

Survey Results- Feeding the Big Data and Artificial Intelligence “Information-Appetite” – *From the Low-Voltage Grid*

In an earlier white-paper, we questioned how to feed information into the ever-hungry maws of the big data and AI platforms, especially focusing on the information coming from the low-voltage grid.

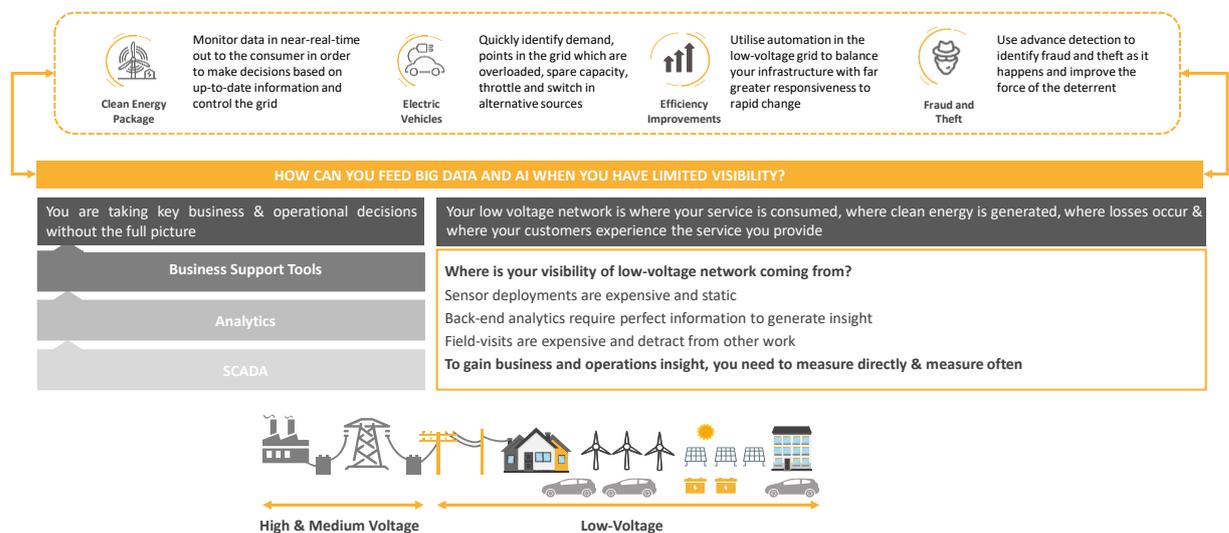
The Question, Re-phased and Summarised

As the Smart Energy Transition picks up pace, the role of the smart grid is coming more into focus. A major driver are the initiatives of Electric Vehicle introduction, distributed and green energy production and storage, and energy community projects and micro-grid. These will have profound effects on the low-voltage grid, as this is where many of these initiatives are being delivered.

Historically, it has been a major challenge to provide cost effective monitoring, management and control into the low-voltage grid. The result we have now, is a low-voltage grid which is essentially passive in nature with manageability limited to the “edges” of a black box and limited means to see and then control what happens within that black-box.



