# Grid Cyber Security

## DISCUSSION PAPER

STANDARDS Australia

# Contents

## Standards Australia

Standards Australia is the nation's peak standards body and Australia's representative to the International Electrotechnical Commission (IEC) and International Organization for Standardisation (ISO). Australian Standards are developed and approved by technical committees, constituted of members representing national organisations including industry associations, government bodies, and universities. Compliance with Australian Standards is voluntary, unless they are called up in local, state, or Commonwealth regulations. Standards Australia also publishes lower consensus documents, including Technical Specifications and Handbooks.

# Introduction

The energy and electrotechnology industry in Australia is evolving at a rapid pace with the application of digital technology to traditional infrastructure changing business models, physical infrastructure requirements and presenting new security challenges for operators, business and consumers. Developments in electrical storage, new types of generation, the emergence of the 'Internet of Things (IoT),' changes in consumer preferences, and other drivers are encouraging innovation and adaptation of existing infrastructure to support new demands and directions.

The electricity grid is also rapidly evolving to include greater information and communications technology (ICT) to monitor and perform real-time control. As a result, the integration of computing and communication capabilities has opened the distributed energy grid to new vulnerabilities that can allow cyber attackers to inflict damage and disruption to critical infrastructure and management systems. With the rapid digital transformation taking over the energy sector, the power grid is shifting from its traditional centralised structure to become more decentralised. With this change comes the rise of a new generation of energy providers called 'prosumers' such as small and medium sized businesses and private homes, who not only consume electricity but also produce it through selling excess energy from their premises back into the grid.

Standards play a key role in supporting operation between technologies, providing consistent frameworks for design and implementation, and promoting safety. With the threat of cyber security causing global concern, the need to put appropriate standards in place to prevent and mitigate breaches to the energy network has never been so important.

In the energy sector, standards help set the requirements for the management of electricity markets, energy supply, and electricity metering among several other areas. Across the energy sector, both nationally and internationally, there are best practice principles relating to risk management, information security techniques, terminology and communication security. These standards have been developed through consensus by industry experts to achieve repeatable and consistent outcomes that increase efficiencies, promote safety and mitigate failure.

This discussion paper has been developed to support the planning of future national and international standards for cyber security of the distributed energy grid. It will also form the basis of discussions during the National Grid Cyber Security Forum to be held on **Thursday 18th October 2018**. Following the National forum, Standards Australia will compile the feedback to support the development of a Grid Cyber Security National Roadmap Report, to be released in December 2018.

We welcome responses on any matters outlined in this discussion paper. However, in light of the tight timeframes for consultation and compilation, we have set out questions to help focus submissions, and would also request feedback on topic areas outlined in Appendix A.

When submitting your feedback, please identify the company or organisation you represent (if any) and consider compiling responses from others within that organisation. Additionally, please inform us if we can publicise the name of your organisation/company as a participant in this process, and if we can publish your submission in its entirety.

The closing date for comment is **Friday 9 November 2018**.

# Stakeholder Consultation

Key stakeholders include consumers, industry, government, regulators and academia. As there are many new players in this industry, we would be very interested in feedback from companies, research institutions, and others who are looking at new technologies or approaches. However, we encourage submissions from all stakeholders. Over recent months, Standards Australia has held consultation meetings around the country in Perth, Adelaide, Brisbane, Melbourne, Canberra and Sydney to build awareness and consensus of critical issues for grid cyber security and the role of standards.

# Background

## What is the genesis for this project?

The Grid Cyber Security Roadmap represents an important component of the larger framework of the joint Electrical Network Transformation Roadmap between Energy Networks Australia (ENA) and the Commonwealth Scientific and Industrial Research Organisation (CSIRO). The Roadmap's stated objectives are:

*In this time of unprecedented change for global energy services, the Roadmap is designed to identify the preferred transition which the electricity network industry must make in the next decade, to be ready to support better customer outcomes under a diverse range of long-term energy scenarios.*

*By setting out a pathway for the transition of electricity networks by 2025, the Roadmap seeks to position network businesses and the whole energy supply chain for the future. The Roadmap also intends to support the evolving needs of customers, innovate and develop new services that customer's value and foster the long-term resilience and efficiency of Australia's energy system.*

*Stage 1 of the ENA/CSIRO Roadmap identified Standards as one important enabler to realise the various potential "futures" of the grid. Standards play a key role in enabling more interactive power systems by supporting operations between technologies, providing consistent frameworks for design and implementation and ensuring safety and security of supply. In fact, the integration of new technologies and distributed energy resources (DER) and interoperability will be fundamental to the performance of the power system of the future.*

Enhanced cyber security was identified as one of the key requirements identified through the Roadmap.

