Standards Development for Low Voltage Monitoring

Electricity Authority

Open Networks - Standards Forum 5/8/2020

Rodger Griffiths,

GM Assets and Engineering, Westpower

GM ElectroNet Technology

What standards are important for any LV monitoring and control?

An EDB perspective

Background and outline

Talked about at the last forum:

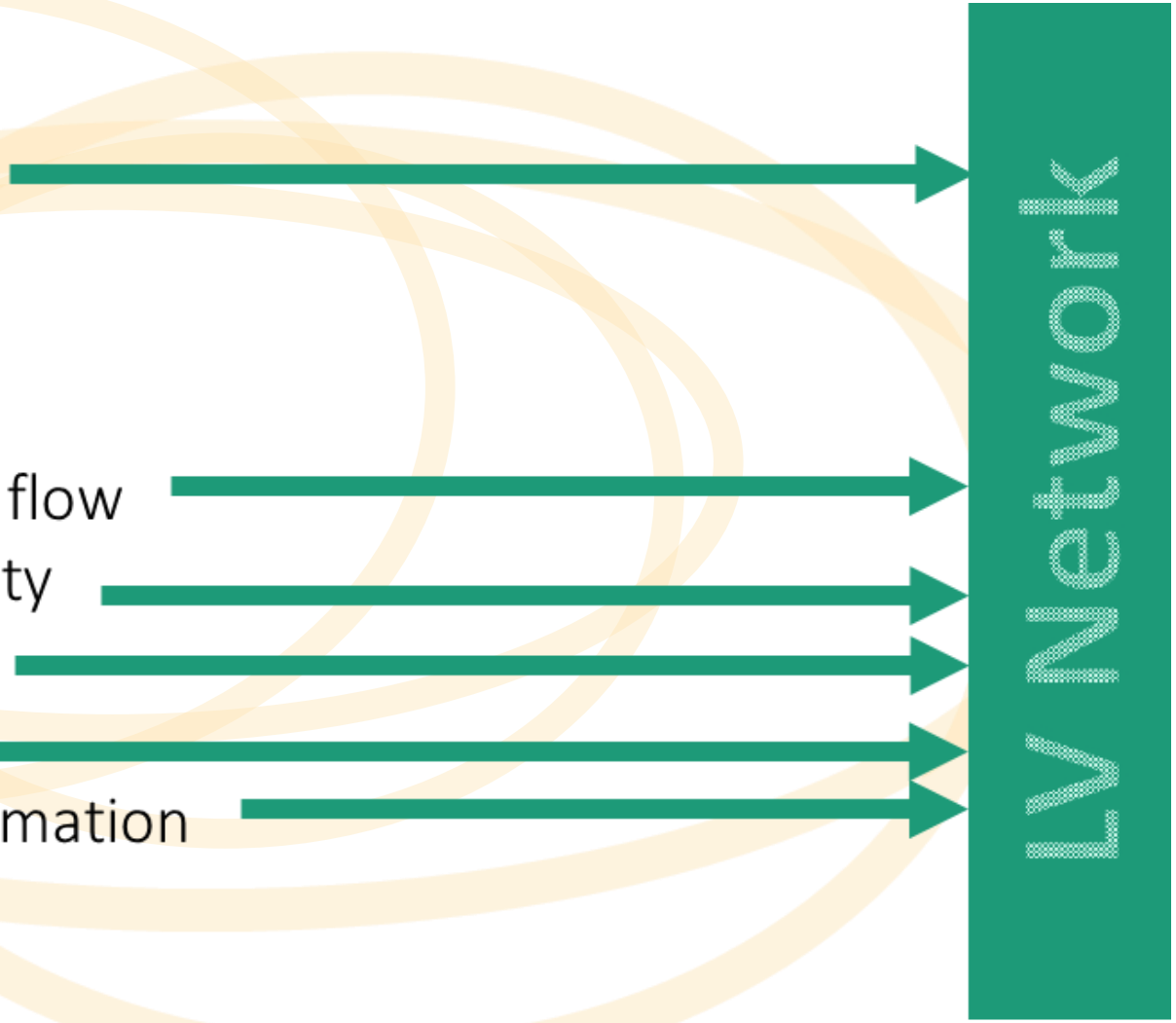
- Technical Equipment standards (AS/NZ)
- Regulations (safety)
- Industry rules (code)
- EDB requirements

