Cyber Security and Energy Networks

In our rapidly growing digital economy and online community, managing cyber security is now a central part of modern life.

The community increasingly depends on digital services and advanced communications to enable essential services, commerce and leisure. The energy system is no exception.

Energy network businesses in Australia recognise the importance of cyber security to ensuring safe, reliable and efficient services to homes and businesses and to enable a rapidly transforming energy system. Cyber security is not a static goal to be achieved; cyber security is an ever-evolving commitment that requires ongoing vigilance.

Energy Networks Australia members actively monitor global developments and have cyber security strategies to deter, detect and respond to threats. Detailed risk management planning, asset management and IT and Communications planning ensures challenges to ongoing cyber security are known and addressed.

This document provides an overview of key dimensions in cyber security relevant to the energy system:

1. The ***Grid Systems and components*** relied on by energy networks, including technology providers, individual components or systems they procure;
2. The ***Control Systems*** used to monitor and control the network to support energy flows safely and reliably;
3. The ***Access to data*** which safeguards privacy and commercial confidentiality; and
4. The diverse and growing ***Distributed Resources*** which increasingly form a core part of the energy system.

Energy Networks Australia

GRID SYSTEMS AND COMPONENTS

Energy networks rely on significant procurement and operation of components (e.g., programmable logic controllers, digital relays, or remote terminal units); systems (such as supervisory control and data acquisition SCADA) or assembled infrastructure (e.g. substations).

Energy networks apply a range of supply chain management strategies to mitigate risks that unauthorised access and control of operating technologies could occur, and the security of information communicated from the device to the network operation control room.

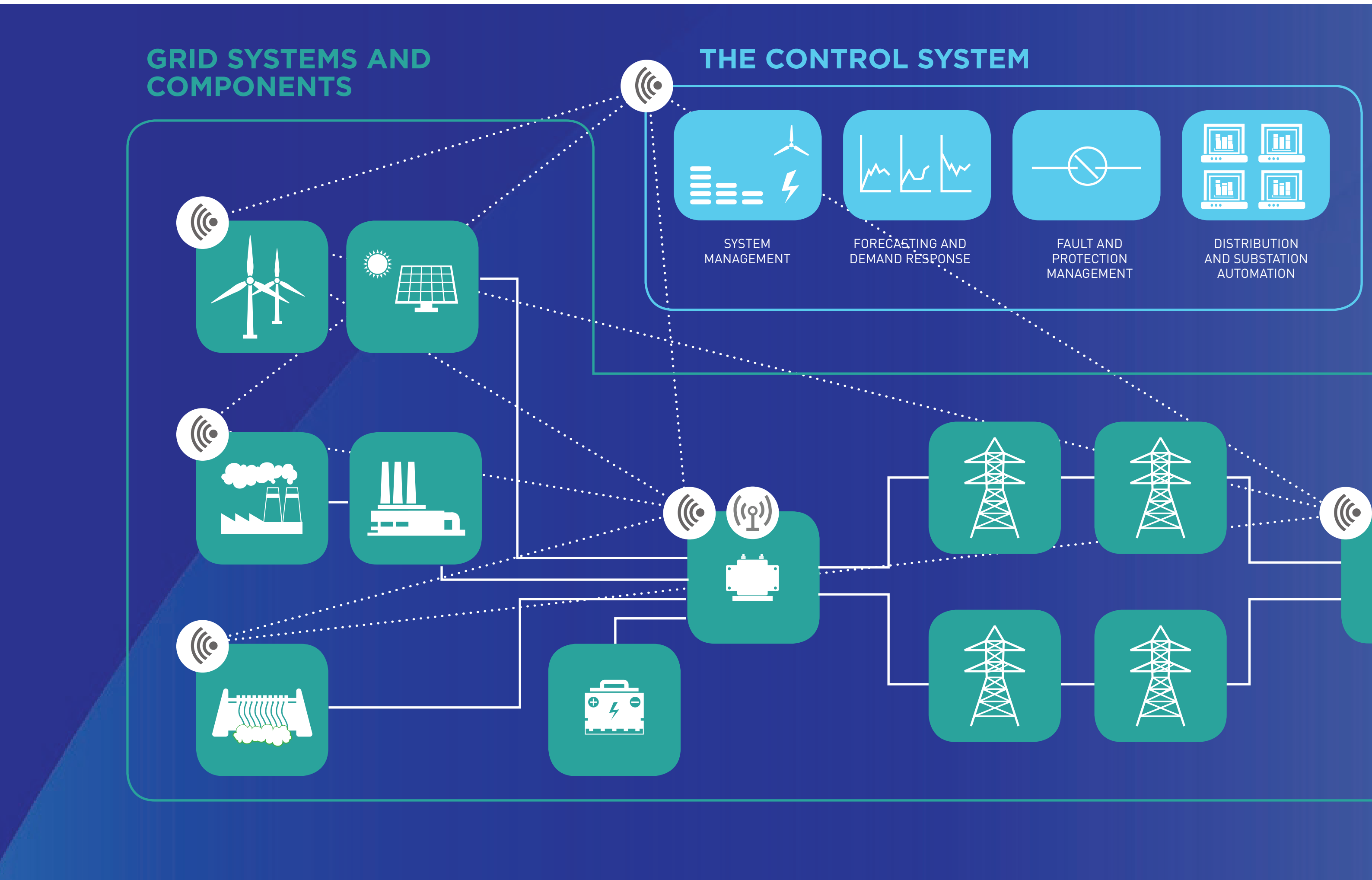
Businesses apply procurement requirements and ongoing life cycle management. These include adherence to standards; security of software and services; access controls; issue logging and auditing; communication restrictions; and malware risk management.