These challenges and potential future gaps in cyber security of the energy grid were also identified in Standard Australia's Roadmap for *Standards and the Future of Distributed*

*Electricity* published in May 2017 which was co-resourced with CSIRO and ENA. Recommendation 2 (ii) of the Roadmap identifies the need for future roadmapping in the area of cyber security for the energy grid. Subsequently, Standards Australia agreed with ENA to develop a Cyber Security for the Energy Grid Roadmap in 2018. The aim of the Roadmap is to assist Australian energy network providers with the challenges posed by cyber security.

## Summary of consultation meetings

There has been broad support for the Grid Cyber Security Project from government, industry and academia. Stakeholders have identified five key focus areas to be discussed at the upcoming consultations and the National Forum on Grid Cyber Security. These include Risk management, Infrastructure resilience, Terminology and Data management and Privacy. In addition stakeholders raised the need to consider hardware, software and supply chain standards to support the future of distributed energy networks in Australia.

Stakeholders agree that cyber security standards for the energy grid are of crucial importance not only for energy companies but also consumers, retailers and the broader economy in Australia. Trust was a consistent theme from consultation with stakeholders identifying internationally aligned standards as important to building confidence and support for the future energy grid. Stakeholders consistently voiced support for a descriptive risk based approach to cyber security rather than prescriptive standards. This is particularly important as the distributed energy system is changing with the emergence of prosumers and new players in an increasingly decentralised system.

Key areas of current vulnerability for the grid include structural change of the grid with greater interconnectivity, building management systems (BMS), Internet of Things (IoT), increased blurring of Operational Technology (OT) and Information Technology (IT) systems, and the rise of cybercrime as a business.

The importance of interoperable internationally aligned standards was supported by stakeholders across government, industry and academia. In addition, there is a need to focus on the training and development of internal and external staff and stakeholders to ensure proper awareness and cyber protocols are followed such as human resource management protocols, authentication protections and the alignment of internal Cyber Security Capability Maturity Models (C2M2) and incentive structures to mitigate cyber security threats.

The majority of Australian power utilities employ Supervisory Control and Data Acquisition (SCADA) systems and often the deployment lifetime of control system equipment is in the 10 to 20 year range. A key point raised by stakeholders was that even if new standards for all these management functions were available today, it would be many years before equipment supporting them would be deployed and some small simple devices such as Industrial Internet of Things (IIoT) devices are never likely to support complex features. In the meantime, stakeholders agree that a Grid Cyber Security Roadmap is needed to help prioritise and raise short, medium and long term standardisation efforts to support the energy system of tomorrow.

# Goals and outcomes

This discussion paper is intended to generate discussion prior to the upcoming National Grid Cyber Security Forum. During the forum, we will undertake the following activities:

### 1. Provide a snapshot of the current standards in the sector

This paper presents a snapshot of the current standards-based activities across a number of different topic areas (see Appendix A), and outlines Australia's relative level of involvement and engagement in those activities. This paper is also intended as a start to identifying any potential gaps in the market, to be further fleshed out during the forum.

### 2. Identifying the priority areas

Based on the analysis of current standards both nationally and internationally, Standards Australia will facilitate breakout sessions where stakeholders can discuss what the priority areas are. These breakout activities will see stakeholders split into groups, where they will discuss standardisation needs for 5 high level themes: (1) Infrastructure resilience, (2) Network and Power systems Communication, (3) Risk management, (4) Terminology and Data management, and (5) Privacy. These groups will discuss the standards needs across these categories, and report back to the group. This feedback will be recorded by Standards Australia and included in the final Grid Cyber Security Roadmap.