For the environment we're talking about, we'll need additional standards, agreements and processes

- Safety and Compliance Standards
- IOT requirements and standards
- Data requirements and standards

Industry Challenges

- We are facing multiple challenges:
  - New DER technologies
    - Exponential EV Growth
    - More Distributed Generation
    - Energy storage
  - Peer-to-peer trading, two way power flow
  - Locus shift from asset to data centricity
  - Optimisation of aging infrastructure
  - Increased safety expectations
  - Regulatory focus on network transformation



Challenge

To gain true visibility and control
at the LV network level

Solution

An innovative IoT based LV network data collection, mining and control system with edge intelligence.

Based on DSO Endpoints

A NZ Solution

- Need near real time data on LV network performance and power flows
- Need reliable and cost-effective but low capacity two-way communication system
- Need to be able to manage load at multiple levels (GXP, Feeder, Zone Sub, Distribution Sub, LV Feeder, Installation and Load)
- Can be cloud-based or in-housed

PowerPilot

Equipment we wish monitor and control

Industry rules and standards for installed equipment which we wish to monitor and/or control

- **AS/NZ 4755** – especially **4755.3.5**, Demand response capabilities and supporting technologies for electrical products, Part 3.5: Interaction of demand response enabling devices (DREDs)and electrical products—Operational instructions and connections for grid connected electrical energy storage (EES) systems.
- **EIPC code – part 6** (Connection of distributed generation) under review, and some of **part 8** (Common quality); What about other standard formats around data – could we re-use something we already have within the industry as a model? More of that later.
- Communication systems perform to standards according to the **LoRaWAN Alliance**; using 865MHz and can interface with Spark 923MHz

