A cybersecurity assessment for hybrid virtualized-physical digital substations

Kabbara, Nadine; Cibin, Nicola; Morais, Hugo; Ştefanov, Alexandru; Gibescu, Madeleine

DOI
10.1016/j.segan.2025.101795

Publication date
2025

Document Version
Final published version

Published in
Sustainable Energy, Grids and Networks

Sustainable Energy, Grids and Networks 43 (2025) 101795

Contents lists available at ScienceDirect

Sustainable Energy, Grids and Networks

journal homepage: www.elsevier.com/locate/segan

A cybersecurity assessment for hybrid virtualized-physical digital substations

Nadine Kabbara [a,b,*], Nicola Cibin [c], Hugo Morais [d], Alexandru Ştefanov [c], Madeleine Gibescu [b]

[a] EDF R&D Paris Saclay, Palaiseau, France
[b] Utrecht University, Utrecht, Netherlands
[c] Delft University of Technology, Delft, Netherlands
[d] Inesc-ID, Lisboa, Portugal

ARTICLE INFO

Keywords:
Digital substations
Virtualization
Cybersecurity
IEC 61850
Cyber-physical power systems
Virtual machines

ABSTRACT

Virtualization in digital substations is a rising trend in the power sector, opening up interesting research avenues. The virtualization of intelligent electronic devices (IEDs) is thought to enable more flexible and agile cybersecurity software updates and patching processes while seamlessly integrating with current physical IEDs. However, no studies have yet considered a general cybersecurity assessment for such novel hybrid systems. To fill this gap, a systematic cybersecurity assessment of a digital substation composed of hybrid (virtual and physical) IEDs is presented in this paper. A testbed was developed to assess the different attack vectors with a focus on targeting virtual machines (resource exhaustion) and injection attacks on IEC 61850-compliant communication streams. A hybrid protection selectivity use case was successfully demonstrated with multiple targeted cyber attacks on the testbed where the non-attacked IED successfully cleared the grid fault. The attacks' impacts ranged from minor to major effects on the IEDs' tripping signals (and eventually circuit breaker actions) including forced signal delays, signal latching, and signal drops. The results of this study highlight the importance of providing a proper *cybersecurity by design* strategy for integrating hybrid substation systems with virtualization technologies.

1. Introduction

The integration of renewable energy sources across all power grid voltage levels, from low to high, along with the increasing electrification of sectors such as transportation, heating, and industry, requires significant changes in how power systems are designed and operated. This evolution involves developing more flexible, resilient power grids and implementing advanced digital technologies to ensure a reliable, efficient, and sustainable electricity supply. Modernization of power systems and integration of advanced operational technology (OT) with information technology (IT), such as virtualization, aim to respond to the increasing need for flexibility of operation in future power systems [1].

Virtualization has revolutionized the IT and telecommunications sectors by abstracting hardware resources and enabling the deployment of multiple virtual instances on a single physical server using virtual machines (VMs) or containers. In the context of power systems, the concept of virtualization can be applied in several areas, such as power transmission and distribution substations [2], metering systems [3], and flexibility management [4]. In the specific context of power substations, virtualization facilitates the consolidation of communicating intelligent electronic devices (IEDs) (implementing protection, automation, and control functionalities) onto fewer hardware components with virtual IEDs (vIEDs), thereby reducing their capital and operational costs as proven by [5]. Moreover, virtualization enables scalable architectures that can adapt to the evolving grid demands and facilitate the deployment of updated and new functionalities. This can also support upgrading protection systems to satisfy the new grid needs with lower inertia due to the high penetration of renewables [4].

At the heart of the digitalization of substations lies the IEC 61850 standard [6], which defines data models (the what) and communication protocols (the how) for the seamless exchange of information between IEDs within substations and across the wide-area communication networks. IEC 61850 enhances system interoperability, simplifies system

[*] Corresponding author at: Utrecht University, Utrecht, Netherlands
Email address: n.kabbara@uu.nl (N. Kabbara).

https://doi.org/10.1016/j.segan.2025.101795
Received 24 January 2025; Received in revised form 21 May 2025; Accepted 4 July 2025
Available online 5 July 2025

integration and engineering, and supports real-time monitoring and control functionalities.

Centralization of protection and control functions within a single hardware was also supported thanks to advancements in communication speed and the IEC 61850 standard. Along with centralization, came the concept of 'hybrid' protection and control systems as first mentioned in [7]. The hybrid infrastructure harmonizes both distributed and centralized substation protection and control between bay and substation levels, thereby providing advanced lifecycle and application management [7]. As an extension to the previously defined hybrid concept, in this paper, a hybrid protection and control concept with both distributed *physical* IEDs and centralized *virtual* IEDs is proposed.

The advantages of such *hybrid* setups compared to traditional physical-only or futuristic virtual-only designs include: (1) supporting progressive roll-out and brownfield integration of IEDs, (2) heterogeneous redundancy and backup, and (3) greater flexibility in digital substation operation. The aforementioned benefits are deemed highly interesting for power system use cases as shown by a survey in the CIGRE B5.77 working group [8]. However, no prior research in the literature has successfully demonstrated the advantages and practical applications of hybrid physical-virtual digital substations beyond simplistic simulations. Another important challenge that has been raised with the integration of renewables is ensuring proper protection selectivity [9,10]. This work thus demonstrates the potential of a hybrid (physical-virtual) protection selectivity scheme.

However, as power grids embrace virtualized IEC 61850 digital substations, they become increasingly vulnerable to more advanced cyber threats and attacks. The convergence of IT and OT networks introduces extended attack surfaces and novel attack vectors that can be exploited by malicious actors. Cybersecurity breaches targeting digital substations can lead to severe consequences, including operational disruptions, financial losses, and risks to public safety such as previous attacks in Ukraine in 2015, 2016, and 2022 [11,12] and the attempted UK power grid attack in 2020 [13].

This paper therefore addresses the cybersecurity challenges that can appear in hybrid IEC 61850 digital substations with both legacy, physical, and new, virtual, IEDs. A case study involving hybrid protection selectivity with virtual IEDs is analyzed under multiple cyber attack scenarios. By comprehensively tackling the intersection of virtualization technology, IEC 61850-compliant digital substations, and cybersecurity, this study conducts a general cybersecurity assessment in hybrid substations covering both the physical and virtual components.

1.1. State of the art: cybersecurity in hybrid digital substations

A complete survey on the cybersecurity of substation communication systems based on IEC 61850 is performed by [14]. Authors in [15] also performed a survey on network security with a focus on software-defined networking, while increasing power system resilience against cyber attacks was tackled in [16]. However, none of these papers had considered attacks specific to virtualized IEDs in digital substations, e.g., focusing on resource exhaustion attacks.

