

Implementation of Smart-Grid technologies for Automation & Control in a grid connected Wind Energy Facility in South Africa

Sagar Dayabhai Pr.Eng
System Control Manager
Energy Solutions Division
Consolidated Power Projects (CONCO)
Midrand, South Africa
sagar.dayabhai@concogrp.com

Peter Diamandis
Systems Engineer
Quadnet Computer Systems
Johannesburg, South Africa
peter@quadnet.co.za

Abstract — South Africa has recently embraced the construction of a number of Renewable Energy Facilities to alleviate the strain and assist the national power grid. These facilities required the implementation of modern automation and control systems using a variety of Smart Grid enabling technologies.

This paper presents a next-generation automation and control solution that was implemented at a wind energy facility (WEF) in South Africa to manage both the electrical and power plant infrastructure. The discussion centres around the Smart-Grid enabling technologies mentioned above which were employed to implement the requisite converged architecture which was essentially required to ensure operational needs, satisfy grid code requirements, comply with turbine operational specifications, and conform to unique customer requirements in a secure manner. Various technical and commercial challenges within these domains are also described as well as the remedial actions which were introduced to mitigate these challenges.

Keywords: *REFIT, IPP, IEC 61850, HMI, WEF, Voice over IP*

I. INTRODUCTION

South Africa's electricity reserve margin has been waning over recent years to critical levels. Economic growth, increase in fossil fuel prices and increasing electricity demand are contributing to this problem. Solutions to this problem are exacerbated by global environmental concerns. This has encouraged the progressive pioneering and initiation of new opportunities to employ renewable energy resources such as wind and solar facilities. The country's Department of Energy (DoE) has instituted the Renewable Energy Feed-In Tariff (REFIT) programme for the purpose of allowing Independent Power Producers (IPP) to construct, operate and maintain grid-connected renewable energy facilities. The long term management challenges of these facilities is being addressed by the implementation of modern automation and control systems using a variety of Smart Grid enabling technologies.

Modern control and automation systems exhibit a clear and intricate convergence of operational and information technology. In many cases, the distinction between operational and information technologies is difficult to identify. Modern substation automation systems are designed and implemented using IEC 61850. High speed, advanced decision making processes and algorithms require flexible and maintainable code using IEC 61131-3. Intelligent Human Machine Interfaces (HMIs) are required for advanced monitoring while data historians are required to maintain long-term operational and grid code compliance data to meet regulatory demands. Carefully designed and scalable network architectures are required to reliably transport high-speed operational data but must also accommodate security and surveillance systems, and telephony systems employing Voice over IP technologies. Secure remote access to the energy facility networks is essential as suppliers (such as wind turbine and STATCOM manufacturers) as well as operations and maintenance staff require such capabilities to maintain plant performance and system guarantees. Local and remote access must further be secured by preventing unauthorized access using Network Access Control and by ensuring correct authorizations by means of Role-Based Access Control philosophies.

System Requirements

A WEF requires an integrated and technologically advanced automation and control system in order to achieve the typical objectives of the IPP. These objectives include:

- Ensure efficient operation of the facility to secure maximum revenue.
- Facilitate long-term operations and maintenance.
- Comply and maintain successful grid integration, Grid Code compliance and contractual obligations.
- Provide high system availability.
- Provide secure IT infrastructure for local administration at the facility.
- Provision a secure platform for stakeholders to remotely monitor, control and manage the facility.

II. CHALLENGES

Many challenges exist with meeting the aforementioned objectives cost-effectively. This applies to both the capital cost of the project as well as the life-cycle operational cost. These challenges are further exacerbated by key requirements introduced by the IPP in order to align and focus the system's design towards the direction which will meet these objectives. These requirements include:

Plant Performance and availability

The highly variable nature of resources such as wind and solar make renewable energy facilities susceptible to discontinuous supply characteristics. This makes it essential for such facilities to operate on a maximum availability factor of the plant. Unnecessary or preventable plant outages not only affect the ability of the facility to provide power at its maximum capacity (taking into account any curtailment that is necessary), but also directly impact the revenue generating capacity of the plant. Considering the typical 20 to 30 year lifetime range of renewable technologies such as wind and solar, preventable losses of revenue are unacceptable to plant owners and investors. As such, plant performance is a key metric. Automation and control technology that is employed at energy facilities must ensure that plant performance is not hampered but is rather enhanced through automation, accurate monitoring, timeous alarming of potential problems and abnormal events, comprehensive reporting, assistance to operators to quickly isolate faults, and remote connectivity for rapid fault diagnosis and system restoration.

