Reliable backbone communication infrastructures for smart grid systems

By T Craven, H3iSquared

Proper planning and research – as well as working with an Ethernet specialist company - will mean that a reliable and stable smart grid solution can be put in place with minimal downtime and expense.

In today's utility industry, Smart Grids are a key topic, with most utilities having already migrated, or in the process of migrating over to a distributed Ethernet network to interconnect various remote sites and control rooms into a single Smart Grid system. But what exactly is a smart grid?

A smart grid is a modernised utility grid that uses communications networks and information technology to gather and act on information in an automated fashion. This is done to improve efficiency, reliability, economics, and sustainability of the production and distribution of electricity. Generally smart grids use an Ethernet based communication network to interlink all substations, control rooms, and other major generation, transmission and distribution sites across a wide area, such as a state or country wide network.

Moving over to a smart grid system can be a daunting task, especially to someone who is not too familiar with the operation and benefits of using Ethernet communications. However, the process can be broken down into various smaller steps that we will run through in this article, in order to alleviate some of the fears and worries involved with planning a smart grid system.

The reason Ethernet is the popular communications technology of choice for smart grid backbone solutions is that Ethernet is based on various open standard protocols, meaning that if a device complies with a part of the standard, it will be interoperable with other devices that comply with the same part of the standard. Also Ethernet runs over a distributed communications network, rather than utilising point-to-point links. This means that cabling and hardware CAPEX (Capital Expenditure) costs are greatly reduced when putting together an Ethernet network, and OPEX (Operational Expenditure) will also be greatly reduced, as adding a new device is simply a matter of providing an Ethernet link to the nearest point where that device can join the rest of the network, rather than having to run a link all the way back to a central control room.

Another benefit to using Ethernet on smart grids is the remote accessibility that is provided. As long as an engineer can connect to the network at any physical point, he will potentially be able to communicate with any device on that physical network (depending on the network configuration, access control lists etc). Using remote Ethernet links such as long range wireless, long range fibre and even WAN (Wide Area Network) links such as 3G connections to the internet or a privately managed cloud, smart grid systems can easily incorporate a large geographical area (country-wide or even possibly spanning multiple countries and continents) into a single smart grid network. This greatly simplifies troubleshooting and maintenance, as well as greatly reducing travel time for engineers and technicians as they can often perform all necessary data collection, analysis and changes from a central location rather than requiring travelling to each remote site.

Hardware

One of the main topics when designing a smart grid communication system is of course the hardware that will be utilised. The hardware chosen must comply with relevant Ethernet standards, such as VLANs (Virtual Local Area Networks), QoS (Quality of Service), PRP (Parallel Redundancy Protocol), IEC 61850 and other standards that may be relevant to your setup. Although the required standards are out of the scope of this article, it must still be taken into account when specifying the hardware to be used.

As it has been stated that Ethernet is based on open standard mechanisms, vendors will be able to supply the Ethernet compliance of their devices, and this info will generally all be contained on their data sheets.

Special care must be taken at this point to not pick vendors that use proprietary standards for a required mechanism, as this can vendor lock a user, meaning that any future expansion or replacement hardware will need to come from the same vendor. For instance

vendors will often have their own implementation of a redundancy mechanism. Using one of these vendors' equipment will mean that every switch in the network will need to comply with the proprietary mechanism, and so will have to come from that vendor. Alternatively, using an open standard redundancy mechanism such as PRP will mean that the user can order hardware from any vendor that has PRP compliance.

Beyond picking the hardware based on its logical compliancy and specifications, one needs to also make sure that the devices can handle the harsh environments typically found in substations. One of the biggest hazards to stable communications in the HV/MV environment is EMI (Electro-Magnetic Interference), which is found in abundance in most HV/MV substations. EMI can severely affect data travelling on copper cables and within devices that are not EMI resistant/immune. For this reason communications between cases and substations should be over fibre optic cabling (which is not affected by EMI) and the hardware should be EMI resistant or immune.

