The role of virtualization in a smart-grid enabled substation automation system.

Mr. 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

In order for an aging power utility to exploit the benefits of smart grid technologies in a modern Substation Automation System, the need for rugged computing platforms with faster processors and an increase in reliable storage capacity is essential. The performance requirements are attributed to modern, distributed software applications which require fast processing. The cost of such industrially-focussed ruggedized computing platforms which meet specific operating requirements can be substantial and the number of devices required per substation can be high depending on the type of applications and/or technologies used and the level of redundancy required. In order to alleviate such costly hardware dependencies, the use of virtualization can be employed to provide an efficient cost effective method of deploying these systems and services.

This paper aims to describe the benefits derived from virtualization in a modern substation automation system and attempts to address the challenges and limitations facing utilities with implementing these systems based on currently available technologies. Leveraging of the common elements within the IT/OT space whilst maintaining the balance in their convergence and ensuring compliance to the NERC-CIP cyber-security requirements is also discussed.

1 Introduction

Many utilities including utilities in South Africa are currently experiencing a financial diet affecting the state of their power systems. With the balance between supply and demand always remaining tight, some utilities are focusing efforts on the generation fleet to meet available demand. A complimentary approach is investment in technologies pertaining to the next generation smart grid but this is often rejected or postponed due to the costs involved with implementation. It is however prudent not to lose sight of the considerable number of benefits that can be derived from smart-grid enabled technologies including demand side management, efficiency, improved plant availability and reliability amongst other key metrics.

Typical smart grid enabling technologies found in a substation automation applications include: intelligent human machine interfaces (HMIs), phasor concentrator units for Wide Area Monitoring Systems (WAMS), localized authentication servers, engineering workstations, data concentrators for analytics and condition-based monitoring systems, system logic processors, substation gateways, data historians, distribution automation servers, facility SCADA systems, and more. These systems and services are designed and built to facilitate long term operations and maintenance; wide area protection; improved system availability and restoration, minimization of disruptions on the power-system, secure and safe operating; prompt notification of alarms/events and disturbances in the power system, and rapid response and diagnosis of the disturbance.

The high capital cost of these solutions and the correspondingly high operating cost over the lifetime of these applications due to the corporate skill levels that are required to maintain them is often the reason that discourages a utility from embracing these new technologies. While the need for

increasing the skill level of the modern power system engineer is indispensable and unlikely to be an area of cost saving, it may be possible to reduce the capital hardware costs of implementing modern solutions by exploring proven concepts such as virtualization for implementing smart-grid enabled solutions. The concept of virtualization allows the utility to consolidate and execute multiple applications on a single or redundant cluster of high performance hardware responsible for executing the hypervisor and virtual machines in a multi-operating system environment. The discipline and process of managing these systems has conventionally been widely adopted in the enterprise / IT environment and its benefits are slowly being realized in the OT space.

2 Smart Grid Technologies

Utilities are currently investigating and implementing various smart grid enabling technologies and developing strategies which describes the new smart-grid paradigm envisioned for their country's electrical infrastructure. This is being done with the idea of improving the efficiency and utilization of the power system amongst other key metrics promised in the smart grid. These technologies are constantly being used in a substation environment in various capacities and include:

a) Advanced Human Machine Interfaces (HMI)

The HMI platform in a substation provides the substation operator with the ability to monitor and control the electrical infrastructure. The system often includes an intelligent annunciator/alarm server; advanced trending for power system disturbance analysis, fault recording capabilities and a series of network management and protocol drivers that are responsible for the data acquisition from all the IEDs in the substation. This role-based access controlled (RBAC) system typically resides in a high performance computing platform in the substation.

b) Substation Gateway

The substation gateway is typically responsible for protocol conversion, collecting metering, status, event and fault data from the serial or LAN-based devices in the substation. This data is then made available locally through an alarm server or remotely to a SCADA master station through a variety of tele-control protocols using serial and/or LAN based connections. In addition, typical gateways provide secure pass through / tunnelling services allowing remote engineering access to substation IEDs via the gateway. Modern gateways are also equipped with advanced automation features which can be implemented using IEC 61131-3 and fault / data recording capabilities. The substation gateway is usually a substation-hardened computing platform that executes a number of applications.

c) System Logic Processors

System logic processors are high-speed processing computers equipped with a programmable logic controller (PLC) which uses IEC 61131-3 and a variety of native protocol drivers to perform logic, arithmetic and complex algorithms to support the protection and automation system. These functions are typically embedded and performed on the substation gateway, however, in certain instances these applications are isolated. Typical functions that these applications provide include: station-wide interlocking, measurement comparisons, power flow summations, live busbar transfer routines, distribution automation algorithms and sequences and more.

d) Authentication Servers

Lightweight Directory Access Protocol (LDAP) and Remote Authentication Dial-In User Service (RADIUS) are two protocols used to facilitate authentication and authorization. Many devices exist in a substation which require the use of a correct username and password combination before access is granted to the device. There exists a dire need for centralized authentication, authorization and accounting in a substation environment. This need is attributed to the following reasons:

- As the number of systems and services increase in a SAS as illustrated in Figure 1, the number of usernames and password combinations increase.