GETTING INFORMATION OUT OF THE LOW-VOLTAGE GRID



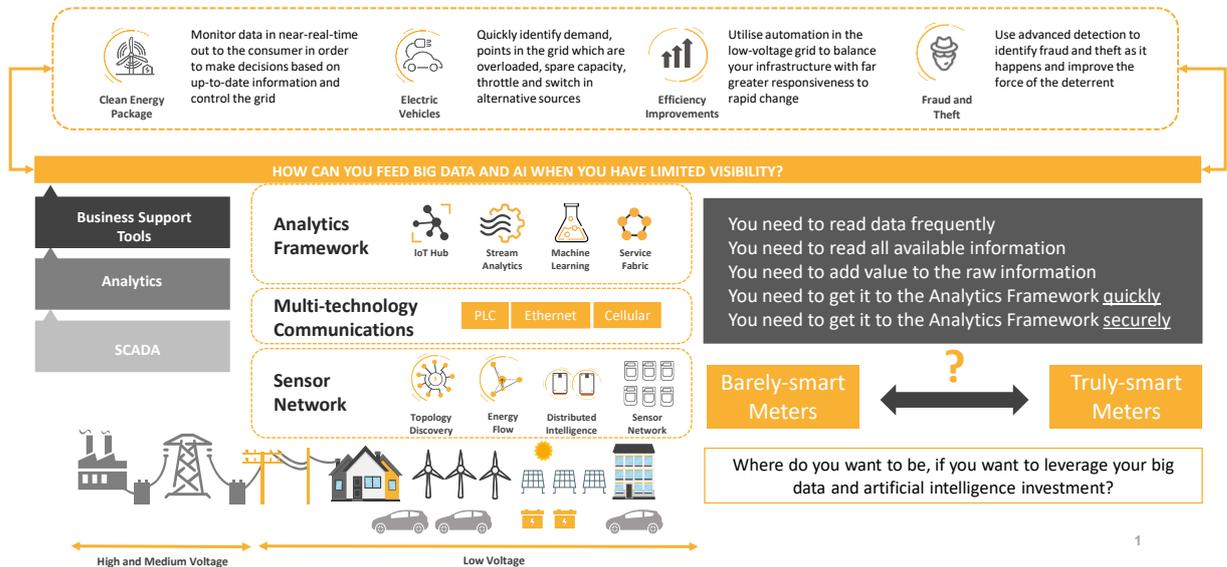
The Answer

The earlier White-paper described a series of “false dawns” where individual technology solutions presented possible solutions; big data and AI itself, IoT to gather information and connect devices, and then the smart meter. These solutions do not work in isolation, and it is only by integrating them into wider systems that it becomes possible to shine a spot-light on the low-voltage grid, and now it supports the Smart Energy Transition. In summary, the need is to have the measurement points in the low-voltage grid, enrich the information close to the source, connect multiple communications

paths to the devices so that the strengths of multiple technologies can be combined and apply robust security to protect privileged information at source and in transit.



GETTING INFORMATION OUT OF THE LOW-VOLTAGE GRID



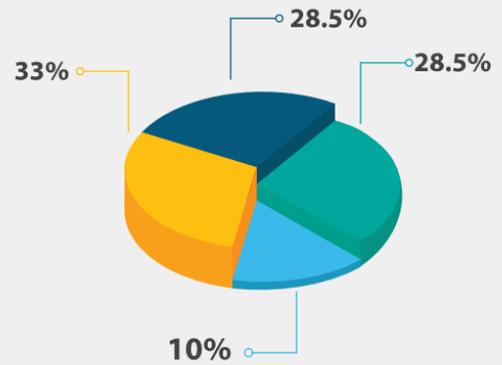
This then starts to drive the decision around investment in the low-voltage grid, especially in smart meters. The question for the procurement strategy for utilities is essentially: “With the major investments in big data and AI solutions, does it not make sense to focus investments on the sources of the information and the means of getting it? Isn’t the alternative simply wasting the opportunity to leverage the investment in the big data and AI platforms, and so have them become starved of information they need to justify their position?”.

A Survey

The results of a short survey conducted by NES, in conjunction with Smart Energy International, goes a long way to confirming some of these positions, and indicates where the utilities industry sits on this important issue. This survey was conducted in the course of a webinar addressing these specific issues which was attended by a blend of utilities, consultants, regulators and technology providers.

Do you currently have **big data** and **analytics solutions** for the **low-voltage grid**?

- Currently Deployed
- Not Planned
- Planned beyond next 12 months
- Planned for next 12 months

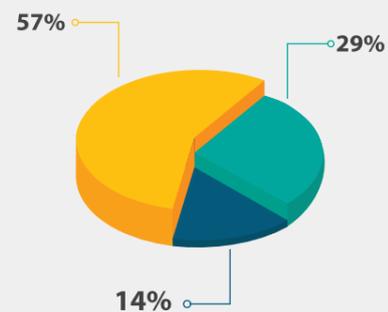


Around 75% of the respondents have investments either on-going or planned for big data and analytics for the low-voltage grid. This confirms the overall investment profile and the perception that it is important to gain more insight into this important part of the network.

The size of the response for the next 12 months is an indicator of projects in the wait status, possibly for external drivers, such as regulation and technology capabilities, to establish themselves more clearly during the rest of 2019 and 2020.

What are the **main challenges** you face in **gathering information** from the **low-voltage grid**?

- Availability of measurements from the low voltage grid
- Communications Reliability
- Communications throughput



What is interesting here is the opinion that the information is fundamentally not readily available. This is clearly a reflection that unless supported by deployments of sophisticated smart meters and using these as sensors in the low-voltage grid, there is little available information. It also indicates that visibility within the black-box of the low-voltage grid is lacking. It may be possible to put some levels of manageability around the edges, but what happens inside is still unknown.

