP154, Zeppelin Bend Evolve DER Project".

The primary objective of the Evolve project is to develop and demonstrate a system for coordinating distributed energy resources (DERs) that will ensure the technical limits of the electricity distribution network are not breached.

In meeting its primary objective, the Evolve project is also seeking to progress outcomes in the following three key areas:

1. Research into methods of calculating operating envelopes for DER assets. An operating envelope is a range of real and reactive power that controllable DER assets must remain within to avoid creating voltage or thermal overload issues in the electricity network. The underlying algorithms used for calculating operating envelopes will also support hosting capacity calculations, and important outcome for longer range forecasting and asset investment decisions;

2. The development and promotion of standards in relation to the modelling of electricity network asset and measurement data, the exchange of these data models, and communications between DER assets and DNSPs; and

3. The development of software systems that can be used to progress the development of new decision support and operational technologies for the management of DER assets.

This report relates to the 3rd area in the above list.

It describes challenges and solutions involved in the practical incorporation of new software systems and operational paradigms within the existing operational technology and information decision support landscape of DNSPs.

Currently, DNSPs manage the operation of their plant and equipment entirely within their own operational technology domains. External entities are not allowed to control assets owned and operated by the networks. Moreover, DNSPs are allowed to disconnect both energy consumers and generators from their networks when needed to protect network assets or for safety reasons, or in response to a request from the market operator when needed to address shortfalls in aggregate generation.

This has allowed DNSPs to design and operate their networks to meet their license and regulatory requirements, and to effectively ring fence and manage the security of their operational technology by creating strongly defended IP network domains that are not exposed to the public internet or the internal IP networks of DNSP corporate systems.

Disruptive impacts of DER

Over the past decade, the emergence of DERs and an increasing amount of non-dispatchable generation is creating challenges to current near-term operational practices for both DNSPs and the overall electricity system, as well as changing some of the fundamental assumptions used for longer planning horizons for network construction, augmentation and maintenance in the distribution networks.

The emergence of DER has happened alongside increasing availability of low-cost ubiquitous data communications, which is making it possible for machines to

communicate with each other and other information systems via the internet – the so called "Internet of Things" (IoT).

DER assets, which include traditional energy consuming devices like air conditioners, water heaters, pool pumps and so on, are increasingly communicating with their maker's information technology "cloud", or to an Aggregator's cloud. This allows the device to send information about how much power it is importing or exporting and the local voltage, as well as accept controls to modify its behaviour – i.e., how much power it is importing or exporting to the network.

However, DERs are not owned or operated by the DNSPs, and the changing consumer behaviour they enable is creating electrical issues for the networks – both voltage and overload – as they are operating in ways the networks were not designed to handle.

The DNSPs would like to be able to control, or at least influence, the behaviour of these DER assets. However, there is nothing in current connection standards and electricity rules that allow this to occur. Moreover, the actual control of these assets in the future may sit outside the tightly controlled operational technology space managed by the DNSPs – DERs may be under the control of ***someone else's*** operational technology.

As well as this, the number of DER assets that will need to be monitored and controlled and the amount of data they will create is several orders of magnitude larger than current DNSP operational technologies deal with, and the nature of communications between DER assets and centralised operational technologies has fundamental differences to traditional remote monitoring and control currently performed by DNSPs for their plant and equipment.

Further, the way in which the networks are operated will need to transition away from passive management under normal operating conditions, to active management of large numbers of DER devices. This will require the development of new computational techniques that continuously calculate optimum operating conditions for the local networks, which will be translated into operating envelopes and communicated to the DER assets, or the operators of the DER assets, in order to co-ordinate their behaviour as part of this optimisation process.

Finally, to make matters more difficult, data about electrical network assets to support the algorithms needed for orchestration of the DER assets, and for longer term decision support, is often incomplete or missing from the DNSP information systems.

We can conclude from this that there are issues of data, scale, cyber security and lines of demarcation in the operational technology space that must be worked through in order for the operational technologies used by DNSPs to adapt to the challenges and opportunities created by the proliferation of DER.

We can also suppose that many of the decision support tools and analytics used to inform asset investment decisions and regulatory submissions will need to be overhauled due to the significant changes occurring in energy consumption and generation patterns.

This report describes current and potential future operational technology landscapes, how they can be secured from a cyber security perspective, and the challenges of transitioning to an electricity system with high penetration DER from an operational technology perspective.

It also makes observations about the need for planning and analytics tools to provide decision support for longer term planning horizons that will align with the future behaviours of operational technologies.

It was compiled with information and learnings gathered through the execution of the Evolve project, through a questionnaire answered by the DNSP project partners and through the experience of the authors gathered while working within the operational technology domain of DNSPs over many years.

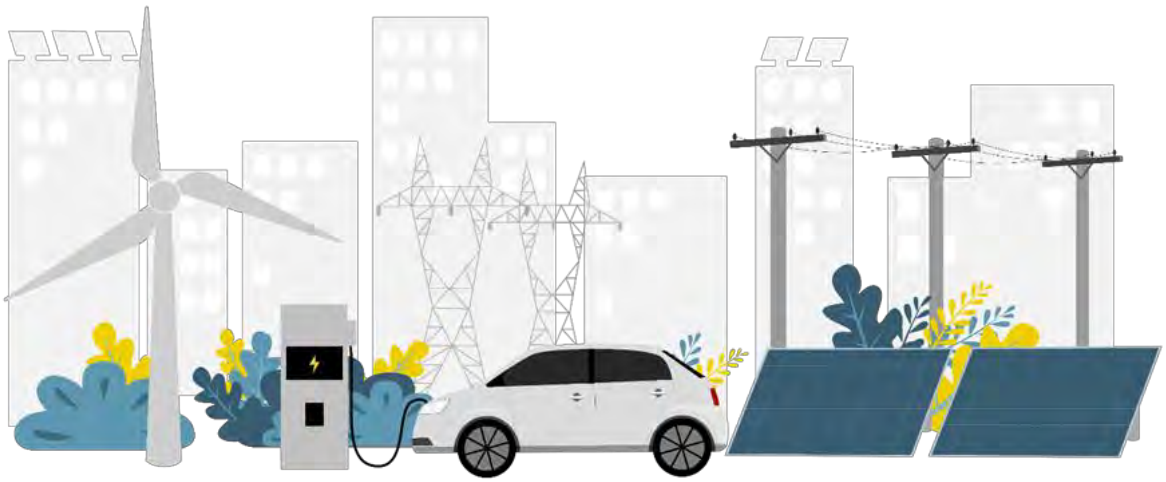
The report is organised into chapters, as described below.

Chapter 1 Introduction and Overview

Chapter 2 The Impact of DER and renewables on operational technologies is discussed, along with commentary about development pathways for operational technology and operating paradigms.

Chapter 3 The mechanisms to secure operational technology are discussed, using the Evolve platform as an example, along with security frameworks and standards relating to the implementation of these frameworks.

Chapter 4 Conclusion.



2 DER IMPACTS ON OPERATIONAL TECHNOLOGY (OT)

2.1 DNSP OT DESCRIBED

In order to describe the impact of DER on Operational Technologies, it's helpful to provide an overview of the operational technology landscape for DNSP's.

To begin with, **Figure 1** below illustrates where DNSP Information Technology, including Operational Technology, has historically being situated within the broader industry information technology landscape. This is a mature operating model with well-defined actors and secure B2B communications between them.

All IP communications related to operational technology occur over secured third party B2B communications channels, or via communications infrastructure owned and operated by the DNSP, TNSP or AEMO. The three tiers of the overall electricity system that own and operate assets have exclusive control over their own assets. Energy flows one way from bulk generation to end consumer.

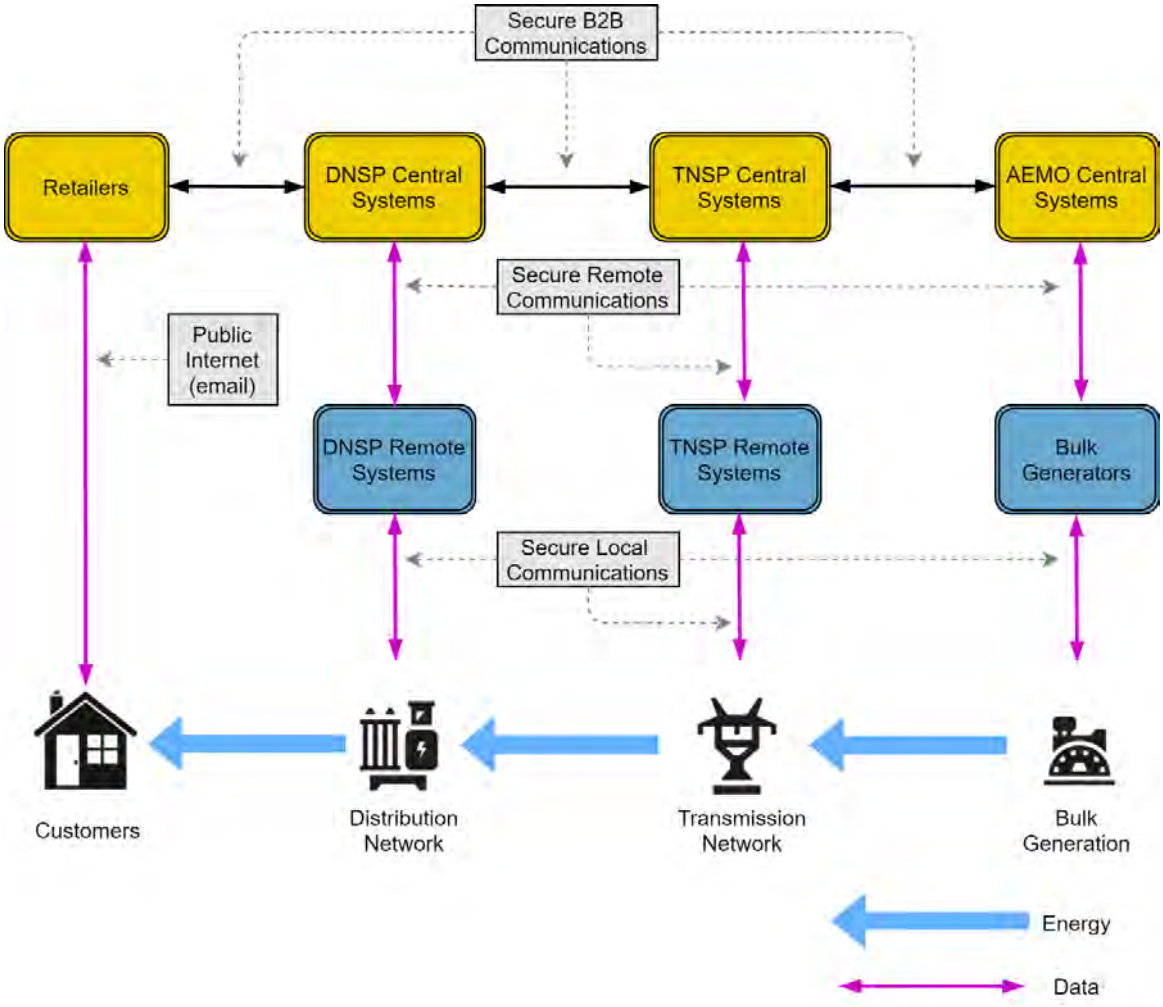


Figure 1: Current State Context for DNSP Information Technology Systems

Within the DNSPs, a range of information technology is used to support business activity, and key operational technology is used to support the operation of the network assets.

Advanced Distribution Management System (ADMS)

The **ADMS** is the major centralised operational technology used by DNSPs to operate the network. The other significant operational technology is comprised of devices installed at major sites that provide remote control and monitoring capability, as well as local control of plant and equipment.

The ADMS supports short term planning horizons for the operation of the network, from real time to several weeks in advance.