System availability is a metric that is intimately linked to plant performance. Modern industrial control systems aim for a system availability of 100% by employing methods such as redundancy. The side-effect is however that redundancy increases the number of components within a system. This increases the number of potential component failures implying that an incorrectly applied redundancy solution may actually decrease system availability. Having said that however, some form of redundancy or fault tolerance is typically employed if a control system malfunction or loss of visibility of the process causes a major loss of revenue, damage to equipment, or injury to people.

The metric of reliability measures the likelihood that a device will perform its intended function over a specific period of time whereas maintainability is the ability of a system to be changed or repaired.

Modern technology is composed of increasingly complex semiconductor and software-based components which make it incredibly difficult to predict failures. It is hence no longer a question of *if* a failure is possible, but how quickly and accurately it can be detected and corrected. [1]

To meet these stringent requirements and improve plant performance, the following challenges need to be addressed by the system as a whole:

1. Prompt notification of any faults or abnormal events which occur.
2. Rapid diagnosis of the fault or abnormal event. If this requires remotely located specialists then remote connectivity to the affected system components must be facilitated.
3. Timeous system restoration or repair.

Grid Code Compliance

- In order for the System Operator to purchase energy from an IPP, it is mandatory for the IPP to comply with the National Energy Regulator of South Africa's (NERSA) and Eskom's Grid Code requirements.
- The latest revision of the South African Grid Code and Information Exchange Code documents outlines the requirements which require compliance in order for the IPP to connect to the national grid and commercially operate [2]. These Codes are further supplemented by Eskom's Interconnection Standard for Embedded Generation which serves to amplify the protection and SCADA requirements outlined in the national grid codes [3].
- The requirements for Category C renewable facilities (>20 MVA) are that control and regulation of the renewable plant remain within the domain of the System Operator [3]. This is achieved through a number of control functions (or modes) which include:
 - Absolute production constraint [2],
 - Delta production constraint [2],
 - Power gradient constraint [2],
 - Voltage Control [2],
 - Reactive Power Control [2],
 - Power Factor Control [2], and
 - Frequency Control [2]

The Grid Code and the Interconnection standard discuss the implementation of these control modes and the required integration with the SCADA systems to facilitate the monitoring and control of the facility both locally at the facility and remotely by the System Operator.

Variances between the South African grid code and the grid codes applicable to other countries means that existing systems need to be adapted to local conditions. The greatest impact is normally to Power Plant Controllers (PPCs) although the integration challenges between the various system components can be significant. This complicates the grid integration process and can often delay commercial operation of the plant which can have severe financial consequences for the IPP. The IPP is thus reliant on the automation and control system to be able to facilitate this process and accommodate the integration of systems such as the wind turbine controllers and Eskom's SCADA system.

Operations and Maintenance

Operations and maintenance during the lifetime of the plant is an essential function that must be carefully considered and planned in order to ensure maximum availability of the WEF on to the grid. Furthermore, the grid code specifies a turn-around time for resolving disturbances/issues which may arise in the plant which affect grid integration and the IPP is required to institute measures to adhere to these timeframes in order to maintain grid code compliance.

Some of the factors which contribute towards a successful operations and maintenance program include:

- Remote monitoring and control of the wind farm
- Automatic event notification systems
- Automatic retrieval of sequence of events (SoE) for analysis of system disturbance
- Automatic generation of customizable reports which allow the IPP to track performance of various components of the plant.

- Automatic backup of the configurations of all mission critical components of the plant.
- High speed broadband communications and telephony network to support operations and maintenance personnel.

The IPP requires the automation and control system design to cater for operations and maintenance and to accommodate the aforementioned factors.

Additional challenges which exist include:

- Commonly available automation and control systems are not natively equipped with the functionality to provide all these requirements and software development is typically required.
- Due to the geographical location of the IPP Energy Facilities in South Africa, broadband communications in these areas are in most cases not easily available from the national telecommunications carrier or other services providers.
- The energy facilities also cover vast geographical areas which adds complexity to protecting the facility from South Africa's perpetual cable and copper theft problems.
- Due to the diverse nature of the system components and the variety of users involved in various aspects of the automation and control system, it is not practical to isolate each portion of the system. Interoperability between the components and their successful integration is paramount.

