21, rue d'Artois, F-75008 PARIS
http : //www.cigre.org

CIGRE US National Committee
2022 Grid of the Future Symposium

Virtualization of Protection & Control – Evaluation and Deployment Considerations

J. VALTARI
ABB Oy
Finland

D. BARADI
ABB Inc.
USA

SUMMARY

Virtualization of Protection & Control systems (VPC) offers to create vendor agnostic Protection & Control hardware in IEC 61850 based Digital Substation and pave the way for a novel model which can readily adapt to an evolving grid and offer a pathway to development of new digital applications. This paper will discuss main system aspects and key technical requirements in considering virtualized Protection & Control systems. The virtualization technology and the networking aspects are discussed using performance benchmarks laid by IEC 61850 standards. Results from deployment of Centralized Protection & Control (CPC) and Virtual Protection & Control are discussed and oscillographic waveform indicating performance results of protection are detailed.

KEYWORDS

Digital Substations, Virtual Protection & Control, IEC 61850

dinesh.baradi@us.abb.com

1. Background – need for reliable flexibility increases

By necessity governmental targets for achieving carbon neutrality are ambitious, with some targets as soon as by 2035. This means that the change needs to happen very fast. Electrical energy will replace other forms of energy, since it is one of most flexible forms of energy that is possible to produce and distribute with a low carbon footprint. Electricity systems are becoming increasingly essential to the functioning of society, and as a result we need to redefine what system resilience means.

With increasing penetration of renewable energy and advent of wide-scale adoption of Battery Energy storage systems (BESS), power generation, distribution has become increasingly complex and less predictable, the grid must become more flexible and consumer-friendly to facilitate bi-directional flow of power and still meet or exceed system reliability requirements. The required rate of change in the system will be exponentially higher compared to slow and gradual changes occurring today. This will create a challenging combination – how does one simultaneously increase the rate of change and improve robustness and reliability? The implication of this is that we will see new approaches when it comes to addressing 'system resilience', with digital technologies playing a key role.

Overall system resilience is a key factor in the electric grid, as it will also determine and limit the maximum speed of systemic change. New innovative technologies viz., 5G, virtualized real-time computing etc. can be connected to the grid only if doing so does not reduce the resilience of this critical infrastructure. With accelerating adoption of EVs, vehicle-to-grid technologies are being piloted or in-phase of deployment. Traditionally resilience has been related to maintaining the power balance and protecting against network faults, resilience of the grid will evolve to a broader definition. During recent years cyber security has also become increasingly important. Furthermore, the aspect of adaptability and updateability of the system will emerge.

Therefore, it is likely that we will see the emergence of new digital platforms that are operating in live mission critical environments, while being constantly updated. The needs are clear, and for the first time, we also have technologies available for realizing such platforms, including, Machine Learning and Artificial Intelligence (AI) along with 5G, virtualized real-time computing. A key challenge will be the optimal integration of these technologies.

2. Protection system evolution

Protection in power systems has been subject to several technological advancements. From electromechanical mechanisms to the microprocessor intelligent electronic device (IED) [1], relaying has been an essential aspect to the continuing development of a more flexible, interconnected, and smart power system that assures dependable and secure delivery of electricity to consumers.

Technologies mentioned above (1) and standardization offered by IEC 61850 has driven an interest towards Centralized Protection & Control system. With increasing adoption of IEC 61850 and evolving nature of the power system there have been products and system engineering tools available on the market that support this architecture. The main idea of the Centralized Protection & Control (CPC) [2] concept is to move the Protection & Control functionality from multiple bay level devices to a single central processing unit within a substation, leaving only the process interface functionality in the bay level Merging Units

(MU). The targeted benefits are related to improved functionality and reduced overall lifecycle costs [3]. An overview of a CPC system, with redundant CPC devices in shown in Figure 1.