- In order to comply with NERC-CIP requirements for reviewing and updating access rights and revoking access rights within a designated time period. In large power utilities with hundreds of substations and thousands of critical cyber assets, this is a complex task and cannot be easily achieved natively should an employee decide to leave the organization.
- Due to the barrage of information and level of integration which now exists in a substation, the number of stakeholders that require access to these systems and services has also increased. This increases the complexity in managing usernames and passwords and the level of authorization that should be given to each user for a specific device.

Centralized authentication can assist in the aforementioned concerns as it allows user authentication and authorization to be controlled and configured from a single point. This point will typically reside in the substation using either a RADIUS server and/or an LDAP Server (e.g. Microsoft™ Active Directory or equivalent). The substation centralized authentication server is then responsible for authorization and authentication to all managed devices and synchronizes to an external authentication server for failover purposes should the centralized substation server fail. These authentication servers can be installed on basic computing platforms requiring a modest amount of processing and storage capacity.

e) Synchrophasor Measurement System

A synchrophasor measurement system is responsible for viewing and analysing real-time and historic data retrieved from a Phasor Data Concentrator (PDC) / Phasor measurement unit (PMU). The system also serves as a data repository for past events allowing stakeholders to analyse past disturbances and do a root cause analysis on the fault. Common systems also include an advanced trending system which indicates frequency, voltage, current and power in order to assist in analysing the disturbance comprehensively. Furthermore, these systems support exporting this data to ASCII, CSV or other equivalent formats for post analysis. This software typically runs on a high performing computing platform with sufficient storage capacity to accommodate the high resolution data that is being archived.

f) GOOSE Applications

In a SAS, the use of IEC 61850 GOOSE messages defined in IEC 61850-8-1 is typically employed for high speed communications between IEDs in order to exchange status information, inter-tripping signals, interlocking and measurement information. However, a number of applications exist which employ the use of GOOSE messages in a computing platform. These include:

- A number of software commissioning tools and applications that support the publishing and subscribing of GOOSE messages the testing support described in IEC 61850 Edition 2. These applications assist in fault finding and commissioning/testing protection IEDs in a substation.
- Digital Fault Recording applications can also employ the use of GOOSE messages to receive status signals for event recording and playback/analysis of a disturbance.
- GOOSE performance testing applications are also used to monitor the status of GOOSE messages traversing through the SAS.

The aforementioned applications required Network Interface Cards supporting VLANs and high processing speed computing platforms capable of supporting the high speed GOOSE traffic.

g) Data Concentrators

The data concentrator is responsible for interfacing and retrieving of data from IEDs within the substation in order to communicate this information to enterprise level systems. This information can then be used by various stakeholders within the power utility for performing data analytics, monitoring system performance, diagnosing faults/disturbances on the network, network optimization, condition

based monitoring, asset/device management and more. These applications are typically stored in a computing platform which can accommodate large capacity storage, multiple serial and Ethernet ports and high processing power.

h) Network Management Systems (NMS)

Various devices exist in a substation which support SNMP. These devices include switches, routers, firewalls, IP Cameras, IP telephones, computing platforms, substation gateways, logic processors etc. Network Management Systems (NMS) are installed in a substation computing platform responsible for monitoring and controlling the managed devices using SNMP. The same computing platform is often used to host centralised logging servers to accommodate devices in a substation supporting the syslog message logging standard.

i) Power Quality Management

Power Quality Management software applications are used for data recording, detection of power quality anomalies, diagnosis and maintenance of the meters, supply verification and generation of compliance reports. Furthermore, the system monitors & analyses trends from voltage, current, frequency, events, harmonics, flicker, power and energy from data stored over a substantial period of time. Due to the high resolution of data available on the quality of supply meters and the long term data repository that is required for detailed analysis; these applications are typically installed and operated in a computing platform providing large storage capacities.

j) Engineering Workstations

The engineering workstation serves as the data repository for all the necessary applications, configurations, firmware, settings and documentation (including substation drawings) required to configure, operate and maintain the systems and services which exist in the substation.

k) Security and Surveillance System

The security and surveillance system is responsible for providing the following functions in a substation:

- Access Control.
- Fire/Smoke detection.
- Security system with advanced notification.
- Surveillance system with night vision, motion detection and 24/7 recording.

These systems are usually accessed through a web-browser or a thin client accessible on the security and surveillance VLAN. They can be accessed via any computing platform in a substation which has access to this VLAN.

