Standard for Intelligent Electronic Devices (IED)

These standards created and made available are for the construction of Ergon Energy infrastructure. These standards ensure meeting of Ergon Energy's requirements. External companies should not use these standards to construct non-Ergon Energy assets.

If this standard is a printed version, to ensure compliance, reference must be made to the Ergon Energy internet site www.ergon.com.au to obtain the latest version.

Approver	Jason Hall
If RPEQ sign off required insert details below.	
Ergon Energy	
Certified Person name and Position	Registration Number
Not Required	Not Required

Abstract: Standard to define common attributes required by intelligent electronic devices if they are to be connected to Ergon Energy's communications and power networks.

Keywords: IED, Standard, Communications, Security, Data

Standard for Intelligent Electronic Devices (IED)

For definitive document version and control detail, please refer to the information stored on the Process Zone.

Revision history

Revision date	Version number	Author	Description of change/revision
24 August 15	1.0	Tendai Chadyiwa	Initial Release

Document approvals

Name	Position title	Signature	Date
Jason Hall	GM Engineering Standards and Technology	STNW3383_GM Approval.pdf	31 August 15

Stakeholders / distribution list

Name	Title	Role
Rob Coggan	Manager Substation Standards	For Information
Carmelo Noel	Manager Distribution Standards	For Information
Greg Nelson	GM Network Monitoring and Processing	For Information

Table of Contents

Standard for Intelligent Electronic Devices (IED)

1 Overview

1.1 Purpose and scope

This document defines the Ergon Energy Operational Communications Network (OCN) IED standard. IED stands for any intelligent electronic device that is installed on Ergon Energy's power network. It provides IED specifications for successful integration of IEDs into the Ergon Energy OCN. This standard applies to all IEDs on Ergon Energy's OCN network. Revenue Metering IEDs are excluded from this standard as they are addressed in a different standard due to the unique regulatory requirements.

Requirements in the following critical areas of the IED integration process are specified in this standard.

- Communications
- Security
- IED data collection
- Device health
- Configuration management
- Asset management

This standard should be applied across Ergon Energy in all cases where an IED procurement specification is being developed and in technical evaluation of all IEDs.

If the IED fails to meet all the mandatory requirements herein and exceptional circumstances warrant the IED's use on Ergon Energy's power network, then an application for exemption should be made to the Group Manager Engineering Standards and Technology detailing the exemption/s being sort and the associated circumstances warranting the exemption/s.

2 Responsibilities

The EGM Network Optimisation is the process owner responsible for approving this standard.

OT Engineers and Specialists - Operational Technology is responsible for maintaining this standard.

OT Engineers and Specialists - Operational Technology personnel are the subject matter experts (SMEs) for the content in this standard.

3 References

3.1 Ergon Energy controlled documents

Document number or location (if applicable)	Document name	Document type
NA000403R479	This standard **supersedes** the Ergon Energy IED Guidelines	Guideline

3.2 Other documents

Document number or location (if applicable)	Document name	Document type
IEEE 1686-2007	IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities– section 5.2.2	External Standard

4 Legislation, regulations, rules, and codes

This document refers to the following: Nil

5 Definitions, acronyms, and abbreviations

5.1 Definitions

For the purposes of this standard, the following definitions apply:

Term	Definition
Base FX	Single mode fibre ethernet interface, running at a speed (MB) value denote by the number before the word Base
Base SX	Multimode fibre ethernet interface, running at a speed (MB) value denote by the number before the word Base
Base T	Twisted pair ethernet cable, running at a speed (MB) value denote by the number before Base

5.2 Acronyms and abbreviations

The following abbreviations and acronyms appear in this standard.

Term, abbreviation or acronym	Definition
ADAS	Alternative data acquisition service
AMI	Advanced metering information
APN	Access point name
ASCII	American Standard Code for Information Interchange
CNOC	Communications network control centre
DH	Group: 2, authentication
DHCP	Dynamic host configuration protocol
DOS	Denial of service
DSCP	Differential services code point
EKE	Encrypted key exchange
GUI	Graphical user interface