ADMS functions include:

1. Real time remote monitoring and control functions via the SCADA sub-system,

2. Outage management functions to support activities associated with restoration of supply following asset failure, including the co-ordination of field crews and the prediction of fault locations,

3. Automatic restoration of supply at the HV level where remote control equipment is available and there are viable ways of routing around the fault,

4. Analysis functions to allow network operators to make predictions about operating parameters in the HV network for current fault conditions, or future planned work, and

5. Situational awareness to provide operators with the tools needed to anticipate and avoid emerging issues in the network such as overloads or voltage violations in the HV network.

To understand the impact of DER on ADMSs, it's important to understand that the ADMS has very little visibility or control of assets in the LV network and that the ADMS does not currently ***actively*** manage or control assets anywhere in the distribution network.

Active management of the ***electricity system*** is currently performed by the market operator (AEMO), which constantly sets the amount of power being exported from dispatchable bulk generators in response to changing demand to balance the production and consumption of power.

The distribution networks are passive actors in this function, they transport the energy but do not influence its production or consumption. Consequently, ADMSs are, currently, not control systems in the sense that they continuously monitor and adjust the inputs and outputs to the system.

The Geographic Information System (GIS)

Geographic Information Systems (GISs) are used by DNSPs for asset management outcomes. The GIS provides the most complete picture of electricity network assets in the DNSP, but is not an operational system updated in real time. It contains the "as-built" model, while the ADMS contains the "as-operated" model.

The representation of the network data model in the ADMS is generally more abstracted with less detail than in the GIS.

Historically, the focus of the GIS has been on the physical location of the assets. In many cases the topology or connectivity of the network assets was not modelled explicitly in the GIS or was not modelled well – particularly in the LV network where the capture of this information for operational needs was not important due to the set-and-forget operating paradigm historically used for network design and operation in the LV network.

Historians

These systems are data stores for time series data obtained from the SCADA sub-system of the ADMS, metering systems and other forms of telemetry. They generally provide functions that can display and perform analytics on time series data. This data is important, as it provides long term views of historical power and voltage measurements that are key inputs into forecasting outcomes for multiple planning horizons.

These systems, provided by vendors such as OSI PI, have been successful over traditional relational database technologies, that have short-comings when dealing with time series data. Systems such as OSI PI have built complete eco-systems for the development of operational technology front ends, and the time series datastore in this type of product is now only a part of the overall product.

More recently, a number of open-source time series databases have appeared[1] that are starting to challenge the traditional providers of historians to DNSPs.

Historians are typically used in both the OT and corporate domains, and are often part of data exchange mechanisms for OT and corporate IT systems.

Customer Information Systems (CIS)

Customer Information Systems are primarily used by DNSPs for billing functions, including integrations with AEMO systems. They also provide data to customer facing systems that provide advice to electricity consumers about connecting DER to the networks, and to customers that want to connect new load to the networks.

The customer connections process and the business of operating the networks have historically been distinct processes with different teams and little integration between the CIS and ADMS. With customers adopting DER, which in turn has impacts on the operation of the network, it is probable that there will be more interaction between the CIS and the ADMS in the future.

Advanced Metering Infrastructure (AMI)

Advanced Metering Infrastructure (AMI) refers to systems that measure, collect, and analyse energy usage, and communicate with metering devices such as electricity meters, gas meters and water meters, either on request or on a schedule – so called "smart meters".

While the original AMI specification for the smart meters rolled out in Victoria required the devices to implement some control mechanisms that would allow DNSPs to curtail load, the specifications for these outcomes have not allowed practical use of AMI for load shaping.

Works and Asset Management Systems (WMS)

These systems are used to schedule, plan and cost work and record information about assets for financial reporting and maintenance. They are sometimes part of the Enterprise Resource Planning (ERP) system.

ERP Systems

[1] https://en.wikipedia.org/wiki/Time_series_database

These include modules to manage finance, reporting and forecasting, procurement, supplier management, human resources and property management.

Planning and engineering applications

DNSPs need to do load flow and fault level studies on their networks in order to understand where the assets are overloaded or voltage issues are present, or where there are protection setting issues. These applications require models of both customer load and generation, and the electrical network.

2.2 THE OT LANDSCAPE WITH DER

The technology landscape with DER is more complicated, as illustrated below.

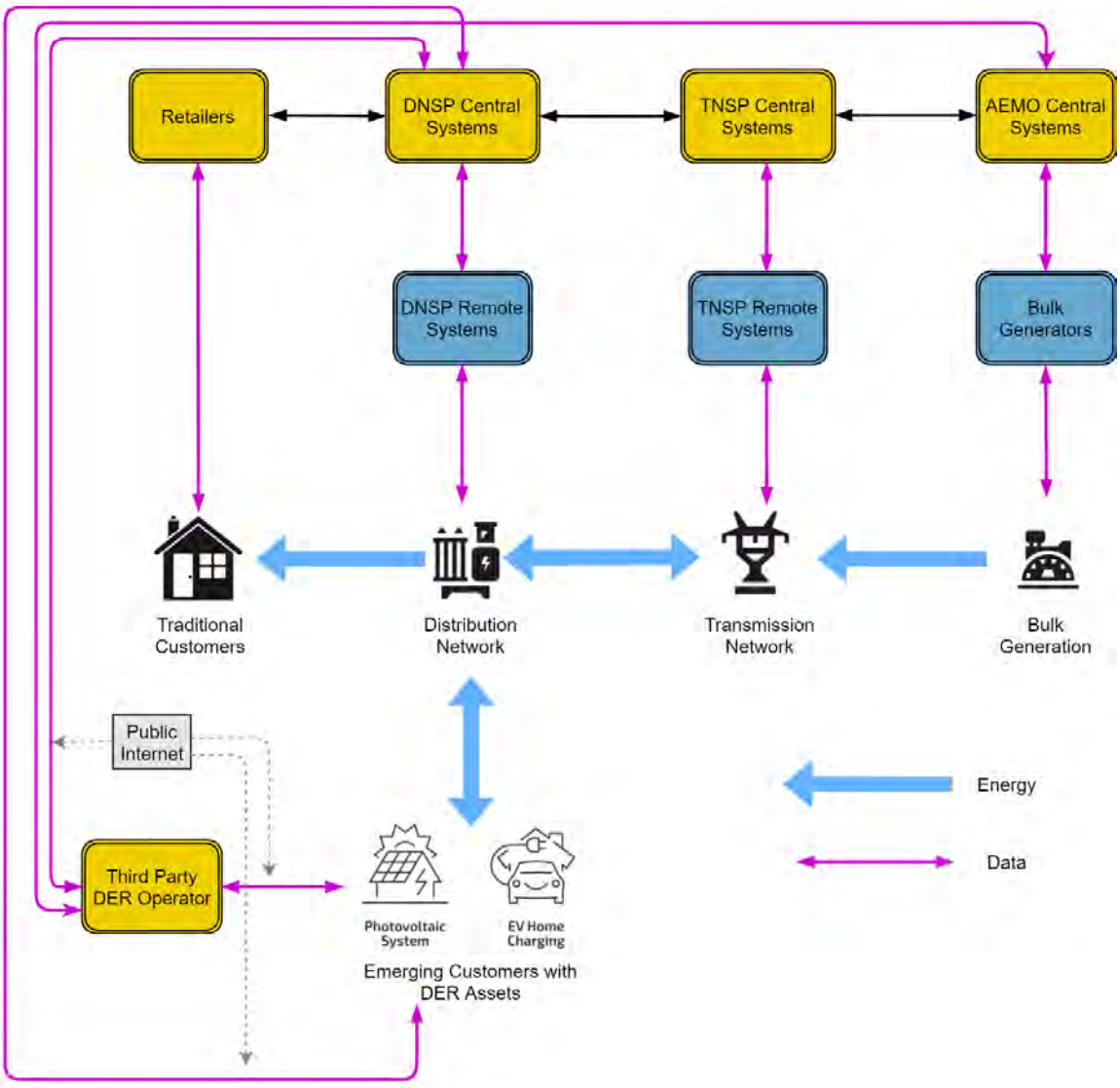


Figure 2: Future State Operational Technology Landscape

In this diagram, we can see that the existing actors and information flows remain, however a new actor – the "Third Party DER Operator" is now present, and energy flows have become bi-directional from customers with DER assets.

It is envisaged that it will be these DER Operators that will orchestrate the behaviour of DER devices. For the Evolve project, this will be done using the IEEE 2030.5 protocol to transport Operating Envelopes to the Aggregator partner's systems which in turn control the local DER devices.

The use of operating envelopes, operating envelope calculations and the IEEE 2030.5 protocol implementation for the Evolve project are covered in other knowledge sharing reports for the project. It is also possible that DNSP Operational Technologies may communicate directly with DER devices that have implemented the IEEE 2030.5 protocol.

2.3 THE IMPACT OF DER

2.3.1 The ADMS

The ADMS is the central operational technology used by DNSPs, however as previously explained, ADMSs do not usually include ***active*** control functions. When they do, they are limited to active control of a relatively small number of high-power devices.

DER will eventually need to be actively managed. As it is connecting directly to the distribution networks, the DNSP's operational technologies will need to contribute to this active management outcome. We could just assume that the ADMS will take on this function. However, there are problems with this assumption, which will be explained further in this report.

Recently, Distributed Energy Resource Management Systems (DERMS) have emerged as a new operational technology, or function.

DERMS ***manage*** DER assets. At the moment, this includes the ability to register and track DER resources, and to "dispatch" groups of DER assets for demand response outcomes involving load reduction.

DERMS functions could, in the future, also include the active management of these DER assets by shaping their real and reactive power behaviour in response to current and predicted network operating conditions.

It is unclear whether DERMS functions will be incorporated into the ADMS, whether the DERMS will sit outside the ADMS as a stand-alone system with appropriate integrations, or some hybrid model of these two options.

The Evolve project is contributing to the development of active DER management outcomes through its work on developing DER communications protocols and the algorithms needed to shape the real and reactive power behaviour of DER, as well as developing data platforms that can perform the required calculations at scale.

These outcomes are prerequisites to the active management of DER assets, wherever that function ends up being implemented.

2.3.2 Remote Device Communications

Operational technologies in traditional DNSPs communicate with remote devices in a master-slave pattern, where the central system (most often the SCADA sub-system of the

ADMS) initiates either a request for data or a control request to a remote device (normally referred to as a Remote Terminal Unit) using a SCADA protocol such as DNP3[2].

While protocols such as DNP3 do support a "report by exception" function, in most cases, the central operational technology initiates the communications with the remote device.

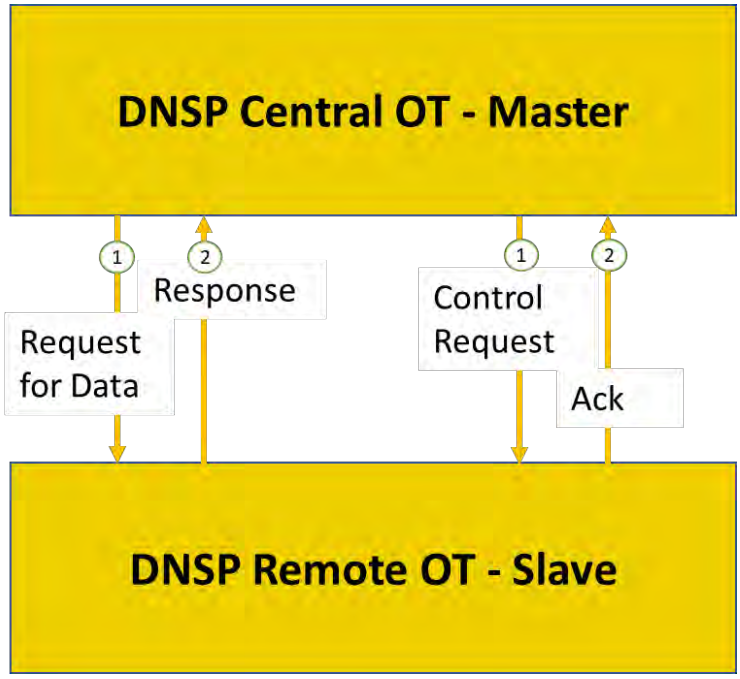


Figure 3: Traditional DNSP Master Slave Communications

In this scenario, all equipment is owned and operated by the DNSP and thus the responsibility of securing the communications pathways between remote and central systems falls entirely to the DNSP.