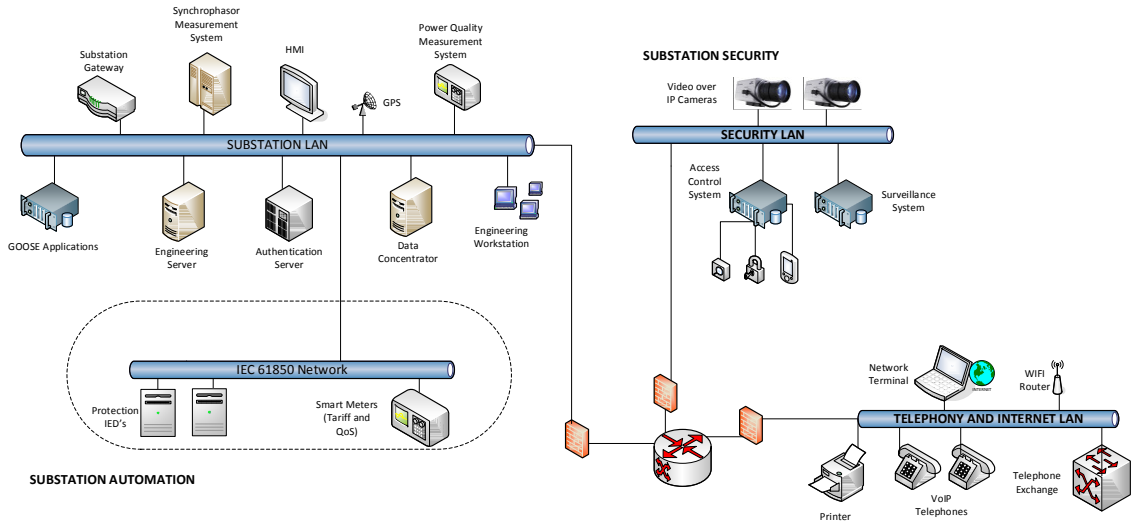

Figure 1: Typical network architecture of Substation Automation System (SAS).

3 Role of Virtualization

The cost of ownership of the aforementioned applications should not be underestimated and coupling fast processing, high capacity storage computing platforms designed to operate in a substation environment to host the applications illustrated in Figure 1 can often increase the cost of the SAS thus discouraging its implementation. In order to alleviate this problem, the concept of virtualization can be employed in the substation environment [2]. Virtualization technology exploits the use of hypervisor to run virtual machines. The hypervisor is responsible for running and managing guest virtual machines each with their own operating system. Each application in the substation will be operating on a separate guest virtual machine. These virtual machines share the virtualized hardware resources which belong to the same computing platform. In this manner, a substation can utilise a high performing computing platform with a hypervisor and multiple guest virtual machines as opposed to purchasing a physical computing platform for each system.

A hypervisor can be classified according to a type 1 (bare-metal) or type 2 (hosted hypervisor). These are defined as follows:

- Type 1: the hypervisor runs directly on the host hardware and manages multiple guest operating systems. Examples of Type 1 hypervisors include VMWare ESX/ESXi and Microsoft Hyper-V operating on Windows Server 2008/2012 [3].
- Type 2: The hypervisor runs above a conventional operating system. Guest virtual machines are abstracted from the host the operation system through the type 2 hypervisor. Common examples of type 2 hypervisors include: VMWare Workstation, VMWare Player and Oracle Virtualbox.

A number of factors exist which a power utility should consider when determining the correct hypervisor for their substations. These include:

- The different operating systems that are supported on the guest virtual machines [3]. The power utility is -required to do a software audit on all applications required in their substations in order to ascertain the different operating system support that is needed on the hypervisor.
- The capacity of RAM that can be allocated per guest operating system.
- The number of processors that be assigned per guest operating system.
- The type of memory management mechanisms that is available on the hypervisor. Typical examples include:

    - VMWare actively monitors all virtual machines and can use RAM from guest VMs that are currently not using their full allocation.
    - Microsoft Hyper-V manages the memory usage of the guest operating system and reports this information to the host which can dynamically assign additional memory to the guest VM.
- The maximum number of guest operating systems per hypervisor [3].
- The ability to perform thin provisioning memory optimization [3].
- Live migration or similar capabilities.
- Networking support and features including VLANs, NIC teaming features,
- The licensing model of the hypervisor and the various scalability options that exist in order to accommodate small (Distribution), medium (Sub-transmission) and large (Transmission) substations.
- The support available from the vendor.

a) Virtualization Architecture in a Substation

Figure 2 describes the virtualization architecture proposed for a substation. In the typical enterprise / data centre environment, the use of virtualization is widely adopted by companies throughout the globe. However, the architecture is predominantly focused on a high availability architecture rather than a disaster recovery architecture. The high availability architecture is based on the following:

- Independence from any hardware failures [1].
- Protection from planned / unplanned outages [1].
- Operating virtual machines in a cluster configuration. Clustering is a technique for ensuring high availability [5]. This technique facilitates replication, fault tolerance and disaster recovery for nodes in a virtualized environment. This technique requires virtual machines to be installed at distributed servers. These virtual machines are logically connected across several physical networks [1].
- No local hard disks are used in this architecture.
- Multiple I/O paths to external storage infrastructure [1].
- No single point of failure (SPOF).

It is not economically or financially viable for power utilities to design for a high availability systems given the costs and complexity associated with its implementation at this stage. It is more cost effective to design for a disaster recovery scenario with adequate redundancy. The hardware considerations for such are scenario are detailed below.