Term, abbreviation or acronym	Definition
ICCID	Integrated circuit card identifier
ID	Identity
IED	Intelligent electronic device
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet engineering task force
IMEI	International mobile equipment identity
iNOC	Integrated network control centre
IP	Internet protocol
IRIG-B	Inter-range instrumentation group
LAP-D	Link access protocol D type
MAC	Media access control address
NAT	Network address translation
NTP (V3)	Network timing protocol version 3
OCN	Operational communications network
PFS	Perfect forward secrecy
RADIUS	Remote authentication dial in user service
RFC	Request for comments – reference to standards set by IETF followed by the standard number after the abbreviation
SHA	Secure hash algorithm
SME	Subject matter expert
TACACS+	Terminal access controller access-control system plus
TCP	Transmission control protocol
UDP	User datagram protocol
VPN	Virtual private network
WAN	Wide area network

6 Communications

Ergon Energy currently uses a wide range of communications network technologies including cellular, satellite, radio and ethernet based WANs to communicate with IED's on the Operational Communications Network (OCN). Some of these services are provided directly by Ergon Energy whilst external services such as NextG and satellite based services are also utilised for specific purposes. While serial communications have traditionally been used to provide connectivity to IEDs by way of terminal servers, due to the increasing requirements around the collection of IED data, Ergon Energy is moving to the internet family of protocols (TCP/IP/UDP etc.). This will facilitate higher bandwidth communications. This section specifies communications requirements for IED's connecting to the Ergon Energy network.

6.1 Field (distribution network) IED's

Ergon Energy has standardised on cellular communications as its primary field solution. Ergon Energy has standardised on a single external cellular modem type, specifically the Cybertech modem. No vendor specified external modem types shall be acceptable as part of a vendor IED solution where a single type of external cellular modem type is used. Due to Ergon Energy's geographical reach, areas outside of cellular coverage will be connected via satellite. The satellite communications connection will have a dedicated Ergon Energy supplied modem that connects to the IED via an ethernet connection. The ability to support both cellular and ethernet connectivity via either of the following methods is mandatory,

- Cellular and ethernet WAN interfaces integrated on-board within the IED
- Separate IED models with either integrated on-board cellular or ethernet WAN interfaces
- Standalone ethernet WAN interface

To be considered a cellular interface and not a cellular modem the cellular device must be integrated with the device board and must not be an external modem mounted in the vendor provided IED enclosure.

6.2 Substation IED's

For substation IED's connecting to the Ergon Energy OCN the following communications preferences exist in order of most desirable to least desirable.

- Ethernet interface
- Cellular interface

6.3 Cellular interface requirements

6.3.1 Mandatory

The following requirements are mandatory for IED cellular interfaces:

6.3.1.1 Packet data technology standard

The cellular interface shall support at a minimum the HSPA standard.

6.3.1.2 Frequency support

The cellular interface shall support communications in the following frequency bands:

- 850 MHz

- 900 MHz
- 1800 MHz
- 2100 MHz

6.3.1.3 Remote and local reset

- The IED shall support the ability to reset the cellular interface via SMS
- The IED shall support some form of watchdog timer / keep alive status that resets the cellular interface on loss of communications.

6.3.1.4 RADIUS authentication

The IED shall support authentication to the cellular network via the RADIUS protocol.

6.3.2 Highly desirable

The following features are required for IED cellular interfaces:

Remote configuration via SMS: The IED shall support the ability to set the following connectivity parameters via SMS:

- Network APN
- RADIUS username and secret

In addition, the modem shall be able to authenticate and authorise remote commands sent via SMS.

6.4 Ethernet interface requirements

6.4.1 Mandatory

The following requirements are mandatory for IED ethernet interfaces. The interface shall have the ability to support speed / duplex auto-negotiation and hardcode speed/duplex settings:

- Copper connector support: 8P8C connector
- Speed: 10 Base T,100 Base TX

And /or

- Fibre connector support
- Speed: 10 Base FL, 100 Base SX, 100 Base FX, 1000 Base SX or 1000 Base FX

6.5 Internet protocol requirements

All IED's shall preferably be equipped for IP-based communications.

The mandatory requirements for IP-based communications are as follows:

- IPv4
- Static IP addressing and/or DHCP or PPP (as appropriate) client for IP configuration.
- Quality of service support via IP DSCP Bits

7 Security

The following section addresses the requirements to ensure the availability, integrity, authenticity and confidentiality of IED's and IED data on the Ergon Energy OCN.

7.1 IED user interface structure

7.1.1 Minimum IED interface functions

The following IED user interface structure complies with the IEEE 1686-2007 standard and represents the minimum interface functions for IED's connected to the Ergon Energy OCN network.