For large electricity networks, data inputs representing analogue measurements typically number in the tens of thousands and data inputs representing status points such as circuit breakers and alarms may number in the hundreds of thousands.

Analogue measurements are often collected at a relatively high frequency (every 10 seconds) for major assets such as power transformers in zone substations, but at a lower frequency for less critical assets such as protection devices on long rural distribution networks.

This has a number of beneficial outcomes:

- Determinism – the amount of data sent between central and remote devices remains relatively similar in all circumstances, so that I/O bottlenecks do not arise during periods of high activity such as storm events,
- Rapid discovery of remote device failure – remote devices that fail, or communications failures, are discovered quickly,

[2] https://www.dnp.org/Products/Implementors

- Good situational awareness, and
- They are relatively easy to secure from a cyber perspective.

DER assets have arrived in the age of the internet, when communications between the cloud and end devices is done differently. In most internet-based technologies, the "cloud" is essentially the slave of the remote device – the remote device initiates a connection to the central system (the cloud) and then interacts with it by posting or getting data.

The is how the IEEE 2030.5 protocol is intended to work, although it is also possible for the DNSP Central OT to send unsolicited messages to the DER devices.

If we add this style of communications to the mix of DNSP operational technology, the picture becomes more complex, as illustrated below.

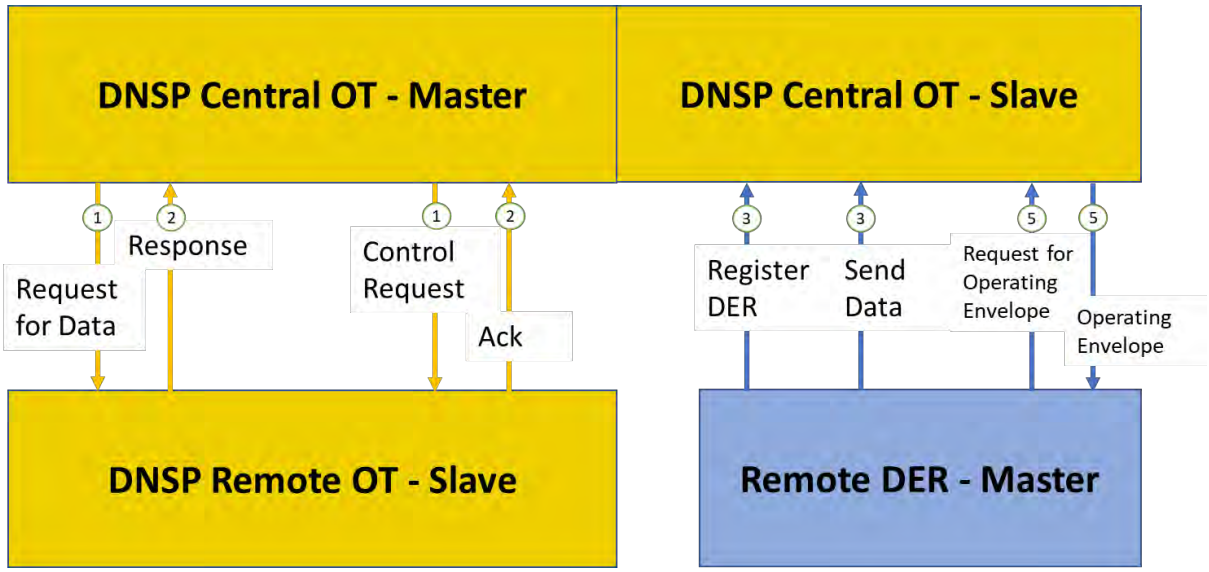


Figure 4: DER Communications

Communications with remote devices will become a mix of DNSP owned and operated technology and communications pathways, and third party owned technology and communications pathways.

The number of devices under control could increase by an order of magnitude or more, as each DER end point is potentially controllable, and in a large network with a million or more customers, this amounts to a million or more controllable end points rather than the tens of thousands of controllable end points in the network itself.

There will also be new control systems for batteries and demand side consumption control. There are many start-ups and established businesses already in this space, including the Aggregator partners in the Evolve project.

These edge technologies are being developed in what is essentially a greenfield situation; the problem space and the solution space are evolving – are being created – together. The technology is complex, and the problem space difficult to understand, however there are fewer problems with incumbent technology stacks to overcome for the developers of this new technology, than the developers of the central OT systems, as will be explained shortly.

2.3.3 Cyber Security

Existing operational technologies do not generally use the public internet for communications between central and remote locations.

However, the public internet has become a communications pathway for the third party DER Operators to talk to the DER assets under their supervision, or potentially to the DER devices themselves.

Why the internet? Because it is expensive to install dedicated communications circuits to every house. Ubiquitous and inexpensive communications via the internet is available to DER assets, that can connect using the homes WIFI. Alternatively, Aggregators can communicate with the DER assets using wired connections locally, and communicate with their central systems using the internet via the homes WIFI.

Even though the internet is being used for DER communications, this does not mean this poses a cyber security risk that cannot be mitigated - communications over the internet can be secured very effectively.

However, this does not happen by default, and the additional complexity in the future state context diagram above in **Figure 2** equates to additional effort to secure the communications, additional attack vectors for malicious actors and additional complexity and hence risk in the overall architecture.

Impacts of DER on cyber security are explained in more detail further in this report.

2.3.4 Visibility and Responsibility

Another issue from the DNSP's point of view is that ***someone else*** may be controlling the DER assets, which are electrically connected directly to the DNSP's assets.

Moreover, the DNSPs do not get automatic visibility of the impact of these DER assets on the low voltage network to which they are connected. They either have to install LV monitoring, or they have to obtain data from third parties.

It is these new integration patterns, and lack of visibility and control in the LV parts of the network that present one of the greatest challenges for DNSPs.

2.3.5 Scale

Current DNSP operational technologies typically deal with sensor data for hundreds of thousands of status points, such as alarms and switch states, and tens of thousands of analogue values, such as HV voltages and power readings. Active management of the network was limited to the transmission and high voltage tiers of the network, with the LV network allowed to work autonomously in a set-and-forget paradigm.

Current operational technologies that manage generating plant were developed to deal with, at most, several thousand medium and large generators, and were located with the market and transmission operator's operational technology stacks.

IF DER becomes ubiquitous across all energy prosumers, there will be a one or two orders of magnitude increase in all of the following:

- the amount of sensor data that needs to be processed and acted upon by the operational technologies,
- The number of generators that must be actively managed,

- The amount of static asset data that must be loaded into the operational technology systems, and
- The amount of compute needed to continuously calculate the acceptable range of real and reactive power for the DER assets.

Existing operational technologies, in particular the ADMS and historians, may not scale up to deal with these new sensor, asset data and computational demands.

Additionally, the operational paradigms that will need to be supported by future operational technologies may not easily integrate within the operational functionality provided by existing operational technologies.

2.4 MANAGING OPERATIONAL TECHNOLOGY TRANSITION

Unlike the development of the actual DER technologies, which is occurring more or less from the ground up, as previously mentioned, things are not so straight forward for existing centralised OT such as the ADMS.

The ADMS has evolved gradually over the past two decades and has become a core system in virtually all large electricity distribution networks, providing functions such as SCADA (Supervisory Control and Data Acquisition), on-demand load flow studies, switching schedules for co-ordination of switching activities between the control room and the field, automated fault isolation and restoration and outage and crew management.

Industry commentators are predicting significant growth of the ADMS because of the anticipated changes to the nature of distribution networks. (Navigant, 2015)

It is likely that the existing ADMSs will continue to provide the operational reference models for the HV network for some time to come, as well as core work flow management and control functions needed for the HV network now and into the future by the electricity distribution network operators.

However, monolithic ADMS solutions by themselves may not be the best way to manage, influence and exploit the opportunities arising from the anticipated proliferation of DER connecting to the LV assets of electrical distribution networks, as so far described in this report.

Most existing ADMSs now in operational use were designed when the problem space of electricity distribution networks was well understood and not undergoing rapid change. As the systems evolved to include more functions and support for more business processes in a problem space that was not changing very rapidly, improvements in the functional complexity of the systems were possible without major refactoring of the software.

The systems have been able to do more of the *same* sort of things, and do them faster and better. They are highly reliable and stable, and underpin all current operational practices for DNSPs. However, a point has now been reached in the evolution of these systems where major changes in the problem space will collide with ADMSs that are brittle.

In computer programming and software engineering, software brittleness is "*the increased difficulty in fixing older software that may appear reliable, but fails badly when presented with unusual data or altered in a seemingly minor way. The phrase is derived from analogies to brittleness in metalworking*." (wikipedia, 2021).

Carol Stimmel sums it up well in her book Big Data Analytics Strategies for the Smart Grid, when she says: "*…The benefits may be terrifyingly convincing, but making major*

changes to the ADMS is what some in the industry call a "big bite". To imagine how difficult it is to upgrade command and control in the utility, consider how difficult it is to change the tires on your car – while it's speeding down the interstate. It's about the same thing". (Stimmel, 2015)

2.4.1 Enabling technologies

It is clear that meeting new challenges presented by the impact of DER on the distribution network and DSNP OT systems requires innovation and adaptation at a pace not previously encountered by DNSPs, and industry more broadly.

DNSPs, and industry as a whole, must find a middle ground between conservative approaches that stifle new technologies, and reactive deployment of technologies that result in unreliable operational technology and technical debt. It is also clear that, in this changing environment, not every experiment or technology will be successful. It is through a process of trialling and experimenting with technical outcomes that the development of new systems occurs in a rapidly evolving space.

What is needed is an environment that fosters this kind of experimental innovation, while retaining the security and stability of existing, tested systems.

This is illustrated in the following diagram, in which the mission critical operational technology continues to be managed for stability, and the more speculative systems development needed due to disruptive changes is partitioned to allow an agile development approach.

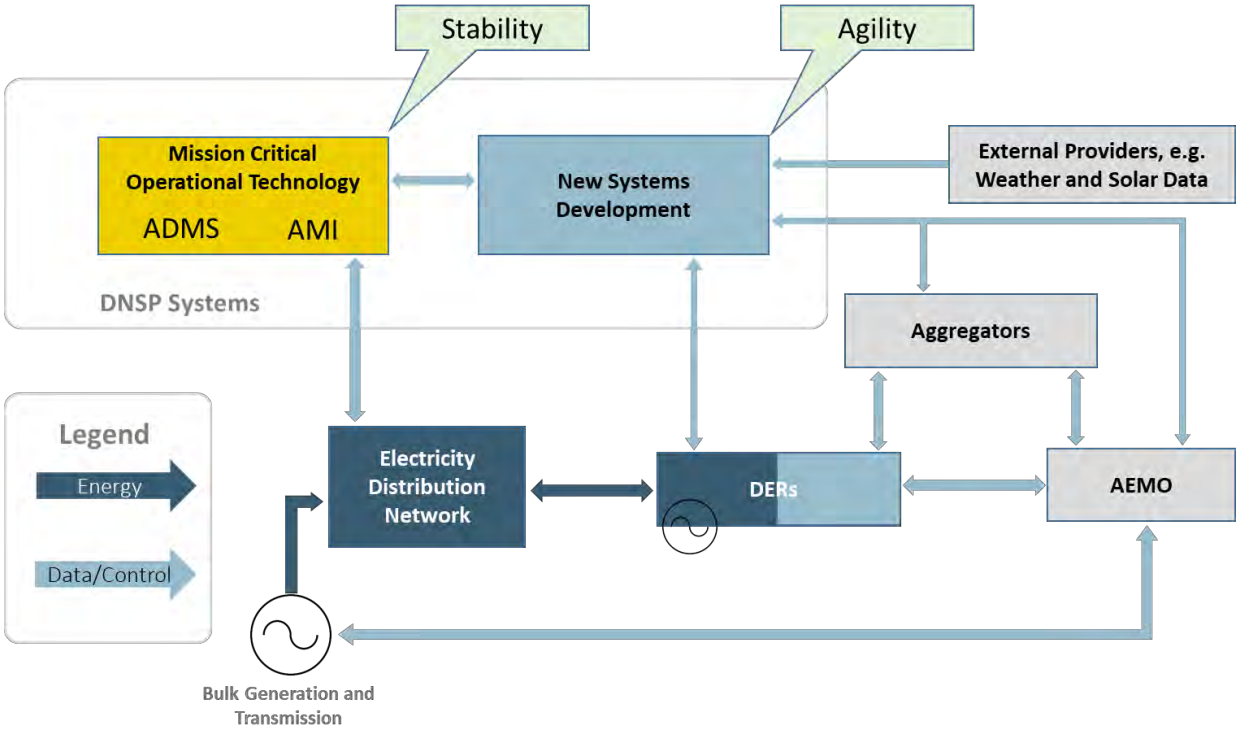


Figure 5: Enabling Operational Technology Evolution

The requirement for ongoing stable operations of the ADMS was reported in the DNSP responses to the OT Questionnaire, where all DNSPs envisaged an "integrated grid management system", but were unwilling to destabilise the ADMS by "experimenting" with operational instances of the system.