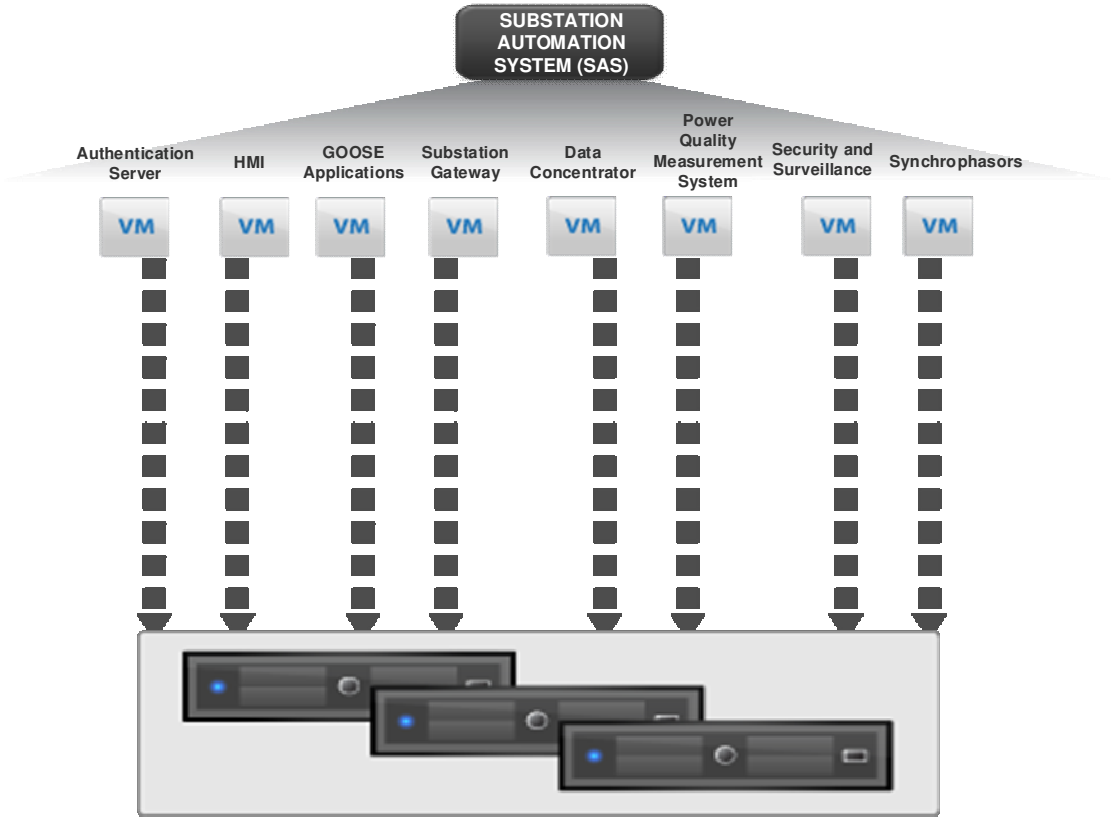

Figure 2: Virtualization Architecture of Substation Automation System (SAS).

b) Hardware Considerations

Adequately sizing and specifying the correct computing platform is essential in order support the architecture described in Figure 2. A number of factors need to be considered by the utility during this evaluation. These include:

- A high speed computing platform is required that can support multiple CPU's, multiple cores per socket and a minimum of 32GB of ECC RAM. This requirement will support the installation of a type 1 hypervisor with a minimum of 3 guest virtual machines.
- Due to the high speed data transfer required and the amount of data being used for storage and processing, the need for hot-swappable solid state disks (SSD) is a key enabler for high performance reliable data storage.
- The computing platform is required to support virtualization (e.g. Intel VT) in order to allow multiple guest operating systems from sharing hardware resources and directly use peripheral devices such as accelerated graphics cards and hard-drive controllers. Typical examples of hardware supported virtualization include the CPU (e.g. Intel VT-x and AMD-V) and the Graphics Processing Unit (e.g. Intel Iris Pro) [3].
- To facilitate disaster recovery, the computing platform is required to support as a minimum RAID 1. This data storage virtualization technology allows the same data to be written to more than one drive. This technology typically used for storage redundancy and performance improvements. Given the costs associated with a high availability virtualization solution, using the RAID 1 virtualization technology offers a much more cost effective solution with minimal downtime in the event of a hard-disk failure.

- The computing environment should be designed and tested to exceed the rigorous industry standards required for harsh operating environments of a substation. The system is required to reliably operate at extreme temperatures, against electromagnetic radiation, electrostatic discharge and extreme vibration/shocks as dictated in different parts of IEEE 1613, IEC 61850-3, IEC 61000-4 and IEC 60255.
- The computing platform should support Network Interface Cards that are VLAN tagging and trunking capable and should include multiple Ethernet ports with different MAC Addresses. This facilitates the segregation for different systems and services per port as described in Figure 3.
- Two computing platforms to be used for redundancy and support for live migration.