The authors in [17] assessed the security of one of the protocols specified in the IEC 61850 standard, namely Generic Object-Oriented Substation Event (GOOSE), and exploited its lack of message authentication and encryption to perform a cyber attack. The attack was implemented in a hardware-in-the-loop setup, and a system dynamics assessment was performed. By injecting the malicious SV stream into the communication network, the authors were able to block the IED, prevent normal protection operations, and cause delays in fault clearance [18]. However, the testbed only included physical IEDs, and no testing or attacks on virtual IEDs were considered. Similarly, in [19,20], a simulation environment was used to examine different schemes against injection attacks. The simulation did not include virtualization, and no physical IEDs were available in the setup. In [21], Martinez et al. tested a software-defined IED platform and an SV analog processing module and its performance; however, no cybersecurity tests were performed.

Existing datasets involving cyber attacks on substation testbeds have previously been presented in [22,23]. Four primary attack targets are identified: physical (hardware, instruments, sensors); network (communication channels, denial of services); protocol data frames (data corruption); and control (software configurations). However, both cybersecurity testbeds did not consider virtualized IEDs nor virtualization-specific cyber attacks, as proposed in this paper.

As for the real-time processes running the protection and control algorithms, it is known that specific attacks targeting the scheduler prioritization in real-time (RT) Linux can break its deterministic performance. Previous works in [24–26] analyzed the security limits and concerns for real-time systems, focusing on scheduling security and network attacks to miss a deadline with no specific case study for industrial power systems. Authors in [27] perform denial of service attacks using configured virtual machines with Modbus communications. The study does not include any IEC 61850 communication or physical IEDs.

Table 1 summarizes the identified gaps found in the literature and addressed by this work. *In summary,* the current state of the art still lacks a comprehensive study that includes cybersecurity aspects concerning physical and virtual IEC 61850-compliant digital substation testbeds. Moreover, no case study exists addressing a hybrid protection selectivity scheme under cyber attack scenarios. Such study is of interest to researchers in substation virtualization cybersecurity to analyze risks, extract trends, and develop intrusion detection and prevention systems.

1.2. Contributions and paper organization

The contributions of this study thus consist of:

1. *Development of a hybrid (virtual and physical) digital substation real-time testbed.*
2. *Identification and simulation of relevant cyber attack scenarios for physical IEDs and virtualized IEDs (in virtual machines).*
3. *Feasibility demonstration of a hybrid protection selectivity scheme where a physical (respectively virtual) IED backs up a virtual (respectively physical) IED under attack.*
4. *Preliminary impact assessment of resource exhaustion and injection attacks on (virtual and physical) IED protection capabilities.*

The rest of this paper is organized as follows: Section 2 describes the architecture of the setup including some background knowledge on IEC 61850 and virtualization in Section 2.1. The hybrid protection selectivity scheme is introduced in Section 2.2, and the presentation of the hybrid setup is provided in Section 2.3. Section 3 introduces the cybersecurity assessment of the setup with the identified attack surfaces in Sections 3.1 and 3.2, and the performed tests detailed in Section 3.3. The results are presented and analyzed in Section 4, and conclusions are provided in Section 5.

2. Case study and testbed architecture

In the following, a brief refresher on the IEC 61850 communication standard and virtualization is presented.

2.1. Refresher on IEC 61850 and virtualization

IEC 61850 is an international standard designed for power system automation; it helps ensure interoperability among networked devices from various manufacturers while streamlining system efficiency [29]. GOOSE and SV are both key protocols for time-critical data transfer in a digital substation [30]. GOOSE is used for fast, reliable transmission of critical event-based messages in a substation, such as protection trips and status updates, ensuring low latency and high reliability (within 3 ms). These messages are multi-cast to all devices on the network

Table 1
Comparison of related state-of-the-art studies and this work.

Lit	Criteria					
	Physical testbed	Simulated testbed	Virtualized IEDs	Virtualization cyber attacks	IEC 61850 cyber attacks	Backup selectivity
[17,18]	✓	X	X	X	✓	X
[22]	✓	X	X	X	✓	X
[23]	✓	X	X	X	✓	X
[28]	X	✓	X	X	✓	X
[19,20]	X	✓	X	X	✓	X
[21]	X	✓	✓	X	X	X
[27]	X	✓	X	✓	X	X
[24–26]	X	X	X	✓	X	X
This work	✓	✓	✓	✓	✓	✓

(at the MAC network level), enabling simultaneous receipt by all subscribed IEDs. Similarly, SV transmits high-speed, low-latency real-time data such as sampled measurements from merging units to protection and control devices. It inherently supports reliable and low-latency data streams needed for accurate instrument measurements and real-time monitoring.

Virtualization is a technology that allows to create multiple simulated environments or dedicated resources from a single, physical hardware system [31]. A hypervisor connects directly to the hardware and simulates multiple, distinct, and secure environments known as virtual machines. By leveraging virtualization, utilities can test and deploy protection, automation, and control systems more flexibly and efficiently. Virtual networks within the VM or container environment enable rapid communication and testing without the need for physical hardware.

Virtualized IEDs running in VMs can communicate over both virtual and physical networks. The virtual IEDs deploy the functions of physical devices and interact with the network using the same IEC 61850 protocols, including GOOSE and SV. The communication interface of a virtual IED is based on an IEC 61850 library and supports its defined services (including data model access, publisher–subscriber definitions, reports, etc.). Therefore, the same substation configuration description file (SCD) can be used to configure the communication interfaces of both a virtual and physical IED, which can then smoothly interact thanks to the configured IEC 61850 services.

When interfacing with physical networks, virtualized IEDs can directly bind (i.e., physical pass-through) or bridge (i.e., virtual switch) to the physical host network interfaces to send and receive messages, ensuring seamless integration and interoperability with existing infrastructure, including physical IEDs. For example, a virtual and physical IED can both be coupled to actuate the same (or different) circuit breakers by each receiving the parallel SV data stream and publishing a GOOSE trip message.

2.2. *Case study: selectivity in hybrid protection systems*

Protection relays are vital components in electric power systems and are characterized by their accuracy and effectiveness in rapidly detecting different types of faults. They perform quick corrective actions to prevent equipment damage and maintain system stability and availability. A critical consideration in power system design is ensuring the balance between protecting electrical equipment and maintaining system availability [32]. Therefore, relays need to operate correctly and consistently under different fault conditions while preventing unnecessary tripping during normal system operation.

Protection selectivity is a vital characteristic that aims to ensure a reliable and resilient power system [33]. Selectivity is designed to clear and isolate only the faulty sections, thereby minimizing system disruptions. Inherent selectivity in relay devices enables them to operate only on faults within their 'zone' of operation. A 'zone' is the region of the power system that is monitored and protected by the relay from faults.