2.4.2 Standards and Data Interoperability

A key enabler of an eco-system such as this is standards around data interchange and electrical network modelling.

While data remains in proprietary formats, or under highly restricted access, innovation will be stifled and any approaches that are developed will be tightly linked to source systems and custom data formats, limiting their ability to be deployed and proven in a broader range of environments.

Through the Evolve project we have successfully imported the network data models from all of the DNSP partners into a data server with the same underlying data model, based on the IEC CIM standard. This has allowed us to implement integrations with the operating envelope engines and IEEE 2030.5 utility server components of the platform once, instead of multiple times.

2.4.3 Modularity and Interfaces

Another key enabler is good software design techniques, including the principles of modularity and clean interfaces.

For software solution providers in the space, this means identifying and implementing software sub-systems that provide re-usable outcomes in a variety of different scenarios.

These are sometimes referred to as "no regrets" solutions. An example of such a functional module would be a data platform that can serve up electrical network models efficiently and in a well-structured and well understood format, and a load flow engine that can use these models to calculate power flows and voltages in a network under different operating conditions.

This approach is important because the electrical networks are not all the same; the rate of adoption of DER, and each DNSP's starting position with respect to their current operating technologies and availability of asset and sensor data are different.

Closely coupling solutions to a particular network's current systems and immediate operational needs without consideration of what parts of the solution are generic would result in fragmented and difficult to integrate technology implementations and poor technical outcomes across the industry.

In the Evolve project, we have endeavoured to follow these principles and have implemented technical solutions in our open-source project that should be applicable to general analytics and network modelling requirements for networks.

The expression of electrical network models using the IEC CIM format has been documented here:

https://zepben.github.io/evolve/docs/cim/evolve/

The open-source projects that implement much of this technology have been published here:

https://github.com/zepben

https://github.com/bsgip/envoy

The structure and components of the Evolve Platform are illustrated in the diagram below.

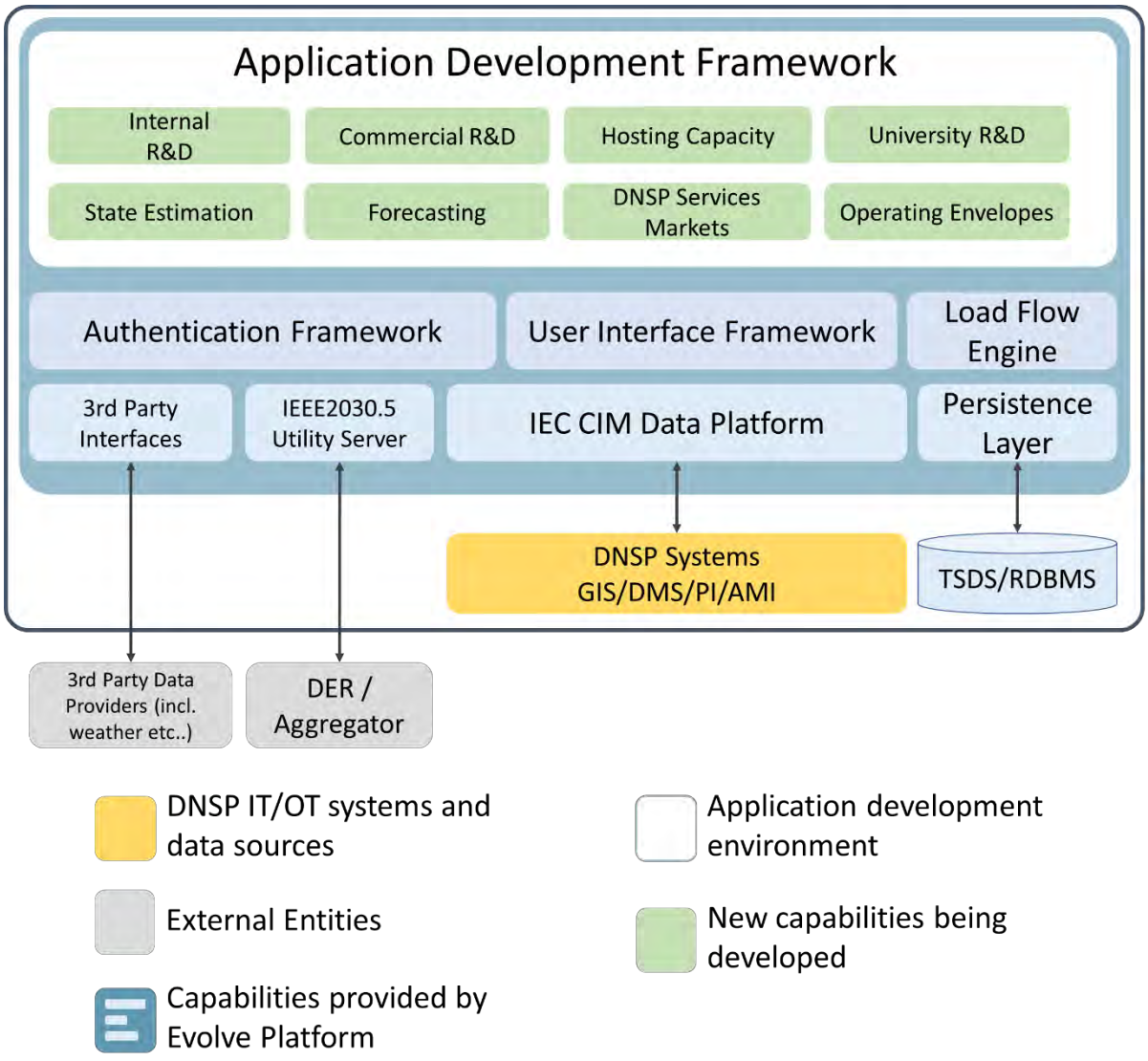


Figure 6: The Evolve Platform.

2.4.4 Modelling and Analysis

If the broader information technology landscape in a DNSP is considered, it becomes apparent that it will not only be operational technology that will be impacted by increasing penetration of DER.

The same network asset and sensor data needed for the real time planning horizon of operational technology will also be needed for the longer-term planning horizons supported by the DNSP's general information technology.

These planning horizons are illustrated in the diagram below.

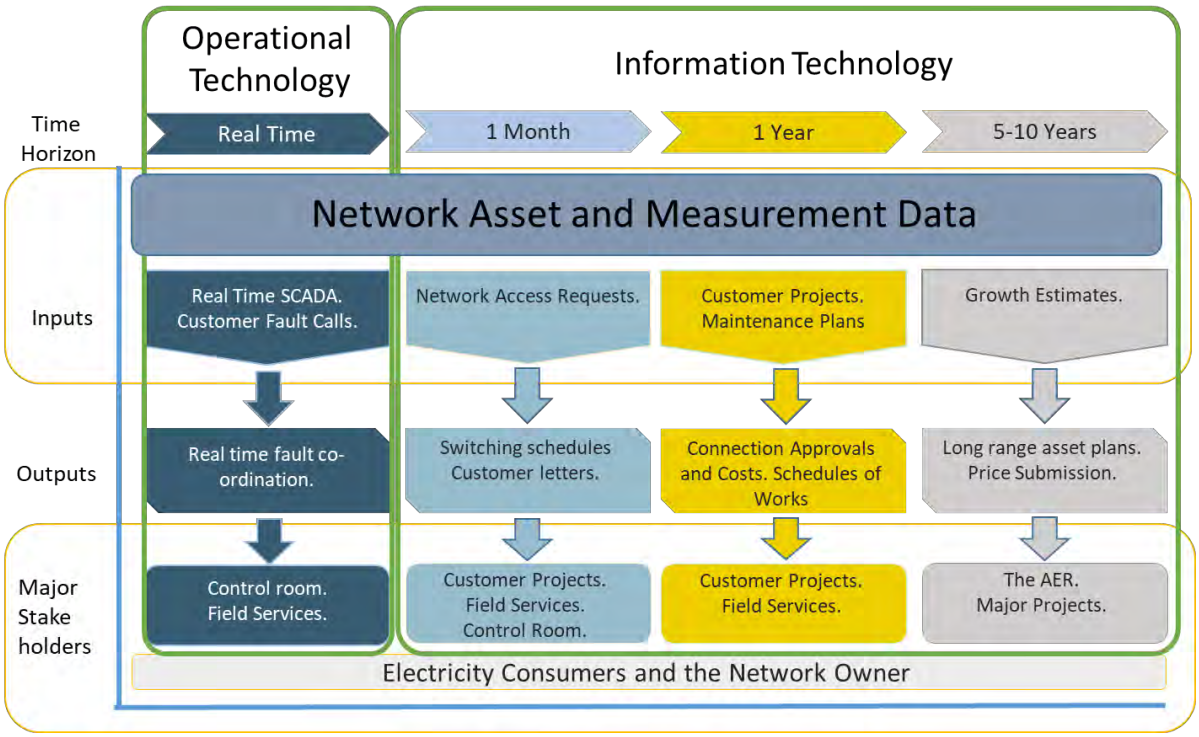


Figure 4: DNSP Planning Horizons

From this, we can see that network asset and measurement data is a common input into all DNSP planning horizons, not just those supported by operational technology.

It follows that if good software engineering principles of modularity and clean interfaces are followed, along with the use of standards for modelling electrical asset and measurement data, then software being developed to support new operational technology outcomes should also be able to support other information technology outcomes for longer planning horizons.

2.4.5 Pathways to Integration

These new systems will not be built in a single leap - instead, they will be iteratively designed and developed as the landscape changes. There are, however, some questions that are common to most potential solutions, that can be answered with software, data and sensor solutions:

- Visibility - static: where are these assets? What capabilities do they have?
- Visibility - dynamic: what are these assets doing? What behaviours do they exhibit?
- Modelling and analysis: Where and when will I have operational problems in the network?
- Orchestration: what behaviours can be enabled or disabled by network orchestration?

From the perspective of the specific technical outcomes for the Evolve project, we can identify several pathways to integration.

Firstly, achieving static visibility of DER assets can be achieved through the registration functions of the IEEE 2030.5 standard. Visibility of the network assets can be achieved through the development of data export tools from DNSP source systems.

Dynamic visibility of DER can be achieved through the capabilities provided by the IEEE 2030.5 protocol for returning measurement data from DER devices.

Dynamic operating envelopes can be incrementally added in targeted locations as DER penetration grows through the operating envelope extensions being developed by the Australian IEEE 2030.5 working group.

The methods to calculate Dynamic Operating Envelopes can be refined over time, with increasing accuracy in required locations.

2.4.6 Data Sharing.

Amongst the DNSP partners in the Evolve project consortium, we have observed different levels of capability to share data about network assets and customer load data. There is confusion about what energy consumer and network asset data can be legally shared with academic institutions and government.

Quite rightly DNSPs are not willing, nor should they be expected, to dump all data about their assets and consumer behaviour into the public domain.

However, there is significant demand from research institutions, government departments, energy consultants and technology houses for network asset and sensor data to support the development of policy, energy forecasting, connection applications and new information technologies, including operational technologies.