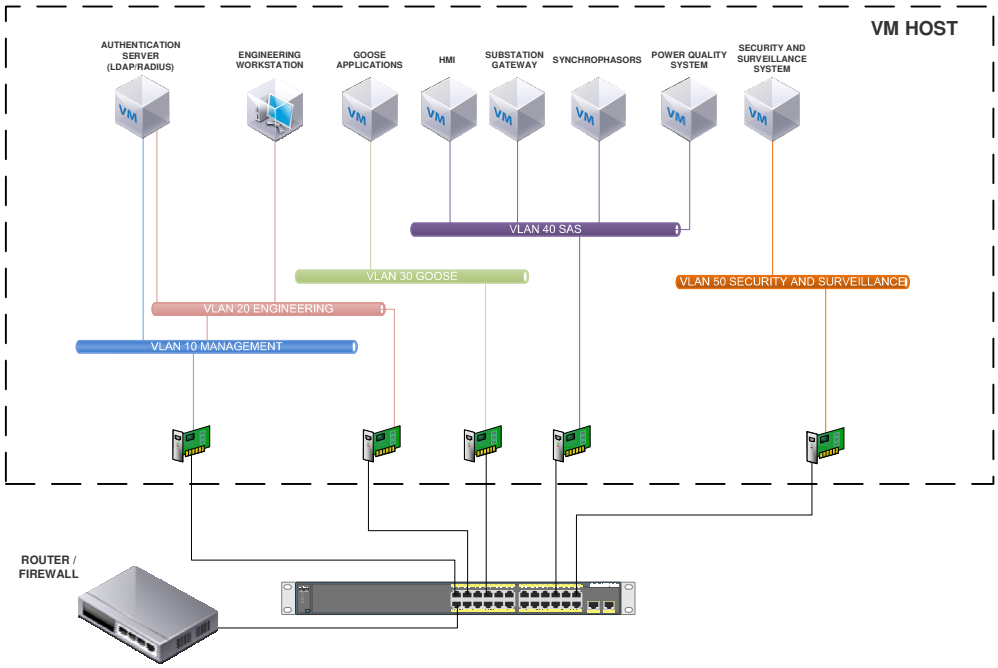

Figure 3: VLAN architecture for a virtualized Substation Automation System (SAS).

Figure 3 describes the VLAN architecture that is employed in a substation using virtualization technology. All authentication and authorization is managed via the authentication server residing in VM1. This virtual machine is not linked to any physical interface but linked through a virtual interface to all VLANs requiring authentication. Each VM is then designated a specific VLAN based on the type of applications that reside in the VM. These VLANs are either associated with a physical network interface or a virtual interface depending on the requirement. The substation router/firewall described in Figure 1 forms a critical component of this architecture in order to manage the inter-VLAN routing and the security functions and policies. Separate interfaces exist for the management VLAN which is directly linked to the host and for the Redundancy VLAN which is used for live migration.

4 Benefits of Virtualization in the Substation Automation System (SAS)

Some of the benefits with implementing virtualization in a substation include:

- Improved operating efficiency and reduced hardware dependencies.
- Reduced costs of procuring and maintaining hardware computing platforms.
- The use of live migration to provide redundancy for critical virtual machines. Live migration provides the ability to move running virtual machines between hypervisors [1]. In a substation

environment, for a disaster recovery scenario, live migration is an elegant method of having a failover system should a critical VM fail.

- Out of band management of operating systems for management and security tasks.
- Hypervisors support software teaming in order to improve the speed and reliability of the communication interfaces.
- Hypervisors support the ability to create snapshots at various instances of the VMs lifecycle. During commissioning and maintenance of the substation, the facility exists to restore a system to a previous point in time. This facility is useful when issues are experienced in the system during new installations, software/file corruption, etc.
- Ease of commissioning using zero touch installation techniques. Using virtual machine management systems, the flexibility exists for the power utility to create a single "golden image" of a virtual machine which can be then be used as a template for multiple substations.
- Backing up VMs in real-time for disaster recovery applications using replication techniques (e.g. Microsoft Hyper-V Replica).

5 Challenges and Limitations on Hypervisors

At present there are a number of challenges and limitations with current type 1 hypervisor products that are commercially available. This is in light of the fact that these hypervisors were developed with the intent of being mass deployed in a data centre environment having the flexibility of being abstracted from the host hardware. These challenges are discussed below.

a) Serial / USB Pass through connections

A number of devices in the substation require the use of serial ports typically for Command Line Interface (CLI) access and firmware upgrades. Currently, common type 1 hypervisors are unable to natively perform serial/USB pass through connections due to the hardware abstracted nature in which these hypervisors have been designed. Furthermore, this abstraction has supported key features which are deployed and large used in a data centre environment (e.g. Live Migration, Zero Touch installation of images etc.). This limitation requires the use of external IP based serial/USB device servers. Furthermore, not all device servers support the option of having multiple VMs connect to the same server despite a different port on the server being accessed.