- View data - View data refers to the ability to view substation operational data (voltage, current, power, energy, status, alarms, etc.) of the IED.
- View configuration settings - View configuration settings refer to the ability to view configuration settings of the IED such as scaling, communications addressing, programmable logic routines, and the firmware version numbers.
- Force values - Force values refer to the ability to manually override real data with manually inputted data and/or the ability to cause a control output operation to occur.
- Configuration change - Configuration change refers to the ability to download and upload configuration files to the unit and/or effect changes to the existing configuration.
- Firmware change - Firmware change refers to the ability to load new firmware and the ability to run a specific firmware version that is resident on the device.
- ID/secret/secret management refers to the ability to create, delete, or modify secrets/secret and/or secret/secret authorization levels.
- Audit log - Audit log refers to the ability to view and download the audit log.
- Polling and reporting by exception capability for a selection of device parameters.

7.1.2 Minimum IED authorisation structure

The following IED authorisation structure represents the minimum IED authorisation structure for IED's connected to the Ergon Energy OCN network.

- Read access level - Read access gives the ability to view all configuration settings and data on the IED.
- Read/write access level - Read/write access gives the ability to do a single setting configuration change (mandatory), download configuration files from the IED (mandatory), upload configuration files(optional) and force values(optional)
- IED admin access level – Has the ability to change any setting on the IED including communications interface and security settings.

7.2 Shared secret

7.2.1 Secret complexity

User-created secrets shall follow a set of rules that must be adhered to in the creation of each secret.

Ideally a minimum of eight (8) characters shall be used. When encoding secrets in plain text, preference shall be given to IEDs allowing secrets containing the following:

- At least one uppercase and one lower case letter
- At least one number
- At least one non-alphanumeric character (e.g., @, %, &, *, etc.)

7.2.2 Shared secret defeat mechanisms

The IED shall have no means, undisclosed to Ergon Energy, whereby the user-created ID/shared secret control can be defeated or circumvented. This includes but is not limited to the following mechanisms and techniques,

- Embedded master secret.
- Chip-embedded diagnostic routines that automatically run in the event of hardware or software failures.
- Hardware bypasses of secrets such as jumpers and switch settings.
- Local secrets should not be visible to users logged onto IED.
- Secrets and keys required for authentication to network or encryption shall not be visible to users logged onto the IED.

7.2.3 User activity timeout

The IED shall have a time-out feature that automatically logs out a user who has logged in after a period of user inactivity. The period of time before the time-out feature activates shall preferably be user configurable and range from one (1) and 30 minutes in one (1) minute intervals.

7.3 User to IED authentication

Preference should be given to implementations closest to the following, which are the ideals for user authentication.

7.3.1 Direct IED interface access

All direct user access to IED's shall be authenticated and logged via one of the following centralised authentication methods:

- IETF Remote authentication dial in user service (RADIUS)
- Terminal access controller access-control system plus (TACACS+)

7.3.2 Local authentication fall-back

An IED configured to use centralised authentication when connected to the network shall automatically fall back to using local username and secret when network connectivity to the centralised authentication infrastructure is down.

7.3.3 IED configuration system

It is a requirement that any vendor provided centralised IED configuration application offers some if not all of the following capabilities,

- The ability to integrate with LDAP/active directory to offer group based access level control to IEDs.
- User access to IED is logged centrally.
- Authentication between management application and IED can be via shared secrets.
- Ability to remotely change local IED secret. This should preferably be easily achievable for one (1) IED or a group of IEDs.

7.4 IED accounting

The preferred IED audit log format would contain the following records as per “IEEE 1686-2007 Section 5.2.2”:

- Event record number
- Time and date
- User ID
- Event type

As a minimum the following actions shall be logged against User ID/ timestamp:

- Sign in
- Update settings
- Update firmware
- Sign out

Preference shall be given to an IED that can send its local accounting information to a centralised logging system via one of the following methods:

- SNMP traps
- Syslog
- DNP3

7.5 IED time synchronisation

The IED shall synchronise its internal time clock with one of the Ergon Energy methods currently in use. The following protocols are supported for IED time synchronisation

- IEEE 1588-2008 or later Precision Timing Protocol
- RFC1305 Network Timing Protocol (NTP) V3 or higher.
- IRIG-B

7.6 IED connectivity architectures

It will be possible (and sometimes desirable) for IEDs to communicate directly with each other rather than via a central application or management platform. However there are significant security risks to Ergon Energy’s operational environment if peer to peer IED communications are allowed. Due to the multiple different underlying telecommunications solutions being used, it is necessary to put some controls on this communication where there is reasonable risk that a connected IED can be spoofed by a rogue device.