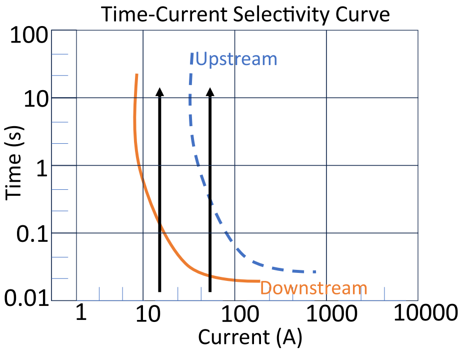


Fig. 1. Time-current curve for protection selectivity with curve to the left as primary protection downstream to the fault and right curve as secondary protection upstream to the fault. Figure adapted from [32].

Selectivity has two main settings: pickup (or threshold) and time delay (intentional delay following a fault) [34]. Time delays allow for another downstream protection device (i.e., with a lower pickup current) that is closer to the fault zone to clear the fault and prevent unnecessary interruptions from occurring [33]. An upstream device (i.e., with a higher pickup current) therefore primarily serves as a backup protection. Two protection devices are selective if the downstream device's time-current curve is to the left of the upstream device's curve and the curves don't overlap, as seen in Fig. 1. A protection scheme design can use two different protection algorithms acting on different timescales with different protection selectivity settings within a particular zone. Given that a failure of a high voltage transmission line is extremely critical, quite often, system backups with primary, secondary, etc., relays ensure the fault is fully contained.

Ensuring complete selectivity, including overload conditions, component damage, control algorithm development, and withstand curves (for equipment overheating) can be very expensive [32]. Therefore, economic feasibility requires that the additional costs can offset the additional operational expenses in case of an outage or equipment damage. It can be noted that infrastructure costs (i.e., controllers, industrial computers, gateways, etc.) also make up part of the complete selectivity costs.

However, in the case of hybrid IED architectures, the reduction in economic capital and operational expenses (CAPEX and OPEX) seems to be an interesting motivation (as demonstrated in [5]) to use virtualization as an implementation in the protection selectivity design. The server running the vIED centralizes multiple functionalities acting on a particular bus. Each vIED can implement a protection function acting on the connected bus zone and is either *backed up by*, or*backs up* a physical protection IED on that same bus. The physical-virtual IEDs hybrid setup will be demonstrated in the case of cyber attacks on the testbed where the non-attacked (virtual or physical) IED aims to clear the fault. A qualitative comparison between the traditional physical scheme and the hybrid

Table 2
Qualitative comparison of traditional all-physical protection scheme (where all IEDs are physical) to a hybrid scheme with virtualized IEDs.

Category	Traditional all-physical IEDs scheme	Hybrid scheme (Physical + Virtual IEDs)
Fault tolerance	Hardware failures often require onsite visits and manual replacements	Can be restored quickly by VM replication
System redundancy	Requires physical backup IEDs	High redundancy via virtualization server availability
Cybersecurity risks	Isolated system with difficult remote access	System exposed to more cyber threats at the VM and hypervisor levels
Scalability	Limited (fixed hardware)	More scalable (easy to deploy new virtual IEDs)

protection selectivity scheme is provided in Table 2. Implementing IEDs in virtualized environments allows one to inherit the advanced features associated with virtualization such as VM backup and replication, live migration, and dynamic scale-ups [35]. These inherent features thus facilitate the deployment of new virtual IEDs in case of system failures or scale-up tests in laboratories with limited availability of physical IEDs.

2.3. Real time hybrid setup with virtualized and physical IEDs

Having established the promised benefits of a hybrid protection system for ensuring selectivity, this section delves into the implementation details of the real-time simulation testbed. The implemented hybrid setup, as seen in Fig. 2, includes a distance protection physical IED from a typical vendor and a virtual IED with an instantaneous overcurrent protection acting as a primary relay within a smaller containment zone. A distance protection algorithm works by measuring a power line's impedance and comparing it to a preset characteristic value. In case of a fault, the line's impedance value falls outside the admissible range. A zone setting is also configured for each IED. Different zone settings have different operating times (time delays) for clearing the fault. The overcurrent protection should operate before the distance protection operates, thereby ensuring a hybrid (physical/virtual) protection selectivity.

An IEEE 5-bus test system is simulated in the Real-Time Digital Simulator (RTDS) [36]; the part of the model under study includes a circuit breaker, fault point, and IEC 61850 GOOSE/SV communication blocks as previously presented in [2]. The RTDS's GTNETx2 card takes care of forwarding the IEC 61850 SV and GOOSE from the simulated IEEE 5-bus model through the RTDS local subnetwork switch. The setup is coupled to one virtual IED running on a physical server and one physical IED, both of which are configured with internet protocol addresses belonging to the RTDS subnetwork. The VM hosting the vIED is coupled to the RTDS process bus subnetwork over a virtual bridge network configured in the PROXMOX host. The physical host server and IED directly connect to the RTDS local (process bus) switch. Both (v)IEDs are also similarly connected to the station bus switch, representing the administrative and engineering subnetwork. The output of a logical 'OR' gate (between the physical and virtual IED) trip signals configured in the RTDS model decides the final position (open/closed) of the circuit breaker.

The vIED is running on a physical server equipped with an Intel® Xeon® CPU running at 3.60 GHz, 64GB of RAM, and operates using the PROXMOX® hypervisor. The vIED is configured with the open source libiec61850 library and initiated with GOOSE publishers and SV subscribers from an internal SCD file [37]. The vIED subscribes to the SV data flow published by RTDS, and publishes a GOOSE trip signal following a grid fault. The implementation of the vIED image is based on the open source repository found in [38].

The host server is time-synchronized with the precision time protocol (PTP) on the local lab network. The VM specifications include an Intel® CPU with 4 cores, 16GB of RAM, and an 82GB hard disk, running the Ubuntu 22.04 operating system. A network time protocol (NTP) network time synchronization service is running inside the VM using the timesync service in Linux.

Also, special attention should be given to ensure the correct timekeeping of the physical host machine with a reliable time source that will be matched to the VM BIOS clock. Mechanisms such as periodic time checking can be activated to detect any possible time inaccuracies.

It should be noted that the VM's Linux OS has not been optimized for deterministic real-time performance as the focus of the obtained results was not on the results' determinism but rather on giving a general