An issue that exists with common hypervisors is the ability to display each VM through a specific video port in the computing platform. Currently applications such as remote desktop services using the RDP protocol can be used to access each VM independently. However, this method does have limitations and requires operators in the substation to be skilled and proficient in working with computers and understanding basic networking principles. In addition, remote desktop services operates in a single shared server environment allowing only a single user per instance. A method of alleviating this limitation is through the use of virtual desktop infrastructure (VDI) which supports multiple instances in a client/server model.

b) Software Licensing

The use of virtualization in a substation introduces a few challenges which need to be addressed by the OEMs and power utilities. These include:

- The ability of the product to operate in a virtualized environment with a licensing model developed for this purpose. Furthermore, vendors are required to develop a pricing model that will accommodate this scenario as typical software licenses are subscription based.
- Traditional operating systems (e.g. Microsoft® Windows™) were installed and licensed by the IT domain within the power utility. The licensing model of these operating systems were typically managed by the IT department on behalf of the power utility for all corporate

business activities. The use of virtualization in a substation environment now introduces this challenge of installing and managing operating system licenses in the OT domain which needs to be managed and addressed decisively in order to control and manage the number of licenses/installations and the costs associated as a result.

- The use of tools such as live migration to aid in disaster recovery and zero touch installations is a key enabler in the substation environment. However, a licensing model needs to be developed by OEMs to accommodate this scenario and prevent duplication of licenses and increase in costs for the power utility.
- A finite number of operating system instances are provided by operating system vendors for VMs. As a result, utilities are required to carefully manage the number of operating systems required for each VM in order to manage licensing costs whilst still maintain the integrity and continuity of software applications in the substation.

c) Hardware Licensing

The advent of type 1 hypervisors has limited the pass-through of USB connections from the host to the guest VMs. OEMs that utilize USB-based licensing devices are required to develop a model that accommodate these devices in a virtualized environment in order to allow applications residing in the guest operating system from accessing the software license.

d) Software Management

Traditionally, the IT domains in a power utility were responsible for anti-virus management, software management, patch management and handling operating system and security updates. However, with the advent of virtualization in substations, traditional methods need to be re-considered and a strategy to manage the cross boundary technology deployment between IT and OT needs to be addressed by a power utility.

e) Hardware Support

At present, additional limitations from a hardware perspective exist in the following areas:

- The need for substation class computing platforms to support the Parallel Redundancy Protocol (PRP). The use of IEC 61850-9-2 process bus based systems recommends the use of PRP in a substation network. At present, IEDs, substation gateways, meters etc. are now being developed to support PRP and the need for the computing platform to support PRP is recommended in order to prevent the use of redundancy boxes for each computing platform which exists in the substation.
- A 10Gbps interface is required between the two computing platforms to perform virtual machine live migration. At present, substation hardened switches are not available with this interface capacity. As a result of this limitation, it would be necessary to physically connect two 10Gbbps interfaces together in order to adequately perform live migration.

f) Skills

There is dire shortage of skills in the OT domain related to virtualization, enterprise level systems typically used in the corporate /business environment and basic networking concepts used in the IT domain. This skills shortages impedes the successful implementation of virtualization in substations and is a challenge that needs to be addressed by power utilities in order to capitalize on the associated benefits.

6 IT/OT Convergence

While OT systems are primarily process oriented, IT systems have traditionally been focused on allowing machines to process information and to exchange information with humans. OT systems are required to ensure the security, availability, integrity and performance of operations and the

equipment used 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 International Society of Automation (ISA), a non-profit, globally operating organization that sets globally accepted standards for automation diagrammatically summarises the IT/OT relationship in organizations as follows:

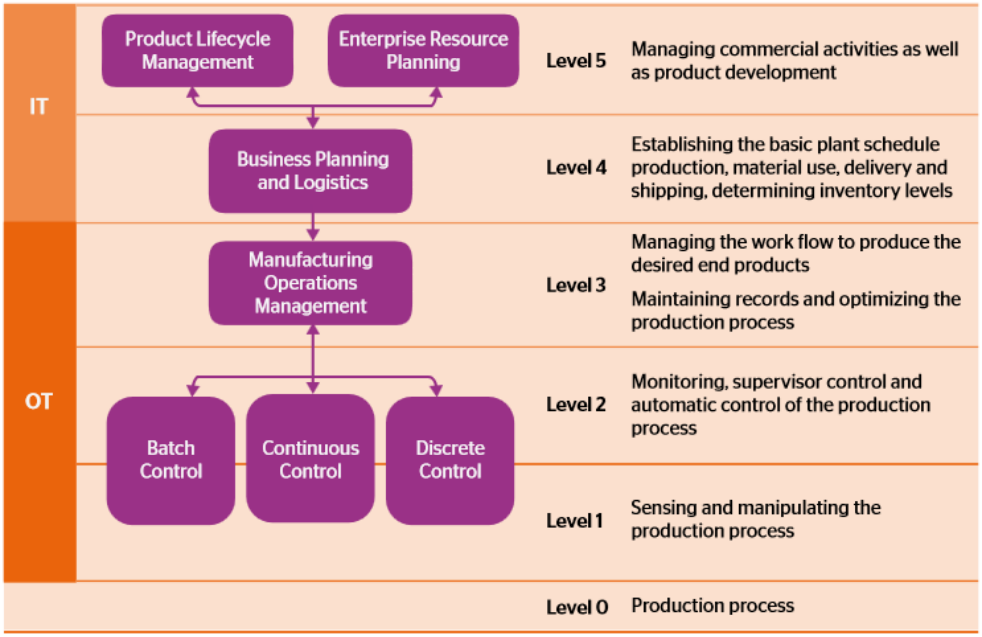

Figure 4: ISA IT/OT Overview

OT, by its very nature has its focus on continuous (24/7) real-time operations and as such, the reliability of equipment is paramount. This makes OT a conservative adopter of technology which has to be well proven before it is even considered for implementation. IT, on the other hand, is focussed on issues of cost reductions, standardisation, and resource optimization and can often get away with an 8x5 approach to operations. IT can therefore afford to be more aggressive in its approach of adopting new technology.

The barriers between the two domains of IT and OT are however being rapidly eroded. The technology and platforms used in IT and OT are becoming more and more similar. 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. This has required the profiles and skills of employees working in the IT and OT disciplines to begin converging.

Industry commentators and analysts such as Gartner have also commented on this trend. "The worlds of IT and operational technology (OT) are converging, and IT leaders must manage their transition to converging, aligning and integrating IT and OT environments, according to Gartner, Inc. Analysts say the benefits that come from managing IT and OT convergence, alignment and integration include optimized business processes, enhanced information for better decisions, reduced costs, lower risks and shortened project timelines." [6]

Successful IT/OT convergence is non-trivial and not always possible. Many organizations insist on strict separation of the domains from a management and operational perspective. For example,

atypical utility may state that IT and OT platforms shall not share the same physical infrastructure (e.g. Ethernet switches, routers etc.).

In organizations where the IT function is largely outsourced, the burden of the harmonization of strategies and the re-skilling of the workforce therefore rests on OT. It is the authors' opinion that OT personnel in the electricity supply industry must incorporate IT skills into their capabilities as part of the process of continuous professional development. This would allow the OT workforce to become proficient in technologies and procurement policies to address, amongst others, the following issues:

- Development of a common governance procedure;
- Development of common standards and policies (as applicable);
- Leveraging of common infrastructure and sharing common technology platforms;
- Sharing enterprise software license agreements and support contracts;
- Utilize corporate contracts for hardware/software procurement (where applicable);
- IP Address allocations for Wide Area Network integration.

IT/OT convergence further means that regulatory requirements and their associated governance frameworks as well as security issues can be jointly addressed by IT and OT, leading to an integrated approach.

The North American Electric Reliability Corporation (NERC) developed a set of reliability standards which include a set of nine Critical Infrastructure Protection standards. These CIP standards address the security of cyber assets with the purpose of ensuring reliable operation of the electric grid. While compliance to these standards is mandatory for North American Utilities, most utilities worldwide subscribe to these standards to varying extents as they present an industry-accepted best-practice approach to most issues governing cyber security.

IT product vendors in both the cyber security and virtualization arenas have integrated compliance modules within their software suites to provide reporting with respect to the aforementioned NERC CIP regulatory compliance requirements. While such modules provide the benefit of aiding with audits and reporting, they still require the correct skills and training to use them correctly.

Compliance issues and the centralised management of infrastructure (e.g. enterprise software licenses) will require significant collaboration among the engineering, IT, and Operations departments.

7 Cyber-security

Within the context of cyber-security it is essential to treat each virtual machine as well as each host server with its own entry on the Cyber Asset register. Interestingly, if any one of the virtual machines is considered critical, then so is the host server hardware.

Cyber-security focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction. The process of securing cyber assets is not static. It is not simply a matter of installing a device such as a firewall in an attempt to secure the "electronic security perimeter" and assuming that the security function is completely addressed. The security landscape is constantly changing and is affected by ever-changing threats, product vulnerabilities, rapidly changing technologies, business processes, and people. Security is an ecosystem and must be treated as such. The United States National Institute of standards and technology depicts this ecosystem as a life cycle framework and is show in Figure 5 below.