III. SYSTEM DESIGN

A large portion of the above requirements and challenges were required to be addressed at the Category C WEF discussed in this paper. The need to minimize the complexity associated with managing these requirements during the commercial operation of the facility prompted development of a single unified solution capable of performing a multitude of tasks. Components of this solution include:

1. Automation and Control system responsible for automatically monitoring and controlling the MV electrical infrastructure associated with the wind farm.
2. Automation and Control system responsible for automatically monitoring and controlling the HV electrical infrastructure connecting the wind farm to Eskom's Transmission network.
3. Facilities SCADA system responsible for concentrating all plant data and managing SCADA grid integration and SCADA grid code compliance. This system is typically included for WEFs which are not natively compliant with the South African Grid Code (SAGC) and Eskom's Interconnection standard. The system controls the WEF based on commands received from the utility in a manner that conforms to Eskom's requirements.
4. Power Plant Controller (PPC) responsible for monitoring and controlling the WEF plant output and performance. This is an essential component for ensuring Grid Code compliance.
5. Wind turbine management system which monitors and controls all wind turbines. This includes the provisioning of a high speed redundant fibre communications network used between the turbines

for data transfer in a ring topology which terminates on to a managed turbine Local Area Network (LAN).

6. Generation forecasting system responsible for aggregating meteorological data and applying WEF availability factors to provide the necessary forecast data which is required by Eskom.
7. Data Historian responsible for retrieving and storing wind farm data for long periods.
8. Human Machine Interface (HMI) for operators to monitor and control the WEF.
9. A Flexible AC Transmission Systems (FACTS) device in the form of a STATCOM to assist in providing the reactive power compensation requirements stipulated in the SAGC.
10. Advanced Security system for access control and surveillance.
11. An advanced telephony system that provides internal calls, cost effective external voice calls, conferencing facilities, voicemail, and optionally a call management system that monitors and provides an audit report per call, per phone and/or per user.
12. A secure high speed communications network provisioned to manage and support the aforementioned components and provide broadband Internet connectivity for operational use.

A high level overview of the system design is depicted in Figure 1 below.

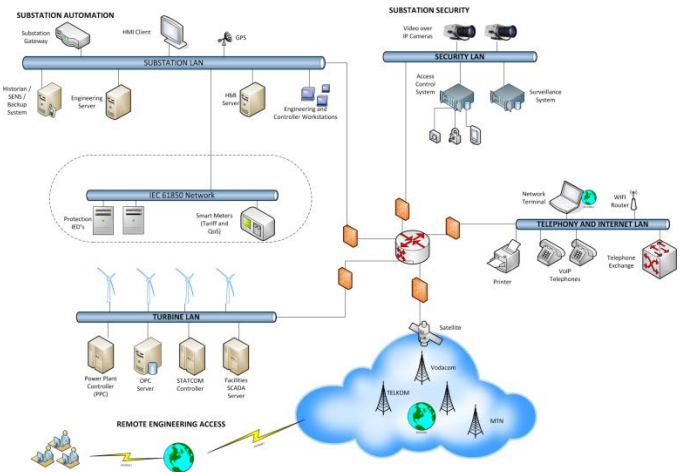


Figure 1: Smart grid architecture designed for WEF

IV. SMART GRID ARCHITECTURE

In order to comply with the requirements detailed above, a smart grid enabled architecture for the automation and control system was designed and implemented as illustrated in Figure 1. The architecture is described below.

Substation Automation

The Substation Automation is built on the IEC 61850 standard. Communications facilities for the Substation Automation system make use of both MMS and GOOSE messaging. This eliminates the need for tedious wiring to transmit signalling information between devices while providing the high-speed data transfer required for mission critical protection functions and inter-bay communications. In addition, plant statuses, controls, interlocking violations and measured data are all monitored on the SCADA system via IEC 61850 MMS.

The Intelligent Electronic Devices (IEDs) are responsible for monitoring and protecting the transformers (132/33 kV) and each collector group 33 kV feeder. The collector group

feeders connect a series of turbines in an electrical ring topology with a normally open point in each ring and two 33 kV switchgear breakers terminating each ring.