### 3. Further engagement

Based on a prioritisation of work, there may be areas which require further consultation and coordination at a future time. Furthermore, during the forum we will be discussing how to best achieve engagement in the existing standards work at the international level, and where standards do not currently exist, we will explore how they can most effectively be developed.

### 4. Next steps and timelines

During the forum we will discuss the next steps and timelines to achieve these outcomes. These will be captured in the Grid Cyber Security Roadmap.

# A Standards snapshot

Stakeholders within the energy and electrotechnology sector are highly engaged and active in the area of standards development. At the International Standardisation Organisation (ISO), International Electrotechnical commission (IEC), Australian stakeholders use their expertise to ensure regional, environmental or existing regulatory factors are considered and as a result, a number of international standards are adopted. International adoptions provide significant benefits to Australia, one of which is harmonisation which allows for ease of trade and alignment for common issues.

Standardisation activity in the area of grid cyber security is growing as the push for infrastructure resilience and effective and secure management controls for the grid becomes apparent. A number of key technical committees both in Australia and internationally have developed, or are currently developing, standards that allow for the protection of the grid.

Appendix A presents a 'snapshot' of the current standards and technical committees for each topic area. The information has been compiled by Standards Australia as part of a high level review to assist in your consideration of current and future standards needs. We also welcome your feedback on any additional information which we should include.

# Potential gaps and additional standardisation needs

While there are committees working on smart grid standards, stakeholders have identified that there is a need for future standardisation activity around the security of critical infrastructure and the effective management of data, among others, to support cyber security resilience of the energy grid.

As such, there is a need for collaboration across a number of different committees, including systems committee SYC Smart Energy, in order to develop standards and address key issues already highlighted. There is also a need to adopt a number of key standards to ensure an appropriate framework around risk management and system controls are in place.

# Feedback

Feedback from stakeholders will be used to inform the Standards Australia Grid Cyber Security Roadmap, which will be published by the end of the 2018 calendar year. We welcome responses on any of the matters outlined in this discussion paper and intend to go into further detail at our upcoming National Forum on **Thursday 18th October 2018**. To aid in discussion at the forum, we have set out questions to gain feedback on key topic areas. The questions have been outlined on page 8.

# Additional Resources

This paper is a start at providing background information on this area, particularly in relation to the relevant standards and technical committees. However, there are a number of additional resources which may be helpful in your consideration.

### Standards Development Public Portal

Full list of Standards Australia technical committees, including current projects, published standards, nominating organisations, and international relationships. www.sdpp.standards.org.au

### IEC Website

The IEC's website provides a full list of IEC Committees and sub-committees, including their work programs, current projects, and published documents. It also provides background and papers on various topics. www.iec.ch

### ISO Website

The ISO website provides a full list of ISO Committees and sub-committees, including their work programs, current projects, and published documents. www.iso.org

# Appendix A – Relevant Standards

In this appendix, a breakdown of the relevant standards have been listed in the below format. Questions have been added to the table below to obtain feedback from you on the relevant current standards and technical committees under each topic area.

<table>
<tr><td>Sub Topics</td><td colspan="2">• If you identify any additional sub topics which could be considered as part of this area, please include this in your response.</td></tr>
<tr><td rowspan="2">Committees operating in this functional area</td><td>Standards Australia Committees</td><td>International Committees</td></tr>
<tr><td>• Relevant Standards Australia committees.<br>• (A) signals Active<br>• (I) signals Inactive</td><td>• Relevant IEC committees.<br>• If they are mirrored by a relevant Australian committee, they will be in the same row.<br>• (P) signals Participating Australian relationship.<br>• (O) signals Observing Australian relationship.<br>• If they are mirrored by an Australian committee which is not directly relevant to the topic area, that committee will not be shown.</td></tr>
<tr><td colspan="2">• Question: Australian Committees: Do you feel that the committees are operating well in managing this area, are appropriately representative, and are their areas of work/functional scopes clear.<br>• If you would like further information, including the nominating organisations which sit on them, you can find that on our Standards Development Public Portal: www.sdpp.standards.org.au<br>• Question: IEC Committees: We ask you to provide your input on Australian participation on these committees – if we are currently contributors, do you feel we are active enough? If not, should stakeholders consider proposing that Australia should mirror that committee?<br>• If you would like further information on the IEC committees, the IEC's website provides work programs and scopes: https://www.iec.ch/dyn/www/f?p=103:6:0</td></tr>
<tr><td>Australian Standards in this functional area</td><td colspan="2">• Significant Australian or Australian/New Zealand specific standards which have been developed in this area, in addition to international standards which have been adopted here (either directly or modified for the Australian environment).<br>• Question: Are these standards current and appropriate? Do they allow for innovation?<br>• Please also consider if there are any additional standards which should be considered in the topic area.</td></tr>
<tr><td>IEC/ISO Standards in this functional area</td><td colspan="2">• Series of IEC standards which have been identified as being significant to this area.<br>• Question: Has Australia adopted sufficient IEC standards in this area?<br>• Please also consider if there are any additional standards which should be considered in the topic area.</td></tr>
</table>