Listed below are some examples of potential risks of a rogue device connecting to some of the various OCN access technologies.

- Rogue device probes/attacks firmware vulnerabilities of IED/modem devices connected to cellular or satellite VPN causing loss of communication to IED.
- Rogue device hacks firmware vulnerabilities of IED/modem devices connected to cellular or satellite VPN allowing them to take control of the modem/IED.
- Rogue device runs secret/secret dictionary attack on IED/modem devices connected to cellular or satellite VPN allowing them to take control of the modem/IED.

- Rogue device launches denial of service (DOS) attack on of IED/modem devices connected to cellular or satellite VPN causing loss of communication to IED.
- Rogue device sends large amount of data over cellular/satellite service causing large financial penalty from cellular provider.

As such Ergon Energy has defined the following IED connectivity models and the security requirements for each one.

7.6.1 Isolated IED connectivity

This is the default connectivity type for all IED's connected to the Ergon Energy OCN.

Any IED connected to the Ergon Energy OCN with no requirement to communicate directly with IEDs within the same network as itself, should be connected as an isolated IED.

An isolated IED on the Ergon Energy OCN network is defined as, "An IED that can only communicate via a head end security gateway to another IED within its own VPN or a backend system".

7.6.2 Community IED connectivity

On some occasions it may be necessary for IED's to have direct communications with other IED's on the same network due to network latency or timing requirements. In this case the IEDs will be connected to the network in some community architecture form. Due to the risks to other community connected IED's from a rogue community connected IED within the same VPN it is necessary to enforce more stringent network access requirements on these IEDs.

Below are the approved methods of ensuring the identity of community IEDs connecting to the Ergon Energy OCN.

7.6.2.1 Network access control

The device should have a method of securely authenticating itself to the network it is connecting to before being allowed to pass data on that network.

7.6.2.2 Inter IED authentication

It is expected that if the application allows IEDs to directly communicate with each other, then the IEDs will have the ability to securely authenticate each other before communication.

7.7 Privacy of network traffic

Where exceptional circumstances warrant end-to-end data encryption for IED links over a public network, the following requirements will apply.

7.7.1 IPSEC requirements

For IEDs requiring encryption back to a security gateway device the following IPSEC requirements apply:

- IKE Phase 1 (Encryption algorithm: AES256, Hash algorithm: SHA1, DH Group: 2, Authentication: X.509 based digital certificates, NAT Traversal)
- IKE Phase 2 (Encryption algorithm: AES256, Hash algorithm: SHA1, PFS Group: 2)

7.7.2 Transport layer security requirements

For IEDs requiring end-to-end application encryption the following requirements apply:

- Implementation of TLS v1.1 or above

8 IED operational data collection

The Ergon Energy operational environment provides three different data collection and storage systems for operational IEDs. These are the only systems available and operational IEDs shall not directly connect to other systems (e.g. vendor research systems) for the purposes of data collection and storage. Determining which system/s to use will depend on the operational role of the IED.

8.1 Supervisory control and data acquisition (SCADA)

The SCADA system is used to collect critical data from IED's within the Ergon Energy operational network. The Ergon Energy SCADA system only supports the DNP3 protocol for both polling and reporting by exception and the ICCP protocol for information exchange at the system level.

8.2 Alternative data acquisition service (ADAS)

The Ergon Energy ADAS system is used to collect non-critical data from IED's within the Ergon Energy operational network. The following protocols are supported by the Ergon ADAS system in both polling and report by exception modes:

- DNP3
- OPC
- IEC 61850 MMS
- Modbus RTU
- Modbus/TCP
- Modbus ASCII

8.3 Advanced metering infrastructure (AMI)

The AMI is used to collect and manage data associated specifically with metering IEDs. Due to the unique requirements in the revenue metering area, IEDs that potentially will use the AMI will need to be reviewed and approved by Ergon Energy's Network Monitoring and Processing group.

8.4 IED data to multiple systems

For certain IEDs it will be expected that critical operational data (usually associated with the HV network) will go directly to the SCADA system. However other operational data (event logs, other non-critical sensor data etc.) will be collected in ADAS. As such, it is preferred that IEDs can make independent connections and send data to both of the systems as depicted in Figure 1.