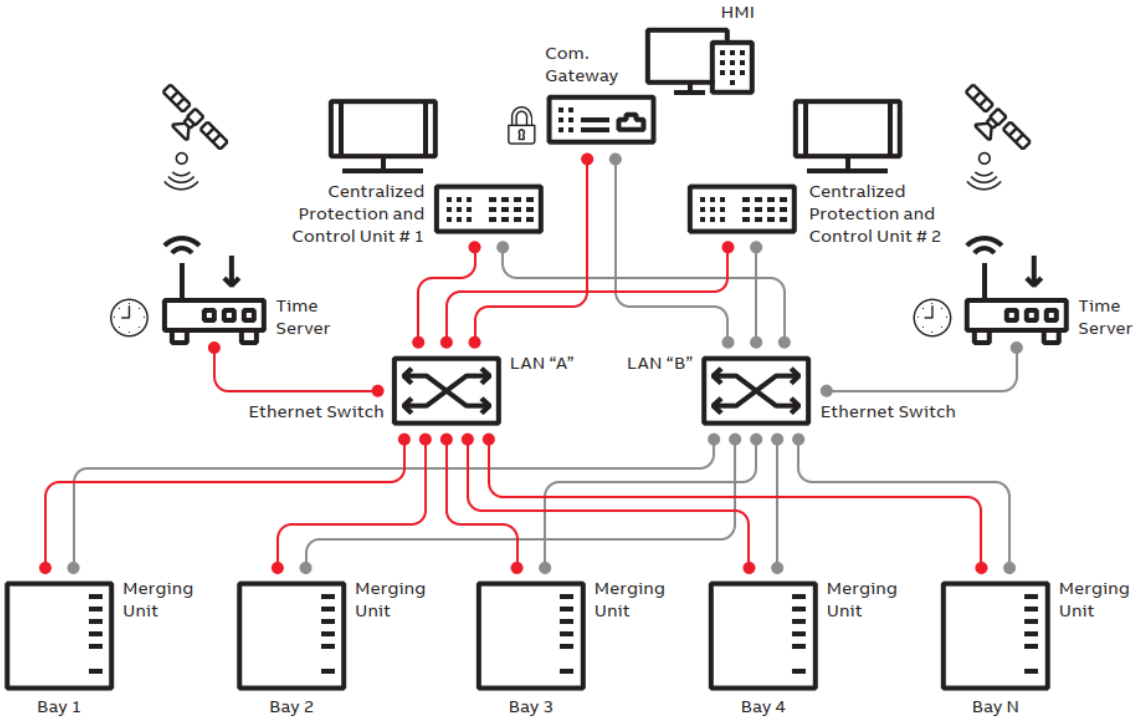

Figure 1. Centralized Protection & Control system with redundant CPC units [4]

An evolutionary step in centralized Protection & Control is to make protection & control more software-driven and hardware-agnostic thus resulting in Virtualized Protection & Control (VPC). This means that the protection application is not anymore tied to a particular centralized device, but it is a software image that can be freely deployed to versatile industrial server architectures in different environments

3. Virtual Protection & Control overview

The term virtualization broadly describes the separation of a resource or request for a service from the underlying physical delivery of that service [5]. Virtualization, as applied to protection & control is the use of software for creation of an abstract image of a traditional protection & control device inside a physical host that is a ruggedized computing hardware; this hardware is based on an open architecture. With a software image providing real-time, deterministic protection & control, replicability of this image for creating several instances becomes easier. Containers with different software applications providing monitoring & diagnostics can reside on the same host machine. For instance, a set of protection, control and metering functions of several electrical apparatus residing in a virtual machine (VM) and can provide amongst several elements, line distance, transformer differential, set of directional overcurrent functions etc. Addition of a UFLS (underfrequency based load shedding scheme) or interconnection specific functions, for IEEE 1547 compliance, would require additional hardware and several different ancillary equipment. In a virtualized environment, this container of functions can be software updated to provide additional schemes and controls. Additionally profiling of load and measurement of system harmonics is no longer restricted to storage and sampling requirements. Utilizing machine learning - system loading and apparatus anomalies can be understood more comprehensively. Dynamic self-regulated control rules can be programmed in separate applications on the same host machine, which can then suggest optimal switching routines.

Real-time and deterministic availability of protection & control is an obvious challenge that can be addressed by dedicating a specific set of CPU cores for such tasks. Allocation of cores to ancillary applications and other VMs can be performed by Virtualization manager, which is a machine level software responsible for resource allocation of the host machine.
Redundancy can thus be addressed at the hardware level with an active host running in parallel to another host/server and still using the same redundant process[1] and station data bus[2] [6]. Station and Process Data may be combined into same physical device but have logical separation by means of VLANs and filter such as MAC-ID etc.
A VPC system with a Virtual Switch (explained in 5.3) is shown in Figure 2.