## Infrastructure Resilience

A critical factor in keeping the energy grid secure from malicious intent is ensuring that the infrastructure supporting the grid is resilient. For this reason it is important that the design and construction of critical infrastructure, such as those used to generate, transmit and distribute energy is secure and resilient. At the moment, there is limited standardisation activity happening in this space with the most recent activity being on microgrids.

| | | |
|---|---|---|
| **Sub Topics** | • Energy Supply ( Generation, Transmission, Distribution)<br>• Microgrids<br>• Asset and Facilities Management | |
| **Committees operating in this functional area** | **Standards Australia Committees** | **International Committees** |
| | • EL-034 Power Quality (A) | • IEC TC 8 System aspects of electrical energy supply (P) |
| | • EL-064 Smart Grids (A) | • SC 8B Decentralised Electrical Energy Systems (O) |
| | • EL-042 Renewable Energy Power Supply Systems & Equipment (A) | • IEC TC 82 Solar photovoltaic energy (P) |
| | • EL-052 Electrical Energy Networks, Construction and Operation (A) | |
| | • EL-001-24 Generating Sets | |
| | • EN-001 Energy Auditing (A) | • ISO TC 301 Energy management and energy saving (P) |
| | • EN-004 Energy Network Management and Safety Systems (I) | |
| | • FP-017 Emergency Management Procedures (A) | • ISO TC 292 Security and Resilience (P) |
| | • MB-025 Security (A) | • ISO TC 251 Asset management (P) |
| | • MB-019 Asset Management (A) | • ISO TC 267 Facilities Management (P) |
| | • MB-022 Facilities Management (A) | |
| **Australian Standards in this functional area** | • AS/NZS 3010:2005 Generating Sets<br>• AS/NZS 4509 series Stand-alone power systems<br>• AS/NZS 4777 series Grid connection of energy systems via inverters<br>• AS/NZS 5033:2014 Installation and safety requirements for photovoltaic arrays<br>• AS 3745-2010 Planning for emergencies in facilities<br>• AS 5577:2013 Electricity network safety management systems<br>• AS ISO 55000:2014 Asset management - Overview, principles and terminology<br>• AS ISO 55001:2014 Asset management - Management systems – Requirements<br>• AS ISO 55002:2014 Asset management - Management systems -- Guidelines for the application of ISO 55001<br>• AS ISO 22301:2017 — Societal security - Business continuity management systems – Requirements<br>• AS ISO 22313:2017 — Societal security - Business continuity management systems – Guidance<br>• SA TS ISO 22317:2017 — Societal security - Business continuity management systems - Guidelines for business impact analysis (BIA) | |
| **IEC/ISO Standards in this functional area** | • IEC 60255 Measuring relays and protection equipment<br>• IEC/TR 62511 ed1.0 — Guidelines for the design of interconnected power systems<br>• IEC/TS 62898-1 Guidelines for general planning and design of microgrids<br>• IEC/TS 62898-2 Technical Requirements for Operation and Control of microgrids<br>• IEC/TS 62786 Distributed Energy Resources Interconnection with the Grid<br>• ISO 14084 series Process diagrams for power plants Requirements<br>• ISO 22316:2017 — Security and resilience — Organizational resilience — Principles and attributes<br>• ISO/TS 22318:2015 — Societal security - Business continuity management systems - Guidelines for supply chain continuity<br>• ISO 28000:2007 Specification for security management systems for the supply chain<br>• ISO 50001:2011 — Energy management systems — Requirements with guidance for use | |