Lack of broad level access to this data is a significant inhibitor of innovation in the sector.

The Evolve project has been able to progress with our development work due to the partnering arrangement we have with the DNSPs. However, even with the confidentiality provisions between the Evolve consortium members in the consortium agreement, there has been significant effort required to clear perceived issues on the part of the DNSPs with critical infrastructure protection, licensing and data privacy concerns.

Through our involvement with other ARENA projects working on problems that require network asset and measurement data, we are aware that those projects have also often encountered significant obstacles to obtaining the data they need.

3 SECURING OPERATIONAL TECHNOLOGY

3.1 THE CONSEQUENCES OF CYBER-ATTACKS ON DNSP OT

It is useful to understand the consequences of cyber-attacks by a malicious actor against DNSP Operational Technologies; these are discussed in the following section.

The discussion includes considerations from several different angles, and includes a description of current state (with low penetration of DER) and future state (with high penetration of DER) vulnerabilities.

3.2 CURRENT STATE

The following discussions refers to operational technology used specifically by DNSPs. This operational technology is most usually comprised of the ADMS, which includes SCADA functionality, along with computer equipment located at major sites such as Zone Substations that communicate with central SCADA systems to allow plant to be remotely operated.

3.2.1 The Consequences of Cyber Attacks Breaking DNSP OT systems

Under ***normal operational conditions***, a disruption to DNSP OT so that it was no longer functional would not result in failure of the electricity system as a whole. As long as nothing else happened, the DNSP network assets that transport energy between the transmission system and end consumers would continue to operate indefinitely.

As previously explained, electricity distribution networks currently operate autonomously, and do not require any form of central control for reliable short-term operations.

A disruption to DNSP OT would disrupt planned maintenance and construction work, and it would delay the restoration of power for currently active faults in the electricity network. Under normal operational conditions, the number of people impacted by faults is extremely small – less than 0.01% of the total number of customers served.

So, by itself, a cyber-attack that caused ***failure*** of DNSP Operational Technology systems would not create a major disruption to the normal operation of the electricity system, but rather it would disrupt day-to-day maintenance, construction and isolated fault restoration activities.

However, under ***abnormal operating conditions***, a cyber-attack that caused a DNSP's OT to fail could have a far more significant impact on the operation of the entire electricity system. Examples of abnormal operating conditions are provided in the following sections.

Major Natural Disaster

During a major event, such as a large-scale bushfire, storm, earthquake or tsunami, where large numbers of customers were without power, disruption of the ADMS would result in significant delays in the restoration of power.

Black Start

A black start is needed when a large part of the electricity system – from bulk generation to transmission to distribution, has failed. In this situation, hundreds of thousands, or millions of customers could be without power. These events happen when a large imbalance between generation and consumption occurs due to one or more faults in the transmission or generation system that the overall system cannot adapt to. This can

happen during a major natural disaster, if multiple failures of backup and protection systems occur, or contingency events that were not anticipated occur.

During a black start event, the TNSPs and AEMO rely on the DNSPs to orchestrate a gradual restoration of load through use of SCADA to progressively restore areas of the network supplying consumers, disruption of the ADMS by a cyber attach at such a time would significantly impair and delay the electricity system restart process.

Generation Short Fall

During generation shortfall events, disruption of the ADMS would prevent the DNSPs from performing an orderly load shed. Typically, during such a short fall, the DNSPs will remove power from "low priority" customers such as standard residential homes, and leave power on to "high priority" customers such as hospitals and businesses. The load shedding may also be rotated around different groups of customers so that the inconvenience is not borne by one particular group of customers.

These programs of load shed and rotation are managed within the ADMS, and any disruption to the ADMS during a generation short fall event would result in far greater customer outages, and the TNSP would be forced to take more drastic action to shed load at the transmission level.

3.2.2 The Consequences of Cyber Attacks taking over OT systems

The other thing that could happen with a cyber-attack is for the attacker to obtain privileges and access that would allow control signals to be sent to plant and equipment.

This would allow the attacker to black out large areas of the distribution network, and also destabilise the entire electricity system in a region by opening and closing bulk supply points creating large swings in power over a short period of time which would result in secondary autonomous protection systems kicking in to protect generation equipment and transmission lines, leading to a collapse of the system and a black start event.

This form of attack, while possible, would be more difficult than simply breaking the operational technology. It would more likely come from an "inside job". However – the consequences would be severe, and require appropriate risk mitigation.

Interestingly, all DNSP's responses to the cyber security questionnaire indicated that psychometric testing of staff supporting the operational technology systems was ***not*** carried out, whereas this sort of testing was carried out on users of the operational technology.

Also, no form of security clearance similar to that carried out by the department of defence is required for users and support staff of DNSP operational technology.

This could be something to be considered by DNSPs in the future to help secure their operational technology.

3.3 How DNSPs Currently Secure Operational Technology

Through our work with the Evolve project DNSP partners, and through their responses to the Cyber Security Questionnaire, we gained an appreciation of the effort that has been invested in securing their operational technology.

We observed that all DNSP partners have very strongly defended operational technology, with multiple technical mechanisms to secure the systems, as well as strong policy around ongoing enforcement of these technical mechanisms, including but not limited to:

- Segregation of OT network from IT network,
- Intrusion detection software,
- Firewalls and API gateways,
- Independent penetration testing,
- Regular Patching,
- User access controls, and
- Whitelisting

In short, all DNSPs employ a "defence in depth" approach which is a "*…combination of physical security, protection of networks, including effective segmentation; intrusion detection; software white listing; access and user controls; appropriate procedures regarding the use of the removable media and password policies; personnel's awareness of the risk and familiarity with appropriate procedures."* (Brij, Dharma, & Haoxiang, 2019)

Additionally, there are strict controls on access to the public internet from devices connected to the OT networks. In some DNSPs, this access is simply not possible. In other cases, it is only allowed to specific addresses.

All DNSPs indicated their operational technology does not run in a hosted environment such as AWS or Microsoft Azure.

In one case the operational technology hardware is hosted in a third-party data centre. In all other cases, the operational technology was physically located in server rooms owned and managed by the DNSP, and co-located with the control room facilities. Backup data centres and control rooms were implemented by all DNSP partners.

The DNSP partners have varying levels of integration of the ADMS with corporate systems, including field computing devices. In some cases, this integration included inbound connections to the ADMS from corporate devices, however in others there was only an outbound push of data. In all cases, multiple levels of protection were implemented to secure these integrations.

3.4 Future State

Through the DNSP responses to the Questionnaire, it is expected that all the current state cyber-security concerns will still apply in a future, and all current technical cyber security measures will continue to be applied, and potentially bolstered.

We can suppose that additional complexity will arise out of the additional actors and integrations; however, the challenge is not so much in creating secure integrations, but rather with ensuring those mechanisms are put in place and maintained.

Perhaps one of the more controversial issues will be around the ***hosting*** of operational technology.

As described above, all DNSP partners indicated they currently manage the infrastructure used to host operational technology; this includes operating systems patching, database maintenance, application support etc.

Cloud based solutions such as AWS and Azure, within which an increasing number of small and large companies locate their information technology[3],[4] are also being used by DNSPs to create "data lakes" and analytics platforms for non-mission critical information technology.

However, based on the responses to the questionnaire, none of the DNSP partners could see a future where their operational technology would be hosted in the cloud. This position is sensible, but not from a cyber security perspective. AWS, Microsoft and other hosting solution providers are very good at securing their hosting solutions – their whole business model depends on it.

The reason DNSPs do not want to move their operational technology to "the cloud" is because it would create a risky interdependency between communications, computing resources and the electricity supply – these systems all depend upon one another to some extent.

During a major event, where for example generation shortfall occurred and the electricity system collapsed in one or more regions, the DNSP operational technology is needed to support electricity system restart processes, as previously described.

If this operational technology was hosted in third party data centres, there is every possibility that the data centres hosting the technology would continue to operate using their own backup generators. However, this may not be the case for communications between the DNSPs operational facilities (the control rooms) and the data centres, which may have to rely on multiple backup power supplier coming on line in a timely fashion.

In any event, the DNSPs want to ensure their operational technology, and the operational staff that will use it to respond to major events, are kept close together and that the backup power systems that will keep it running are maintained and able to keep things running for extended periods of time if needed.

The Evolve project has been hosting some of its technology in Microsoft's Azure platform; this has allowed the software development team latitude to easily deploy servers at different times to support different functional outcomes – it is a good ***development*** environment.

However, if any of the technologies being developed by the Evolve project were to become part of the DNSP's operational technologies, it is likely those technologies would move back to a DNSP-managed hosting solution.

Things get more interesting with the third-party controllers of DER in a future state system with high penetration DER – these actors currently don't have the same concerns with maintaining high availability and reliability of the overall electricity system as AEMO and the TNSPs and DNSPs do.

Loss of data centres or communications over the internet in a future state with DER operational technologies hosted in the cloud would have serious implications for the operation of the overall electricity system. Dealing with this will require a mix of measures including sensible autonomous behaviour of DER assets, and appropriate policy and laws around where operational technology and communications can be hosted.

---

[3] https://www.contino.io/insights/whos-using-microsoft-azure-2020

[4] https://www.contino.io/insights/whos-using-aws#entry:1177:url

3.5 SECURING THE EVOLVE PLATFORM

Note: For the Evolve project, the central data services, interfaces with Aggregators and operating envelope calculation engines were located in Azure to provide flexibility for the development team in the amount of computer resources they had access to during the development phase, and to allow a DevOps approach to the software development.

In a production Evolve system used by a DNSP for *operational* purposes, these services could be partially or completely moved to a DNSP op-premise hosted solution.

Other than the use of blob stores to hold files, no Azure proprietary technologies have been used to develop the overall solution.

For *non-operational* purposes, such as analytics for longer range planning, the Evolve platform could continue to he hosted in Azure.

The Evolve platform consists of three components when considering security: Agents for data processing and ingestion of DNSP sourced data, the Evolve data servers and endpoints, and client applications like user frontends and Aggregator systems.

There are 5 boundaries which need to be secured:

1. The interface between agents and the DNSP systems they communicate with,
2. The interface between agents and the Evolve platform,
3. Internal communication between services within the central Evolve platform,
4. The Evolve APIs used by the Evolve client applications and Aggregators, and
5. Access by system administrators

These security boundaries constitute the main vectors for attack against the systems that form part of the overall solution, and we have implemented industry best-practices to secure these boundaries, as described in the following sections.

3.5.1 Agent Interfaces to DNSP systems

Agents are applications that obtain data from DNSP source systems. This can be periodic snapshots of data for network model or historical measurement data, or it can be streaming real time or near real time sensor data.

Below is a diagram showing a typical agent deployment, indicating the direction of IP connection.

In this example, the Evolve agent receives data from a DNSP developed data migration tool that ingests data from multiple internal systems, some of which may be classed as Operational Technology, and produces a consolidated output in the form of a file or set of files, or alternatively by writing to a blob store[5].