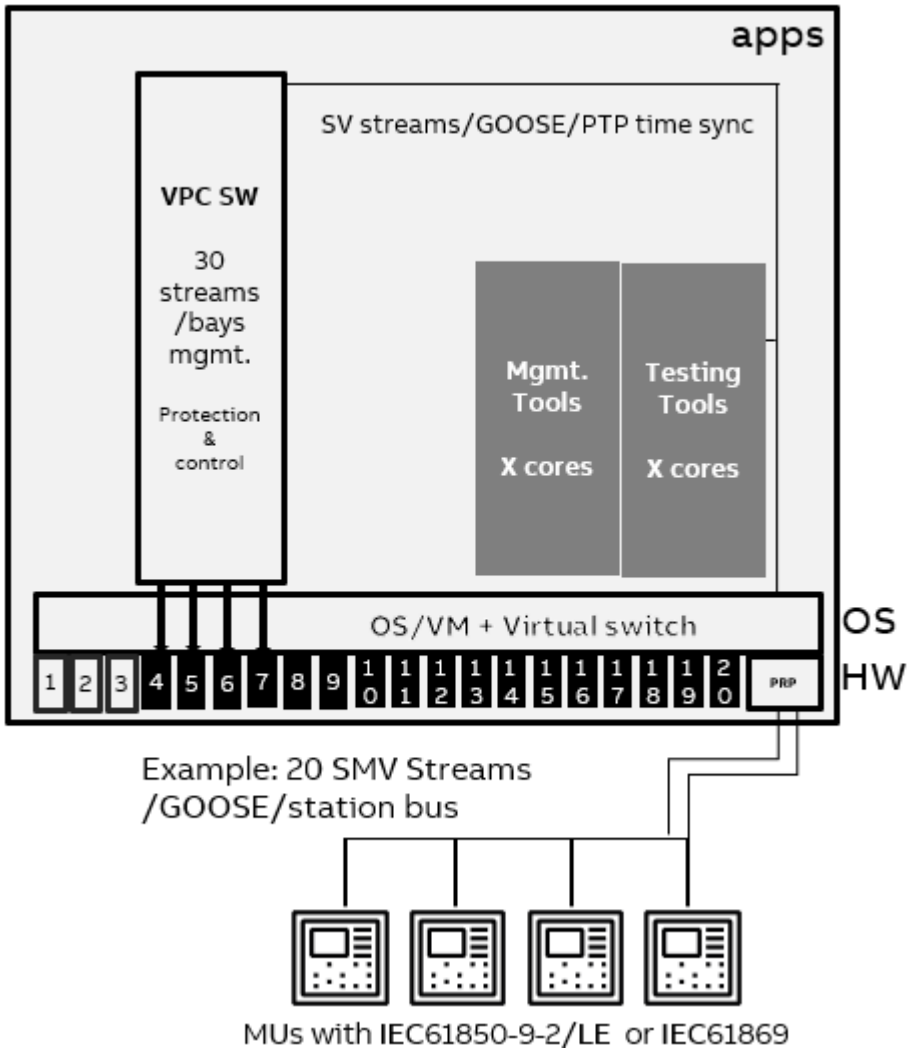

Figure 2. Virtual Protection & Control system overview

An example architecture of a substation with VPC is shown below; the choice of virtualization technology between servers may vary and benefits and considerations are further described in 5.1.

[1] Process Bus connects the primary measurement and control equipment (merging unit)) to the VPC. It is expected to provide real-time quality of service.
[2] Station Bus interconnects the while substation and provides connectivity between central management and the individual bays. It provides only soft real-time quality of service i.e., some jitter in delivery time is acceptable depending on the nature of traffic.

