2024 Paris Session

10852
B5 PROTECTION & AUTOMATION
PS2 Acceptance, commissioning, and field testing for protection, automation and control systems

How to Test Virtual Protection, Automation and Control Systems (vPACS)

Paulo S. Pereira JUNIOR[1]* Rodolfo Cabral BERNARDINO[1] Gustavo Silva SALGE[1] Cristiano Moreira MARTINS[1] Paulo Sergio PEREIRA[1] Gustavo Espinha LOURENÇO[1]

[1]CONPROVE, Brazil
*paulo.junior@conprove.com.br

SUMMARY

Due to an increasing number of fully digital substations based on IEC 61850 being implemented worldwide, the next stage in the evolution of protection, automation and control systems involves software decoupling from its dedicated hardware, virtualizing functionalities and thereby creating a software-defined grid.

Considering that vPACS is at the vanguard of the technological development of SAS (Substation Automation Systems), this paper aims to explore the test requirements in this new paradigm by comparing the requirements for testing physical IEDs with those for testing virtual IEDs (vIED). The similarities and differences between these two testing approaches will be discussed as well as testing suggestions. In addition, testing in the vPACS context will be investigated using both physical test sets and virtual test sets, comparing the differences, pros and cons of each testing method. The different test stages as commissioning tests (FAT – Factory Acceptance Tests and SAT – Site Acceptance Tests) and maintenance tests, the general steps for testing (isolate DUT – Device Under Test, simulate and capture feedback), and time synchronization issues will be approached in the vPACS context. Also, a comparison between applying a COMTRADE file from a physical test set and applying a PCAP file (a popular file format that records network traffic) from a virtual test set for disturbance record analysis will also be approached in this paper.

The paper begins with a historical analysis of power protection systems, tracing the development from the initial relays implemented with electromechanical switching to the evolution of virtualization. Then, some basic concepts of the virtualization mechanisms inherent to the comprehension of vPACS will be explained. The basic requirements of vPACS, along with its implementation challenges, will also be addressed.

Finally, the evolution of testing tools, in addition to the evolution of IEDs, will also be explored, along with the methods of implementing the test setup in a virtualized environment.

KEYWORDS

vPACS, IEC 61850, software-defined smart grid, virtual IED, virtual Test Set

1. INTRODUCTION

The history of power protection systems dates back to the end of the 19th century, when the first protection relay was developed with an electromechanical switching system in order to interrupt a fault current. Around 1960, the first solid-state or static relays were introduced with electronic components. Then, in the 1980´s, numerical or digital relays were launched with microprocessor control system, digital signal processing and digital network communication. After 2003, IEC 61850 standard changed the paradigm established until then through the new implementation of Protection, Automation and Control Systems (PACS). In this context, protection relays gave way to the Intelligent Electronic Devices (IEDs) that concentrate in a single Physical Device, several Logical Devices with different functionalities in addition to protection functions. The communication protocols standardized by IEC 61850 are based in data model and allow for interoperability, as different vendors are able to exchange data between them.

With the increasing number of fully digital substation based on IEC 61850 worldwide, the next natural step in the evolution line is the virtualization of PACS. Digitized current and voltage values are published in Sampled Values (SV) frames, trip and logical signals between IEDs are published in GOOSE (GO) frames, substation´s time synchronism is performed via Precision Time Protocol (PTP), and communication between IEDs, in bay level, and SCADA, in station level, is performed via Client/Server (MMS) protocol. All these facts lead to conclude that a virtual IED is fully capable of fulfilling the role of a conventional physical protection. Therefore, all the protection, automation and control functionalities can be virtualized which means no longer needing the use of a custom hardware, as they can be implemented via software without compromising performance.

Figure 1 illustrates this evolution line of protection systems over time [1].

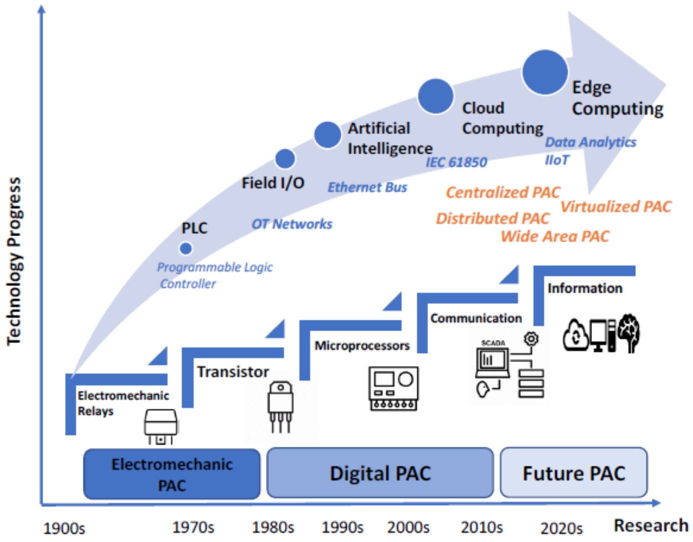


Figure 1 - Evolution Line of Protection Systems

Some basic concepts of virtualization mechanisms must be discussed to facilitate the comprehension of how vPAC can be implemented. These concepts are based on the comparison between hypervisor and container technology. While hypervisor is responsible for creating and managing virtual machines, container technology utilizes the host operating system itself to implement applications. Container systems include some examples of open-source container engines.

As any protection system, virtual protection, automation and control systems must meet the basic requirements of selectivity, speed, simplicity, reliability and economy [2]. In this context, several challenges must be analyzed in the vPACS implementation, including those faced by the industrial agents as well as technical issues. Some of these challenges are related to the maintainability of the system, supportability by the technology vendors and interoperability between different vendors.