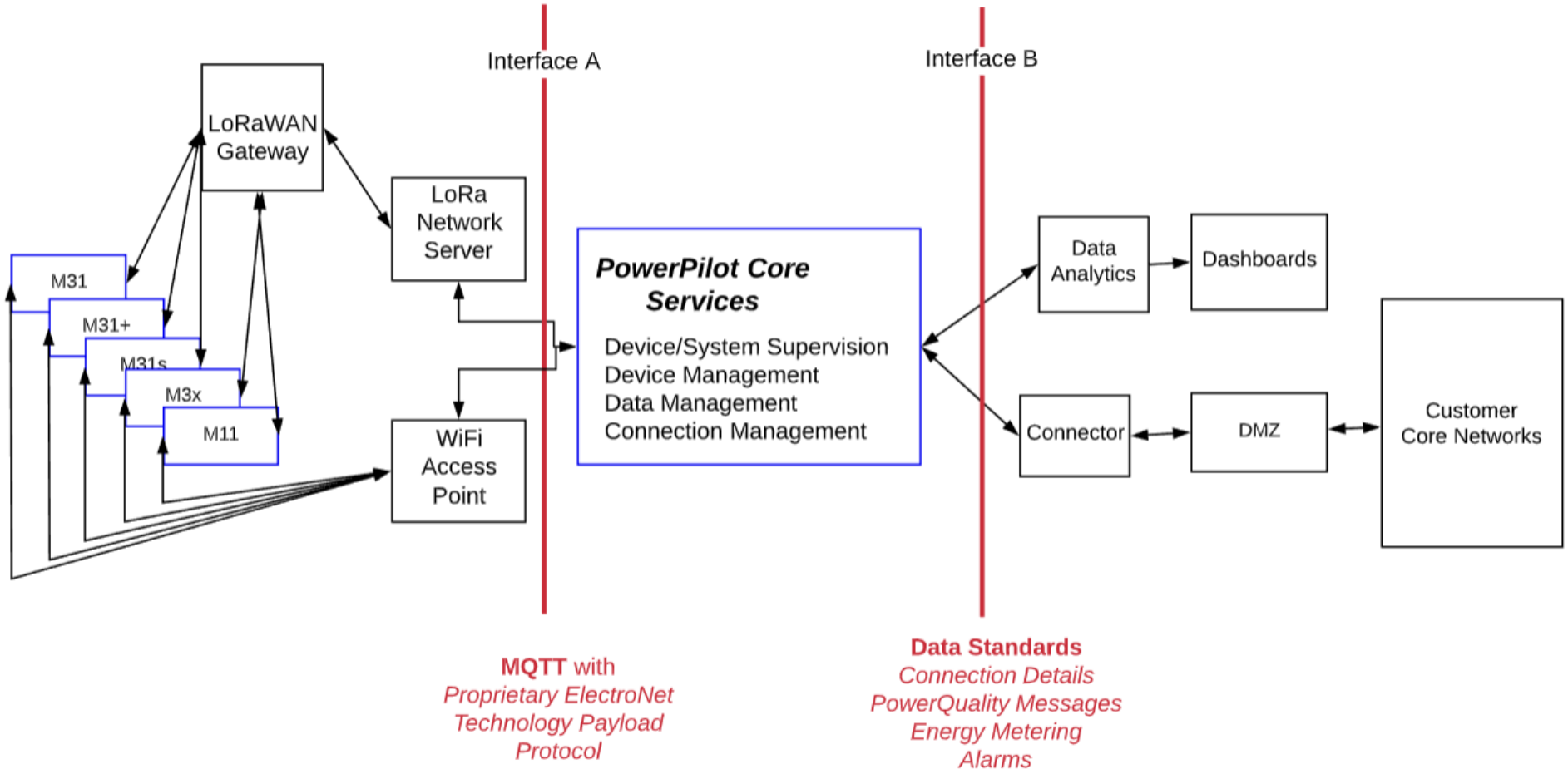
Technical Equipment Standards (AS/NZ/IEC) and Safety Regulations for equipment to be installed on our networks

We need equipment we install either on our network equipment or in customer's premises to comply with technical equipment standards and safety regulations for electrical safety reasons.