THE CONTROL SYSTEM

A range of industrial control systems (ICS) including SCADA, protections systems, and distribution management systems are employed by energy network operators. SCADA is vital to ensuring efficient, reliable and safe delivery of energy within technical limits, such as voltage and frequency on electricity networks or pressure within gas networks.

The security of such systems and the interfaces between them is crucial.

While ICS and other related systems are structured and configured to reduce the number of potential entry points, utilisation of the most up to date software, as well as restricting administrative privileges, security monitoring and access of personnel to the ICS, are all elements of an effective security strategy.


GRID SYSTEMS AND COMPONENTS
THE CONTROL SYSTEM
SYSTEM MANAGEMENT
FORECASTING AND DEMAND RESPONSE
FAULT AND PROTECTION MANAGEMENT
DISTRIBUTION AND SUBSTATION AUTOMATION

ACCESS TO DATA

Energy networks are leveraging significant volumes of data in more ways than ever before in order to improve energy reliability and efficiency. Management of such volumes of sensitive information requires robust data security strategies to manage hazards which are common to many businesses holding operational or customer data. They require robust data security strategies to manage hazards which are common to many businesses holding customer data. Hazards may include criminal enterprises seeking to access customer information, payment data, identities, and commercially sensitive information.

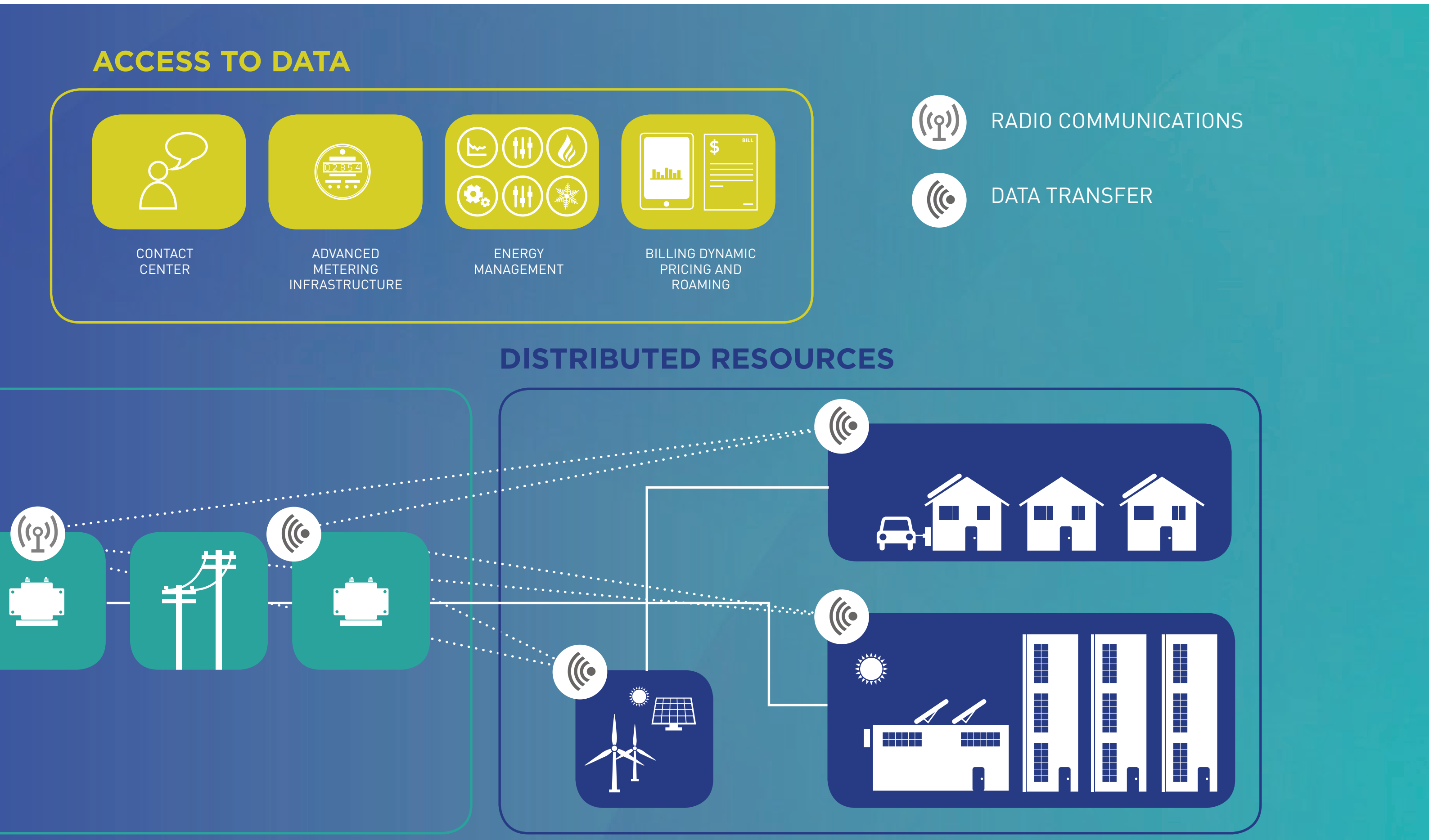
Energy networks are subject to data privacy laws, which set obligations on businesses which collect and store consumer data. Energy networks also seek to ensure consumers are aware of their rights when providing personal information for the purposes of establishing connection agreements, allowing access to property and during other interactions.