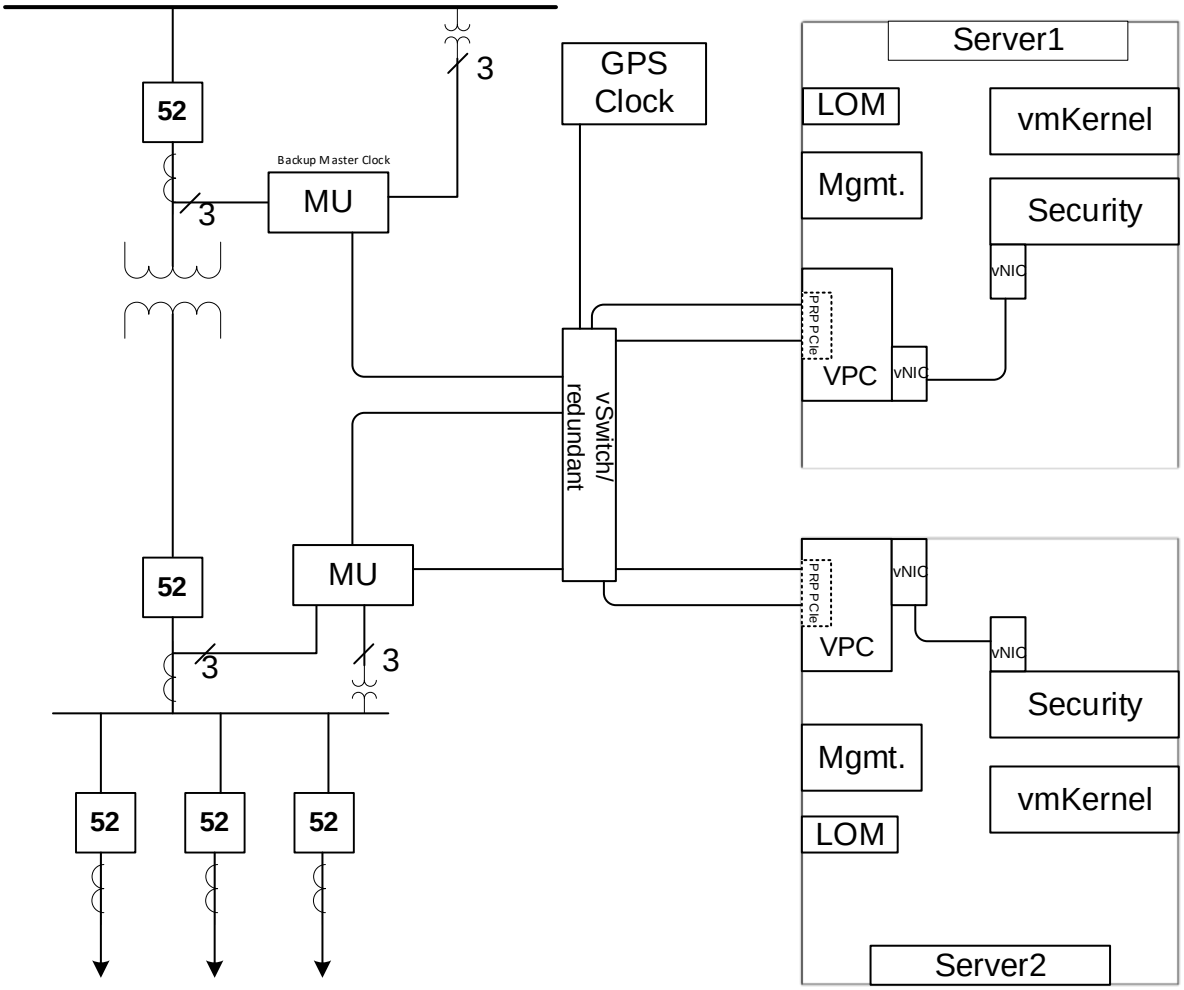

Figure 3: Simplified architecture of Redundant VPC in Example Substation

Merging Units that can auto-configure or provide instrument transformer name plate data in digitized format to a Virtual Protection hardware during initialization/ boot-up can decrease any margin of human error by removing the process of manually entering data during the engineering phase of the VPC. Since several merging units will be transmitting Sampled Measured Values (SMV); SMV ID can remain the only parameter setting that would need to be modified in merging units if system engineering tools can generate unique MAC-ID and APP-ID. Time synchronization using IEEE 1588v2 over IEC 62349-3 standard can generate added level of redundancy in guaranteeing SMV accuracy is maintained in the virtual environment.

4. Main system aspects

When a virtual Protection & Control solution is being deployed, first it is important to think about the overall system aspects, so that main benefits of the approach are achieved. Some key aspects are elaborated below.

4.1. Standardization

One key driver behind the virtualization trend is to increase flexibility and scalability of the utilized solutions and systems. This also indicates a need for an open system, that reduces the risks of vendor lock-in situations and increases the possibilities to combine (and reuse) best solutions from different vendors in one solution. Interoperability and interchangeability of all

SW and HW components is then an essential requirement. In practice this means basing the solution on widely used global standards.

In the area of electricity distribution automation systems, the most important standard is the IEC 61850. Due to wide coverage of the standard and increased acceptance if it, it has been the de-facto choice for all modern Protection & Control systems. With Ethernet-based communication and IT-centric modeling concepts it is also the most natural basis for virtualized Protection & Control solutions.

4.2. Performance requirements

IEC 61850-5 defines already application-level performance requirements, below in Figures Figure 4, Figure 5 and Figure 6, that can directly be used as performance requirements for virtualized Protection & Control solutions. Since the requirements are made from the actual protection & control application needs point of view, they stay the same regardless of the actual technology that is being used (conventional relay-based Protection & Control, CPC, or VPC)

Table 3 – Application of time synchronization classes for time tagging or sampling

Time synchronization class	Accuracy [µs] Synchronization error	Application
TL	> 10 000	Low time synchronization accuracy – miscellaneous
T0	10 000	Time tagging of events with an accuracy of 10 ms
T1	1 000	Time tagging of events with an accuracy of 1 ms
T2	100	Time tagging of zero crossings and of data for the distributed synchrocheck. Time tags to support point on wave switching
T3	25	Miscellaneous
T4	4	Time tagging of samples respectively synchronized sampling
T5	1	High precision time tagging of samples respectively high synchronized sampling

Figure 4. Application time synchronization classes [7]

11.2.1.2 Type 1A "Trip"

The trip is the most important fast message in the substation. Therefore, this message has more demanding requirements compared to all other fast messages. Same performance may be requested for interlocking, intertrips and logic discrimination between protection functions.