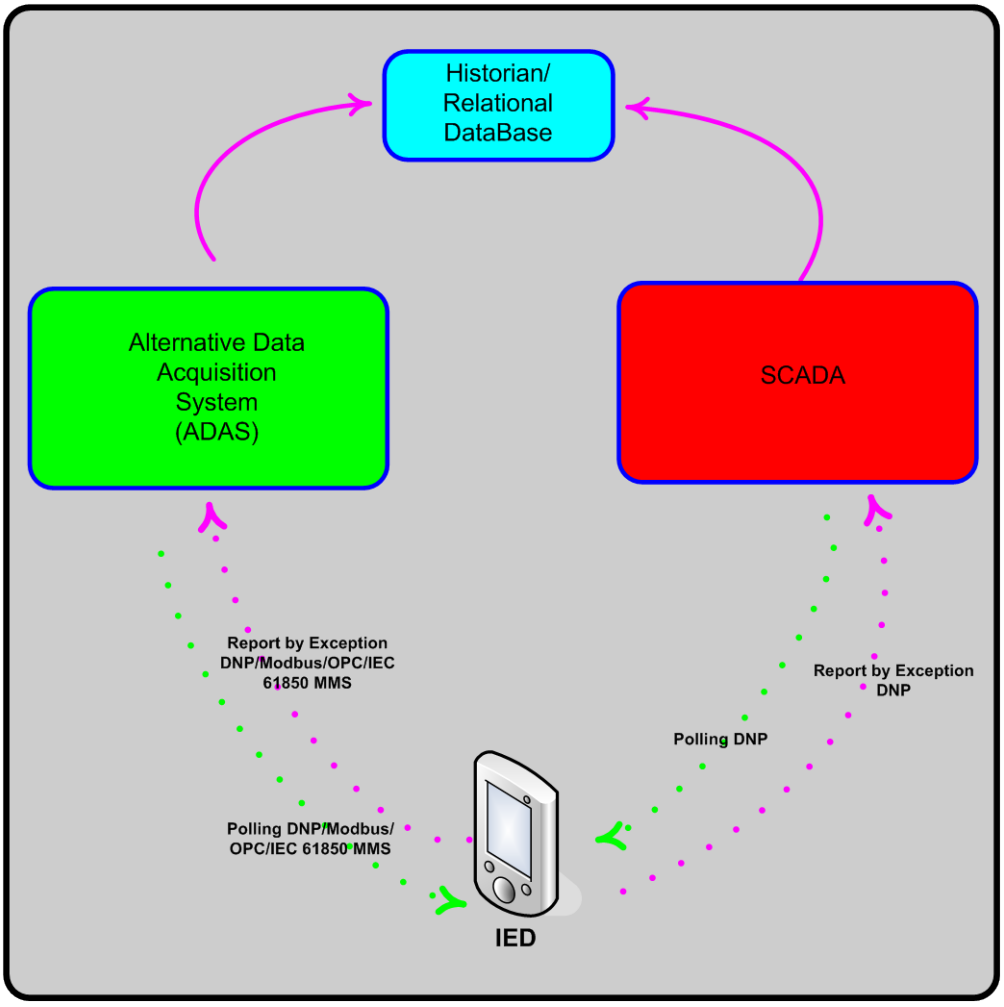

Figure 1: Standard IED operational data support model

9 Device health

Each device is expected to provide some form of device health information. Device health is important for the identification of performance issues that may lead to device failure or abnormal operation. There are two approaches to device health:

- Proactive management and
- Failure recognition

9.1 Proactive management (preferred)

Proactive management refers to actively polling or having a device report on parameters that when outside a certain range could indicate the future inability of a device to fulfil its function within the system. Proactive management is the preferred approach to device management for Ergon Energy IED's. Examples of proactive management include:

- Polling a device interface for errors.
- Having a device report by exception when it's processor utilisation or communications link errors exceeds a certain threshold.

9.2 Failure recognition (minimum required)

Failure recognition refers to the ability of a system to detect a total failure of a device within the system. Examples of failure recognition include:

- Failure of a device to respond to SNMP/DNP3/Modbus or ICMP (ping) polling
- Device-dying-gasp functionality
- Device watchdog alarm

It is a requirement for devices connecting to the Ergon Energy OCN to at least support one of the above device failure recognition capabilities. Preference shall be given to devices that have comprehensive failure recognition functions.

