Prototyping of virtualized central adaptive protection and control: performance analysis and resiliency

Author(s): Mekkanen, Mike; Dang, Duong; Vartiainen, Tero

Title: Prototyping of virtualized central adaptive protection and control: performance analysis and resiliency

Year: 2025

Version: Accepted manuscript

Please cite the original version:

Mekkanen, M., Dang, D., & Vartiainen, T. (2025). Prototyping of virtualized central adaptive protection and control: performance analysis and resiliency. *IET Conference Proceedings* 2025(14), 880. 28th International Conference and Exhibition on Electricity Distribution (CIRED 2025). https://doi.org/10.1049/icp.2025.2106

PROTOTYPING OF VIRTUALIZED CENTRAL ADAPTIVE PROTECTION AND CONTROL: PERFORMANCE ANALYSIS AND RESILIENCY

Mike Mekkanen[1], Duong Dang[1], Tero Vartiainen[1]

[1]School of Technology and Innovations, University of Vaasa, Vaasa, Finland

Keywords: VIRTUALIZATION, CENTRAL PROTECTION AND CONTROL, RESILIENCY, IEC61850, CYBER PHYSICAL SYSTEM SECURITY

Abstract

This study addresses the limitations of conventional protection relays in microgrids (MG) by presenting the development and testing of Virtualized Central Adaptive Protection and Control (VPC) systems. VPC systems were chosen because they help to reduce physical size, complexity, and costs while increasing flexibility and scalability, effectively managing protection applications within the electrical grid. The research compares two VPC solutions to a commercial relay, all implementing the IEC 61850 standard. Using a simulated MG model in a real-time simulator, the performance was analysed under various scenarios, including islanding, load and DG connections/disconnections, and cyber-attacks. Preliminary results show that VPC solutions perform identically to commercial relays, confirming their feasibility as alternatives. The study also proposes moving target (MT) defense techniques to enhance power system resiliency. Our solution provides a more adaptable and resilient solution for power grid protection and control, highlighting the need for VPC systems to meet various security, safety, and time-critical requirements thanks to virtualized technologies. This research underscores the importance of VPC systems in addressing the evolving demands of power system protection and control.

1 Introduction

Conventional protection relays use predefined setting groups (SGs) to adapt to different topologies, but their limited capacity to store SGs often falls short of the diverse electrical grid topologies [1]. These relays consolidate protection and control functions across multiple levels (process, bay, and station) within complex communication networks, which can restrict adaptability and resilience. This is problematic because protection system reliability and quality directly impact the grid's power supply. While protection systems aim to isolate compromised equipment or network segments, this can alter the network topology and necessitate updates to the system's functionality. Consequently, the limitations of conventional protection relays hinder the adaptability and resilience required for modern power systems.

Literature indicates that advanced technologies and techniques, such as multi-core processors, cloud computing, high-speed communication technologies, and virtualization, have opened up new possibilities for enhancing power system protection [1]. For example, virtualization technology, defined as "the separation of a resource or request for service from the underlying physical delivery of that service" [2], has been widely used in information technology (IT) for non-real-time applications. Virtualized central adaptive protection and control facilitates the consolidation of protection automation and control (PAC) functionalities, decoupling them from the physical resources of the integrated platform. The VPC solution consolidates a substation's PAC functions from multiple bay-level devices into a single, central unit. In other words, VPC is a software representation of traditional protection and control solutions within conventional relays. This software offers significant flexibility, as it is not tied to a specific physical relay and can be deployed across various environments. The VPC system reduces physical size, complexity, maintenance, and costs while enhancing flexibility and scalability. It manages PAC applications in the electrical grid with operational freedom, simplifying production and providing a more adaptable and resilient solution for PAC functionalities in power networks.

However, we lack detailed knowledge about the specific steps and performance outcomes of VPC solutions compared to conventional relays in a laboratory testing setup. The implementation of the VPC is important to address various security, safety, and time-critical requirements of the power system. These include, for example, high-speed secure communication technologies, high-speed computing, and hosts with substantial capacity, as protection functions must be executed within a quarter of a frequency cycle (0.005s at 50 Hz) [3]. Recent studies indicate that a range of virtualization technologies, from virtual machines (VMs) to containers, can deliver real-time performance in PAC systems. While recent works suggest that various virtualization technologies can provide real-time performance in a PAC system[4][5] comprehensive empirical study is still needed.