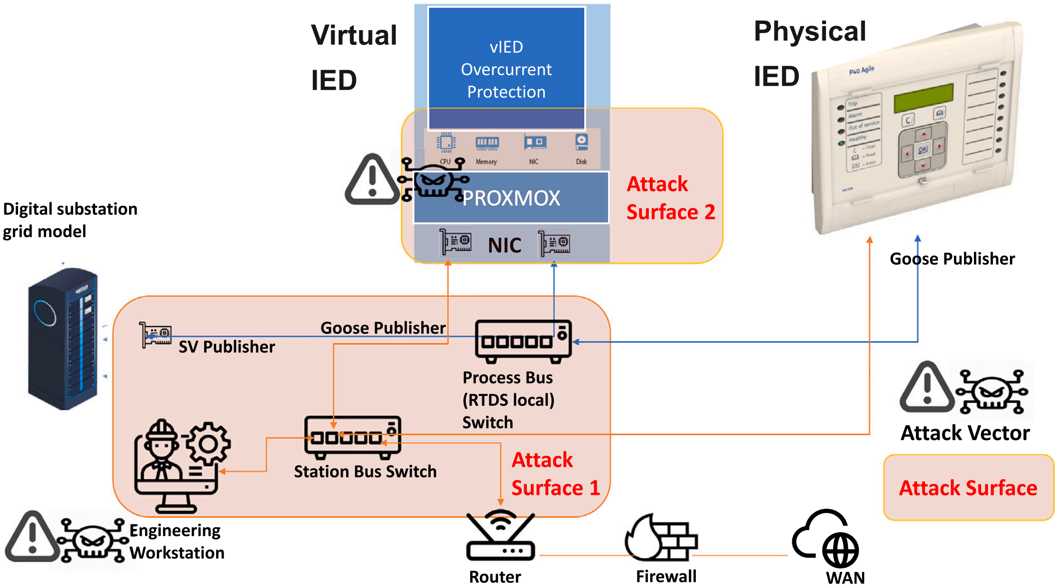


Fig. 2. Hybrid setup with virtual IED, physical IED, and real-time power system simulator.

overview of the different possible impacts on the physical grid following a targeted cyber attack on the hybrid environment. Therefore, the results will not focus on jitter or latency delays arising from the processing overhead. Instead, the results provide a stochastic range and order of magnitude of the attacks' impact on the protection tripping signal.

3. Cyber security assessment of the hybrid IEDs setup

Identifying the cyber attack surfaces on the hybrid setup involves analyzing the attack vectors in both the virtual and physical components of the setup. Two major attack surfaces have been identified: (1) the physical IED and communication network, and (2) the virtual machines hosting the vIED and the vIED itself. The identified surfaces are depicted in Fig. 2. The first attack surface can be exploited from the local engineering workstation connected to the station bus switch, whereas the second one relies on the attacker being able to gain initial access to the hypervisor, the VM, or the vIED service. In the following, these two identified attack surfaces are further discussed.

3.1. Physical IED and communication network attack surface

Vulnerabilities affecting the physical IED can be exploited by the attackers by sending specifically crafted packets to the IED's open ports. Examples of such vulnerabilities are CVE-2023-28766 [39] and CVE-2017-8779 [40], which affect the HTTP and RPC services exposed by some IEDs. These vulnerabilities could be exploited to cause a Denial-of-Service to the targeted physical IED.

IEC 61850 GOOSE and SV protocols can also be affected by critical vulnerabilities due to their lack of inherent authentication and encryption, making them susceptible to sniffing, spoofing, injection, and replay attacks [17,18]. These security mechanisms are often not implemented due to strict real-time constraints mandated by the IEC 61850 standard and the consequent message overhead caused by digital signatures or message authentication codes [17].

3.2. Hypervisor, virtual machines and virtual IEDs attack surfaces

VMs offer numerous benefits, such as improved resource utilization, scalability, and ease of management. However, they can also introduce specific security challenges, as summarized in Table 3. These include vulnerabilities in the hypervisor, which, if exploited, can lead to VM escapes (between VMs and Host) [41]. Examples of such vulnerabilities are CVE-2022-31705 [48] and CVE-2024-22273 [49], which can lead to data leakage and control takeover of one or multiple hosted VMs. Moreover, attacks can exploit incorrect VM isolation, eventually leading to possible data stealing or virtual disk compromises.

A VM's resources can be overwhelmed by a targeted exhaustion attack on its running services [44–46]. As for the real-time processes running inside the VM, specific attacks targeting the scheduler prioritization can disrupt the performance of the VM [24–26]. This can lead to critical damage to the monitored and controlled systems, given the importance of ensuring real-time performance for protection algorithms.

Other potential threats also include attacks on virtual switches and routers, as well as virtual network vulnerabilities like port scanning and traffic interception, which can eventually cause a network availability or denial of service (DoS) issue.

In deployment scenarios in which multiple redundant servers are used to increase systems' availability and reliability, exploits targeting the live migration of VMs are important threats that should be considered [47].

3.3. Simulated attack scenarios

The hybrid virtual and physical IED setup is designed to simulate various operational and cyber attack scenarios to enhance the security and reliability of power utility automation systems. Scenarios include normal operating conditions where both virtual and physical IEDs communicate using the protocols specified in the IEC 61850 standards, ensuring interoperability and performance under typical system operation. Fault scenarios, such as a temporary one-phase fault, test the resilience and response of the system. Cyber attack scenarios are critical for evaluating system security, and they include resource exhaustion, network scanning, and GOOSE and SV injection attacks. More in detail, the simulated scenario consists of the following:

1. **Basic operation**: corresponds to a normal grid and system functioning with no ongoing faults or cyber attacks.
2. **Fault operation**: corresponds to a power grid operation where a fault is simulated in the power system. A tripping signal should be issued in order to open the circuit breaker (CB) and clear the fault within the allowed time.
3. **Network scanning**: corresponds to simulating an active information-gathering process performed by a malicious actor who has gained access to a system connected to the local process bus network within the hybrid setup. The attacker scans the various hosts connected to the network to detect any open ports, exposed services, and vulnerabilities. Different levels of stealthiness of the performed scanning are tested.
4. **Resource Exhaustion Stressing**: corresponds to simulating the impact of the resource exhaustion attack on the vIED VM. The attacker intercepts and alters the priority of the vIED process and stresses its resource access. The impact of such an attack on

Table 3
Main cyber attacks on real-time virtual machines.

Cyber attack type	Description	Possible impact
VM escape (VM to VM or VM to host) [41,42]	Exploiting vulnerabilities in the hypervisor to break out of a VM and interact directly with the host OS or other VMs.	Unauthorized access to the host system and other VMs, execution of arbitrary code, control of host resources, potential compromise of all hosted VMs.
Data stealing (virtual disk) [43]	Accessing and extracting sensitive data from virtual disk files. Attackers may exploit vulnerabilities or gain unauthorized access.	Exposure of confidential information, intellectual property, and other sensitive data stored within virtual disks, leading to security breaches.
RT security [24–26] and resource exhaustion [43,44]	Overwhelming a VM's resources (CPU, RAM) using techniques like creating multiple processes, process re-prioritization and scheduling, memory (cache) leaks.	Degraded VM performance, slowdowns, crashes, potential denial of service (DoS) for the affected VM, impacting service availability, and deterministic RT.
Availability: network DoS [45,46]	Flooding a VM's and host network interface with excessive traffic to overwhelm its network resources.	Service unavailability due to consumed network bandwidth, exhausted network stack processing capabilities, significant downtime, and potential data loss.
Live migration (with more than 1 physical server) [47]	Exploiting vulnerabilities during the process of moving a running VM from one physical server to another.	Data breaches, VM hijacking, disruption of services, potential alteration of the VM's state, or injection of malicious code during migration.