The Substation Automation system comprises a high speed, redundant, substation-hardened Ethernet backbone using a hybrid topology for improved availability.

Grid Integration

SCADA grid integration is a critical path project phase and is a pre-requisite for attaining grid code compliance and commercial operation of the farm. It is then essential to examine all operating parameters and functions of the system including the power plant controller and analyse these parameters against the interconnection standard and the SAGC in order to evaluate compliance.

In some cases it has been observed that the PPC is unable to meet these stringent requirements and additional software development is required in order to achieve compliance.

This is typically done by introducing a real-time automation controller into the network which serves as the overall facility controller. Figure 2 portrays the architecture of the facility's automation controller.

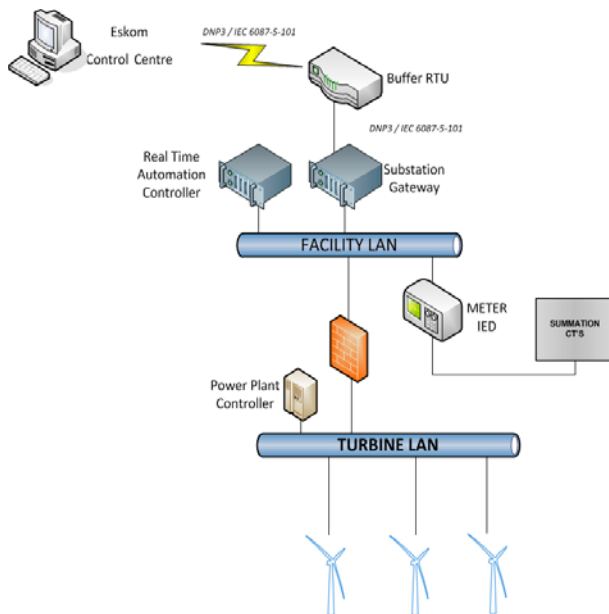


Figure 2: Facility Controller for typical WEF

The facility controller is responsible for the following tasks:

1. Acquire real-time measurements from a facility meter connected at the Point of Connection (PoC) using IEC 61850 MMS.
2. Communicate this data to the Power Plant Controller (PPC). This is typically achieved using Modbus TCP/IP or DNP3/IP depending on the protocols implemented on the PPC.
3. Communicate with the Eskom Buffer Remote Terminal Unit (RTU) interfacing to Eskom's Control Centre SCADA Systems using IEC 60870-5-101 for the Transmission System control centre and DNP3 for the Distribution control centre.
4. Compute acquired data using a real-time algorithm implemented using IEC 61131-3 running on the platform for intelligent decision making processes on how to control the plant

based on signals received from the system operator.

Historian

The availability of the turbine on the grid is a critical function of revenue protection. As a result, the IPP requires periodic reports of turbine performance availability in order to facilitate operations and maintenance and maximize availability of all turbines. Furthermore, it is essential for the WEF to maintain a data repository which stores all operational data which can be used for post-event analysis and investigations. It thus becomes a requirement to acquire and store all operating parameters, alarms, events and turbine statistics in a Historian functioning on an independent server specified with adequate processing power and storage capacity.

The historian provides the following functionality for the wind farm:

1. Provides historic data over a 10 year period.
2. Affords the IPP with the ability of using a process analyst to record historic trends of different measurands and generates trend plots for post-event analysis and investigations.
3. Provides a historic chronological site-specific alarm/events bin which allows the IPP to monitor and analyse events which have occurred in the facility and produce reports which can be used for post-event analysis and investigations.

Wind Turbine System

A typical wind farm incorporates a number of SCADA components which compromise the wind farm system. These include but are not limited to:

1. Power Plant Controller (PPC)
2. Reactive Power Control System (RPCS)
3. Turbine Management System
4. Turbine Measurement System
5. Operations and Maintenance System (OMS)
6. Meteorological Data Management System

In some cases, a requirement from the IPP is to provide an integrated SCADA solution providing a single unified platform to access all systems and services. Due to the disparity and proprietary nature of the communications interfaces to devices such as wind turbine controllers, data from the aforementioned systems and services are typically acquired using an OPC interface. This information can then be used by system components such as the Historian, notification system, and HMI. This level of integration provides the user with a single unified solution with access to real time information from single console/user interface.