## Network and Power Systems Communications

As the energy grid transitions from a 'one-way' power flow of energy to a 'two-way' flow, communication has never been more critical. International standards such as IEC 61850, IEC 62351 and IEC 62443 provide guidelines for effective communication among network and power systems. There is an opportunity for Australia to adopt these standards.

| | | |
|---|---|---|
| **Sub Topics** | • Network Communication<br>• Power System Control | • Smart Grids<br>• Metering |
| **Committees operating in this functional area** | **Standards Australia Committees** | **International Committees** |
| | • EL-011 Electricity Metering Equipment (A) | • IEC TC 13 Electrical Energy Management and Control (P) |
| | • EL-050 Power System Control and Communication (A) | • IEC TC 57 Power systems management and associated information exchange (P) |
| | • EL-052 Electrical Energy Networks, Construction and Operation (A) | |
| | • EN-004 Energy Network Management and Safety Systems (I) | |
| | • EL-062 Smart Grids (A) | • IEC PC 118 Smart grid user interface (P) |
| | | • ISO TC 184 Automation systems and integration |
| | | • IEC TC 72 Automatic electrical controls |
| | • IT-006 Industrial Process Measurement, Control and Automation (A) | • IEC TC 65 Industrial-process measurement and control (P) |
| **Australian Standards in this functional area** | • AS 5577-2013 — Electricity network safety management systems<br>• AS 61508 series Functional safety of electrical/electronic/programmable electronic safety related systems<br>• AS 1284 series Electricity metering<br>• AS 62052 series Electricity metering equipment (AC) - General requirements<br>• AS 62053 series Electricity metering equipment (AC) - Particular requirements<br>• AS 62054 series Electricity metering equipment (AC) - Tariff and load control<br>• AS 62056 series Electricity metering - Data exchange for meter reading, tariff and load Control<br>• AS ISO 14649.1:2004 Industrial automation systems and integration | |
| **IEC/ISO Standards in this functional area** | • IEC 61069 series Industrial-process measurement, control and automation - Evaluation of system properties for the purpose of system assessment<br>• IEC 61158 series Industrial communications networks - Fieldbus specifications<br>• IEC 61334 series Distribution automation using distribution line carrier systems<br>• IEC 61850 series Communication networks and systems for power utility automation<br>• IEC 61968 series Application integration at electric utilities - System interfaces for distribution management<br>• IEC 61970 series Energy management system application program interface<br>• IEC 62325 series Framework for energy market communications<br>• IEC 62351 series Power systems management and associated information exchange – Data and communications security<br>• IEC 62361 series Power systems management and associated information exchange - Interoperability in the long term<br>• IEC 62443 series Industrial communication networks - Network and system security<br>• IEC 62746 series Systems interface between customer energy management system and the power management system<br>• ISO 16484 series Building automation and control systems<br>• ISO/IEC 14908 series Information technology - Control network protocol | |

## Risk Management Techniques

The cyber security standards developed by ISO/IEC JTC 1 provide a robust toolkit for information security management. The key challenge is to leverage these techniques to maintain the availability and safety of control systems. There are a number of international and Australian adopted standards in this area, the key is to integrate security management technologies into critical infrastructure.