Another environmental hazard to the hardware is the temperature. Utility grade hardware should be able to handle a high running temperature, as often substations in Africa can be in extreme temperature zones, with high temperatures in the day and low temperatures at night.

Some vendors will offer special high temperature hardware, or will have all of their hardware able to handle high temperature ranges and both high and low temperature extremes.

For hardware that will be installed in high humidity or dust areas, conformal coating is an option that can greatly extend the life of hardware. Conformal coating involves coating all PCBs (Printed Circuit Boards) in the hardware with a thin layer of silicon, effectively sealing them from contact with any outside contaminants, such as conductive/corrosive dust or moisture. In some areas this can mean a difference of a couple of years before hardware failure/troubles.

Other factors such as the size of device, available port types, mounting options etc. will depend on your specific requirements. It is best to try source a single vendor for all communications hardware, as this will aid with aspects such as catering for a certain amount of spares and general troubleshooting.

One special hardware type must also be discussed here, and that is a serial device server. This is a piece of hardware that can be used to encapsulate serial data into an IP packet, suitable for transfer over an Ethernet network. On the other side a second serial device server or alternatively a virtual serial COM port application running on a PC will be able to 'unpack' the serial data from the IP packets, and forward that on to the end device or application. Effectively these devices are used for extending serial connections to any point on an Ethernet network, which becomes invaluable when upgrading a system to a smart grid solution.

Many legacy devices will not support Ethernet directly; however replacing these devices can prove very costly, both monetarily and in terms of time required. Using serial device servers can greatly simplify the setup, as well as save time and money until those end devices are upgraded to more modern, Ethernet enabled devices.

Abbreviations

ACL – Access Control List
CAPEX – Capital Expenditure
CIP - Critical Infrastructure Protection
EMI – Electro-magnetic Interference
I/O – Input/ Output
IP – Internet Protocol
MAC – Media Access Control
MMS – Manufacturing Message Specification
NERC – North American Electrical Reliability Corporation
NMS – Network Management System
OPEX – Operational Expenditure
PCB – Printed Circuit Board
PRP – Parallel Redundancy Protocol
QoS – Quality of Service
RMON – Remote Monitoring
SAM – Secure Access Management
SCADA – Supervisory Control and Data Acquisition
SNMP – Simple Network Management Protocol
VLAN – Virtual Local Area Network
VoIP – Voice-over Internet Protocol
WAN – Wide Area Network

Security and access control

The next point to discuss in terms of designing an Ethernet networks for a smart grid, is security and access control. A smart grid network is a highly critical network, and access by a user with malicious intent can cause damage to the grid and attached devices, as well as losses of production and income. Security and access control are key components to having secure, stable smart grid.

Security can be divided into two basic categories, physical and logical. Physical security deals with protecting the hardware from direct access by those with malicious intent, or even those who do not know what they are doing and could accidentally cause problems. This involves controlling the access to devices using components such as locked gates, biometrics or card controlled access etc.

Access control is greatly facilitated by the Ethernet network, as most access can be remotely controlled from a central control room rather than requiring a gate guard at every substation for instance. Using a camera system along with attached digital I/O devices, one or two users can control access to a variety of different remote sites. VoIP (Voice over IP) allows for the central users to communicate to the remote sites if necessary, even if those sites do not have cellular phone signal. Modern biometric systems will also often be Ethernet ready, allowing these to also be controlled from a central point.

With Ethernet being a distributed communications technology, logical security is even more critical than physical security in most cases, as access to any devices can potentially be granted from any point on the network. This is why controlling the access to the network is such a priority, especially in the case that public WAN interfaces exist (Such as a 3G connection from a remote site to a central control room using a public 3G cloud). Connections like this means that the network now interfaces to the internet, and thus potentially anyone with internet access could access the smart grid network.