The test devices must evolve according to advancements in protection systems. During the era of electromechanical relays, there were features such as single-phase protection functions with low precision and complexity, and mechanical switching components. Consequently, test tools were designed with functionalities to achieve these characteristics, including generation channels with single-phase and high-power sources, and settings tests of protection functions.

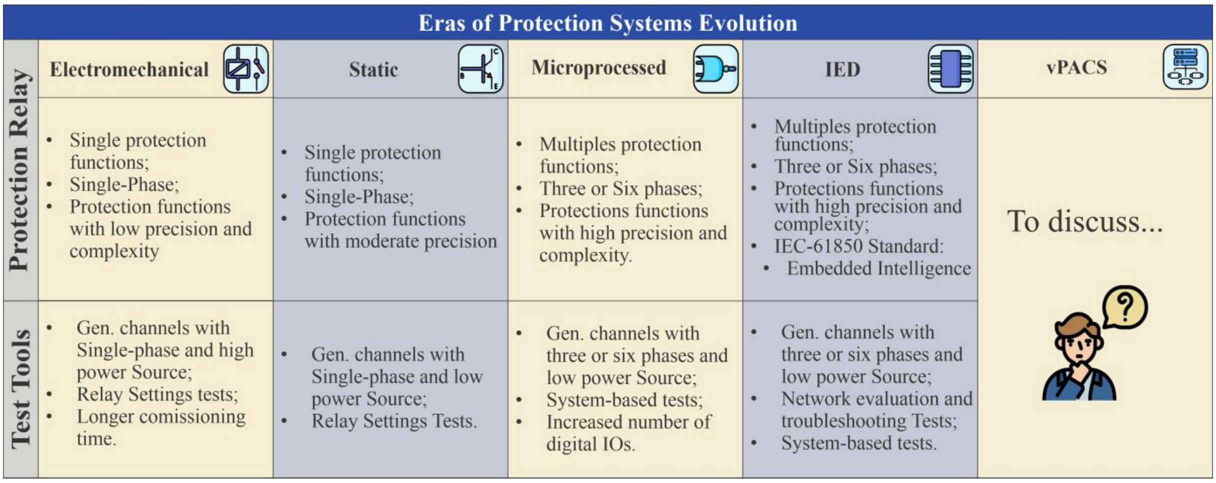
In the era of static relays, there were features such as single-phase analog input, single protection functions with moderate precision and complexity, and electronic switching components. Therefore, test tools incorporated diverse functionalities adapted to these characteristics, like generation channels with single-phase and low-power sources, as well as settings tests of protection functions.

With the transition to numerical or microprocessed relays, there were features such as three or six phases analog inputs, multiple protection functions with high precision and complexity. Thus, test tools had to modernize their functionalities to align with this paradigm, incorporating generation channels with three-phase or six-phase and low-power sources, along with system-based tests of protection functions.

Due to the advent of the Intelligent Electronic Devices (IEDs) era, there were some features such as three or six phases analog inputs, multiple protection functions with high precision and complexity, and implementation of IEC 61850. So, test tools had to implement additional features beyond the existing ones. Related to IEC 61850, these new features included standardized signal sampling, communication protocols, time synchronism, network architecture, redundancy, and more. Nowadays, with the implementation of virtual Protection, Automation and Control Systems (vPACS), test tools must go through adaptation, and their requirements need to be discussed.

Table 1 provides an illustrative and summarizing overview of the evolution of protection systems technology in parallel with the evolution of test tools technology.

Table 1 - The Evolution of Protection Systems and Test Tools



	Eras of Protection Systems Evolution				
	Electromechanical	Static	Microprocessed	IED	vPACS
Protection Relay	• Single protection functions; • Single-Phase; • Protection functions with low precision and complexity	• Single protection functions; • Single-Phase; • Protection functions with moderate precision	• Multiples protection functions; • Three or Six phases; • Protections functions with high precision and complexity.	• Multiples protection functions; • Three or Six phases; • Protections functions with high precision and complexity; • IEC-61850 Standard: • Embedded Intelligence	To discuss...
Test Tools	• Gen. channels with Single-phase and high power Source; • Relay Settings tests; • Longer comissioning time.	• Gen. channels with Single-phase and low power Source; • Relay Settings Tests.	• Gen. channels with three or six phases and low power Source; • System-based tests; • Increased number of digital IOs.	• Gen. channels with three or six phases and low power Source; • Network evaluation and troubleshooting Tests; • System-based tests.	

In the next topics, some issues will be addressed as a theoretical basis for the discussion of testing requirements in the vPACS.

2. BASIC CONCEPTS OF VIRTUALIZATION MECHANISMS

The first interesting virtualization mechanism to be examined is the hypervisor technology. It is a software layer responsible for creating "virtual machines" (VMs) and controlling multiple operating systems (OS) that share the same "Host", which are the physical computing resources, in a process called "virtualization". An important feature of the hypervisor is that it ensures portability and independence among VMs, in such a manner that if one operating system experiences a crash or a security failure event, the others will continue to operate properly [3]. However, since each VM has a complete OS instance, depending on the hypervisor type, more computing resources are allocated from the host, resulting in higher processing overhead and a longer boot time for the virtual machine itself. In relation to the first, scalability may become a challenge.

Hypervisors are classified in two types and both have different purposes. They are chosen based on system requirements and the environment where they will be implemented. The descriptions of each hypervisor´s type are presented below:

- Type 1 (Bare-Metal):

It is also known as “bare-metal hypervisor” and is installed directly on the hardware of the physical machine, eliminating the need for a dedicated operating system on the Host. Since there is no additional layer of the OS, this Type 1 hypervisor is preferred in environments where efficiency and performance are critical, such as servers. There are some examples of bare-metal hypervisors available as both proprietary and open-source applications.