As a result, this paper aims to demonstrate the development steps of VPC solutions and test their performance compared

to conventional relays using a laboratory testing setup. Thus, our research question is how can VPC solutions enhance the flexibility, resilience, and performance of power grid PAC compared to conventional relays?
We contribute by proposing a VPC system that consolidates PAC functionality, isolated from the integrated platform's physical resources. This study highlights the need for VPC systems to meet various security, safety, and time-critical requirements in the power systems. Our contribution lies in using virtualized technologies to host protection and control functionality, offering a more adaptable and resilient solution for power grid PAC [6]. This is achieved using the open-source libiec61850 package and multiple operating systems on different hosts [7]. We also propose MT defense techniques to enhance power system resiliency.

2. Related Work

Literature related to our study has focus on the following topics. First, literature explored VPC solutions as a transformative approach in power system protection using a host server [8].
Second, scholars also presented a hardware-in-the-loop setup for adaptive centralized protection schemes utilizing clustering algorithms [9]. The authors introduced and compared three novel clustering methods, focusing on minimizing relay operation time delays in offline mode, which may not accurately represent the dynamic activity of the electrical grid. Also, a robust smart grid was proposed.
Third, literature addressed limitations of existing protection solutions by deploying a VPC solution using ABB software in a real-life environment [10]. The setup included a commercial protection relay as the main system (active protection system) and two VPC solutions in different containers in standby mode (passive mode). Over a year, a monitoring system recorded all operational parameters and protection system activations. The results showed that VPC systems performed identically to the conventional relay. However, several limitations were identified in this work: (*i*) *Reliance on a Single Vendor*: This study relied on a single vendor, which reduced the implementation of the interoperability concept raised by IEC 61850; (*ii*) *Vendor Product Line Dependency*: The test setup depended on the vendor's product line development solution, which limited capability. The VPC solution was based on the vendor's software image, including predefined functionality from the PAC vendor's product line development, constraining the development of new functionalities dictated by application needs; and (*iii*) *Lack of Diverse Testing Scenarios*: The study lacked diverse testing scenarios, including the 'what-ifs' concept for unforeseen scenarios such as intentional failures or cyber-attacks. This was crucial for resilience assessment prior to system deployment in a real-life substation. As a result, this study aims to address these limitations

3. Methodology

To address the research question, we configure a set up with two VPC solutions running on different operating systems (VPC1 on Linux Preempt and VPC2 on Linux Ubuntu) at the University of Vaasa FREESI Lab using the libiec61850 library. The study compared these VPC solutions with a commercial relay. VPC1 features an FPGA Altera SoC Cyclone V, dual 925MHz ARM processors, 1009MB memory, and a 1Gb network adapter. VPC2 runs on a Lenovo PC, Virtual Machine (VM) VirtualBox with a 2795MHz processor, 4096MB memory, and a 1Gb network adapter. Both VPC solutions and the relay adhere to the IEC 61850 standard. The setup also includes a real-time simulator from a leading company, running a MG simulation model. This model, developed with RT-simulator software, simulates a 25-kV MV grid. The simulator connects to external solutions in a star topology, using the hardware-in-the-loop (HIL) concept, as shown in Fig (1). Details of the MG are described in Table 1 and Table 2.

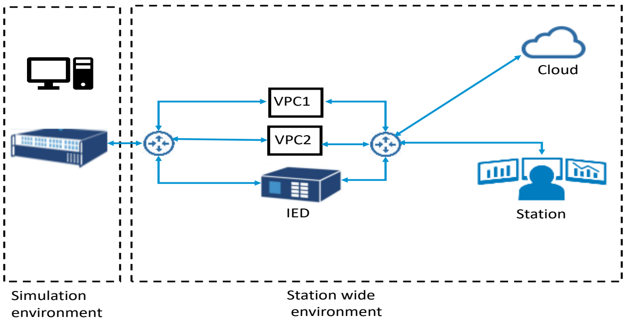
Table 1. MG Loads description

MG Load	Magnitude	Description
L1	4000kW	Critical load
L2	4000kW	Critical load
L3	4000kW	Priority load
L4	5000kW	Residential load