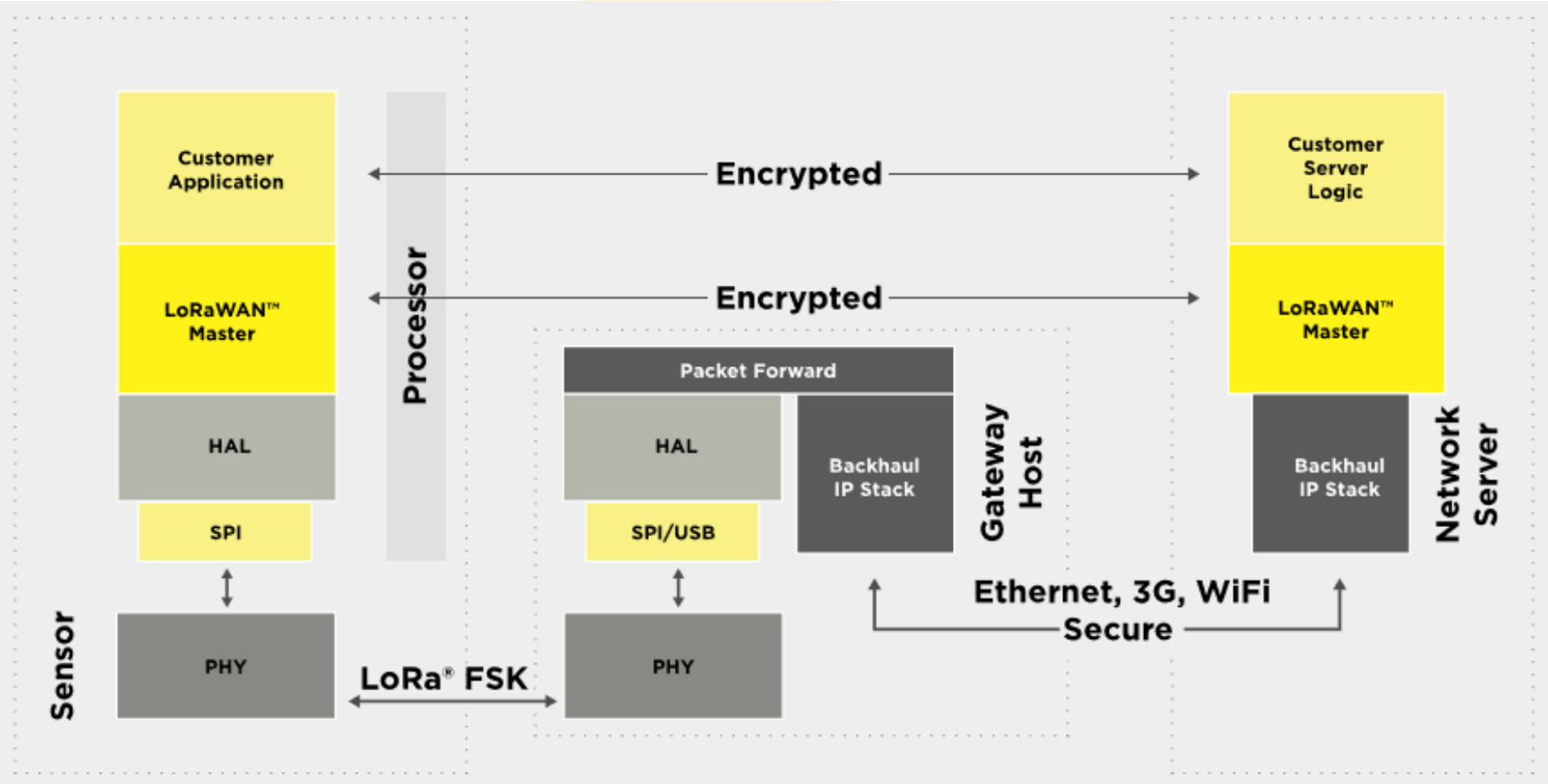
Examples are:

- **AS/NZ 3000** - requirements for the design, construction and verification of electrical installations, including the selection and installation of electrical equipment forming part of such electrical installations. In addition, guidance is provided so that the electrical installation will function correctly for the purpose intended and takes into account mitigating the foreseeable adverse effects of disruption to supply.
- **AS/NZS 3820** – Essential safety requirements for electrical equipment
- **IEC 61326** – EMC compatibility - provide the information for industrial, scientific and medical equipment for the radio disturbance characteristics for electromagnetic compatibility compliance. We picked levels appropriate for an industrial environment
- **IEC 62053-21** – Electricity metering equipment a.c. – Static meters for active energy class 1 and 2

Interfaces Standards Needed



LoRaWAN® Architecture



Standard: AS923, AU915 or US915 or other?

- **Interface 'B'**
  - RESTful API (Representational State Transfer)
    - Existing HTTP methodologies from RFC 2616 (GET, PUT, POST etc)
  - Self documenting interface
    - Swagger, now called
    - OpenAPI Specification (OAS)
    - Defines the API Contract
      - Request parameters and response objects
  - Payload – YAML, JSON or XML(?)

Interfaces Standards Connection Details, Metering, Alarms, Power Quality

CONNECTIONS	FIELD NAME	DATA TYPE
	IDNUMBER	TEXT
	SERIALNUMBER	TEXT
	TOWN	TEXT
	LATITUDE	DOUBLE
	LONGITUDE	DOUBLE
	TRANSFORMER	TEXT
	CONNECTIONTYPE	INTEGER
	RATING	INTEGER
METERING	**FIELD NAME**	**DATA TYPE**
	TIMESTAMP	DATETIME
	IDNUMBER	TEXT
	SERIALNUMBER	TEXT
	PHASE	INTEGER
	ENERGYIMPORTREAL	DOUBLE
	ENERGYEXPORTREAL	DOUBLE
	ENERGYIMPORTREACTIVE	DOUBLE
	ENERGYEXPORTREACTIVE	DOUBLE
ALARMS	**FIELD NAME**	**DATA TYPE**
	TIMESTAMP	DATETIME
	IDNUMBER	TEXT
	SERIALNUMBER	TEXT
	PHASE	INTEGER
	ALARMTYPE	TEXT