Algorithm 1 GOOSE or SV-based injection attacks required steps [17].

```
Monitor communication network traffic
Sniff IEC 61850 protocol related frames
Tamper data contained in the frames
Inject spoofed frames into the communication network
```

both the cyber network and the eventual physical grid (with a delayed or dropped tripping of the CB) is observed for different configurations.

5. **GOOSE and SV injection**: corresponds to simulating the injection of maliciously crafted packets into the communication network as described in [17]. These types of attacks exploit the lack of authentication and encryption in the protocols specified in IEC 61850 and allow to maliciously open circuit breakers or to report false measurements to IEDs. Depending on the communication network location of the device used by the attacker to perfom the GOOSE/SV injection attack, and on attacker's mode of operations, this class of cyber attacks can also be classified as Man-in-the-Middle (MitM) attacks. In a MitM attack, an attacker intercepts and potentially alters the communication between two parties without their knowledge. When it comes to FDI, the attacker injects false data into the communication stream, which can lead to incorrect decisions or actions by the system. In Algorithm 1, the steps required to perform GOOSE or SV-based injection attacks are presented.

The objectives of the attacks on the hybrid testbed are to: (1) identify the vulnerable points of the design, (2) assess the cyber attack impact, and (3) demonstrate the robustness of the hybrid backup protection scheme. To effectively demonstrate the hybrid physical-virtual backup scheme, the attacks only targeted a single IED, either physical or virtual at a time. This allows for having only one IED down, virtual, respectively physical, and ensures that the non-attacked physical, respectively virtual, IED clears any occurring fault in the meantime. Note, however, that in the specific case of the SV injection attacks, both the physical and virtual IEDs are attacked simultaneously.The cyber attacks were simulated from a VM running in parallel to the vIED on the same server.

As previously mentioned, the study focuses on exhaustion attacks in VMs. In order to simulate the impact of a resource exhaustion attack, the Linux 'stress' and 'renice' commands were used to simulate multiple resource-exhaustive threads with high priority allocated by the CPU. The priority of the vIED process running the protection algorithm was also modified to simulate a situation where the priority scheduling is compromised, adding even more stress on the vIED process. Scenario with stress priority B is thus deemed a cyber attack with a higher intensity of impact. We note base priority O as 0, priority A as + 15, and priority B as +19.

The following Algorithm 2 shows the commands used to reset the vIED process priority and simulate the effects of a resource exhaustion attack.

Algorithm 2 Resource exhaustion with priority rescheduling.

```
# Stress Priority O
stress --cpu 3 --i 2 --m 1 --vm 5 --vmbytes 1024 M --timeout 60
# Stress Priority A
sudo nice --10 stress --cpu 3 --i 2 --m 1 --vm 5 --vmbytes 1024 M --timeout 60
sudo renice 15 --p $vIED_process_id
# Stress Priority B
sudo nice --15 stress --cpu 3 --i 2 --m 1 --vm 5 --vmbytes 1024 M --timeout 60
sudo renice 19 --p $vIED_process_id
```

3.3.1. Limitations

Several limitations inherent in our simulated testbed are discussed in the following. As introduced in the previous sections, the paper aims at analyzing the physical impact of the most relevant cyber attack against IEDs and vIEDs in digital substations. For this reason, the initial attack vector(s) used by the attacker to gain initial access into the digital substation communication network and compromise the systems used as the source of the attacks is out of the scope of this study; these considerations can be found in [50]. Only the last phases of the cyber attack and the impact on the IED and vIED reactions are measured and evaluated. Moreover, even though only single line to ground faults were simulated in RTDS, SV injection attacks were used to report various three-phase current and voltage values to simulate different types of false data injection attacks. These different types of false data injection attacks can be referred to different types of faults, and thus showing that the study reported in this paper can be generalized. On the other side, details on attack detection, prevention, and mitigation are out of the scope of this study, as is the distinction between system disturbances and cyber attacks.

The choice of the simulated cyber attacks is primarily based on the most relevant and reputable attacks available in the literature [43,44] that can have a measurable impact on the physical grid operation. In the following, only the resource exhaustion attack on the virtualized IED running inside the VM is considered for assessing the 'virtual' part of the hybrid setup. It is assumed that this attack is one of the most relevant and can give a good representation of the possible impacts on the attacked setup. Also, no assessment on virtual IEDs is available in the literature to the best of the author's knowledge.

In general, we have focused on attacks that target and block a single IED (physical or virtual) at a time and are thus limited to a single cyber attack at a time. In the current hybrid protection selectivity scheme, resilience is only guaranteed in case where a single IED (hybrid or physical) is down; the case where both IEDs are blocked simultaneously was outside our scope and is not included in the design of the current hybrid selectivity scheme. Also, the different cyber attacks that have been tested are meant to be launched at different steps of the cyber kill chain. When performing cyber attacks, attackers try to be as stealthy as possible to avoid causing any alarm (raised by intrusion detection systems, for instance). Launching multiple simultaneous cyber attacks against the same device would only increase the likelihood of being detected; therefore, it is a less probable scenario and thus deemed unlikely for our feasibility study. We also note that intrusion detection system features are outside the scope of this paper. Interested readers may consult the extensive survey in [51]).

4. Testbed validation and simulated attack scenario results

For data collection of the simulated scenarios, the process involves gathering both physical (RTDS) and communication and resources data over a period ranging from one minute (in base cases, resource exhaustion, and injection attacks) to five minutes (for port scanning attacks).

The voltage and current measurements, trip signals from both the vIED and the physical IED, and circuit breaker status are continuously monitored in RTDS. All communication between the IEDs and other network devices is captured in Wireshark® [52]. Also, the resources of the virtual machine hosting the vIED and the vIED process, such as CPU usage, memory consumption, and network throughput are measured. All the physical data (from RTDS) and resource monitoring data are saved in .csv file formats. The Wireshark® network packet captures are saved in .pcap format.

The simulation time step is set at 50 μsec in RTDS, but due to some limitations on the total number of data samples that can be saved in

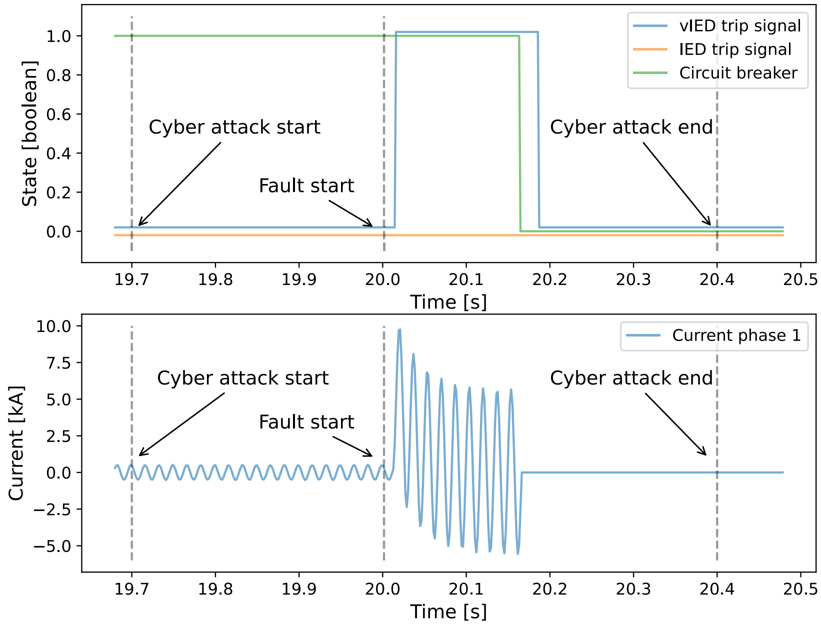


Fig. 3. Demonstration of protection selectivity with virtual IED that trips following a fault when a cyber attack (SV injection) blocking the physical IED is in process.