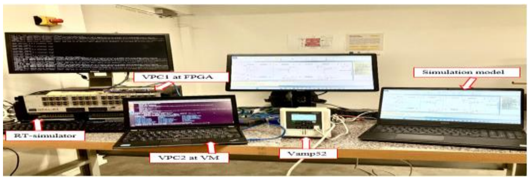
Table 2. MG DER description

MG DER	Magnitude	Description
DER 1	1500kVA	Photovoltaic
DER2	1500kVA	Photovoltaic
DER3	500kVA	Energy storage systems 100kWh
DER4	500kVA	Energy storage systems 100kWh
DER5	1000kVA	Energy storage systems 5000kWh
DER6	10000kVA	Combined Heat and Power

MG is connected to the main grid through 15000 kVA transformer. In grid-connected mode point of common coupling (PCC) CB is closed, and the MG energize the four loads effectively. Measurements are calculated and gathered from the MG units and their CBs status. These measurements and CBs status will be send to MG controller via IEC 61850 protocol Generic Object Oriented Substation Event GOOSE messages to sense and stabilize the MG operation as illustrated in Fig (2).



(a)



(b)

Fig1. Testing environments (a) concept (b) lab setup

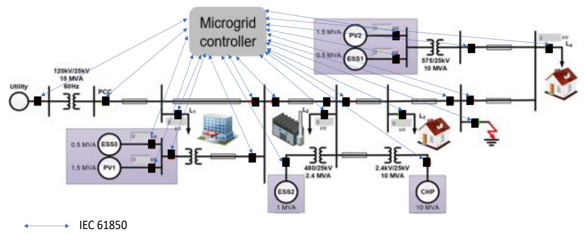


Fig2. MG simulation model

On the other side, VPC solutions and the conventional relay will subscribe to the real-time simulator GOOSE messages. Extract the information from these GOOSE messages and take the action based on extracted data. The laboratory environment allowed for a controlled evaluation of their performance, reliability and interoperability through various measuring and recoding tools. Performance evaluations are presented for the two VPC, and the relay, in a number of MG situations including islanding and cybercrime scenarios. The proposed methodologies were set up to make thorough examinations about the efficiency and reliability of the VPC system in comparison with the conventional relay. Development steps considering the VPC solutions, relay configuration and set up are described in the following section.

3.1 VPC solutions development

This section, describes the VPC solutions development process as illustrated in Fig (3). To begin with the development process is by create/design IEC 61850 IED Capability Description (ICD) files. This file is essential for creating the VPC solutions data model and it recognized as a core for the developments process of the VPC solution adhering the IEC 61850 standard. The file will be adapted to be used at the VPC1 host board, and Virtual Machine (VM) as VPC2 host. Within the IEC 61850 ICD file, various IEC 61850 entities need to be assigned and configured as outlines in Table3.

Table 3. IEC61850 ICD data model hierarchy

ICD file	Assigned parameters	Description
IED	SERVER-GOOSE	IED selected name
LD	SERVER-GOOSEDevice1	Logical device top level of the data
LN	LLN0	Logical Node Zero contains data objects
LN	OV2PTOV1	Logical node unique
DO	Ovp1 to Ovp6	Data object container
DA	intA and intB	Data attribute
FC	ST	Functional Constraints
CDC	stVal	Common Data Classes define type
GCB	GOOSE_OV2PTOV	GOOSE Control Block
GOOSE datSet	reference of data	collection of data objects and attributes
GOOSE ID	SERVER_GOOSE	GOOSE identification
confRev	100	Value increments with each change
GOOSE MAC	01-0C-CD-01-00-01	48-bit GOOSE address identifier

Next step is generating system files. A hierarchy of C code data structure related to the data model (built in step one) is created by loading the ICD file to generate tool offered by the libiec61850 package. This tool will generate two system files data structure file (file name.c) and header file (file name.h).

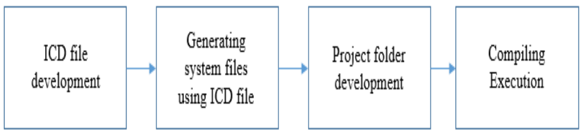


Fig3. VPC solution development steps

Besides the generated system files, VPC application file need to be created in C code. This file contains the definition of the VPC application algorithm. This algorithm's definition is dependent on the functionality dedicated to the VPC solutions e.g., protection, control etc., Subsequently, the developed files will be collected into one project folder.

This project folder include also execution file. Lastly, following the procedure to compile and execute the VPC project application.