Performance class	Requirement description	Transfer time		Typical for Interface (IF [a])
		Class	ms	
P1	The total transmission time shall be below the order of a quarter of a cycle (5 ms for 50 Hz, 4 ms for 60 Hz).	TT6	≤ 3	3,5,8
P2	The total transmission time shall be in the order of half a cycle (10 ms for 50 Hz, 8 ms for 60 Hz).	TT5	≤ 10	2,3,11

[a] Interfaces according to Figure 2.

Figure 5. Trip message performance requirements [7]

11.2.4 Type 4 – Raw data messages ("Samples")

This message type includes the output data from digitizing transducers and digital instrument transformers independent from the transducer technology (magnetic, optic, etc.). The data will consist of continuous streams of synchronized samples from each IED, interleaved with data from other IEDs.

Transfer time means for the stream of synchronized samples a constant delay resulting in a delay for the functions using the samples e.g. for protection. Therefore, this transfer time shall be so small that no negative impact on application function is experienced.

Performance class	Requirement description	Transfer time		Typical for Interface (IF)
		Class	ms	
P7 [a]	Delay acceptable for protection functions using these samples	TT6	≤ 3	4,8
P8 [b]	Delay acceptable for other functions using these samples	TT5	≤ 10	2,4,8

[a] equivalent to P1.

[b] equivalent to P2.

Figure 6. Raw data performance requirements [7]

4.3. Application architecture

When virtualization enables totally free allocation of functionality, it is important to build application architecture based on system needs. IEC 61850 modeling gives also here good tools for new kind of application architecture, as each application entity can be modelled as a separate 'Logical Device' (LD). It is not needed, and often not even beneficial to repeat old relay-based thinking, where todays bay level relays would be just designed as bay-level protection applications running in a VM. Instead, new station (or system) level Logical Devices can be built, where e.g., Low-Impedance Bus-Bar Differential protection, Interlocking logics, or directional protection with back-up schemes can be better engineered.

4.4. Cyber security

Cyber security (CS) requirements mean both specific technical requirements (e.g., requirements from CS standards like IEC 62443, IEC 62351) and operational requirements (flexible updates in case of CS improvements or vulnerability handling). These requirements touch both virtualization environment as well as individual VMs or containers. Also, in this case the recommended best practice is to base the solution on widely used standards and prefer solutions where efficient updating procedures can be achieved. Operational requirements customized to the substation (Bulk Electric System or otherwise) can be designed per NERC CIP interpretations and applicability [8] [9]. Role Based Access Controls (RBAC) configurations can be automatically tied to an enterprise LDAP (Light-Weight Directory Access) or Radius server/application which can then provide MFA (Multi Factor Authentication) and rotate passwords on-demand or based on frequency. Thus, compliance reporting is simplified without adding additional microprocessors/ controllers and networking infrastructure. Collection of Sequence of Events (SoE) and disturbance records from each electrical bay/ switchyard/ protection application is centralized into VPR and stored at single location that can aid in compliance and reporting.

4.5. Testing

When protection & control application is virtualized, also new possibilities for testing are achieved as the testing can be handled in the digital domain. IEC 61850 provides tools also for this, as it defines specific Test Modes for LDs (Logical Devices) and allows all Ethernet traffic to be tagged as 'Simulated' for testing purposes.

In addition to these new benefits there are also new testing requirements, as virtualization layer adds a new element to the system that also needs to be tested, and constantly monitored. This means that self-supervision functionality of the system needs to also include new aspects, real-time operation of the virtualized application. This self-supervision functionality may reside in the actual protection & control VM, or in the hypervisor component, or both.

4.6. Deployment of new firmware

New firmware updates of individual protection applications can be deployed in standby mode in a separate container and real-time performance can be tested over a period before actual deployment. Incremental updates can be pushed for containers and deployed in batches once fully tested.

4.7. Main operational aspects

After technical details and system design it is important to also evaluate the operational side of things – how to operate and maintain the system. If an existing organization does have intermediate level of understanding of VMs and how to deploy them; setting a VPC with guidelines and instructions maybe followed. However prior experience of IEC 61850 engineering would be needed to ensure that technology leap and learning curve are not too steep that create execution delays. Choice of such technology can be made with qualified system integrators that can bring advanced expertise.

5. Key technical considerations

Virtualization technologies have been available for a several years, but so far, the real-time performance for mission critical applications has not been sufficient. Now the situation is changing, and promising solutions are becoming available [10], [11]. Below main technical aspects are evaluated.