| | | |
|---|---|---|
| **Sub Topics** | • Cyber Security<br>• Information security<br>• Physical Security | |
| **Committees operating in this functional area** | **Standards Australia Committees** | **International Committees** |
| | • IT-012 Information Systems, Security and Identification Technology (A) | • ISO/IEC JTC1 SC27 Information Technology Security Techniques (P) |
| | • MB-025 Security (A) | • ISO TC 292 Security and Resilience (P) |
| | • OB-007 Risk Management (A) | • ISO TC 262 Risk Management (P) |
| | • CE-008 Chainlink Fabric Security Fences and Gates (A) | |
| **Australian Standards in this functional area** | • AS ISO/IEC 27001:2015 Information technology - Security techniques - Information security management systems<br>• AS ISO/IEC 27002:2015 — Information technology - Security techniques - Code of practice for information security controls<br>• AS ISO/IEC 27004:2018 — Information technology - Security techniques - Information security management - Monitoring, measurement, analysis and evaluation<br>• AS ISO/IEC 27035.1:2017.— Information technology—Security techniques—Information security incident management. Part 1: Principles of incident management<br>• AS ISO/IEC 27035.2:2017 — Information technology—Security techniques—Information security incident management, Part 2: Guidelines to plan and prepare for incident response<br>• HB 167:2006 Security risk management<br>• AS 1725.1-2010 Chain link fabric fencing - Security fences and gates - General requirements<br>• AS/NZS 3016:2002 Electrical installations - Electric security fences<br>• AS/NZS 4421:2011 Guard and patrol security services<br>• AS/NZS ISO 31000-2009 — Risk management - Principles and guidelines | |
| **IEC/ISO Standards in this functional area** | • IEC 62351 series Power systems management and associated information exchange - Data and communications security<br>• ISO/IEC 27000 series Information technology - Security techniques - Information security management systems<br>• ISO/IEC 27019:2017 Information technology - Security techniques - Information security<br>• ISO 18788:2015 Management system for private security operations - Requirements with guidance for use<br>• ISO 31000: 2018 Risk management - Guidelines | |

## Terminology and Data Management

An understanding of how data is generated and used is vital as the power grid becomes smarter. The data generated from networking devices such as meter and sensors can be transformed into analytics that impact strategic decision making. Standards relating to data management in the energy sector are limited and there is a need to collaborate with other sectors to develop and/or adopt standards in this area.

| | | |
|---|---|---|
| **Sub Topics** | • Vocabulary<br>• Frameworks | |
| **Committees operating in this functional area** | **Standards Australia Committees** | **International Committees** |
| | • EL-062 Smart Grids (A) | • IEC PC 118 Smart grid user interface (P) |
| | • JTC 1 SAC (Strategic Advisory Committee) (A) | • ISO/IEC JTC 1 Information Technology (P) |
| | • IT-012 Information Systems, Security and Identification Technology (A) | • ISO/IEC JTC1 SC27 Information Technology Security Techniques (P) |
| | | • ISO/IEC JTC1 SC32 Data management and interchange |
| | • MB-025 Security (A) | • ISO TC 292 Security and Resilience (P) |
| **Australian Standards in this functional area** | • AS 5711:2013 Smart grid vocabulary<br>• ISO 22300:2018 — Security and resilience — Vocabulary | |
| **IEC/ISO Standards in this functional area** | • IEC 62939-3 Smart grid user interface - Part 3: Energy interoperation services | |

## Privacy

As the grid transforms, it is important that exposure to privacy and personal data breaches are mitigated. Standards offer an avenue to provide guidelines on how to assist in meeting customer and community expectations pertaining to privacy.

| | Standards Australia Committees | International Committees |
|---|---|---|
| **Committees operating in this functional area** | • IT-012 Information Systems, Security and Identification Technology (A) | • ISO/IEC JTC1 SC27 Information Technology Security Techniques (P) |
| **Australian Standards in this functional area** | | |
| **IEC/ISO Standards in this functional area** | • ISO/IEC 27018:2014 Information technology - Security techniques - Code of practice for protection of personally identified information (PII) in public clouds acting as PII processors<br>• ISO/IEC 29100:2011 Information technology - Security techniques - Privacy framework<br>• ISO/IEC 29100:2011/Amd.1:2018 — Information technology — Security techniques — Privacy framework AMENDMENT 1: Clarifications | |

# Appendix B - Relevant Technical Committees

- **IEC TC 57: Power systems management and associated information exchange**

  **Scope:** To prepare international standards for power systems, control equipment and systems including EMS (Energy Management Systems) and SCADA (Supervisory Control and Data Acquisition).

  Australian Mirror Committee: EL-050

  https://www.iec.ch/dyn/www/f?p=103:7:0::::FSP_ORG_ID:1273

- **IEC TC 8 System aspects of electrical energy supply**

  **Scope:** Standardisation in the field of terminology for the electricity supply sector, systems network management, connection of network users and grid integration, as well as design and management of decentralised electricity supply systems e.g. microgrids and systems for rural electrification

  Australian Mirror Committee: EL-034

  https://www.iec.ch/dyn/www/f?p=103:7:0::::FSP_ORG_ID:1240

- **IEC SC 8B Decentralised Electrical Energy Systems (O)**

  **Scope:** Standards enabling the development of secure, reliable and cost-effective systems with decentralised management for electrical energy supply, alternative/ complement/precursor to traditional large interconnected and highly centralised systems.