Furthermore, a number of these systems embed a web-server which uses secure HTTP to access data. This flexibility allows the Human Machine Interface (HMI) to offer the user the ability to access all web-servers securely through the web-enabled HMI.

Data acquisition from the turbines is achieved by means of a high speed fibre-optic backbone. Figure 3 illustrates a typical network architecture of a wind turbine system comprising managed switches, a router and firewall to effectively manage the traffic on the network, optimize the

quality of service regimes and provide adequate security on the turbine security perimeter.

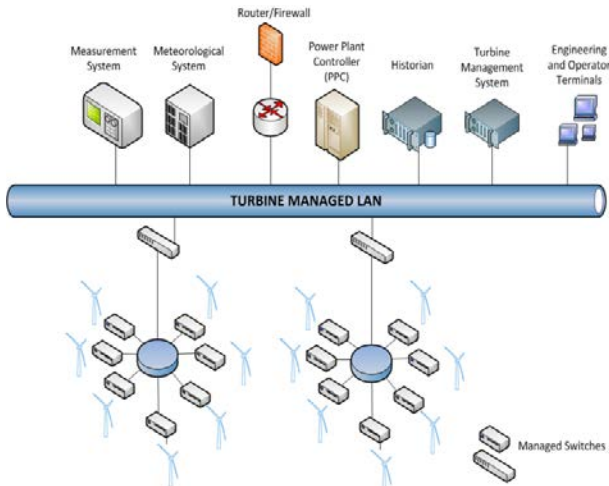


Figure 3: Typical network architecture of the turbine network

Human Machine Interface (HMI)

The typical SCADA system for a wind farm consists of multiple disparate components, each with its own user interface. The HMI integrates these interfaces such that a unified platform is presented to the operators. The HMI was designed and engineered to provide the following information and functionality to the user:

1. Secure role-based access with full audit trail.
2. Overview of the WEF including turbines.
3. Overview of the HV/MV electrical infrastructure.
4. Geographical layout of the WEF showing roads, transmission lines, turbines, substations, etc.
5. Bay level monitoring and control of all primary plant equipment.
6. Indication of all earthing, interlocking and station authority applied to prevent incorrect controls being executed to plant.
7. Turbine level monitoring of each wind turbine.
8. Communications layout showing health and status of all devices connected on the network.
9. Integration of the security system. In one instance, due to the issue of theft, the IPP further required the software development of an automatic fault analysis system which predicted a cable fault between any two turbines using fault path indicators situated at the turbines. Fault analysis logic is programmed using IEC 61131-3 on the automation controller. This allows security personnel to access the HMI security screen and establish the location of cable theft down to the connection between two turbines.
10. Management of networking equipment using the Simple Network Management Protocol (SNMP).
11. Temperature monitoring for all SCADA equipment cabinets. This was achieved using an IEC 61850 capable IED connected to PT100 temperature sensors.

12. Historical and live trending system.
13. Historical and current alarms and events. Alarms are prioritized based on severity.
14. Read-only access to power quality and tariff meters.
15. Access to UPS and power management system.
16. Access to network equipment (routers, firewall, Ethernet switches etc.)
17. Access to the Turbine management system.
18. Access to the Historian system.
19. Access to the System Event Notification System.

System Security

For system security in a WEF it is essential for all SCADA equipment (servers, routers, firewall, gateway) to be protected from damage either due to loss of supply/inconsistent voltages and/or corruption and loss of data from a software and hardware perspective. Reliability is built into the system design by introducing three components to cater for such scenarios. These include:

1. Managed Uninterrupted Power Supplies (UPS)
2. Automatic Backup System with a disaster recovery procedure and policy
3. Engineering workstation which serves as a data repository for all software applications and configurations required to perform engineering on all devices attached to the network.

The continuous supply of power is the single most important reliability factor for electrical equipment that should not be overlooked or neglected. As such, a dedicated UPS supplies constant power to all critical SCADA equipment for more than 6 hours in the event of a loss of power supply. In addition, the UPS is fully managed and monitored using SNMP. Information such as the current status of the UPS, active alarms and measurands such as voltage levels are monitored by the SCADA system and visible from the HMI. Equipment supplied through the substation's DC supply is further secured by the battery backup facility and standby generator.