5.1. Virtualization solutions and hypervisors

Virtualization solution can be divided into Hardware Virtualization, Kernel-based Virtualization and OS-level virtualization.

Hardware Virtualization is based on abstracting the underlying physical hardware from the guest Operating System (OS), by using specific software components called hypervisors for allocating virtualized system resources and managing the execution of virtualized applications, called Virtual Machines (VM). Hypervisors can be further divided into Type-1 hypervisors that run directly on system hardware, and Type-2 that run on top of host OS. Type-1 hypervisors are more suitable for providing predictable performance to virtual machines (VMs) than Type-2 hypervisors because they directly interact with the hardware and have full control on hardware resources allocated to VMs. The host OS layer between the hardware and the hypervisor in Type-2 hypervisors can introduce unexpected and unpredictable delays to the hosted hypervisor and then to the VMs on the hypervisor. In addition, any security vulnerabilities and flaws in the host OS could potentially compromise the Virtual Protection & Control VM.
Kernel-based Virtualization means that virtualized applications are executed as part of an operating system. Applications with different safety and security levels can be run on the same hardware, protected from each other by means of software partitioning (also called as virtual machines). The partitions can contain different applications with their own operating systems. KVM offers features such a live migration, resource scheduling and control. For virtual protection & control this helps is balancing the computing capabilities between two physical

host machines and eliminates hardware dependencies. Live migration offered may not be desirable for critical SMV traffic as the failover and recovery times are in millisecond range.

OS-level Virtualization is the newest way of handling virtualization, where the OS components (such as memory access, file system and network access) are abstracted to the guest OS. In this case Host OS is the same as the one used in each guest OS. Due to so tight coupling OS-level virtualization imposes low (if any) overhead in terms of resource usage. OS based services such as backup and recovery, security management as well as integration with Active Directory (AD) are available which can help in compliance management for CIP

Different solutions have their own strengths and weaknesses, that are extensively elaborated in literature. Hardware Virtualization provide strongest isolation between different VMs, whereas OS-level virtualized containers provide lowest overheads. Main aspect to highlight is, that with all mentioned solutions it is possible to achieve required deterministic operation and reliability for Protection & Control purposes.

5.2. Case for hardware acceleration in Protection & Control

Hardware acceleration technologies have enabled the idea of adoption virtual protection as it can provide guaranteed service to SMV and GOOSE traffic for protection functions. Since Protection & control is a process-intensive task, using such technology can allow better hardware resource allocation and performance. Type 1 hypervisors use hardware acceleration (enabled through BIOS of the host hardware) and would be mostly preferred for Protection & control virtualization, Type 2 hypervisors can rely on hardware acceleration through their host OS layer but will fall back on software emulation in absence of native support.

5.3. Network virtualization

In virtual protection & control solution one key aspect is reliable handling of network virtualization. Protection & Control (P&C) applications are dependent on SMV and GOOSE data coming from Merging Units, so handling this traffic in real time is as important as is the execution of the actual P&C application. Virtualization of Network Interface card (NIC) can occur at the Media Access Control (MAC) layer. The physical NIC simply becomes a port forwarding backplane. The Process and Stations Bus traffic from individual bays can be virtualized on the physical host where the VPC is running. With virtualization, it is possible to utilize guaranteed bandwidth feature that allows vNICs to reserve a hardware traffic lane [12] for SMV traffic which is a stream of 80 Samples/cycle (approx... 5..6 Mbit/s) constant load on the network. [3]

Different network virtualization technologies are evaluated in more detail in Linux environment in [13]. Simplest solution is to use direct *host* access, but it provides no isolation and can lead to issues in both network performance and management. Physical Ethernet switch can be emulated as a *bridge*, or as a *MACvlan (version of software bridge in Linux)*. Single root I/O virtualization (*SR-IOV*) is an extension to the PCI Express specification, and allows a device, such as Network Interface Card, to virtualize its resources. Results in [13] show that different network virtualization technologies are indeed sensitive to system and network load situations,

[3] 5 Mbit/s (50Hz) or 6 Mbit/s (60Hz) per one MU streaming three phase current and voltage and ground/neutral current and voltage. Actual size depends on SMV ID, OptFlds as well as length of control block and data set name.

and can fail in stress tests, if not engineered properly. The results also show however, that with proper design (e.g., hardware assisted SR-IOV solutions) robust operation can be guaranteed. Internal delays such as any store-and-forward delay, vSwitch (virtual switch providing logical connection between different applications and/or VMs) latency and packet queue latency is minimized compared to a traditional system and the delay settings for SMV traffic can be internally set for each MU.