DISTRIBUTED RESOURCES

Australia's energy system is experiencing the rapid adoption of distributed energy resources, such as smart meters, smart inverters, electric vehicles, rooftop Solar PV, battery storage and home energy management systems. Many of these technologies are connected through the 'Internet of Things' (IoT) and represent a fast evolving relationship of millions of IoT devices with energy networks, where they are not simple 'loads' on the system, but providers of energy, demand response or ancillary services. Communication within this ecosystem of IoT devices will be increasingly relied upon by energy networks to play a key role in real-time system balancing and operations supporting the reliability, safety and quality of energy supply.

As a result, a core capability of energy networks must be managing cyber security as devices are integrated. This requires careful management of interfaces, strong communication protocols and setting of safe operating parameters to manage risks to other IoT devices, network components to ensure continued quality of service delivery.

The cyber security management strategies of the new service providers in this ecosystem will also be vital. Energy networks will need to work closely with such providers as 'smart grid architecture' and technology standards are developed.



Frameworks used by Energy Networks Australia members

Standards

Standards play a key role in supporting the connections between technologies, providing consistent frameworks for design and implementation. Several Australian and International Standards apply to security of information and relevant management systems. Australian energy networks service providers may be certified or aligned to a number of such international or domestic standards, including but not limited to:

- ISO 27000 (International Standards Organisation series for Information Security Management Systems);
- Payment Card Industry Data Security Standard (PCI-DSS); and
- North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection Standards.

Significant changes to Australia's energy system are requiring the thorough overhaul of Australian Standards to enable transformations in distributed energy, smart grids and empowered customers. Energy Networks Australia is working closely with Standards Australia to identify and update Standards including many that rely on or impact on cyber security. These include Standards relating to: system security; electrical system operation; micro grids; and data frameworks and privacy.

Resources

Energy Networks Australia members also utilise publically available resources such as:

- Australian Government Department of Defence Intelligence and Security Information Security Manual;
- Australian Signals Directorate (ASD) Top 35 strategies for Mitigating Targeted Cyber Intrusions;
- SANS Institute 20 Critical Controls;
- Centre for Internet Security (CIS) Security Benchmarks;
- Open Web Application Security Project (OWASP) guidance;
- USA Government National Institute of Standards and Technology (NIST) Vulnerability Management Database;
- NIST Cyber Security Framework; and the
- USA Government Department of Energy Cyber security Capability Maturity Model (C2M2).

Planning for the Future

Australia's Cyber Security Strategy

In April 2016, the Australian Government set out its philosophy and program for meeting the dual challenges of the digital age—advancing and protecting our interests online—in *Australia's Cyber Security Strategy*. The Strategy establishes five themes of action for Australia's cyber security over the next four years to 2020:

- A national cyber partnership between government, researchers and business;
- Strong cyber defences to better deter, detect and respond to threats;
- Working with international partners to champion a secure, open and free internet;
- Helping Australian cyber security businesses to grow and prosper; and
- Creating more Australian cyber security professionals through education.

Energy Networks Australia is committed to working with the Australian Government to assist where it can in actioning these five themes.'

Electricity Network Transformation Roadmap

Cyber security is a core focus of the Electricity Network Transformation Roadmap (ENTR) being developed by Energy Networks Australia and the CSIRO. The Roadmap has been undertaken to map the preferred transition which the electricity network industry must make in the coming decade, to be ready to support optimised outcomes for customers under a range of long term energy generation and use scenarios.

In a transformed energy system which takes advantage of digital technology and decentralised resources, a strategic focus on cyber security will be an essential priority.

Contact details

Energy Networks Australia
info@energynetworks.com.au
02 6272 1555