  Australian Mirror Committee: EL-064 (Observer Membership Status)

  https://www.iec.ch/dyn/www/f?p=103:7:14408085223671::::FSP_ORG_ID,FSP_LANG_ID:20639,25

- **IEC PC 118 Smart grid user interface**

  **Scope:** Standardisation in the field of information exchange for demand response and in connecting demand side equipment and/or systems into the smart grid

  Australian Mirror Committee: EL-062

  https://www.iec.ch/dyn/www/f?p=103:7:0::::FSP_ORG_ID:8701

- **IEC TC 65 Industrial-process measurement and control**

  **Scope:** To prepare international standards for systems and elements used for industrial-process measurement and control concerning continuous and batch processes, carried out in the international fields for equipment and systems operating with electrical, pneumatic, hydraulic, mechanical or other systems of measurement and/or control.

  Australian Mirror Committee: IT-006

  https://www.iec.ch/dyn/www/f?p=103:7:0::::FSP_ORG_ID,FSP_LANG_ID:1250,25

- **IEC TC 13 Electrical Energy Management and Control**

  **Scope:** Standardisation in the field of a.c. and d.c. electrical energy measurement and control, for smart metering equipment and systems forming part of smart grids, used in power stations, along the network, and at energy users and producers

  Australian Mirror Committee: EL-011

  https://www.iec.ch/dyn/www/f?p=103:7:0::::FSP_ORG_ID,FSP_LANG_ID:1258,25

- **SYC Smart Energy**

  **Scope:** Standardisation in the field of Smart Energy in order to provide systems level Standardisation, coordination and guidance in the areas of Smart Grid and Smart Energy,

  Currently Australia is not represented in this systems work committee

  https://www.iec.ch/dyn/www/f?p=103:186:0::::FSP_ORG_ID:11825

- **ISO/IEC JTC 1 Information Technology**

  **Scope:** International standardisation in the specification, design and development of systems and tools dealing with the capture, representation, processing, security, transfer, interchange, presentation, management, organisation, storage and retrieval of information

  Australian Mirror Committee: JTC 1 SAC (Strategic Advisory Committee)

  https://www.iec.ch/dyn/www/f?p=103:7:14408085223671::::FSP_ORG_ID,FSP_LANG_ID:3387,25

- **ISO/IEC JTC 1 SC27 Information Technology Security Techniques**

  **Scope:** The development of standards for the protection of information and ICT. This includes generic methods, techniques and guidelines to address both security and privacy

  Australian Mirror Committee: IT-012

  https://www.iec.ch/dyn/www/f?p=103:7:14408085223671::::FSP_ORG_ID,FSP_LANG_ID:3401,25

- **ISO/IEC JTC 1/SC 32 Data management and interchange**

  **Scope:** Standards for data management within and among local and distributed information systems environments. With specific focuses on frameworks, data structures and definitions.

  Currently no Australian Mirror Committee

  https://www.iso.org/committee/45342.html?view=participation

- **ISO TC 292 Security and Resilience**

  **Scope:** Standardisation in the field of security to enhance the safety and resilience of society.

  Australian Mirror Committee: MB-025

  https://www.iso.org/committee/5259148.html

- **ISO TC 262 Risk Management**

  **Scope:** Standardisation in the field of risk management

  Australian Mirror Committee: 0B-007

  https://www.iso.org/committee/629121.html

- **ISO TC 184 Automation systems and integration**

  **Scope:** Standardisation in the field of automation systems and their integration for design, sourcing, manufacturing, production and delivery, support, maintenance and disposal of products and their associated services. Areas of Standardisation include information systems, automation and control systems and integration technologies.

  Currently no Australian Mirror Committee

  https://www.iso.org/committee/54110.html

- **ISO TC 301 Energy management and energy saving**

  **Scope:** Standardisation in the field of energy management and energy savings

  Australian Mirror Committee: EN-001

  https://www.iso.org/committee/6077221.html