Loops between redundant LANA, LANB virtualized network(s) in both physical domain and virtual domain can create broadcast storms that will impact protection system reliability; to mitigate these network load monitoring, balancing and rate limiting algorithms need to be embedded into vSwitch. The merging units, network switch would need to have rate limiting functionality at minimum to mitigate the effects of broadcast storms.

5.4. Time synchronization

With Ethernet-based technology it is possible to achieve software-based time synchronization with an accuracy of 1 ms quite easily, and without any help from HW. This is also what the IEC 61850 standard refers to as the basic time synchronization accuracy class (T1). An older and more common protocol is the SNTP (Simple Network Time Protocol), which is suitable for local substation synchronization in relatively small systems. However, if the SNTP server is behind multiple Ethernet nodes, the latency increases, which reduces the accuracy of the time synchronization. Therefore, SNTP is not an ideal solution for system-wide implementation. Normally a GPS or equivalent time synchronization resource is required in every substation. IEEE 1588v2 and IEC 61850-9-3 deal with these issues and makes it possible to achieve a time synchronization accuracy of 1 μs. This is required if an IEC 61850-9-2 process bus [6] is used. In case of a loss in GPS clock; one of the merging units can take over as a master clock per Best Master Clock Algorithm of IEEE 1588v2 and synchronize the servers and other MUs. PTP pass-through between different VMs and applications in server can provide highly accurate level of time synchronization. VMs and Apps can themselves be transparent clock and publish processing time in the stack as ‘ΔT’ in the correction field. For non-time sensitive applications that are ancillary NTP can be utilized.

5.5. Redundancy

High availability and high reliability of a communication network are two very important parameters for architectures utilizing a virtual P&C system. IEC 61850 standard recognizes this need, and specifically defines in IEC 61850-5 the tolerated delay for application recovery and the required communication recovery times for different applications and services. The tolerated application recovery time ranges from 800 ms for SCADA, to 40 μsec for sampled values. The required communication recovery time ranges from 400 ms for SCADA, to 0 for sampled values. To address such time critical need for zero recovery time networks, IEC 61850 standard mandates the use of IEC62439-3 [14] standard wherein clause 4 of the standard defines Parallel Redundancy Protocol (PRP) and Clause 5 defines High-Availability Seamless Redundancy (HSR). Both methods of network recovery provide “zero recovery time” with no packet loss in case of single network failure. Handling of redundancy within the server using dedicated PRP PCIe interface is a preferred option when large number of bays are to be connected. Using HSR topology for connecting MUs with VPC can restrict the number of MUs but can save hardware[4]. Redundancy can be strictly provided for Station and Process Bus traffic

[4] To comply with sampling rate of 80 Samples/cycle; some 6 devices are supported at 100 Mbit/s; for increased number of devices 1 Gbit/sec interface maybe considered and evaluated against cost of using PRP based topology and associated hardware.

but other Apps such as management, security may use Virtual Red-box (provides Singly Attached Nodes access to redundant LAN A and LAN B).

5.6. Hardware

The goal with virtualization is to provide as much flexibility as possible for the hardware selection. However main environmental (e.g., Electromagnetic Compatibility, EMC) needs to be fulfilled, so that Hardware reliability and robustness are in a level suitable for electricity substations. These requirements are more elaborated in IEC 61850 [7] and IEEE 1613. It is assumed that most ruggedized server will not be installed in outdoor environments, as such outdoor operating temperature ranges would not be applicable.

6. Practical experience

Virtual Protection & Control has been explored by ABB in real life substation, with the target to compare performance between existing Centralized Protection & Control solution on the market, and virtualized version. A following real life overcurrent incident was successfully detected by the physical CPC unit and virtual algorithm exactly at the same time. Directional Phase Overcurrent, low stage element (NSI. 67/51P) function picked at the same instance in bay J07. Oscillographic (Comtrade) indicate both J01 and J07 observed a fault involving Phase B, C at instant of pickup.