In order to prevent the loss or corruption of data, an automatic backup system was developed that performs the task of retrieving configuration and log files from each device on a scheduled basis and stores it in the data repository.

System Event Notification System (SENS)

The highly distributed nature of renewable energy facilities means that it is unlikely that an operator will be constantly monitoring alarms and events at the HMI. As the data from all the disparate systems is available at the SCADA system it was possible to implement a system event notification system that provides the facility to notify stakeholders of alarms and events as they transpire on the system. The system provides the following functionality:

1. Sends an SMS/Email when an event has occurred.
2. Events and alarms can be grouped (e.g. protection trips/alarms)

3. The system has the ability to take time of day into consideration to prevent SMS/emails from being sent to personnel who are not on duty.
4. The system has the ability to pause the sending of an SMS for a configurable time period allowing local action to be taken if possible.

Network Architecture

Ethernet networks have become the de facto standard for modern industrial automation and substation automation networks are no exception. Since the advent of switched Ethernet, the available network capacity and data transfer rates have made switched Ethernet a viable option for industrial applications. Industrial and substation automation networks require careful planning and design for performance and redundancy. Mission-critical processes require data within strict time constraints but other important data flows also need to be accommodated on the same networks. Traffic partitioning using VLANs can address data separation while traffic prioritisation is used to ensure network performance criteria are met when multiple data flows are required to share common trunks. Modern networks are expected to handle the transfer of data from a wide range of equipment ranging from Intelligent Electronic Devices to IP cameras and IP Telephony while meeting the demands of each category of data.

In this application the substation automation system (SAS) network was separated from the rest of the operational and SCADA network due to the phasing of implementation and the multi-vendor infrastructure that was employed. This configuration reduces the design effort for prioritization of critical GOOSE traffic which only needs to contend with MMS traffic. All other communications to and from the SAS network is managed by the firewall. The substation automation network operates in a Rapid Spanning Tree Protocol (RSTP) configuration with dual links from critical IEDs.

The remaining devices all connect to the multi-service network which handles the traffic associated with the FACTS device controller, the PPC, the HMI clients, the Historian, SENS and backup system, the IP Telephony system, the reporting system, and the operations and maintenance related traffic. As mentioned previously, these traffic flows are duly partitioned into separate VLANs with their own IP subnet ranges. All traffic between VLAN partitions is strictly controlled by the firewall.

Remote access to the site for operations and maintenance purposes is facilitated by the firewall using IPSec VPN tunnels to the relevant vendors.

IT/OT Convergence

The convergence of the worlds of Information Technology (IT) and Operational Technology (OT) is a certainty that must be embraced and carefully managed if the benefits of optimized business processes, enhanced decision making potential, reduced costs and improved manageability are to be realized.

The reality is that many modern OT systems are underpinned by platforms, software, security and communications standards that have traditionally been associated with the IT world. These traditional associations often cause engineers to forget that the IT world is not necessarily the source of the aforementioned standards. A common example is that the standardization body for Ethernet is the Institute of Electrical and Electronic Engineers (IEEE).

While OT systems are primarily process oriented, IT systems have traditionally been focused on allowing machines to exchange information with humans. OT ranges from equipment such as circuit breakers and sensors to protection IEDs and SCADA systems that monitor and protect the network.

Utility IT systems include Enterprise Resources Planning (ERP) and Geographic Information Systems (GIS) and most technical personnel interact with the organisation's IT and many OT systems using mobile devices.

The distinction between IT and OT is however being rapidly blurred. The Smart Grid is transforming utility operations and pushing IT across its traditional boundary into OT. This integration promises smarter, more cost effective, and more reliable operation. [4]

In the context of renewable energy facilities, the roadmap to leveraging the benefits of the accelerating IT/OT convergence is a flexible communications infrastructure and an architecture that leverages them. The architecture that was applied in this context aims to achieve this. However technology rarely stays stagnant for very long. The key to long term success is adaptation and agility in this area.

High Speed Connectivity and Secure Remote Access

While the technology platforms supporting the underlying SCADA and automation infrastructure can largely be considered hardened IT systems, the same applies to the communications standards that are used for data and information exchange between these systems. TCP/IP is not only used to facilitate device configuration and to provide maintenance interfaces, but is also used for mission-critical data transfer.