3.2 Relay configuration

Setting up the relay to subscribe to the RT-simulator GOOSE messages is a step forwarding, since the configuration of the GOOSE subscribing parameters can be manually incorporated to match the GOOSE publishing parameters. Relay configuration software is used as illustrated in Fig (4). The relay has two setting groups (SGs) active and passive. The active SG can be change when the network topology is changed [11]. This changing can be done by a digital input (DI). In Relay logic panel "GOOSEIN" is used to activate the DI in which that will be used to change the SG at the relay.

Fig4.Relay tool shows logic and output matrix panels

4 Results

The result is described as follows. First, the testing system includes the RT-simulator, two VPC solutions, and the relay. The relay synchronizes using the PC internal clock, while Network Time Protocol synchronizes the VPC solutions based on the UTC time zone.

Second, the test begins by running the simulation model on the RT-simulator. After one second, islanding occurs, meaning the PCC point circuit breaker (CB) opens. The control function monitors the PCC grid point and defines the islanding condition.

Third, if islanding is detected, an imbalance between power generation and load consumption is expected, as the generated power is insufficient to energize all loads. Therefore, uncritical loads should be shed to stabilize the grid, with Load4 being shed by sending a GOOSE message to open its CB.

Fourth, in this islanding scenario, all HIL-connected solutions need to sense this instance and shed Load4 immediately. The results show that during different testing trials, both VPC solutions matched the relay's behaviour, successfully subscribing to the RT-simulator's GOOSE messages and capturing the PCC status.

Fig (5) shows the VPC solutions and relay performance evaluation. The experiment was successfully accomplished, with a matching behavior between the conventional relay and the VPC solutions. However, there is a slight difference in GOOSE message subscribing latency for the different solutions, which is normal due to various factors such as communication link conditions, VPC solution internal parameters (CPU, memory, OS, etc.). Furthermore, the interoperability among different solutions (RT-simulator, two VPC solutions developed on different hosts, and relay) proves the multi-vendor environment interoperability concept raised by the IEC 61850 standard.

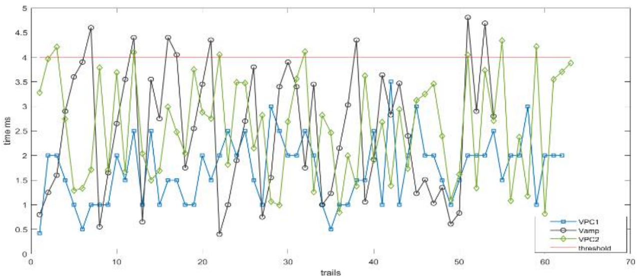


Fig5. GOOSE messages latency (relay with black (circle), VPC1 FPGA with blue (square), VPC2 VM with green (diamond) and threshold IEC61850 read line.

From another point of view, to test cyber-physical system (CPS) security, two cyber-attacks were developed. First, a delay attack was implemented by introducing a delay to the Load4 trip signal (0.5s and 1s). The grid RMS value dropped to 23KV with a 1s delay, and the frequency oscillated between 49.7Hz and 50.3Hz. This test showed that the more the delay, the greater the frequency and voltage disturbance, potentially leading to a blackout.
Next, we launched a GOOSE duplicate attack by generating a replica of the original GOOSE message using the GOOSE simulation tool. All HIL solutions could not differentiate between the original and duplicate GOOSE messages. Therefore, other cybersecurity measures such as authorization, authentication, and light encryption should be used to secure the GOOSE implementation.

5 Discussion

We evaluated the test outcomes using a normal distribution probability density function mean and standard deviation (std) of the GOOSE subscribing latency (e.g., VPC1 mean = 1.700s and std = 0.6873, VPC2 mean = 2.5940s and std = 1.055, and relay mean = 2.4889 and std = 1.3114). The results show that the means are compliant with IEC 61850 requirements (≥4ms), and the std shows the spread of the data around the mean. This confirms the feasibility of VPC solutions as an alternative to conventional protection relays.

As a real-life example to illustrate our proposal, we consider the cyber-attack on CPS security during the Ukrainian power system attacks in 2015. In this attack, malware stayed in the power grid SCADA system, sensing and learning from the grid's regular operation before executing critical commands to open power grid CBs at critical times, leading to blackouts. One solution to prevent such attacks is the moving target (MT) defense, proposed by scholars to improve power grid resiliency. Attackers typically collect information about the target system, such as configuration, OS version, applications, and vulnerabilities, to develop and launch attacks. MT defense principles involve dynamically changing the properties of the running application platform to prevent static nature exploitation.