Figure 2 illustrates the Type 1 hypervisor.

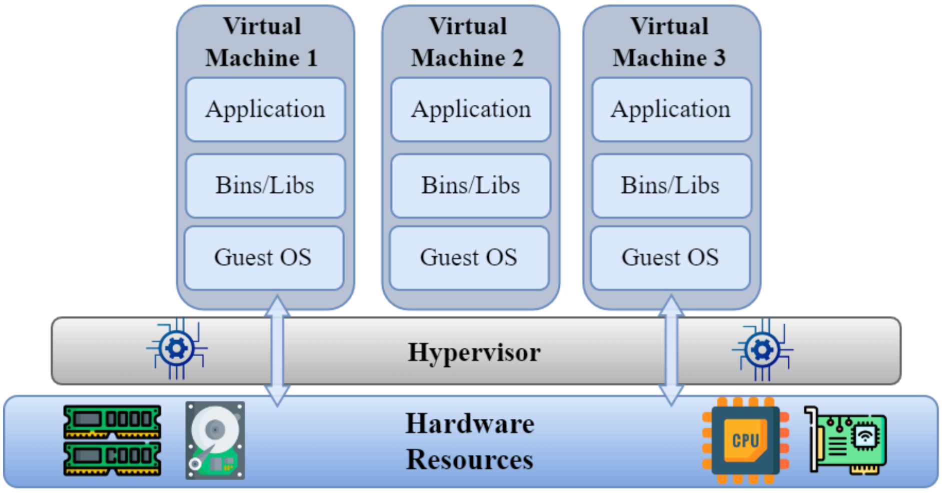


Figure 2 - Type 1 Hypervisor

- Type 2 (Hosted)

It is also known as “hosted hypervisor” and it is installed as an application on a conventional host operating system. Since there is a need for a host OS to work, this Type 2 hypervisor has lower performance and efficiency compared to the Type 1. Therefore, it is more suitable for desktop or laptop contexts. There are several examples of hosted hypervisors available as both proprietary and open-source applications.

Figure 3 illustrates the Type 2 hypervisor.

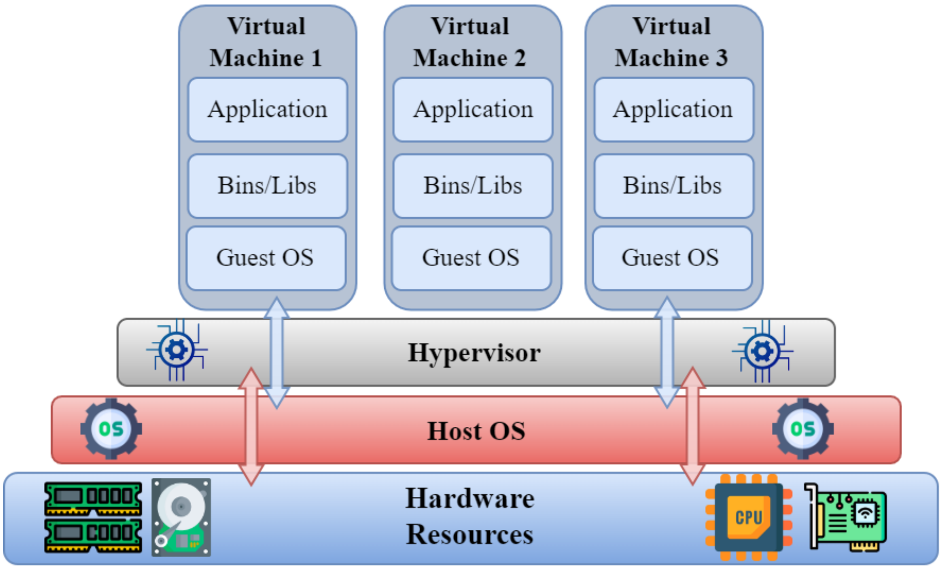


Figure 3 - Type 2 Hypervisor

Another interesting virtualization mechanism to be examined is the container technology. The container engine is a software enabler that allows the packaging and isolation of applications and their dependencies into units known as “containers”. Each one of them is an independent instance that can run on the same kernel, i.e. without the need for a separate operating system for each container. This results in lower processing overhead and faster application startup, in addition to advantages in terms of portability, efficiency, and scalability. On the other hand, if the host OS is compromised in terms of security failures or crashes, all containers will be compromised as a consequence.

Some examples of container engine platforms used to create and manage containers include widely-used open-source projects.

Although both Type 1 and Type 2 hypervisors create a complete OS instance for each VM, when related to bare-metal hypervisors, the environment is specifically configured to meet the performance and efficiency requirements. Then, considering that the servers are designed with sufficient computing resources that meet the application demands, there is not much difference between the bare-metal VM and container applications in relation to efficiency.

Figure 4 illustrates the architecture of container technology compared to bare-metal hypervisor.