RTDS/RSCAD, data is down-sampled where every 32nd data point is saved. This is equivalent to 32*50 μs = 1600 μs or 1.6 ms time step of saved data. The VM's and vIED process's resource consumption is measured at a 2-second rate. We note that the CB re-closure was set at 4 secs in RTDS.

The dual cyber-physical data collection[1] enables the detection of correlations between physical power grid behaviour and cyber attacks. This aids in better understanding the impact of cyber attacks on power systems with virtualization, and eventually helps in developing robust systems with enhanced mitigation and intrusion prevention/detection strategies.

4.1. Hybrid protection selectivity results

Before investigating the cyber attack scenarios, the first step is to validate that the hybrid setup works as intended. The observed results shown in Figs. 3 and 4 confirmed the feasibility and robustness of the hybrid protection selectivity designed for this study. The expected IED tripping time is around 25 ms, while that from the vIED is around 11 ms. In case the physical (respectively virtual) IED was attacked and targeted to fail, the virtual (respectively physical) IED successfully opened the circuit breaker and was able to clear the fault within the expected timings as seen in Figs. 3 and 4. It can be noted that even though the simulated failure here was due to a specific cyber attack, the hybrid setup can also act in case of other types of failures that block one of the (v)IEDs beyond the simulated cyber attacks and can include traditional system hardware failures for example. Such a hybrid approach can thus contribute to enhancing the overall system flexibility, reliability, and availability. It can also help promote the deployment of virtual IEDs within brownfield substation projects requiring upgrades.

4.2. Network reconnaissance

Network reconnaissance is one of the first phases required to prepare for more complex and advanced cyber attacks, and involves a malicious actor with access to the local network gathering information on the network topology, connected devices, and possible vulnerabilities in their exposed services. Nmap (Network Mapper) [53] is a powerful open-source tool used for network discovery and security auditing. It can identify hosts and services on a network, scan for open ports, detect operating systems, and discover vulnerabilities. Nmap is widely used by network administrators, penetration testers, and security professionals to assess the security of their networks.

Multiple Nmap scans with different levels of stealthiness were performed on the RTDS local network from the attacker VM. Most of the time, this type of attack does not have any immediate impact on the operation of the scanned systems. Indeed, only harmless probes are sent to the various systems to gather information about their configuration. Thus, such an attack, despite not having any direct impact on the physical substation equipment, is very critical due to the acquisition of sensitive data from the substation by a malevolent actor. As previously mentioned, the gathered information can be used by the attacker in the design of more elaborate cyber attacks, which could be performed in a subsequent time frame. For these reasons, it is crucial to detect and prevent active scanning techniques from being successful in gathering sensitive information. Some detection and prevention techniques include the correct setup of firewalls and data diodes and the deployment of intrusion detection and prevention systems [54].

In this study, Nmap scans were performed with varying intensities using the timing options, which range from very slow (polite) to the very fast, aggressive, and insane scans. The logs coming out of these scans allowed the detection of any open ports in the hybrid setup that are susceptible to vulnerabilities as well as a map of the network topology. Based on the knowledge of the network topology, attacks at the communication level and VMs can be better crafted.

4.3. Resource exhaustion attack

As previously explained, the impact of the resource exhaustion attack was simulated using different stressing commands presented in Algorithm 2 on the vIED process and with different scheduling priorities.

There were three main patterns observed on the virtual IED trip signal during the cyber attacks including: (1) signal delays (i.e., trip signals are time delayed); (2) signal latch (i.e., trip signals stay at value = 'True' for an extended time greater than 200 ms); (3) signal drop (i.e., trip signal is never issued and the fault is thus never detected), as seen in

[1] We note that the open dataset is described in detail in another paper, and a reference will be added as soon as the article is accepted for publication

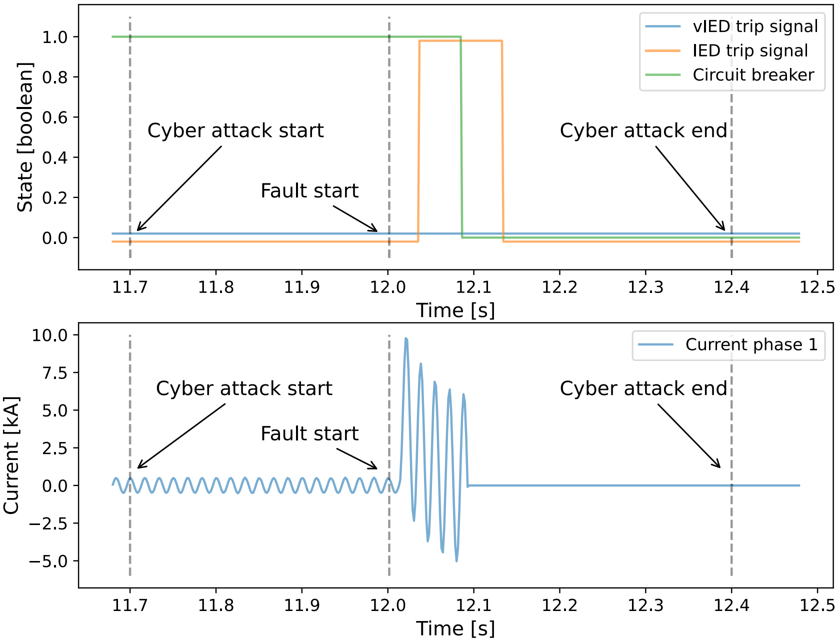


Fig. 4. Demonstration of protection selectivity with physical IED that trips following a fault when a cyber attack (Resource exhaustion) blocking the virtual IED is in process.

Table 4
Resource exhaustion attack results. $\underline{A}$ *(underline)*: vIED Trip Delay; –: vIED Trip Drop; C^* (star):vIED Trip Latch; $\underline{D^*}$ *(underline and star)*: vIED delay and latch; (*other*): vIED Trip normal.