In our study, to prevent attacks like the one in Ukraine, we propose using MT defense in power system PAC. For example, the application could run on different platforms, including VPC1, VPC2, and the relay. This dynamic platform MT technique can improve power system resiliency by preventing platform-dependent attacks and increasing the attack cost (time and effort), as attackers need to develop advanced attacks incorporating different exploits against various platforms.

6 Conclusion

In this paper, we used virtualized technologies to host protection and control functionality, offering a more adaptable and resilient solution for power grid PAC by using the open-source libiec61850 package and multiple operating systems on different hosts. We adopted VPC in our study because it is argued that VPC reduces physical size, complexity, and costs while increasing flexibility and scalability by integrating protection and control into software-based solutions. It effectively manages protection applications within the electrical grid, offering operational freedom and simplifying production, which leads to cost savings and easier scalability. Two main outputs came from our study:

First, the preliminary results demonstrate that the VPC solutions perform identically to a commercial relay, making them a viable alternative to conventional protection systems. They also show consistent performance and reliability.

Second, we propose moving target defense techniques to enhance power system resiliency based on VPC solutions tests. This study thus highlights the need for VPC systems to meet various security, safety, and time-critical requirements in power systems.

7 References

[1] Yohanandhan, R. V., et al.: 'A specialized review on outlook of future Cyber-Physical Power System (CPPS) testbeds for securing electric power grid', Int. J. Electr. Power Energy Syst., vol. 136, p. 107720, 2022, doi: 10.1016/j.ijepes.2021.107720.

[2] Critchley, T.: 'Virtualization Overview', High-Performance IT Serv., pp. 325–334, 2016, doi: 10.1201/9781315367217-15.

[3] Schweitzer, E., O., Kasztenny, B.: 'Distance protection: Why have we started with a circle, does it matter, and what else is out there', 71st Annu. Conf. Prot. Relay Eng. CPRE 2018, vol. 2018-Janua, pp. 1–19, 2018, doi: 10.1109/CPRE.2018.8349791.

[4] Kabbara, N., Mwangi, A., Stefanov, A., Gibescu, M.: 'A Real-Time Implementation and Testing of Virtualized Controllers for Software-Defined IEC 61850 Digital Substations', IEEE Open J. Ind. Appl., vol. 5, no. June, pp. 300–310, 2024, doi: 10.1109/OJIA.2024.3426321.

[5] Guibout, C., Wataré, A., Carli, F., Carbonne, A., Mourier, K., Rudolph, T.: 'Centralized Protection and Control for Transmission System Operations: Practical Applications and Perspectives', IEEE Power Energy Mag., vol. 22, no. 3, pp. 67–78, 2024, doi: 10.1109/MPE.2024.3357442.

[6] Aleixo, A. C., et al..: 'Challenges and considerations for the design and implementation of a centralized protection and control solution for mv networks user-level requirements', 27 th International Conference on Electrici,” no. June, pp. 12–15, 2023.

[7] Roomi, M. M., Ong, W. S., Hussain, S., M., S., Mashima, D.: 'IEC 61850 Compatible OpenPLC for Cyber Attack Case Studies on Smart Substation Systems', IEEE Access, vol. 10, pp. 9164–9173, 2022, doi: 10.1109/ACCESS.2022.3144027.

[8] Dean Samara-Rubio, I., McKenzie, G., Khajuria Kalkitech -Roopesh Ariya, P., Gopalakrishnan, P.,Ravindran, V.: 'Virtual protection relay', pp. 1–17, [Online]. Available: https://www.intel.com/content/www/us/en/energy/resources/virtual-production-relay-whitepaper.html

[9] Pashaei, M., Rastegar, H., Zandrazavi, S., F., Kauhaniemi, K., Laaksonen, H.: 'Real-time hardware-in-the-loop approach for adaptive centralized protection schemes using clustering algorithms', Expert Syst. Appl., vol. 255, no. PC, p. 124707, 2024, doi: 10.1016/j.eswa.2024.124707.

[10] ABB, 'Real-life pilot of virtualized protectionand control – Experiences andperformance analysis', (White Paper) 2023.

[11] VAMP, 'Vamp 52' Manual