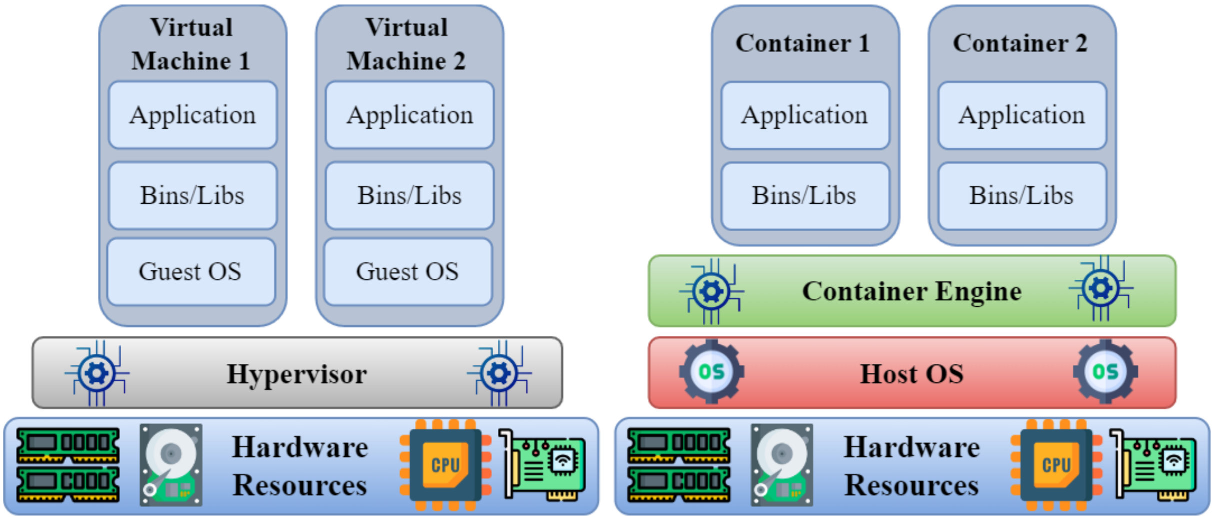
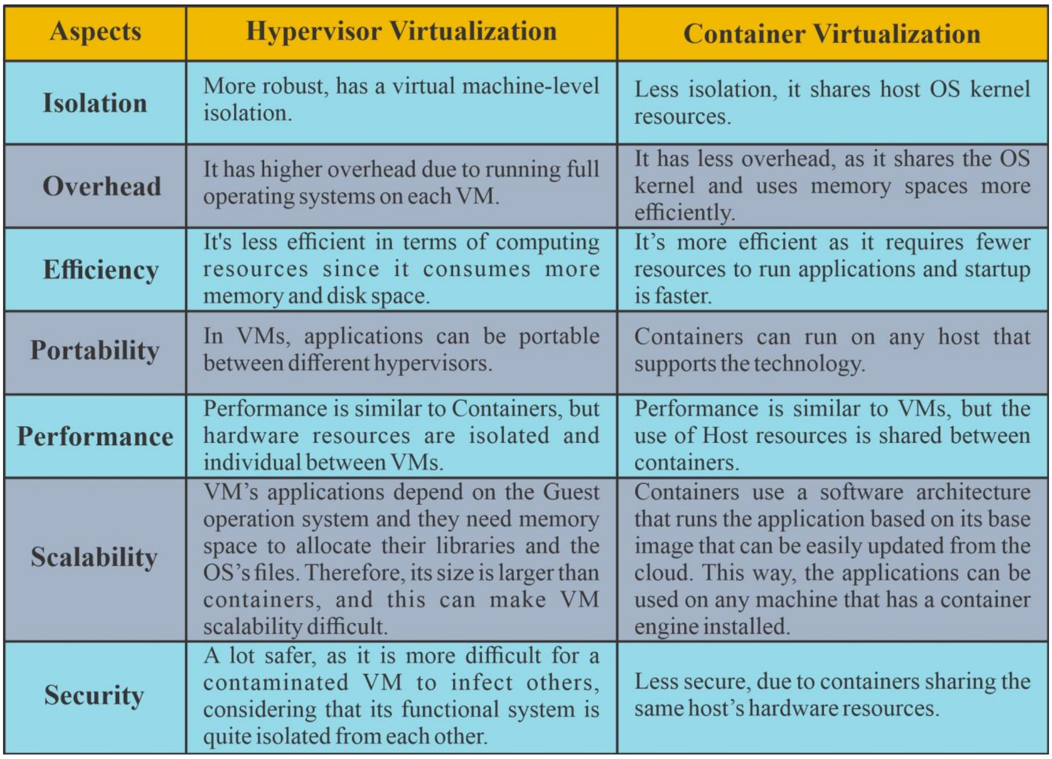


Figure 4 - Architecture: Type 1 Hypervisor x Container Engine

Table 2 summarizes the comparison between virtualization using Type 1 hypervisors and container technologies.

Table 2 - Comparison summary: Type 1 Hypervisor x Container



Aspects	Hypervisor Virtualization	Container Virtualization
Isolation	More robust, has a virtual machine-level isolation.	Less isolation, it shares host OS kernel resources.
Overhead	It has higher overhead due to running full operating systems on each VM.	It has less overhead, as it shares the OS kernel and uses memory spaces more efficiently.
Efficiency	It's less efficient in terms of computing resources since it consumes more memory and disk space.	It's more efficient as it requires fewer resources to run applications and startup is faster.
Portability	In VMs, applications can be portable between different hypervisors.	Containers can run on any host that supports the technology.
Performance	Performance is similar to Containers, but hardware resources are isolated and individual between VMs.	Performance is similar to VMs, but the use of Host resources is shared between containers.
Scalability	VM's applications depend on the Guest operation system and they need memory space to allocate their libraries and the OS's files. Therefore, its size is larger than containers, and this can make VM scalability difficult.	Containers use a software architecture that runs the application based on its base image that can be easily updated from the cloud. This way, the applications can be used on any machine that has a container engine installed.
Security	A lot safer, as it is more difficult for a contaminated VM to infect others, considering that its functional system is quite isolated from each other.	Less secure, due to containers sharing the same host's hardware resources.

3. VIRTUAL PROTECTION, AUTOMATION AND CONTROL SYSTEMS

In the evolution line of protection systems, the implementation of the IEC 61850 standard, in addition to the advancements in digital communications and other embedded technologies, is paving the way for a new era in protection, automation and control of power systems [4].
The deployment of IEC 61850 communication protocols as GOOSE for data exchange between IEDs, Sampled Values carrying current and voltage information from instrument transformers to IEDs, time synchronism being carried out by PTP and the supervisory system receiving information from IEDs via MMS, all demonstrate that a centralized virtual protection solution, decoupling software from hardware, makes the implementation of a software-defined PAC perfectly possible.