Stress/Priority A	Trips	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
	vIED trip delay (ms)	$\underline{91.2^*}$	$\underline{27.2^*}$	12.8^*	30.4	$\underline{68.8}$	$\underline{62.4}$	24	$\underline{41.6^*}$	$\underline{59.2^*}$	$\underline{233.6}$	–	$\underline{16,972.8^*}$	11.2^*	$\underline{40}$	$\underline{40^*}$	27.2	24
	IED Trip Delay (ms)	27.2	24	24	33.6	22.4	28.8	27.2	24	28.8	32	28.8	30.4	30.4	20.8	33.6	35.6	33.6
Stress/Priority B	Trips	1	2	3	4	5	6	7	8	9	10							
	vIED trip delay (ms)	$\underline{220.8^*}$	–	$\underline{124.8^*}$	$\underline{92.8}$	24^*	$\underline{51.2^*}$	$\underline{182.4^*}$	$\underline{158.4}$	$\underline{76.8}$	$\underline{288}$							
	IED trip delay (ms)	27.2	37.2	28.8	32	30.4	28.8	27.2	28.8	22.4	33.6							

Table 4. It was also observed via monitoring the vIED logs in the VM that the GOOSE and SV counts in the vIED were no longer chronological, with many wrong count warnings.

4.3.1. *Signal delays*

The resource exhaustion attack had a significant impact on the trip delay. As seen in Fig. 5, the trip signal from the vIED was delayed in 70 % of the cases compared to the expected trip time of around 11 ms. The consequences of such delays can be critical in case of a permanent fault. It can disturb the overall system frequency on the power grid and eventually lead to cascading failures and widespread blackouts. Given that the hybrid protection selectivity backup was implemented, the physical IED tripped eventually, opening the CB and clearing the fault within the correct time. Given that Priority B included a more intensive attack that stresses the CPU at higher levels and gives a very low priority to the protection algorithm process, consequently, performance under Priority B was more prone to increased signal delays. This experiment thus shows the importance of well-designed backup protection in case the virtual IED is attacked.

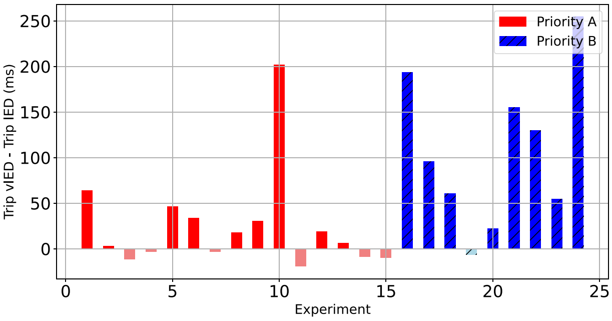


Fig. 5. Tripping time difference for 24 experiments with priority A, B (excluding signal drops and case 12 in priority A Table 2) in the resource exhaustion attack with values below zero corresponding to 'normal' behaviour and over zero denoting 'signal delays'.

4.3.2. *Signal latch*

The latch behaviour was unexpected and quite a critical one that can have a significant impact on the connected grid as it forces the CB to remain open even after the fault is over. The re-closure mechanism cannot be activated with the latched trip at 'True' due to the logical 'OR' deployed in this setup. With the CB open, the electrical load stays disconnected. During the signal latch, the resource usage of the vIED process was around 0 % at numerous incidents showing signs of overload. The CPU overload can also explain the added processing delay and eventual latching of the trip signal before processing the 'normal' data values.

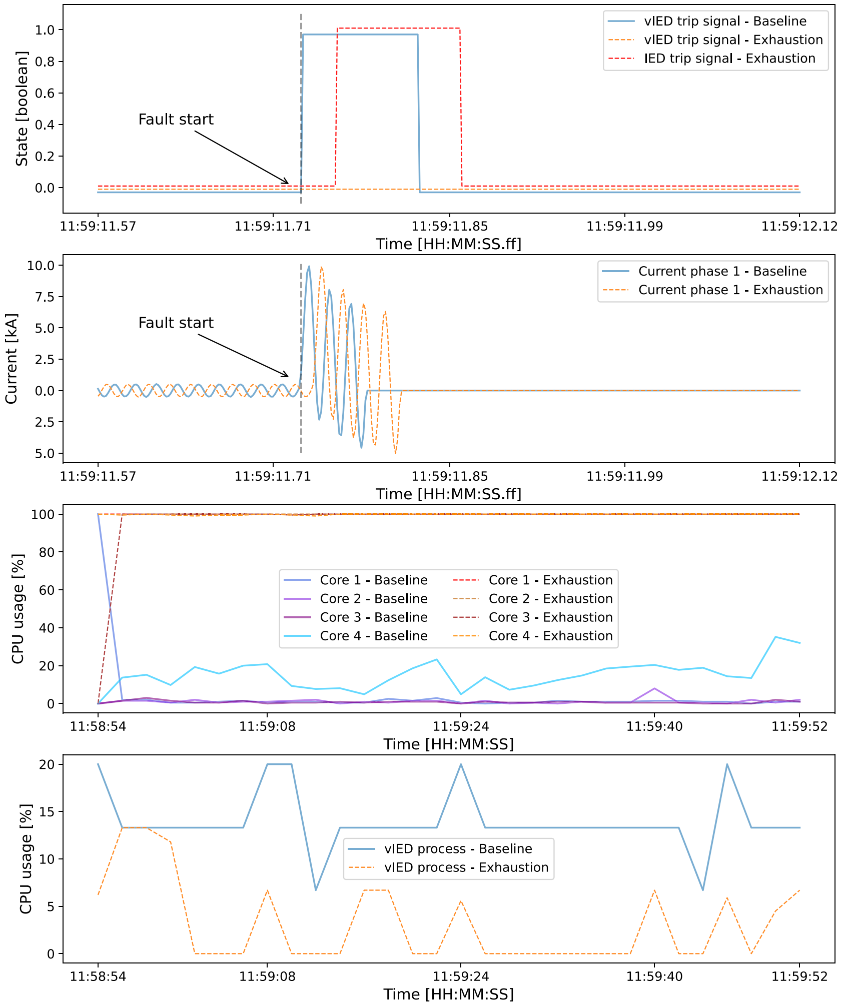


Fig. 6. Baseline vs Resource exhaustion attack vIED trip signals (dropped case), grid current, and CPU usage per VM and per vIED process.

4.3.3. *Signal drop*

During two extreme stress tests, the vIED trip signal was dropped and therefore never detected the fault. A possible explanation is related to the use of libiec61850 [37], where the timeout functionality for SV receivers is usually implemented as part of the handling of the SV streams. The library allows for the configuration of the expected data rates and will monitor the reception of messages. If the SV ethernet socket is not ready within the expected interval, a timeout (set here at 100 ms) or error condition can be raised which can explain the dropped trip signal. Test 12 in Table 4, which was run right after Test 11 with the dropped signal showed a significant delay in issuing the trip signal of over 16 s. Test 11 with the dropped signal might have influenced the large delay in test 12 as the system was regaining some CPU access after total blockage and more ‘normal’ values were being measured again.