The migration to TCP/IP based communications standards is not yet ubiquitous. There still exists a high dependence on legacy industrial control systems and their proprietary communications interfaces. However standardised, TCP/IP-based communications protocols and open architecture standards are replacing proprietary and legacy systems. This replacement has significant impact in the areas of system integration and support.

Erstwhile systems have always demanded onsite maintenance from integrators and vendors. Control and automation systems were always kept physically separate from information systems. One of the key reasons for this was the complexity of integrating these disparate systems. This is no longer the case though as modern communication mechanisms easily facilitate remote connectivity from almost anywhere. [5]

The benefits provided to operators and asset owners for having remote access facilities can only be fully quantified on a case-by-case basis. Examples of the multiple use-case scenarios that exist for secure remote access to mission critical systems include:

1. Suppliers and/or vendors that are located overseas can often take corrective action when problems manifest through remote access to devices. The turnaround time for physical, onsite access can take days or weeks to resolve problems. This can be often be reduced to minutes or hours.
2. Performance monitoring, continuous diagnostics and regular reporting can be done from remote locations by trained staff as an outsourced service where locally trained, site-based staff may be difficult to attract or retain for long periods.

3. Optimisation of control loops and automation algorithms can be remotely monitored and improved at the owner's request.
4. Routine maintenance tasks such as adding or removing users from the systems due to staff turnover.
5. Infrastructure management can also be facilitated remotely as an outsourced service.

While other use-cases can be easily identified, it is clear that there are a number of business cases for providing remote access to the various system components. The key to a successful remote access solution is to identify the use cases and the user roles correctly and implement it appropriately. Examples of user roles include:

- System operators
- Vendors
- System integrators
- System support specialists and maintenance engineers
- Field technicians
- Reporting or regulatory entities
- Customers
- Supply chain representatives
- Managed service providers [5]

A second important key to a successful remote access solution is the speed of connectivity that can be secured for the site. The remote nature of renewable energy sites often limits the options for wide area network connectivity to wireless solutions in the form of satellite or cellular technologies. While satellite links can provide high speed data transfer, the increased latencies experienced on such communications links may hamper certain remote access options.

Once use-cases and user roles have been mapped and a suitably high speed connection option has been procured, a remote access architecture cannot be implemented without due consideration of cyber risk. The reason is simple: protocols and communication standards that provide increased interoperability are in many cases, the same technologies that have been exploited and compromised on the Internet and corporate networking domains. [5]

Control systems of any type cannot afford any undesirable security vulnerabilities. Securing remote access is an integral part of any defence-in-depth strategy. It is essential therefore that any remote access strategy is defined by establishing who requires access to which resources as well as understanding attack vectors that can be created unintentionally.

Virtual Private Networking (VPN) is often considered the best approach in securing trans-network communication – particularly when the Internet is to be traversed. Site-to-site VPN tunnels are built using highly secure encrypted IPSec sessions with constantly changing encryption keys. IPSec is modular in nature and has the embedded capability of allowing the VPN endpoints to negotiate compatible encryption and key exchange algorithms.

Strict access control lists overlay the VPN tunnels thereby ensuring that stateful firewall policies will apply to traffic that has been transported through the VPN tunnels. This adds an additional layer of security designed to limit the devices that a remote access connection is allowed to access and to limit the types of traffic that are allowed into the system.

While remote access is considered indispensable by some renewable energy facilities, it is nonetheless evident that remote access to critical infrastructure resources will always remain a highly controversial topic with solid arguments for and against its implementation. While clear business cases can be made, the risk of potential breach may be considered too high and may be rejected by proponents of control system isolation. A carefully designed and well-tested solution by a trusted integrator can mitigate potential risks to levels where they may be considered acceptable.

Telephony and VoIP

Telephony is an essential communication mechanism and is a critical service for industrial systems. Operators will always need to communicate verbally with remote control centres and other operational staff. All operational matters in industrial plants require verbal communications and the need for telephony infrastructure should not be overlooked or ignored. The reliance on mobile telephony does not always fulfil the requirements of renewable energy facility owners.

Modern IP telephony systems allow for the further leveraging of the Ethernet communications infrastructure. IP telephones connected on the multi-services network make it possible for on-site staff to communicate with each other. This is further enhanced when features such as extension mobility are employed whereby a user can log into any handset with his/her extension number and configuration profile being made available at that handset.