POWER QUALITY	FIELD NAME	DATA TYPE
	TIMESTAMP	DATETIME
	IDNUMBER	TEXT
	SERIALNUMBER	TEXT
	PHASE	INTEGER
	VOLTAGEMAX	DOUBLE
	VOLTAGESMA	DOUBLE
	VOLTAGEMIN	DOUBLE
	CURRENTMAX	DOUBLE
	CURRENTSMA	DOUBLE
	CURRENTMIN	DOUBLE
	POWERACTIVEMAX	DOUBLE
	POWERACTIVESMA	DOUBLE
	POWERACTIVEMIN	DOUBLE
	POWERREACTIVEMAX	DOUBLE
	POWERREACTIVESMA	DOUBLE
	POWERREACTIVEMIN	DOUBLE
	THDVSMA	DOUBLE
	THDISMA	DOUBLE

Data Visualisation Standard

PowerPilot Connections

MESSAGE STATS

Map type

Installation Progress | Comms | Alarms | Firmware

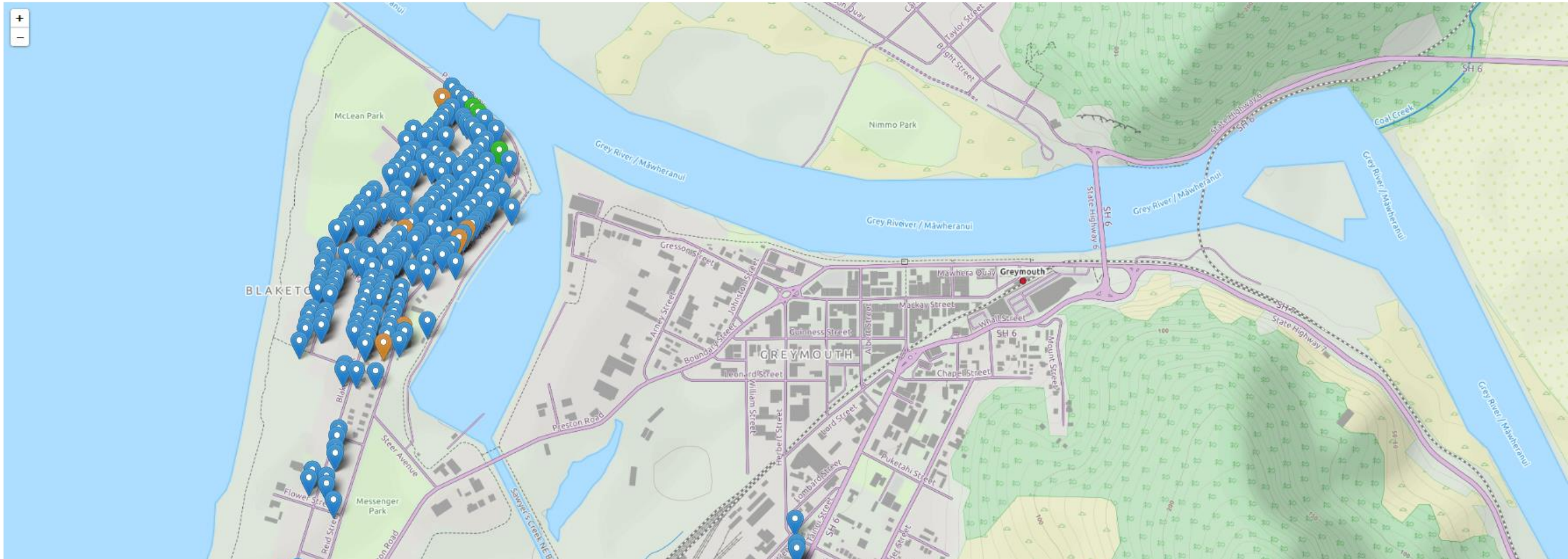
NEW CONNECTION

Installation states

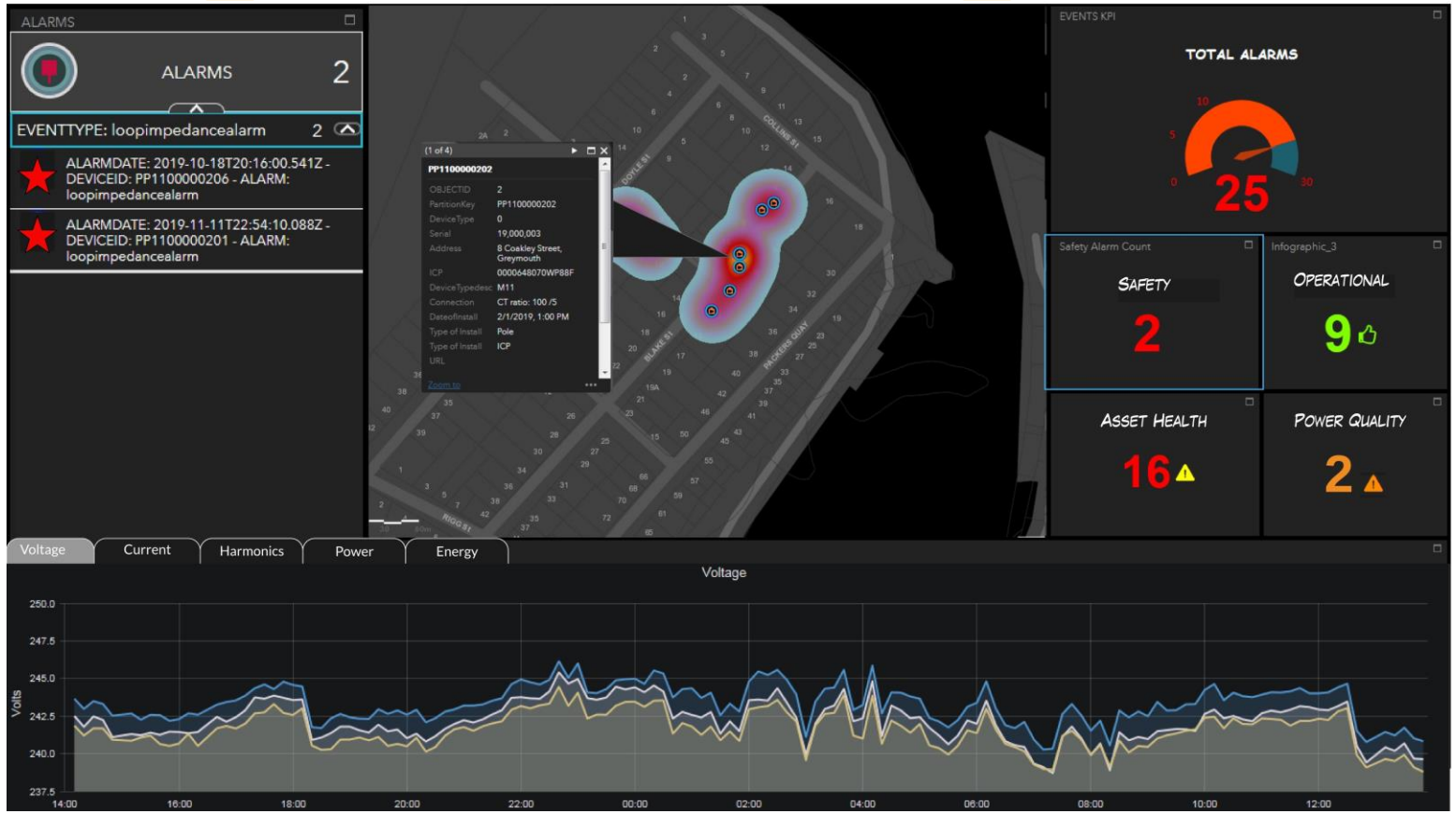
REFRESH

Install pending | Configured | Tested, awaiting sign off | Connected | Install failed