For this reason it is highly important to properly control all WAN interfaces, and use stateful firewalls in such a way that access to critical sections of the network is highly controlled. Separating any corporate sections of the network from the critical parts using firewall devices is also essential in order to stop malicious or accidental users from affecting the grid operation.

When looking at firewalls offered by different vendors, again it is essential to make sure that the hardware can handle the environments it will be used in, as well as provide the compatibility to any protocols relevant to your setup. For instance, smart grid networks will often be divided on a VLAN basis. If routing between the different sections or aspects of the smart grid is required, it is essential to confirm that the router is IEEE 802.1Q [2] compatible. This means that this device will understand standard VLAN tagged packets from the switches on the network. When purchasing a router or firewall, first look at the core package/device functionality, and then confirm what additional functionality (often in the form of separate modules or licensing on the unit) you will require and that this functionality is offered by the manufacturer.

Although firewalls provide control over specific interfaces or protocols, even specific devices, they do not actually provide secure access management on a user based level. In today's smart grids, this level of granular access management is highly desirable, and in some countries that require NERC CIP (North American Electrical Reliability Corporation – Critical Infrastructure Protection) compliancy, this level of access control is mandatory. For this one would look at the concept of a SAM (Secure Access Manager) solution. This is a system that controls access to end devices based on the user's access rights (Unlike a firewall which works more off device access rights or actual communication properties such as port numbers or protocol type). A typical SAM will be an application running on a server in the central control room. Users wishing to log onto end devices will instead log onto the SAM with their individual credentials. Once logged in, the SAM will present them with a list of devices they are allowed to access. They can then pick the device to access, as well as the application to be used for this access (Such as telnet, PuTTY, or a vendor specific application). Most SAMs will allow either a 'thin-client' environment, where all relevant applications are stored on the SAM itself, or a 'fat-client' environment where all client PCs will have the application installed directly. Once the user has picked the device they wish to access, the SAM will log them into that device in a manner that is transparent to the end user. In other words the user will not need to know the username or password for the device itself, as the SAM will handle that authentication. A good SAM solution will offer additional functionality as well, such as automatically changing all end device passwords on a schedule basis, or automatically retrieving firmware versions and configurations from end devices periodically to check them against a 'master' version for any discrepancies. Many of these functions are required for NERC CIP compliance, and although this is not yet a requirement for utilities in Africa, the general trend seems to be moving to more secure, access controlled networks for utilities worldwide.

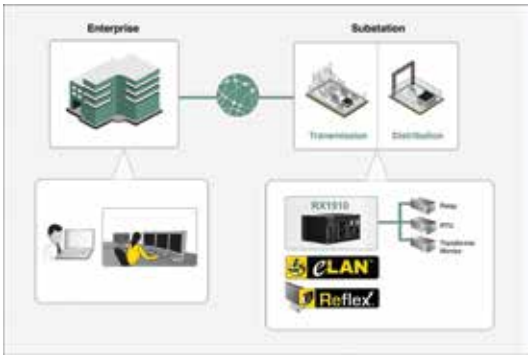
As the SAM will be handling all logins to end devices, it is essential to make sure that the SAM package you choose allows for a scenario where the remote substation has lost access to the central control room (And thus to the SAM server). As the users will not be aware of the current password on the end device they will not be able to access the device directly or through the SAM. There are two options in this scenario, of which some SAM solutions will have options for both. The first is to allow an administrative user to log into the SAM in the control room, and request the current passwords for the end device. These can then be passed on for direct access, and changed again once the remote user no longer requires access. The second option is to have a lightweight version of the SAM server that resides within each substation. This does not need to have the full functionality of the main SAM server, but will store all passwords and ACLs (Access Control Lists) for the end devices, allowing users to log on locally to a device even if the link to the main SAM server is down.

Depending on the scenario and SAM server, additional automation functionality may be available, the use of which depends on your end requirements. When planning to purchase a SAM solution first look at the core functionality offered, and then inspect what additional functionality can be offered in the form of additional modules. This way you will confirm that you are purchasing a SAM solution that will work to your requirements.