9.3 Communicating device health information

Ergon Energy has a centralised device health alarm support system. This is referred to as the integrated Network Operations Centre (iNOC). The preferred method is that IED's can communicate directly with the iNOC for device health. However it is recognised that not all IED's have advanced IT capabilities and therefore their device health information will be transmitted to the iNOC via the SCADA, ADAS or AMI infrastructure. The following device health methods/modes are supported by Ergon Energy.

9.3.1 Report by exemption

- SNMP/ Syslog traps/Modbus to iNOC
- DNP3/Modbus/Conitel to SCADA
- DNP3/ OPC/ IEC 61850/Modbus to ADAS

9.3.2 Polling

- SNMP- direct/Modbus from iNOC
- DNP3/Modbus/Conitel from SCADA
- DNP3/ OPC/ IEC 61850/Modbus from ADAS
- ICMP (ping)

10 Configuration management

Configuration management when applied over the life cycle of a system or IED provides visibility and control of its performance, functional and physical attributes. A configuration management system saves time and money during troubleshooting of operational issues by visibly tracking changes to systems or IED's. This section prescribes rules around the procurement of systems aimed primarily at collecting and tracking changes to IED configurations.

It is expected that the configuration tool will operate in a centralised configuration and not require local installations of the tool for configuration of the IED. The following are the minimum requirements for a proprietary centralised configuration management solution.

10.1 IED configuration functionality

The proprietary centralised configuration management system shall support the following requirements.

10.2 Mandatory

- Upload configuration from IED
- Compare configuration with known good configuration and report on differences
- Upload event logs
- Do single setting changes
- Retrieve firmware version
- Upload a complete firmware version to the IED

The functionality above shall be supported on a scheduled or ad-hoc basis.

10.3 Minimum requirements

- IED firmware update that is capable of being initiated locally and preferably remotely. This shall preferably be supported by the IED having the capability to store two consecutive firmware versions at any given time with the latest version being the active one and the older version being the default in the event of malfunction of latest version.
- Full IED configuration download
- Support of bulk change functionality to roll out same change to multiple IEDs

10.4 Authentication

Refer to User to IED authentication requirements in Section 7.3.

10.5 Authorisation

The proprietary centralised configuration management system shall support the Authorisation Levels specified in Section 7.1.

10.6 Accounting

The Proprietary Centralised Configuration Management System shall support logging of the same accounting information specified in Section 7.4.

10.7 Reporting

The proprietary centralised configuration management system shall support the following reporting requirements on a scheduled and/or ad-hoc basis.

- Deviation from known good configuration
- Settings/configuration changes
- Firmware version report

The capability to automatically send reports via SMTP to a designated user will be a preferred function.

10.8 Change management approval system

It is desirable that the proprietary centralised configuration management system support the ability for users to schedule changes and have those changes approved within the system by a designated responsible person prior to change execution.

10.9 Local IED management

In the case where the user has no access to a centralised configuration management system IED access shall be via at least one of the following methods.

For security reasons, Ergon Energy will only accept configuration of an IED whilst connected to the OCN (i.e. the user is authenticated). The acceptable methods are:

- Command line using SSH
- Graphical user interface using HTTPS

10.10 Initial configuration access (all IED's)

The IED shall support either of the following methods of setting initial connectivity parameters on the IED.

Console interface

The IED provides terminal access via a console port (serial or USB) allowing for setting of an IP address on the ethernet/cellular interface where further configuration can be supported via GUI/ command line or configuration upload.

Ethernet interface/DNP3/Modbus

The IED is configured with a default DNP3/Modbus address and secret for initial configuration purposes in the case of DNP3/Modbus. The ethernet interface the IED should be DHCP capable.

11 Asset management

To enable the management of IEDs connected to the Ergon Energy OCN, certain information is required to be kept from an operational technology point of view. It is preferred that the following IED information be accessible/obtainable, where possible, via remote engineering access.

- Device serial number
- Operational communications name – assigned by Ergon Energy's CNOC/iNOC
- Manufacturer name
- Model number
- Manufacture date
- Firmware version
- Software version
- SIM card ID (ICCID) – cellular IED's
- Cellular service number – service phone number
- International mobile equipment edentity (IMEI Number) - cellular IED's
- Device IP address
- Device MAC address