MAP | TABLE



Data Visualisation Standard

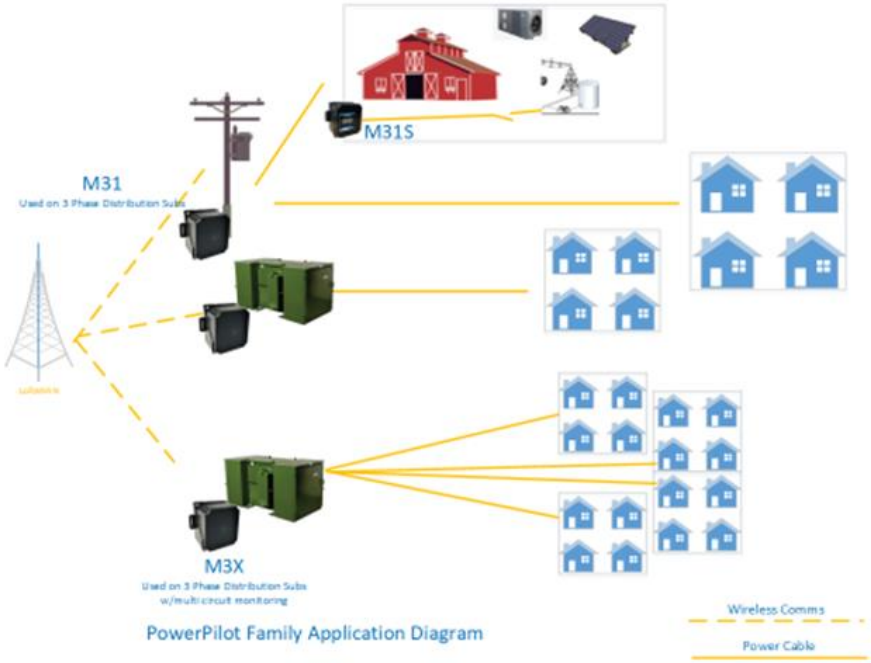


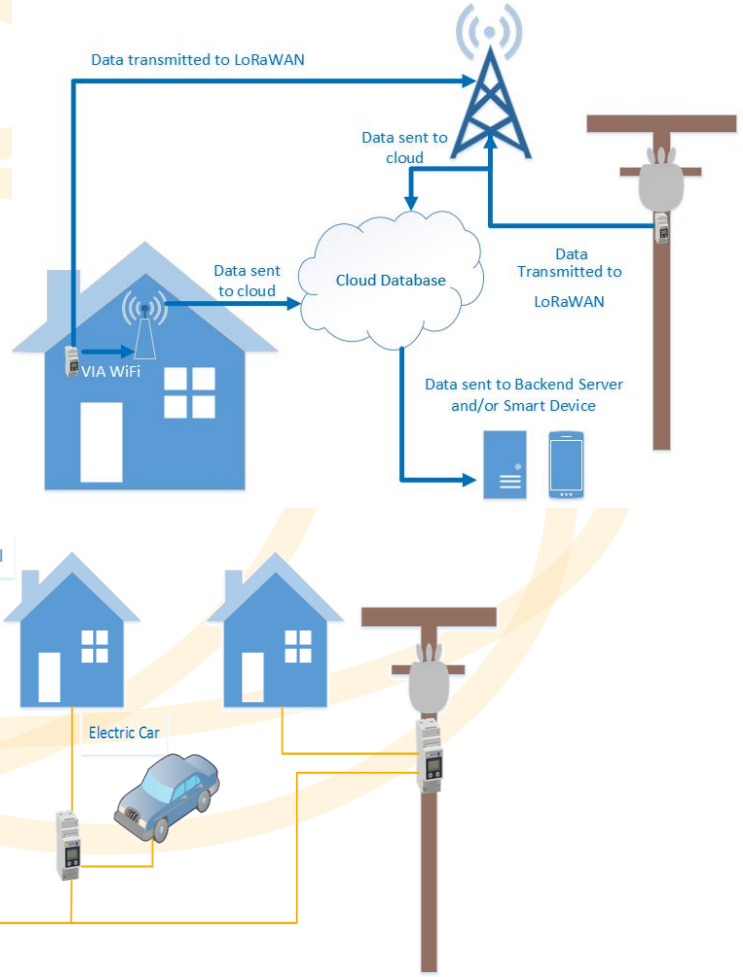
Data Protection Standards

IOT requirements and standards

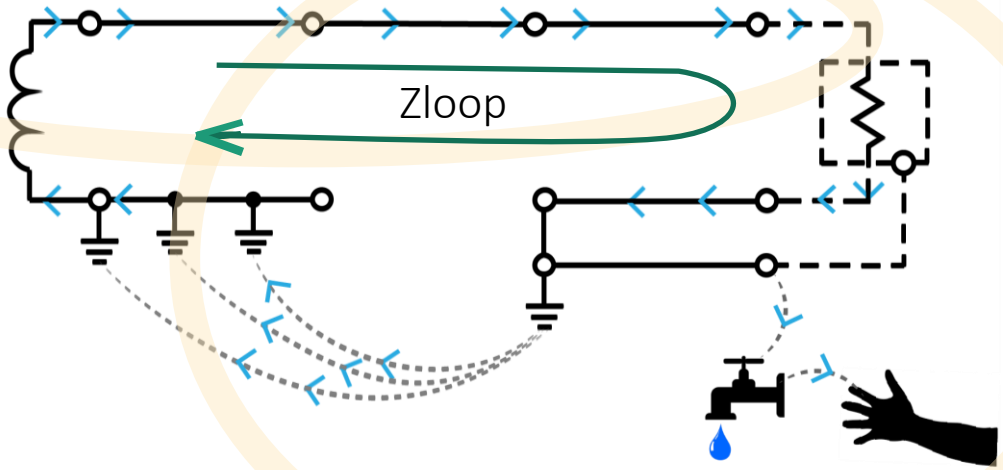
- PowerPilot is “secure by design” by following best security practice recommendations to limit attack vectors and removing vulnerabilities.
- The power sensors deployed are field upgradable over SSL, using modern chipsets, the firmware is encrypted using 256 bit AES keys and no port opened during normal operation.