In the times of IEDs, the protection system was composed of physical devices incorporating various protection functions according to their purpose, either in a centralized or distributed scheme, such as Line Protection IEDs, Generator Protection IEDs, Transformer Protection IEDs, and etc. In the transition to vPACS, the protection system becomes centralized and it can be deployed through virtual IEDs (vIEDs) acting as identical physical devices, concerning the human-machine interface (HMI) and parameterization, each one admitting the specifications of its vendor. This vPACS deployment is referred to here as “Vendor Specific vIED”.

The implementation of vPACS must be performed on servers with computational resources that meet the required demands. Therefore, the current virtualization mechanisms that can achieve the implementation requirements of vPACS are Type 1 Hypervisors or Containers.

Figure 5 illustrates the implementation of vPACS.

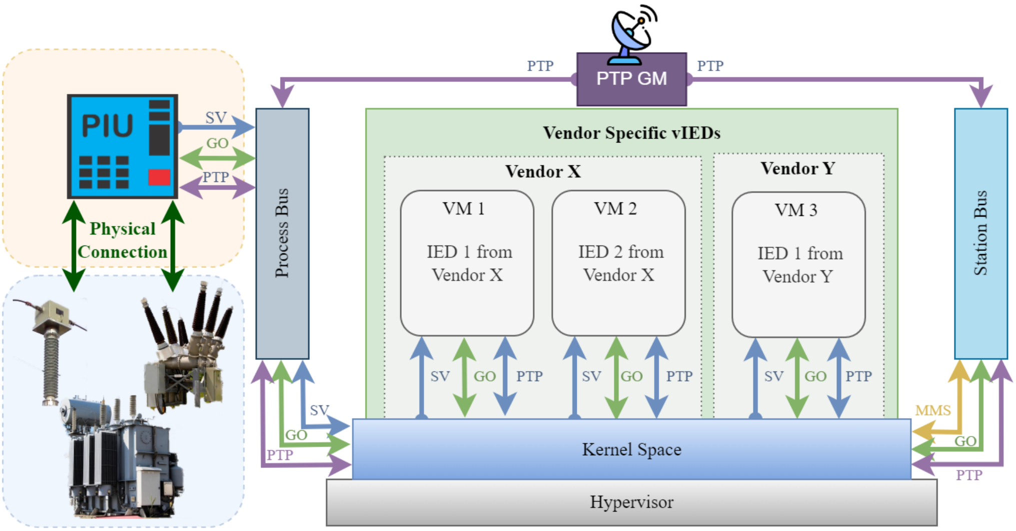


Figure 5 - Vendor Specific vIED

As vPACS can be implemented via bare-metal hypervisor or containers, there are some technical aspects challenges that must be taking into account. They are listed below:

- **Interoperability**: only the communication interoperability between different vendors is not enough, but interoperability at software development level such as architecture and APIs. That means, for example, describing the vIEDs requisites in an independent way of specific hypervisor or container engine, through hardware descriptors;

- **Performance**: real-time systems implemented in vPACS solutions must meet the time-critical processing requirements that SV and GOOSE protocols demand;

- **Reliability**: vPACS is composed of various sub-components, and the required logical control is very complex, thus being subject to inherent failure risks;

- **Scalability**: each VM or container has its bottleneck due to the quantity of data running on the network. Therefore, considering this fact, each scale-up of Logical Nodes in IEC 61850 data model, could affect the performance in vPACS;

- **Security**: studies related to intrusion detection systems applied to the vPACS environment must be conducted to verify issues such as user authentication, security protocols, encryption, and so forth.

It is important to note that virtual protection, automation and control must achieve the same generic requirements of selectivity, speed, simplicity, reliability and economy. In addition, some specific requirements of vPACS must be considered: the maintainability of the system, supportability by the technology vendors and interoperability among different vendors and the necessity of being tested by independent tests solutions during commissioning and maintenance. The latter is the core of this work and implies investigating and defining test requirements for the virtual environment.

4. PROTECTION TESTS ON vPACS

Firstly, a brief review of the test requirements in the context of physical IEDs [5] is performed in order to better comprehend the test requirements of virtual IEDs.

IEDs works based on embedded software named firmware. When the manufacturer provides firmware update the devices can be considered as a new one, and the historical of the devices behavior has to be reset, requiring that new tests should be made.

Errors in IEDs can occur due to hardware, firmware, parameterization, or even connections, which can lead the IED to operate improperly or not operate, resulting in money losses and even human lives at risk. New operating conditions require new conditions to be analyzed, meaning new tests.

In the context of a digital substation, when analyzing only the IED itself, the testing equipment no longer needs to generate power signals, as it would not need to reproduce signals of secondary analog Voltage (V) and Current (I). It would only be necessary for the equipment to have the capability to send SV messages to the IED under test. To test other parts of the system, such as the Stand Alone Merging Unit (SAMU) or Current Transformer (CT)/Voltage Transformer (VT), the testing equipment still needs the ability to inject current and voltage.