Operational features such as voice recording when communicating with control centres can be critical when identifying the cause of operator errors. Conferencing facilities supported by the telephony system make it easier for on-site and off-site staff to be able to communicate on a common platform. Other features, are also typically implemented to enhance the functionality available to operational and maintenance staff over the lifecycle of the plant. These include features such as voice mail, pickup-groups, and Interactive Voice Response

Security & Surveillance:

Access control and video surveillance are essential to managing a large, geographically dispersed facility. Basic security measures such as access control can provide the necessary deterrent for petty theft while simultaneously maintaining a record of personnel movement. In many environments, access control is used to verify timesheets and to confirm employee and contractor working hours. However, as with all such systems, they can only be effective if they are monitored and not bypassed due to inconvenience. While technology can provide part of the solution, it is clear that the successful implementation of security solutions is highly dependent on the human nature element of the equation.

Video surveillance implementations are essential for post-event analysis. Proper recording of the movement of people and vehicles is essential but video recordings are useless if the recording quality is too low or if recording at low light or dark environments yields poor quality content.

SCADA system integration of video surveillance is on the increase with electrical utilities and renewable energy facilities wanting to include operational equipment in video feeds. Modern video surveillance systems are highly intelligent with the ability to trigger signalling or initiate video recordings based on complex algorithms (including fire detection where supported by the camera).

Video feed and camera quality are however only part of the picture when one specifies a video surveillance system. Modern video surveillance is done over IP networks and storage and retrieval of video footage is digital in nature. Once again, adequate allowance must be made for the increased processing, storage and network traffic when implementing such systems.

I. CONCLUSION

The concept of the Smart Grid is evolving. So too are the enabling technologies that make it a reality. As the technologies evolve, more intelligent Smart Grid solutions will be realized in the renewable energy sector. Advances in monitoring, control, and automation systems coupled with advances in primary plant technologies will allow for more converged and integrated infrastructure solutions.

It is foreseen that more automation will be applied in future systems and has the potential to enhance existing systems. Secure automated off-site backups (in the form of private cloud storage), virtualization and clustering of critical services to improve reliability and availability, and remote infrastructure management centres are just some examples that may become common in the industry.

IT and OT convergence will inevitably produce a homogeneous mixture of technologies which will invariably increase in complexity but more importantly in functionality. Ultimately the economic and technological benefits will dictate the evolution of the industry which will measure success in terms of operational efficiency and profit maximisation.

REFERENCES

- [1] A. Pietrzyk, B. Root, P. Gruhn, "Designing a Control System for High Availability", Allen-Bradley, Bulletin 1492
- [2] B. Magoro, T. Khoza, "Grid Connection code for renewable power plants (RPPs) connected to the electricity Transmission System (TS) or the Distribution System (DS) in South Africa," National Energy Regulator of South Africa (NERSA), Version 2.6, November 2012.
- [3] A. Craib, "Standard for the interconnection of embedded generation," Eskom Group Technology, Revision 1, Doc no. 240-61268576, October 2013.
- [4] J Meyers, "How the Convergence of IT and OT Enables Smart Grid Development", Schneider Electric, 2013.
- [5] "Configuring and Managing Remote Access for Industrial Control Systems", Centre for the Protection of National Infrastructure, Homeland Security, November 2010.

BIOGRAPHIES

Sagar Dayabhai received his BSc Eng (Electrical) degree from the University of Witwatersrand, South Africa in 2009 and his MSc Eng (Electrical) degree in 2014. He is a registered professional engineer with the Engineering Council of South Africa (ECSA). After working at Eskom in the field of Telecommunications and SCADA, he moved to Consolidated Power Projects (CONCO) as a Senior SCADA / Automation Engineer. Sagar now holds the position as the System Control Manager at CONCO Energy Solutions Division.

Peter Diamandis received his BSc(Eng)Elec from the University of the Witwatersrand in 1991. He started his career in Eskom's Measurement and Control Department in 1992. Since 1996 he has been implementing and consulting on the design of substation control systems with particular emphasis on data communications. He has worked on numerous projects both locally and abroad and is a strong supporter of IEC 61850 and its related technologies. He also provides extensive training in these fields.