- The communication to the backend is anonymous, encrypted and authenticated using 128 bit AES keys.
- The backend and frontend applications are deployed on a secure and trusted managed cluster behind a firewall with any public endpoints secured by TLS encryption and OAuth or JWT token authentication.

Possible Implementations



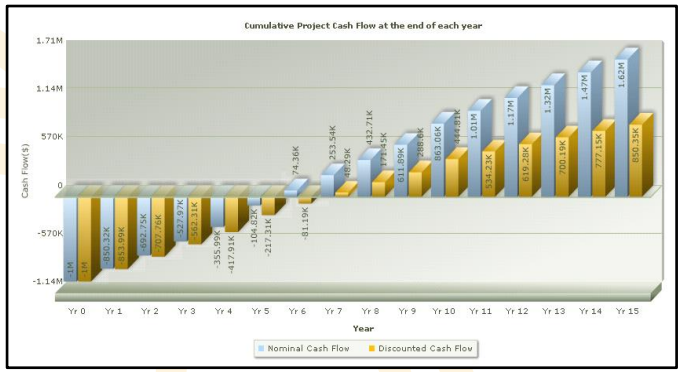


Safety Standards



Safety Standards

Other Standards



We need standards

- At the edge
  - For endpoint devices
  - For communication with DERs in the Installation
- For the communications channels
- For data storage and interfaces
- For safety outcomes