Figures 6 and 7 draw an analogy between the classic analog secondary current and voltage method and the Process Bus:

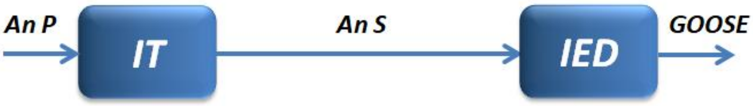


Figure 6 - Classical Method with Copper Hard Wire Connections

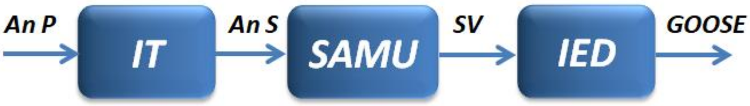


Figure 7 - IEC 61850 Implementation

In Figure 6, it is possible to observe that for the classic method, there is the Analog Primary Value (AnP), which is converted by the Instrument Transformer (IT) to the Analog Secondary Value (AnS) that arrives at the relay where it is measured and can result in the Binary Output (BO) closing.

In the process bus, the IT output is connected to the SAMU, responsible for converting the secondary analog signal into digital according to the SV format. The digital signals are publishing to the IED through the Ethernet network, and depending on the values, the device can modify the data in the GOOSE message, as illustrated in Figure 7.

Regarding testing, the Process Bus can be approached in a segmented manner. Tests can be divided into parts, always considering inputs and outputs taking into account their specific characteristics. In Figure 8 below, the system is divided, and different testing conditions are exemplified.

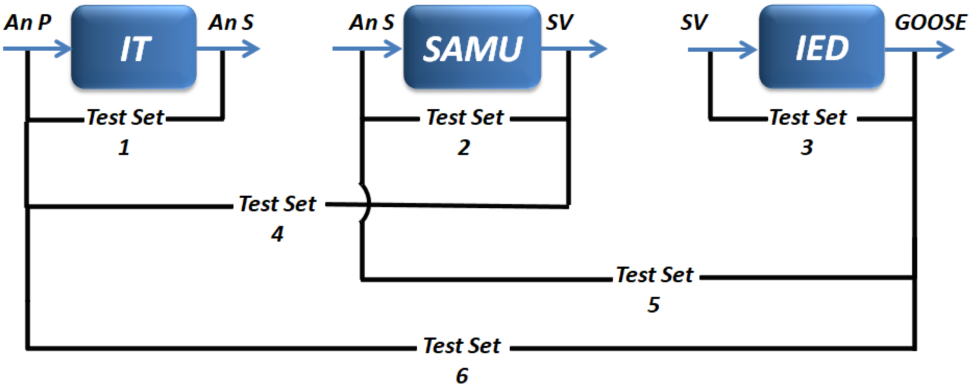
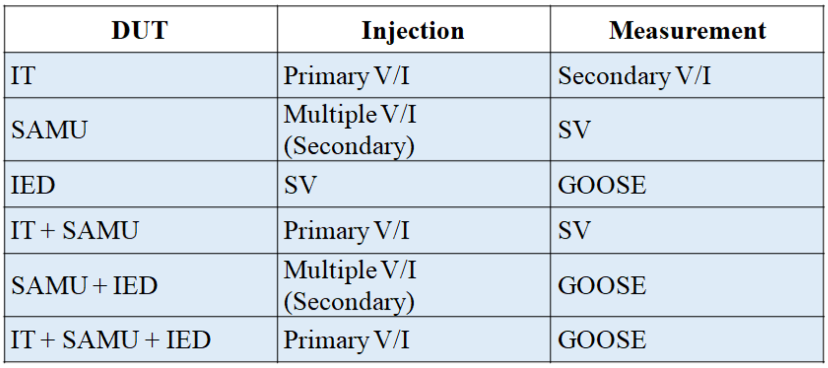


Figure 8 - Segmented Test System: Several Test Conditions

According to the previous scheme, there are 6 different testing options, with each approach focusing on one device or set of devices under test. Therefore, the test set must be capable of injecting and measuring various types of signals to interact with the system under test, as described in Table 3:

Table 3 - Summary of Segmented Test System



DUT	Injection	Measurement
IT	Primary V/I	Secondary V/I
SAMU	Multiple V/I (Secondary)	SV
IED	SV	GOOSE
IT + SAMU	Primary V/I	SV
SAMU + IED	Multiple V/I (Secondary)	GOOSE
IT + SAMU + IED	Primary V/I	GOOSE

Considering this previous analysis, it is possible to verify that the test solutions in the IEDs era must be capable of generating and measuring binary I/O signals, GOOSE messages, current and voltage analog signals, and SV, as illustrated in Figure 9. Other essential requirement to verify, in this context, is about time synchronism. It can be implemented through the following mechanisms: IRIG-B, 1PPS, GNSS and PTP.

It is important to note that tests must be performed based on power system's parameters, in a holistic view, that is, not just only based on IEDs settings. Thus, all the system's components and their influences are analyzed.

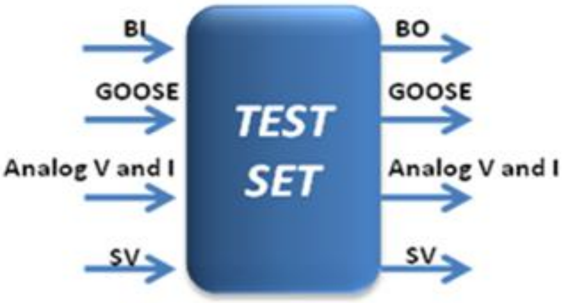


Figure 9 - Summary of Tests Requirements in the IEDs Era

Considering the upcoming vPACS era of protection systems, tests solutions can be divided in two ways : physical tests set and virtual tests set. Each one has its features, advantages and disadvantages and they will be discussed below.

The physical test set can be valuable in the role of testing the complete protection system chain, covering primary and secondary tests along with protection algorithms. For this purpose, analog channels are mandatory alongside the digital features. In the case of virtual test set, it can be valuable in the stage of protection system tests chain related to protection algorithms.