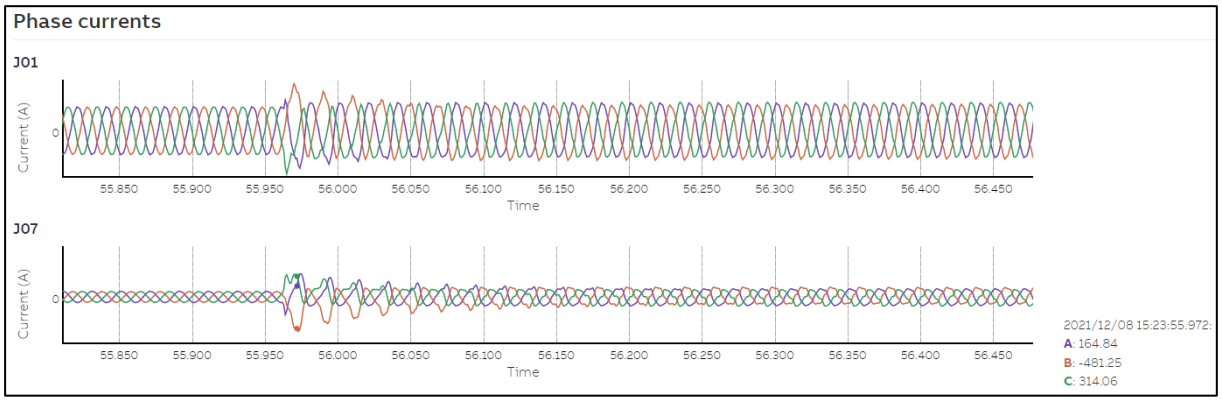

Figure 7. Short circuit fault, disturbance record

TIMESTAMP	SUBSTATION	BAY	FUNCTION	DESCRIPTION	VALUE	IDENTIFIER
8.12.2021 15:23:55.990	VPC1	J07		Start	True	LD0.DPHLPTOC15
8.12.2021 15:23:55.990	VPC1	J07		Start	True	LD0.DPHLPTOC15
8.12.2021 15:23:55.990	CPC	J07		Start	True	LD0.DPHLPTOC15

Figure 8. Short circuit fault analyzed by different applications (1 CPC device, 2 VPC images)

7. Conclusions

Virtualization has lot of potential, and technology starts to be ready for wider usage. There are benefits that can be achieved by going towards virtualization, but it is important to take many factors into consideration, so that result is reliable and secure. It is recommended to partner with good technology vendors and proceed via pilots, to determine what is the best solution for different solutions. Centralized protection & control solutions are already available on the market, so they are a good path forward. Software orientation and overall concept is the same as with virtual protection, but just with a dedicated HW.

BIBLIOGRAPHY

[1] B. Lundqvist, *100 years of relay protection, the Swedish ABB relay history,* Technical report, ABB Automation Products, Sweden, 2010.

[2] R. Das et al., *Centralized Substation Protection and Control*, WG K15 Report, IEEE Power System Relaying Committee, 2015.

[3] J. Valtari, *Centralized Architecture of the Electricity Distribution Substation Automation - Benefits and Possibilities,* Ph.D. Thesis, Tampere University of Technology, Finland, 2013.

[4] ABB, *Centralized protection and control – Enhancing reliability, availability, flexibility and improving operating cost-efficiency of distribution substations*, ABB White Paper, 2022, [ONLINE]. Available : https://campaign.abb.com/l/501021/aper-SSC600-2NGA001420-ENa-pdf/z6kh63

[5] VMWare, *Virtualization Overview*, White Paper, 2022, [ONLINE]. Available : https://www.vmware.com/pdf/virtualization.pdf

[6] IEC. *Communication networks and systems for power utility automation - Part 90-4: Network engineering guidelines*. Technical Report, The International Electrotechnical Commission, 2020.

[7] IEC, *Standard for Communication Networks and Systems for Power Utility Automation, IEC Standard 61850-5 Edition 2*. The International Electrotechnical Commission, 2013.

[8] "ERO Enterprise CMEP Practice Guide," NERC, [Online]. Available: https://www.nerc.com/pa/comp/guidance/CMEPPracticeGuidesDL/CMEP%20Practice%20Guide%20%20Virtual%20Systems.pdf.

[9] "Compliance Guide," NERC, [Online]. Available: https://www.nerc.com/pa/comp/guidance/Pages/default.aspx?View={873894d8-c688-4340-9c23-7cece8f0af5c}&SortField=Standards_x0020_Grouping&SortDir=Asc.

[10] A. Moga, T. Sivanthi and C. Franke, *Os-level virtualization for industrial automation systems: are we there yet?,* SAC '16: Proceedings of the 31st Annual ACM Symposium on Applied Computing, p. 1838-1843, 2016.

[11] L. Abeini, A. Balsini and T. Cucinotta, *Container-Based Real-Time Scheduling in the Linux Kernel,* SIGBED Rev., vol. 16, no. 3, p. 33–38, 2019.

[12] Anjing Wang et al., *Network Virtualization: Technologies, Perspectives, and Frontiers*, Journal of Lightwave Technology, 2013.

[13] G. Albanese, G. Giannopoulos, T. Sivanthi, R. Birke and T. Sivanthi, *Evaluation of Networking Options for Containerized Deployment of Real-Time Applications*, 26th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), 2021.

[14] IEC, *Industrial communication networks - High availability automation networks - Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR) Edition 4*, The International Electrotechnical Commission, 2021