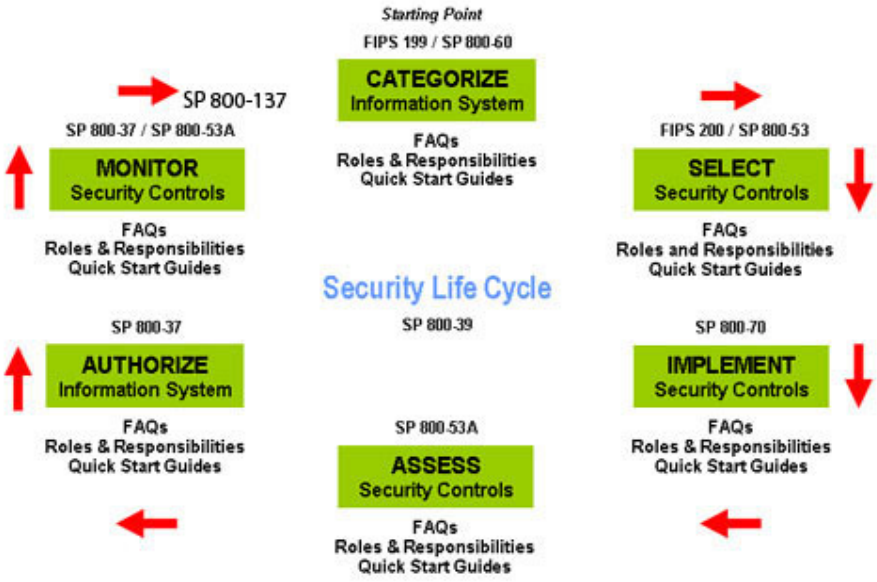

Figure 5 - NIST Security Framework

With reference to Industrial Control Systems, the NIST SP 800-82 Guide to Industrial Control Systems (ICS) Security states: "ICS security objectives typically follow the priority of availability, integrity and confidentiality, in that order."

In order to ensure that an industrial control system can continue performing the task it was designed to perform, it must prioritise data by availability because ensuring that the process remains within normal operating parameters is paramount. Data availability is followed by data integrity and confidentiality. In IT, the data priorities are reversed because in the world of IT security, information security is paramount.

"Information security has its roots in cryptography, where historically the paradigmatic problem was to protect military secrets that were broadcast by radio. The object to be protected is static in information security; it is information content that may ultimately be printed out. For control there is no static object to be protected. The aim here is to reliably execute control logic within real time constraints."[7]

Modern cyber-security solutions must encompass features that far-exceed familiar access control lists. Intrusion prevention, advanced threat prevention, heuristic determination of unknown threats, application control, control system protocol inspection, logging, forensic analysis, micro-segmentation, best-practice recommendations and regulatory compliance capabilities are some of the many features available on modern cyber-security systems that are designed for control system applications.

Cyber-security and security are broad topics and must be designed into all IT and OT systems at all layers and levels of implementation. It cannot and should not be added as an after-thought with the intention of merely meeting a deliverable. Security must be a part of an organisation's DNA and must be taken seriously to achieve its desired goals of ensuring reliability, service-continuity and safety. Gone are the days where control and automation systems were considered "secure" because they were not directly connected to corporate IT systems. Modern systems require at least some level of interconnectivity to enhance business processes and service delivery.

Securing systems is a complex and daunting task and is complicated infinitely because the process requires humans to perform the task – continuously. Planning, common sense and a keen sensitivity to business and regulatory requirements is required to ensure success in this area.

Security is a multi-layered discipline that is the responsibility of every member of an organisation and must be managed accordingly.

8 Conclusion

Virtualization is clearly an emerging technology in the electricity supply industry. It is not a silver bullet but it is nonetheless a disruptive technology which will, in all likelihood, displace the established solutions. By its very nature, it has ingrained features that cannot be duplicated without additional cost and difficulty with the traditional solutions. The promise of high availability, backup and recovery, disaster recovery, the ability to run legacy applications and the cloning and snapshotting capabilities make for a very persuasive value proposition. However, as with all technological advancements, virtualization is a two-edged sword. Virtualization requires us to be careful of how we describe security in this context. It also adds a layer of complexity and integration difficulty. The challenge of the training of OT staff in a field that is historically seen as IT can also not be neglected. Furthermore, there is also the perception of higher costs although this is typically limited only to the initial procurement of high-performance systems.

The pace of technology disruption is increasing and it is affecting the traditionally conservative OT world at an alarming rate. The only practical way to take control of the pace of change is by up-skilling staff and ensuring that governance issues and compliance with regulatory frameworks are constantly revisited and addressed – not only for the purpose of checking the right boxes but for the purpose of providing reliable solutions.

REFERENCES

[1] B. Berger, "*Hyper-V Best Practices*", Pakt Publishing, ISBN 978-1-78217-609-1, November 2014.

[2] M. Brown, "*Virtualization with SEL Rugged Computers*", Volume VII, Application Guide, AG2015-11, November 2015

[3] S. Lowe, "*Hyper-V™ vs vSphere™: Understanding the differences – whitepaper*", SolarWinds, Inc., 2012.

[4] C. Gordon, "*Configuring a Windows® Server for Centralized Authentication with LDAP-Enabled SEL devices*", Application Guide, Volume II, AG2013-14, November 2014.

[5] K. Hwang, J. Dongarra, G. Fox, "*Virtualization: Physical vs. Virtual Clusters*", TechNet Magazine, April 2012.

[6] 2012, "Gartner Says the Worlds of IT and Operational Technology Are Converging", Press Release, http://www.gartner.com/newsroom/id/1590814

[7] R. Langner, "Robust Control System Networks: How to achieve reliable control after Stuxnet", Momentum Press, 2012, ISBN-10: 1-60650-300-6

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) and a member of the IEC under Technical Committee 57 Working Groups 10 and 15. 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 poistion as the System Control Manager at CONCO Energy Solutions Division responsible for Automation & Control, Telecommunications and SCADA systems.

Peter Diamandis received his BSc Eng (Electrical) degree 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 this field.