The main difference of testing tools compared to the previous era of IEDs, is not to be mandatory analog channels but only digital ones can achieve the demands. Current and voltage data can be received by subscribing through SV input channels, and they can be sent by publishing through SV output channels. The same way, binary information can be received by subscribing through GOOSE input channels, and they can be sent by publishing through GOOSE output channels. Regarding virtual tests set, there is another difference related to time synchronism mechanism, the most feasible manner to implement it is through PTP.

The virtual test set originates from the migration of an independent hardware application to a software application that can run on hypervisor or container systems of the same hardware that is running the virtual IED. This way, in vPAC paradigm, virtualized network architecture is implemented, including virtual Switch to allow the traffic of the IEC 61850 communication protocols as GOOSE, SV and MMS between the different software applications of virtual IEDs and virtual test set.

The operational features of a virtual switch can be clearly illustrated in Figure 10. As evident, the virtual switch is an exact replica of its physical counterpart. However, it functions as a software-based emulation that enables the flow of data between connected virtual devices through virtual ports within the same virtual environment. All aspects of traffic forwarding management, security, access control, and traffic isolation can also be implemented in the virtual switch.

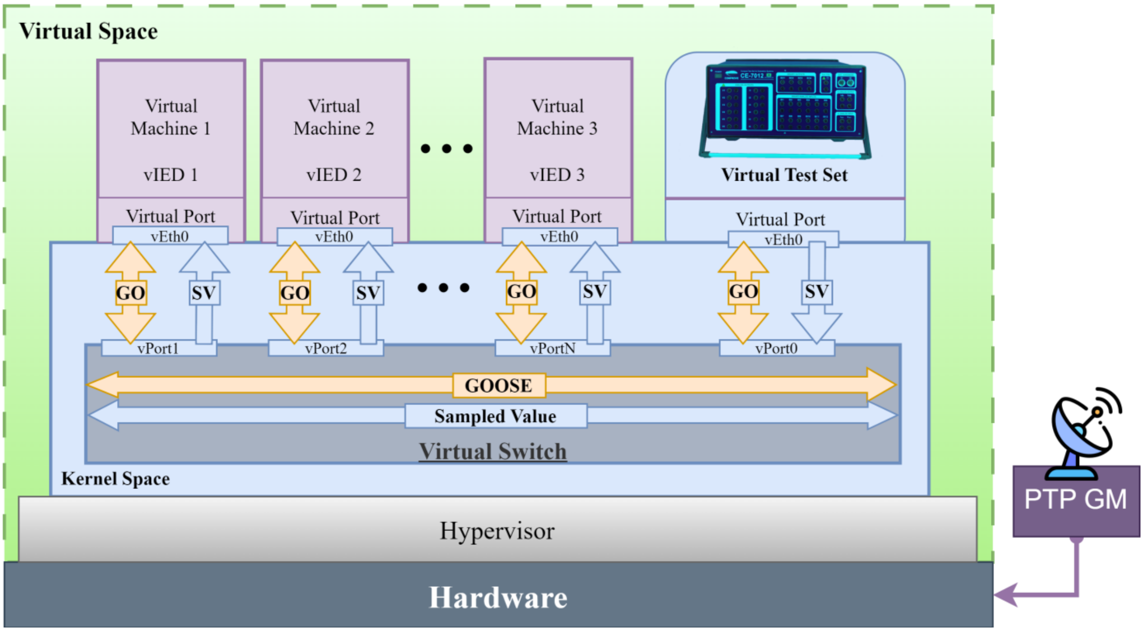


Figure 10 - vPACS with Virtual Tests Set

A more detailed investigation of the virtual test set's role in the vPACS environment, as demonstrated in Figure 10, can be conducted by having the virtual test set publish V and I information through SV frames in vPort0 of the Virtual Switch. This simulates a fault situation, aiming to trigger the actuation of the vIEDs. Alternatively, the virtual test set can publish GOOSE frames indicating the status of the circuit breaker. For instance, vIED 1 may subscribe to these SV frames and publish trip information through GOOSE frames in vPort1. In this way, the virtual test set can subscribe to these GOOSE frames and perform a protection verification. All this information traffic occurs within the virtual space.

During the transition period to the new era of the protection system, pilot projects are essential for gaining both reliability and expertise. They may be implemented in a hybrid way, that is, with centralized virtual protection coexisting with the conventional physical protection scheme, the physical tests set has its advantages over the virtual test set in this scenario. Firstly, the physical test set has hardware features to interface with various time synchronization protocols, in addition to PTP, such as IRIG-B, GNSS and 1PPS ; whereas, virtual tests set do not have hardware features to interface with time synchronization protocols beyond PTP.

On the other hand, when the protection system is fully implemented with centralized virtual protection scheme, there will be no need to incorporate hardware features to meet time synchronization protocols beyond PTP. However, even so both virtual and physical tests set can interface with the system and fulfill the tests requirements.

Figure 11 exemplifies a test setup within the vPACS context, with physical tests sets.