[5] https://azure.microsoft.com/en-au/services/storage/blobs/

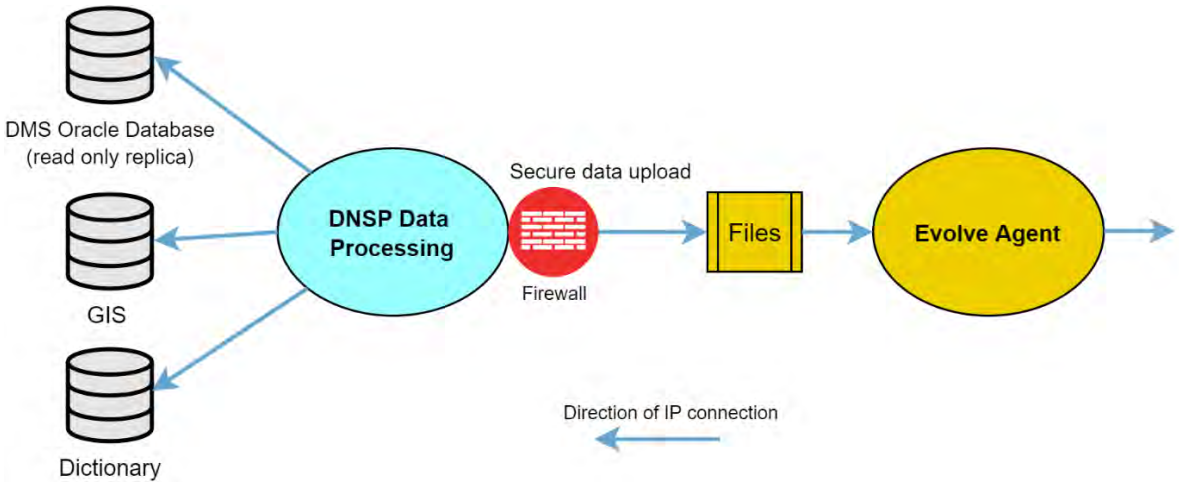


Figure 8: File Ingesting Agent

The files in this case could be CIM RDF files, one for each electrical network feeder. The Agent will ingest these files to create a database, which is held in a single file, which is then sent to the Evolve data services, which for the project are hosted in Azure.

There is some flexibility in where the Agent executes, so as to allow the overall architecture to be flexible and align with DNSP security requirements. In some cases, where the agent is making a direction connection to an RDMS, the agent will need a high speed, low latency IP connection, and would need to run on a "local" network segment.

In another example, provided below, the Evolve agent makes an IP connection to the DNSP's Historian located in the corporate network, and then makes an outbound IP connection to the Evolve data services.

In all cases, the Agent provides an intermediary process that obtains data from internal systems via files or IP connections, and then initiates an outbound connection to the Evolve data platform. This approach allows the DNSP architecture team to avoid external processes making inbound IP connections to DNSP managed networks.

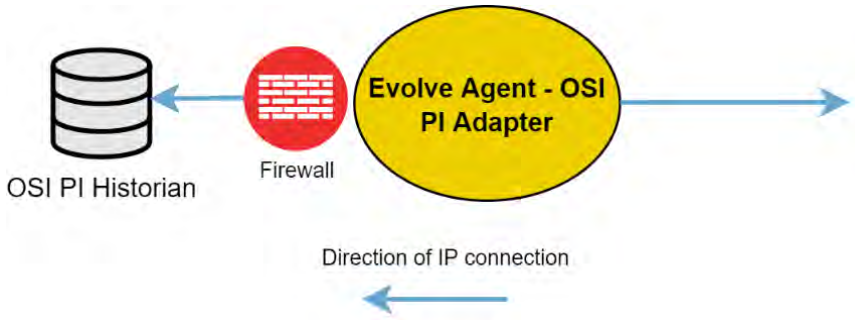


Figure 9: Streaming Agent

When an Evolve agent is located within a DNSP network it is sometimes required that credentials be stored and retrieved for accessing both DNSP systems, as well as Evolve systems. In these cases, credentials may be stored in a DNSP's secret storage system.

In cases where data is a file drop from a source system, security mechanisms are provided by the security practices of the IT department. The common implementation is via an encrypted, read-only network mount provided to the agent host and controlled by the DNSP's system administrators.

The following reusable Agents have been developed for the Evolve platform

1. CIM RDF[6] Agent – Ingests electrical network models using the CIM RDF format.
2. GeoJSON[7] Agent – Ingests electrical network models using an Augmented GeoJSON data format.
3. OSI PI Agent – Streams sensor data from an OSI PI Historian
4. GE PowerOn Fusion Agent – Builds an electrical network model from the GE PowerOn Fusion ADMS.

Other agents are developed as needed to obtain data from DNSP source systems.

3.5.2 Agent Interfaces to the Evolve Platform

Agents forward source system data to the Evolve platform through a single API interface, or a data drop onto a dedicated Evolve platform Azure object storage container for that agent. Security details for each of these methods is described below.

The Evolve platform exposes a HTTPS gRPC[8] API[9] for receiving streaming data from agents. This interface is secured by OAuth2 token-based access control, with an option for PKI, where the agent requires a certificate signed by the Zepben Evolve CA to be able to establish a connection with the API.

PKI provides an extra layer of security, but cannot be used on its own as there is no mechanism for access control - this is only provided through OAuth2.

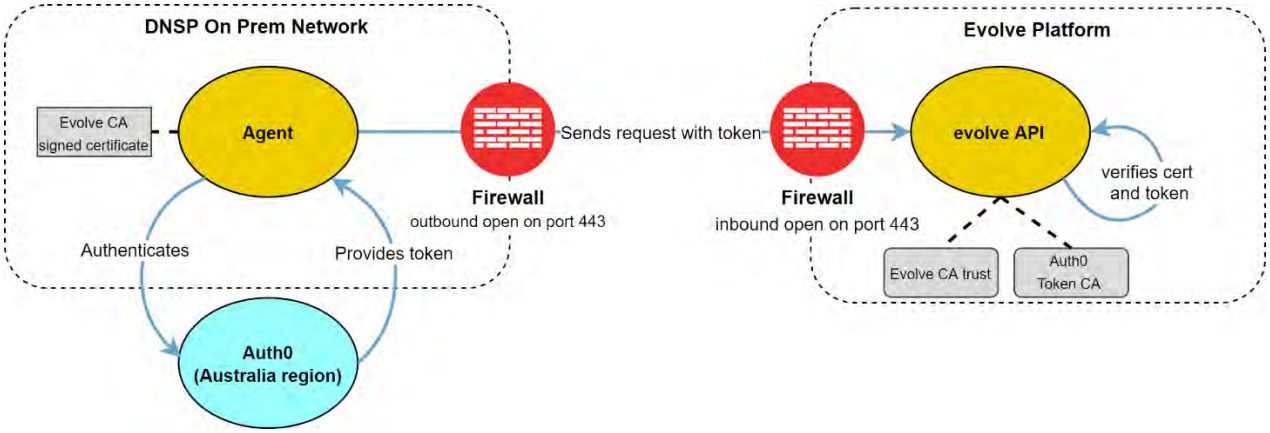


Figure 10: Agent Communications with the Evolve Platform

Our OAuth2 flows provide role-based access control to the Evolve APIs. These flows are typically delivered through a third-party product such as Auth0, with integration between

---

[6] https://arena.gov.au/knowledge-bank/using-the-cim-for-electrical-network-model-exchange/

[7] https://geojson.org/

[8] https://grpc.io

[9] https://github.com/zepben/evolve-grpc/blob/cde82161ad69c1d93888210ef1134f2283085657/proto/zepben/protobuf/np/np.proto#L19

the Evolve platform and DNSP/Aggregator authentication/authorisation systems. In the agent's case each agent is given service credentials that uniquely identify the agent and grant permissions to the various gRPC endpoints required.

Auth0 is an authentication service provider used for managing access to APIs. It is widely used and well supported[10]. Auth0 gives application developers access to a significant amount of token handling libraries; the security aspects of the protocol are implemented by experts in their field. Note that in the diagram above, the agent provides a token as retrieved from Auth0 that is sent to the platform. This token is signed by an Auth0 certificate dedicated to this API and is verified against that certificate on the platform side.

This means that there is some communication between the agent and an Auth0 server, however this functionality can also be brought on-premise.

The platform side does also perform limited communication with the Auth0 service; however, this is only to retrieve the current certificate for verifying tokens and occurs only rarely when a new certificate is rolled out.

3.5.3 Aggregator Interfaces to the Evolve Platform.

Aggregators communicate with the Evolve platform using an HTTPS IEEE2030.5 REST API. This interface is secured by OAuth2 token-based access control in a similar way to the OAuth2 access flow used by agents.

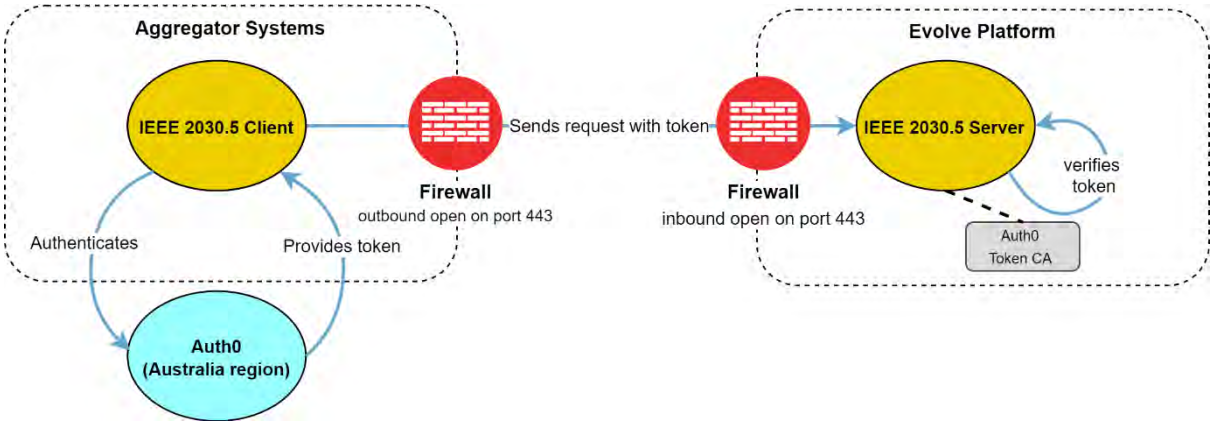


Figure 11: Aggregator Communications with the Evolve Platform

3.5.4 Internal communications

Internal communications between Evolve services occur over HTTPS REST and gRPC APIs, in a manner consistent to how agents interact with our services. This enables us to have a consistent solution to managing our authorisation, authentication, and audit needs.

As previously discussed, these APIs operate on Auth0 based OAuth2 workflows. In addition, our services are segregated at the DNSP level, with a single dedicated VNet (Azure virtual network) for each DNSP deployment. These virtual networks are locked down in a way that only enables external connections from sources we expect, such as:

[10] https://auth0.com/docs/protocols/protocol-oauth2

1. Agents
2. Aggregators, or
3. External clients (Evolve Web User Interface (UI) or other applications)

3.5.5 System administrators

System administrator access to the Evolve central platform is via a bastion host[11], as illustrated in the diagram below.

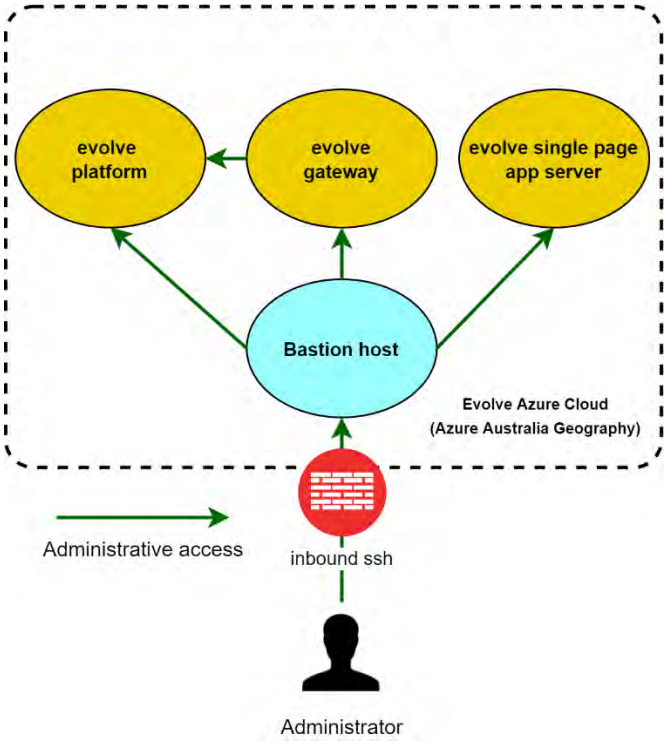


Figure 12: User and Administrator communication with the platform

3.5.6 Hosting

All servers are located in the Azure Australia geographic region to ensure data sovereignty is maintained, with all hard disks encrypted using Azure Disk Encryption. Administrator access is limited to only those that need access to manage the servers, although by design we operate on highly automated workflows and strive for minimal system administration requirements.