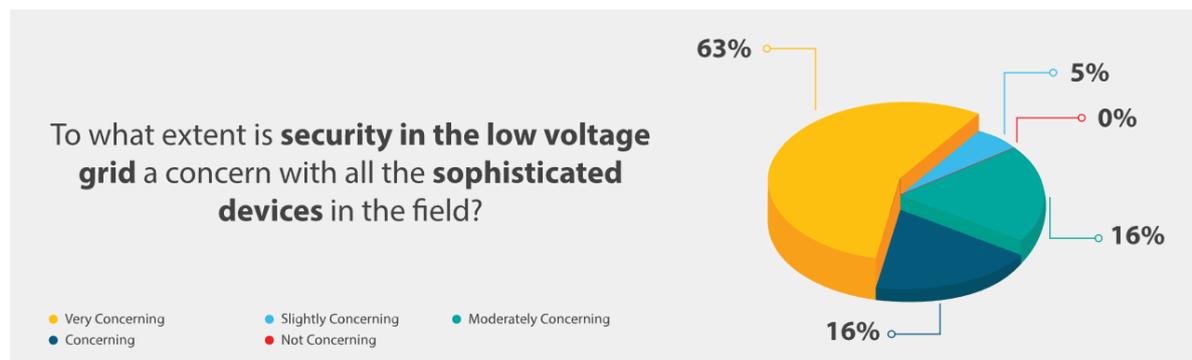
The second outcome was the reliability of getting to the information. This has been a major problem historically – whilst communications infrastructure exists, it is often not tuned to the specific demands of a smart meter deployment, and so reachability can be a challenge. This leads to the need for improved tooling for managing the communications outcomes – not communications network management but tooling to monitor SLAs on the business transactions of gathering information, and then using these to drive improvement plans. Related to this is the overall deployment of O&M tooling to keep the smart devices in the grid functioning properly.

Once availability and reliability improve, it is probable that the next bottle-neck will become throughout. The information will be there, and the challenge becomes how to get to it.



This question focused more on the balance between procurement policies aiming to maximise margin by reducing cost and the need to invest in infrastructure. In the case of this survey, the underlying point is does the investment in the big data and AI solutions balance the investment in the equally important sensors and communications infrastructure in the low-voltage grid.

Currently, there seems to be a balance between future-looking functional requirements and the need to control costs. Interestingly, there is a very slight bias towards the future-looking functional requirements, which may indicate that procurement departments are starting to become aware of the need to invest in the low-voltage grid in order to leverage the investment in the big data and AI platforms.



The focus of this question was not just IT security generally, but specifically related to the increased deployment of advanced devices in the field, which, themselves, can open up the opportunities for cyber-attack, directly as a result of their sophistication.

Unsurprisingly, people are generally very concerned. As more information is gathered from the low-voltage grid to feed big data and AI, there is more opportunity to capture that information, falsify it or simply block the flow. Whilst this is deemed to be simply operational data, the scope of impacts are limited to the utilities operational efficiency, but as more information comes from the smart meters, there is more of a perception that this is personal information, which would bring GDPR (and similar legislation beyond Europe) into the equation.

What is interesting is that there are people who are only Moderately or Slightly Concerned; possibly driven by (1) the lack of publicised attacks, (2) the hope that it will happen to someone else and (3) technology will provide an answer in time.

NES Perspective on the Survey

NES provide smart grid devices and complementary operations, analytics and security software solutions.

Consequently, such results relate strongly to NES capabilities:

Devices

NES provides high-quality smart grid devices for the low-voltage grid which provide sensors, multiple communications options and protection of the valuable information. Investment in high-quality smart meters is the cornerstone of gathering information from the low-voltage grid.

All NES devices are built to these underpinning principles.

Analytics Software

NES provides enrichment of the sensor information by discovering the topology of the low-voltage grid, and then assessing phase balancing and energy flows within this grid. As well as providing for operational improvements and outage impact detection, this provides more of the information required to perform capacity and loading analysis in readiness for EVs, distributed generation, fraud/theft and community energy. This is the information required from the low-voltage grid to drive the Smart Energy Transition forwards.

NES Grid Navigator and Grid Flow provide these functions.

Operations and Communications Monitoring Software

Operational efficiency and monitoring communications SLAs are a key aspect of maximising the information which can be gathered from the low-voltage grid by identifying areas of poor performance, and then using this to assess root-causes and resolve them. As well as the assuring the communications, robust O&M activities, supporting by tooling, ensure that the availability of the devices is maximised together with the communications. Finally, reception of events and alarms can also indicate problems in the low-voltage grid – the meter sees the symptoms of wider problems.

NES Grid Operations solutions implement both these key functions.

Security Software

The smart grid industry has focused on maintaining an IT security perimeter. Most ICT strategies now recognise that the perimeter will be breached, and protection in depth is required. This is achieved through intrusion detection and response systems.

NES Grid Watch provides intrusion detection and response solutions specifically for the devices now being deployed into the low-voltage Smart Grid.

Summary

A very interesting survey and thanks to all the contributors.

Overall, the results indicate that there is a significant on-going investment in big data and AI, specifically as it relates to the low-voltage grid. There is at least a balance between procurement policies of back-end analytics and sensors in the low-voltage grid compared to cost control, meaning that utilities recognise the dependency between the two areas of investment. Using the meters as a

sensor is clearly a major opportunity, but more can be done to expose what is actually happening in the low-voltage grid black-box. Finally, getting all this information and keeping it secure is a major concern.

NES Smart Grid solutions are well placed to assist utilities as they move through the Smart Energy Transition and use Big Data and AI as a means to drive their business and technology decisions.