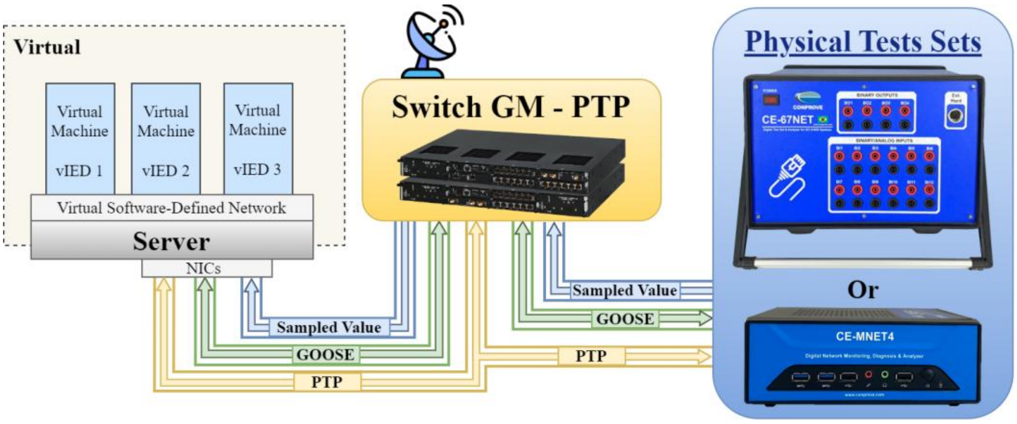


Figure 11 - vPACS with Physical Tests Sets

Just as with the physical IEDs, the comissioning (FAT and SAT) and maintenance tests must be performed with the virtual IEDs. In this virtual context, the general steps for testing will be executed the same way: DUT will be isolated, fault will be simulated by the virtual tests set via SV, and the feedback will be captured by it via GOOSE.

Furthermore, the physical test set is capable of performing network monitoring and complete statistical analysis because it is physically connected to the network. Therefore, beyond monitoring the network for failure events, the physical test set can execute time-critical statistical analyses, such as the transfer time of GOOSE frames, digitization and processing times of SV frames, time between frames, and more.

In this context, the virtual test set, running on the same server as the vIEDs, is also capable of performing network monitoring and some time-critical statistical analyses on traffic from devices external to the server, such as SV and GOOSE frames published by PIUs. Regarding the latter, the virtual test set must run on a separate server from the vIEDs to be able to carry out complete time-critical statiscal analyses.

Some examples of tests that can be performed in the virtual environment are: characteristics searching, shots faults simulations and transients reproduction. Below, they will be briefly addressed.

- **Characteristics searching**: this test aims to determine the vIED characteristic tolerance/boundary. The test involves injecting test points outside the characteristic and adjusting them until the vIED trips. This process is repeated across the vIED characteristics to ensure a comprehensive check;

- **Shots points simulations** (simulations of one or more fault conditions): this test involves publishing SV with dynamic amplitude conditions of current and voltage, representing faults inside or outside the protection operating zone. The goal is to evaluate the vIED’s behavior under specific conditions defined by users;

- **Transients reproduction**: these tests can be performed with virtual tests set that provides software for modeling the power system. This allows for simulating the real conditions of the system and generate the transient waveform of a fault condition, verifying the vIED´s response. An interesting point to be noted here is that just as a COMTRADE file can be applied from a physical tests set for disturbance record analysis, a PCAP file can be applied from a virtual tests set to execute this same task.

It is important to emphasize the use of IEC 61850 standards for testing and simulations in the virtual environment. The mode and behavior configurations, as defined in IEC 61850-7-4 [6], can be applied to the vIED. Consequently, there will be duplicated traffic in the virtual network: real frames published through PIUs and vIEDs, and simulated frames published through virtual testing tools.

Therefore, it is essential that the projected bandwidth supports this traffic. The paper cited in [7] demonstrates a helpful and clear manner to calculate the network bandwidth according to the number of SV streams.

5. CONCLUSIONS

This paper aimed to set the groundwork related to test virtual protection, automation and control systems. As this matter is at the vanguard of substation automation systems, a comprehensively knowledge base was established to facilitate understanding of the theme.

First, it was conducted a historical analysis about the eras of protection systems, including the tests requirements of each one. Then, some basic concepts of virtualization mechanisms were addressed. Generic basic requirements and implementation challenges of vPACS were also approached. Finally, it was explored the evolution of the testing tools, in addition to the evolution of the IEDs, resulting on the verification of tests requirements on vPACS environment, along with the test setup implementation.

Among the many benefits of the transition to virtualization can be included improved safety, reliability and intelligence within the substation. So, due to all the matters this paper approached in the vPACS context, it will contribute to pave the way for its effective deployment.

Due to the evolution of protection, automation, and control systems toward virtualization, creating a software-defined grid, new testing requirements and opportunities will arise. Therefore, testing tools must also evolve with modernized features to meet these demands.

6. BIBLIOGRAPHY

[1] Nadine Kabarra; et al.; Towards Software-Defined Protection, Automation, and Control in Power Systems: Concepts, State of the Art, and Future Challenges; Energies 2022, 15, 9362; https://www.mdpi.com/journal/energies.

[2] Dean Samara-Rubio; et al.; Virtual Protection Relay - A Paradigm Shift in Power System Protection; May, 2022; Intel and Kalkitech; https://kalkitech.com/whitepaper-virtual-protection-relay/.

[3] Alailton José Alves Junior; Implementação de um sistema de Proteção, Automação e Controle virtualizado para subestações digitais baseado na Norma IEC-61850; 2023; Trabalho de Conclusão de Curso Curso de Graduação em Engenharia Elétrica da Universidade Federal de Uberlândia; Brazil.

[4] Cigre WG B5.60; Technical Brochure - Protection, Automation and Control Architectures with Functionality Independent of Hardware; February 2023 - Reference 891.

[5] Pereira Junior, P. S.; Martins, C. M.; Rosa, R. R.; Pereira, P. S.; Lourenço, G. E.; A New Approach For Test In Substation With Entire Application of IEC 61850 Including the Process Bus; Cigre SC B5 Colloquium, 2013; Belo Horizonte, Brazil.

[6] Standard IEC IEC 61850 – Communication networks and systems for power utility automation – Part 7-4: Basic communication structure – Compatible logical node classes and data object classes, Ed. 2.1 – 2020-02.

[7] Pereira Junior, P. S.; Bernardino, R. C.; Martins, C. M.; Pereira, P. S.; Lourenço, G. E.; Analyzing the Limits of Data Transmission in the Process Bus; Cigre Session 2020; Paris.