3.5.7 Client APIs

Client APIs also operate on OAuth2 token-based APIs over HTTPS. Authentication is again provided through Auth0, and user management is provided through integration with corporate systems. Clients can either be Evolve Web UI users or programmatic actors utilising the Evolve SDKs. In the Web UI case users are redirected to Auth0 which performs our authentication and authorisation. Once a user logs on they are redirected back to the Evolve Web UI and allocated an expiring token from Auth0 containing the

[11] https://azure.microsoft.com/en-au/services/azure-bastion/

user's permission set, and this is used in requests to the Evolve gateway for content. As per the other examples, the token is signed and can be verified efficiently server side providing authentication and authorisation.

Our Web UI operates as a single page application, which means the website is executed entirely from the user's device. All data visible on the UI - confidential or not - must be requested from the gateway API and thus go through the auth process, as it is not possible to store dynamic data within the web application. This model enables an easy separation between sensitive and public content ensuring that confidential data is never exposed to those without authorisation.

Client services can also utilise the Evolve APIs through the Evolve Software Development Kits (SDKs)[12]. These SDKs utilise the HTTPS gRPC APIs that are secured in the same manner as above and allow client services to request network data their own outcomes.

Authentication mechanisms are provided in the SDK to enable ease of use for developers, who simply have to provide their Auth0 token when connecting and the SDK will handle refreshing tokens and sending the required data to the platform for authorisation.

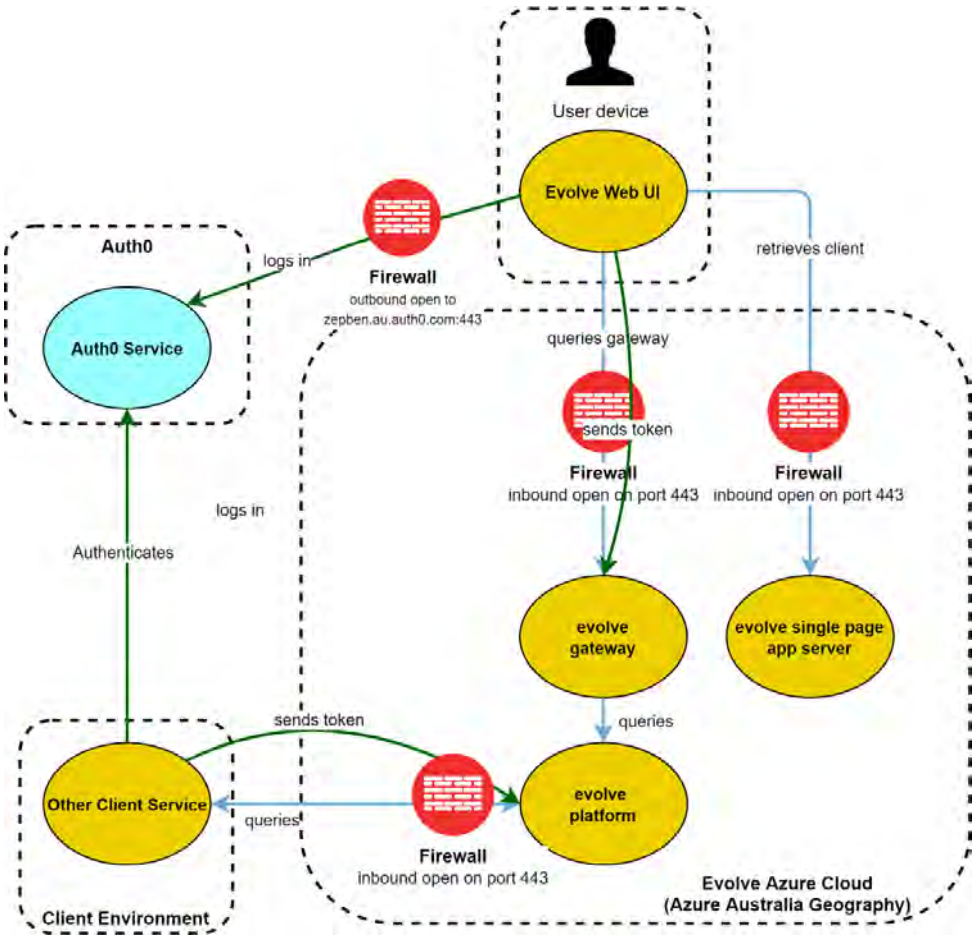


Figure 13: Client and User Communications

[12] https://github.com/zepben/evolve-sdk-python

https://github.com/zepben/evolve-sdk-jvm

As described above, all services live in a dedicated VNet in highly secure Australian data centres in Microsoft Azure, and each DNSP has an isolated deployment to ensure security cannot be breached across networks and that they can be managed independently in our systems.

3.6 Security Frameworks and Standards

Typically, when people hear "cyber security" their minds turn to hackers, cybercriminals and other malicious actors tapping away at their computers, cracking passwords and stealing data or installing malware. While the consequences of a cyber-attack can be severe, as discussed above, protections against cyber-attacks are only one portion of cyber security. For an organisation to ensure they have a balanced, robust and effective digital security system in place, a cyber security framework or standard can provide the overall coverage required.

Cyber security frameworks are typically designed to have some flexibility in their implementation whilst still providing complete and robust coverage. This allows organisations that may be constrained, financially or otherwise, to still protect their digital and information assets.

Some frameworks, such as AEMO's Australian Energy Cyber Security Framework (AESCSF) (AEMO, 2018), are created for a specific field, sector, or other target audience. Frameworks such as these contain less general best-practices, and instead provide more detailed and specific measures and controls that can be implemented to ensure security.

The AESCSF was developed by the Australian Energy Market Operator (AEMO) in conjunction with the Australian Cyber Security Centre (ACSC), Critical Infrastructure Centre (CIC), and the Cyber Security Industry Working Group (CSIWG). The framework was established in 2018 to address the increasing cyber security risks faced by the Australian energy sector. It involves a criticality assessment for each participant and a cyber security capability and maturity self-assessment.

The AESCSF was developed for individual organisations and entities to assess their cyber security capability, and then use these assessments with implementation guidelines from other standards to increase the cyber security readiness.

However, this framework does not provide adequate coverage for the cyber security issues that come with projects such as Evolve that involve multiple parties including DNSPs, Aggregators, academic institutions and technology vendors. As such it was deemed unsuitable to use for the Evolve project, however as it contains strong industry-standard practices, it has been utilised as a beneficial reference source.

3.6.1 Security Frameworks and Standards in the Evolve Project

DER projects, such as the Evolve project, are developing technologies that, at scale, would be classed as Operational Technologies that should be subject to the same level of cyber security assurance as the ADMS used by a DNSP.

DER-related projects invariably involve the use of sensors to collect data from energy prosumers. This data is generally considered to be personal and private information and must be protected. The technology must therefore be developed with cyber security in mind at the outset.

In the case of the Evolve project, we are also collecting a significant amount of asset and customer load data from the networks, as well as developing integrations with on-premise operational technologies that are considered mission critical and subject to high level cyber security assurance.

A selection of security frameworks was assessed against the above security requirements, as well as the business constraints of the project, to ensure that not only the Evolve platform was protected, but also that the business and development processes were also secure.

The diagram below shows the various security frameworks that were assessed by Zepben to be used organisationally, and by extension to provide security assurance for the Evolve project.

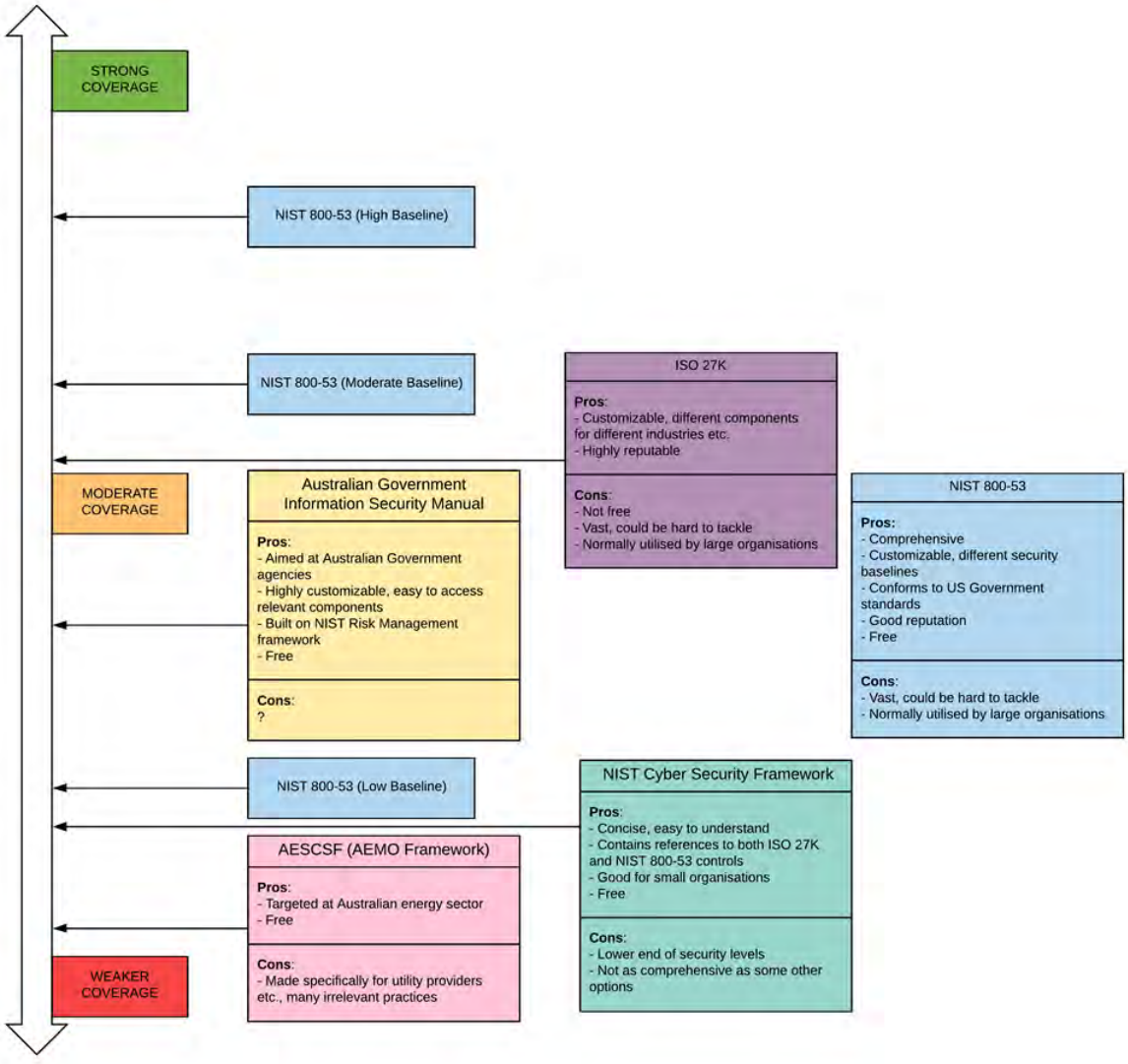


Figure 14: Cyber Security Frameworks

ISO/IEC 27000

We chose the ISO/IEC 27000 standard to base our cyber security policy and processes upon, as it provided the appropriate balance between security assurance and complexity and practical implementation.

The International Standards Organisation (ISO) and the International Electrotechnical Commission (IEC) 27000 series is a family of international standards for information security. The central standard, ISO/IEC 27001, provides requirements for an information security management system (ISMS). The standards operate on a risk-based framework

for protecting the confidentiality, integrity, and availability of an organisation's information assets.

AS ISO/IEC 27001:2015 is the Australian version of the 27001 standard and is widely considered industry best practice for establishing an ISMS. Zepben uses this standard as the basis for its internal ISMS policies, controls and procedures.