Data concentrator

A second software solution that can be invaluable (whether expanding an existing smart grid or upgrading to a smart grid) is a data concentrator. This will consist generally of a software application once again, occasionally with extra hardware attached. The purpose of a data concentrator solution is to normalise various different protocols into a single protocol that can be understood by a master server, such as a SCADA system.

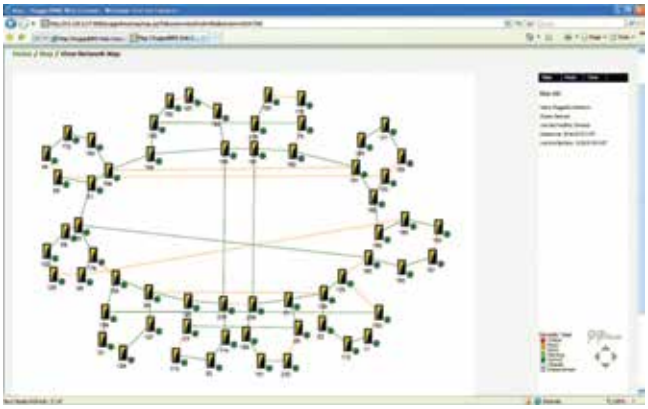
This is especially useful when upgrading an existing system that has multiple end devices from different vendors. Different vendors will often use different protocols for communications between IEDs, which are not directly compatible with one another. A data concen-



trator will act as a 'translator' for these devices, allowing them to all interface to one another even though they are speaking a different native 'language'. A data concentrator can save a large amount of CAPEX for the upgrade, and will allow the legacy devices on the system to be upgraded on a piece by piece basis, rather than all at once.

Network Management System

Finally, a third solution that can be considered quite essential for a smart grid, is a reliable NMS (Network Management System). A NMS generally uses SNMP (Simple Network Management Protocol) and RMON (Remote Monitoring) mechanisms to collect information about end devices and communication devices on the network, and present this information in an easy to understand, visual format for operators. These systems will generally either work off polling (where the NMS requests status updates periodically from devices) or using traps (where the devices will send a notification to the NMS on discovering any problems such as link or device component failure). A good NMS system will have options for both polling and traps, depending on the requirements of the solution. The trend in the industry is to move towards using the relatively new MMS (Manufacturing Message Specification) protocol instead. If your requirements call for MMS support, take care to make sure that your devices and NMS server can support this protocol.



A NMS system is essential to being pro-active on the network maintenance, as administrators of the network will be informed of networks problems before they turn into huge outages, allowing them to be resolved in a timely fashion.

For instance, a critical network running a smart grid will have redundancy in place to prevent a link down from bringing down the entire system. However without a NMS, users will not be aware that a redundant link has taken over from a main link that failed. If the redundant link then fails in the future a section of the network could be unreachable from the control room, causing havoc. A NMS in place would have alerted operators to the fact that the main link had gone down, allowing them to resolve that problem before any downtime is imposed on the network.

Conclusion

As we can see, smart grids may be daunting at first, but the benefits they provide far outweigh the effort required to implement them. Proper planning and research, along with working with an Ethernet specialist company, will mean that a reliable, stable smart grid solution can be put in place with peace of mind and minimal downtime and costing.

The overall time and effort saved in maintenance and troubleshooting once a smart grid is in place will be invaluable to increasing productivity and profits from the grid.

Acknowledgement

Images provided courtesy RuggedCom Inc.

References

[1] IEC 61850. 2013. Communication networks and systems in substations.

[2] IEEE 802.1Q. 2011. IEEE Standard for Local and metropolitan area networks - Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks

Tim Craven joined H3iSquared in 2008 in a technical support role, and has been with the company since then, providing technical support, network auditing and training to leaders in the industrial, utility and ITS industries. Enquiries: Tel. 011 454 6025 or email info@h3isquared.com. Visit www.h3isquared.com.

About the author