The international standard AS ISO/IEC 27002:2015 - *Code of practice for information security controls* is used as a basis for the security controls established in the Evolve project. The following key elements from this standard have been included in the project's cyber security:

- Development of Information security policies.
- Cryptography
- Operation security
- Communication security
- System acquisition, development and maintenance, with extra consideration given to the "security in development and support processes" and "system security testing" elements of the standard.
- Information security incident management
- Compliance

3.6.2 Security Frameworks and Standards used by DNSP Partners

Three DNSP partners responded to the cyber security questionnaire within a timeframe that allowed their responses to be included in this report. All three indicated they had used AEMO's AESCSF to access the criticality of their operational technology. Unsurprisingly, all the DNSPs concluded they have a high level of criticality for their operational technology systems.

None of the DNSP partners had formally implemented a security framework or code of practice in line with a recognized international standard such as the IEC 27000 series, however, one DNSP is looking to implement the IEC 27000 series for information security, and the ISA/IEC 62443 (62443, 2018) standard for cyber security.

This does not mean that the DNSPs have not implemented rigorous cyber security assurance measures, but rather they have not implemented these measures in accordance with a standards-based framework.

3.6.3 Security Frameworks and Standards used by other Partners

The questionnaire was not given to the other partners in the Evolve project, as they are not running what would be considered Operational Technology at present. However, we intend to provide a modified questionnaire to the Aggregators for an update to this report in the following reporting period, as we expect their solutions will start to become part of the overall operational technology landscape DNSPs will need to function within, as described elsewhere in this report.

4 CONCLUSIONS

Challenges and Solutions for Operational Technologies

We have concluded there will be significant challenges for both DNSP operational technologies and information technologies supporting longer range forecasting to adapt to the disruption caused by DER.

ADMSs - the core operational technology used by DNSPs, and modelling tools and techniques cannot simply be lifted out and replaced with a new set of systems in a "big bang" approach. The changing nature of the problem space requires strategies that allow evolution, not revolution.

Further, more data about network assets and the behaviour of prosumers will be needed to support the development and ongoing operation of network and DER modelling and orchestration software systems. There is an opportunity now for the industry to adopt standards for network modelling and data sharing so that these data resources can be pooled to increase their value, and to establish the mechanisms and rules by which this data can be effectively and securely shared.

Additional integrations will be needed between DNSP asset and customer management systems and operational systems such as the ADMS and emerging DER management systems. Initially, this will provide insights into changing consumption and generation patterns that will enable DNSPs to more effectively respond to these changing patterns within existing operational paradigms and network infrastructure.

As the DER and operational technology matures and DER ramps, new paradigms for the short-term planning horizon will need to be operationalised. These new paradigms will involve communications with multiple Aggregators or stand-alone DER to modify real and reactive power behaviour at the edge of the network to keep the network within acceptable operating margins.

The number of "generators" involved in the supply chain will increase from hundreds – the number of generation plants under the control of the market operator today – to millions in the future, as more and more prosumers in the distribution networks install some form of DER.

There are opportunities for everyone in the supply chain to benefit from the widespread deployment of this DER, provided however the electricity distribution networks can adapt their operational and information technologies to provide the mechanisms needed to maintain network and system stability and reliability in these new conditions.

Cyber Security Issues

We have concluded that there are additional challenges for cyber security assurance arising out of the additional complexity, integrations and systems involved with high penetration DER.

The ***technical*** work needed to secure systems is understood. Good governance and regulation are needed to ensure the technical outcomes to secure the systems are implemented, monitored and maintained.

These requirements for securing operational technology and protecting sensitive data were recognised at the outset of the Evolve project, and significant effort has been expended to ensure the Evolve platform can be secured at a technical level, and that the

project had the correct governance to ensure the technical work was carried out and tested for compliance.

Cyber security frameworks and standards provide strong foundations for any organisation seeking to protect their information assets and systems.

The AESCSF is an excellent choice for organisations in the Australian energy sector seeking to improve their cyber security preparedness, due to the tailor-made industry best practices included within it. However, due to its industry-specific nature, technology developers such as Zepben and academic institutions such as the ANU are not recognised as actors within the framework and as such it could not be utilised effectively for the Evolve project.

The ISO/IEC 27000 international information security standards are robust, scalable frameworks that can be applied to organisations in almost any field. As such, the standards AS ISO/IEC 27001:2015 and AS ISO/IEC 27002:2015 have been used to provide cyber security protections for Zepben and the Evolve project as a whole.

As a closing comment: Good cyber security practices are essential to secure operational technology and prevent the disastrous consequences of a malicious actor disrupting critical infrastructure.

However, to allow people and systems to function, and more importantly to allow the development of new operational and information technologies, and new ways of working, the enforcement of cyber security policies must be reasonable and adaptable and allow benign actors who are innovating in this space access to the data and systems they need to do their work.

Acknowledgements

Zepben would like to acknowledge the significant contribution to the development of this report, and to the overall Evolve project, made by our academic Partner; The Battery Storage and Grid Integration program at the ANU.

We would like to thank our DNSP project partners for providing their insights into the current and future operational technology space, and for contributing to the overall outcomes of the Evolve project.

We would like to thank our Aggregator project partners for their contributions to the ongoing development of the IEEE 2030.5 protocol, and for making data obtained from DER assets under their control available to the project.

This project received funding from ARENA as part of ARENA's Advancing Renewables Program and from the NSW Government.

We would like to thank ARENA and the NSW Government for their significant funding support, and ARENA for providing an excellent eco-system for ongoing knowledge sharing and innovation.

5 REFERENCES

62443, I. (2018). *ISA/IEC 62443*. Retrieved from https://www.isa.org/intech-home/2018/september-october/departments/new-standard-specifies-security-capabilities-for-c

AEMO. (2018). Retrieved from https://aemo.com.au/en/initiatives/major-programs/cyber-security/aescsf-framework-and-resources

Brij, G., Dharma, A., & Haoxiang, W. (2019). *Computer and Cyber Security.* CRC Press.

Fowler, M. (1999). *Refactoring: Improving the Design of Existing Code.* Addison Wesely.

Hilmer, P. F. (1993). *National Competition Policy Review.* Australian Government Publishing Service.

Howlader, A. M., Sadoyama, S., Roose, L. R., & Sepasi, S. (2017). *Distributed voltage control method using Volt-Var control curve of photovoltaic inverter for a smart power grid system.* IEEE.

McKinsey. (2018). Retrieved from https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/the-potential-impact-of-electric-vehicles-on-global-energy-systems

Navigant. (2015). Retrieved from http://www.navigantresearch.com/research/advanced-distribution-management-systems

Stimmel, C. L. (2015). *Big Data Analytics Stragegies for the Smart Grid".* CRC Press.

wikipedia. (2021). Retrieved from http://en.wikipedia.org/wiki/Software_brittleness

Yarrow, G. (2016). *Applying Hilmer Principles in changing energy markets.* Consulting, Synergies Economic.

Appendix A - QUESTIONNAIRE

In developing this report, the DNSP partners were provided with the following questionnaire. The responses to this questionnaire contributed to the development of this report.

Evolve Project - Questionnaire

Integrating with Operational Technology

The purpose of this questionnaire is to elicit information from key information technology decision makers and strategic thinkers within electricity distribution networks (DNSPs) who are responsible for shaping the future of operational technology.

<organisation> is part of the Evolve Project - a consortium of industry and academia that is undertaking research and technology and standards development to help answer questions and provide solutions to the challenges networks will face in the future if high penetrations of Distributed Energy Resources (DER) materialise.

If you have not had any involvement with the Evolve Project to date, more information about the project can be found here:

https://arena.gov.au/projects/evolve-der-project/

The questionnaire will be an input into one of the knowledge-sharing reports that is being produced by the project. The report will provide commentary around the challenges and solutions involved in the integration of 3rd party and cloud-based software platforms with the operational technology domains of electricity distribution networks.

These integrations may become necessary in the future if new or existing market participants begin to control distributed energy resources on behalf of end consumers. At scale, these resources will have a material impact on the operation of the networks, and their behaviour may ultimately need to be managed by DNSP systems within the operational technology domain.

It is hoped that the report will become a useful source of information for the industry to help shape the development of secure information technology over the next decade as the electricity supply system evolves to support higher penetrations of renewables and DER.

The questionnaire is anonymous and confidential, and will not be made public or shared with any other organisation. Responses to the questionnaire will support general commentary around approaches and opinions to the integration of DNSP managed operational technology with external systems over the public internet. Specific responses made by you will not be included in the report, and <organisation> will not be named in relation to any of the questionnaire responses.

Contributions to this questionnaire may be made by multiple people within <organisation>, so some of the questions may not be relevant to your function, or you may not feel comfortable providing a response. In this case, please leave the response field blank

Thank you for taking the time to fill in this questionnaire to provide your valuable insights.

Your Role/Position in the organisation:

Section 1 – Current State Technology

	Which systems are considered "operational technology" in your organisation? Do you have differing levels of criticality in your categorisation of operational technology?
	Organisationally, does the team that supports your operational technology report to the corporate information technology department, or a business unit? Or is there another other organisational structure? Is the development and enforcement of cyber-security policy for corporate information technology and operational technology a shared service in your organisation, or is it managed by separate groups? Is support for RTU's, Protection Devices and electronic devices that control plant and equipment managed by the same group that supports central operational technology such as the DMS or ADMS?
	What mechanisms do you currently use to secure your operational technology. ☐ Segregation of OT network from IT network. ☐ Intrusion detection software. ☐ Firewalls and API gateways. ☐ Independent penetration testing

	☐ Other – please explain
	Are any parts of your operational technology solutions currently hosted "in the cloud", for example using cloud-based solutions such as Microsoft Azure or AWS?
	Are any of your operational technology solutions currently hosted in data centres managed by a third party?
	Is internet access possible from any computers running in the operational technology domain, for example from machines that host ADMS client or server software?
	Do you allow remote access to your operational technology systems by the vendors of those systems? If you, how do you manage that access?
	Does your organisation perform any sort of psychometric testing on staff that are working with operational technology systems?

	Has your organisation implemented a code or practice for information security controls based on international standards, for example the AS ISO/IEC 27001:2015 standard?
	Has your organisation used AEMO's Cyber Security Assessment Framework? https://aemo.com.au/en/initiatives/major-programs/cyber-security/aescsf-framework-and-resources
	Is any of your SCADA data (such as via DNP3 traffic) carried over the public internet? If you, how do you secure this.
	Does the monitoring and control of devices connected to the "Internet of Things" (IoT) feature in your operational technology domain? For example, do IoT devices communicate with your SCADA or ADMS? If so, how are these secured?
	What integrations, if any, currently exist between your ADMS and other corporate systems, and what is the nature of these integrations?
	Does your ADMS vendor provide API's that facilitate integrations. for example ☐ Open database schema

	☐ Electrical Network Model extraction processes ☐ Outbound event API's to allow capture of real time, or near real time events such as SCADA alarms or the opening of hand dressed switches ☐ API's that allow events about other operational information to be captured, for example operational restrictions. ☐ API's for Real time Analogue data ☐ Accessing Historical Analogue data ☐ Other – Please explain

Section 2 – Future State Technology

	Which system or systems do you believe will be used to manage and control DER devices? ☐ Unsure – no firm position at the moment. ☐ DER will be managed by the ADMS, using functionality supplied by the ADMS vendor. ☐ DER will be managed by a separate system that will have integrations with the ADMS. ☐ Other architecture – Please explain.
	Are there any plans or investigations underway, or being contemplated, in your organisation to move some or all operational technologies to hosted solutions such as AWS or Microsoft Azure?

	Are there any plans or investigations underway, or being contemplated, in your organisation to move some or all operational technologies to external data centres where the technology is still hosted on DNSP managed servers?
	Has there been any consideration in your organisation of how existing operational technology will be safely integrated with external systems over the public internet? If so, can you provide general commentary on the outcomes, or share any technical reports?
	Are there any significant data quality improvement initiatives currently underway in your organisation to improve the quality of electrical network model data? If so, can you explain in general terms what those initiatives involve?
	Does your organisation hold data that needs to be protected to ensure critical infrastructure is not damaged by malicious actors?