Given that the protection selectivity is ensured by the physical IED, the CB was eventually opened within 30 ms in Test 12 by a trip signal from the physical IED (Fig. 6 top). This example details the performance of the hybrid selectivity scheme in case of a malicious cyber attack targeting the virtual IED which totally blocks it out as presented in Fig. 4. We note that the trip signal drop occurred only twice (in test 11-priority A and test 2-priority B) during over 27 runs of the stress tests (in Table 4). It thus remains a less probable event to occur with important consequences for the physical grid’s security.

The vIED VM’s CPU resources were topped at 100 % for the duration of the attack. Under normal conditions, the vIED process requires from 13 % to 20 % CPU usage to function properly. Due to the exhaustion attack, the VM does not provide the required CPU usage for the vIED to operate properly. Also, given that the VM uses a 4-core CPU, and the vIED process is not multi-threaded, the maximum CPU usage that can be allocated to this process is 25 %. The vIED protection application process’s CPU access fluctuated heavily ranging from almost 0 % to a maximum of 14 % CPU, as seen in the bottom plot in Fig. 6, indicating signs of overload. The resource consumption of the vIED process showed exhaustion of around 0 % for around 50 % of the simulation period. This overload can explain the added processing delay and eventual delay (or drop) in sending the trip signal. It can be observed that the vIED process’s CPU at 0 % indicates that it is not being granted access to the stressed computing resources of the VM due to its low priority. Thus, the process will be blocked as a result of the attack.

4.4. *GOOSE and SV injection*

Different maliciously crafted GOOSE messages and SV frames were injected into the communication network as crafted in [17] and seen in Figs. 8 and 9. Specifically, in the case of injecting a GOOSE packet (Fig. 8), the PTRC trip was manipulated to either a fake ‘True’ or fake ‘False’ boolean value. This allows forcing the opening of the CB during normal conditions and the closing of the CB during a fault. Given the lack of message authentication and encryption, the spoofed messages were accepted by the GOOSE subscriber defined in RTDS and caused the

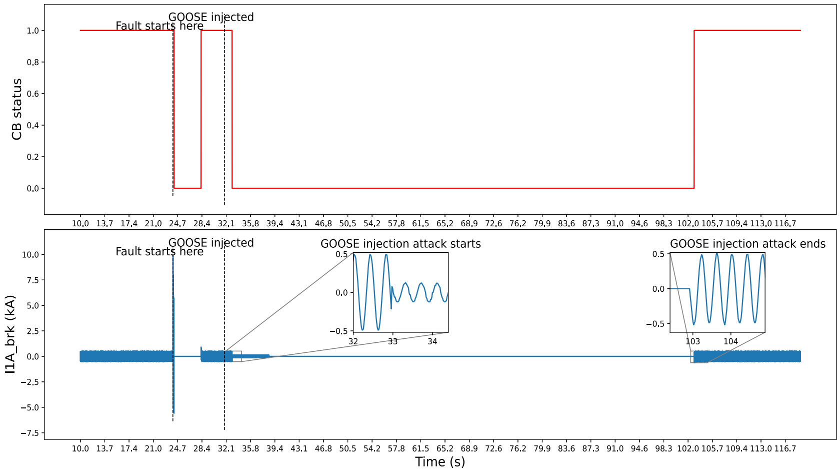
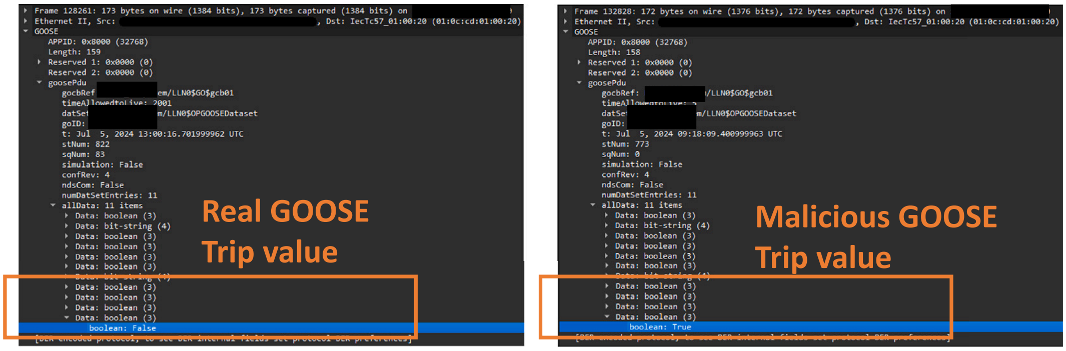


Fig. 7. GOOSE injection attack with circuit breaker position and line current evolution.



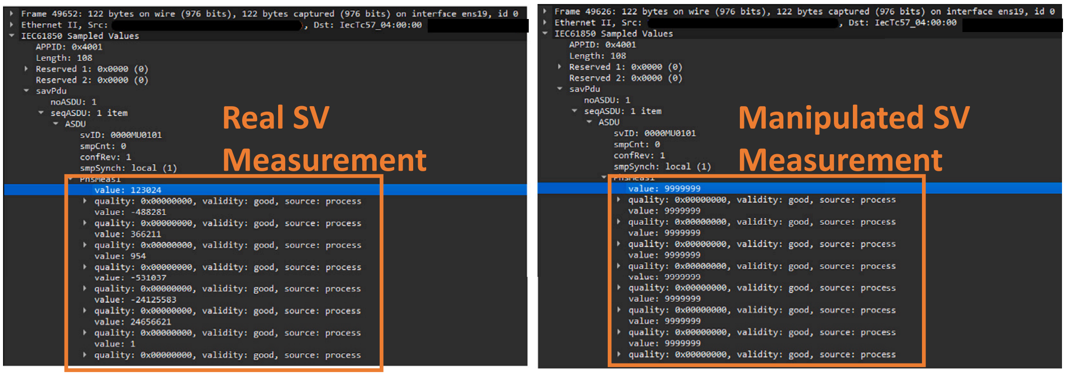
```
Frame 128261: 173 bytes on wire (1384 bits), 173 bytes captured (1384 bits) on [redacted]
Ethernet II, Src: [redacted], Dst: IecTc57_01:00:20 (01:0c:cd:01:00:20)
GOOSE
    APPID: 0x8000 (32768)
    Length: 159
    Reserved 1: 0x0000 (0)
    Reserved 2: 0x0000 (0)
    goosePdu
        gocbRef [redacted]em/LLN0$GO$gcb01
        timeAllowedtoLive: 2001
        datSet [redacted]m/LLN0$OPGOOSEDataset
        goID:
        t: Jul  5, 2024 13:00:16.701999962 UTC
        stNum: 822
        sqNum: 83
        simulation: False
        confRev: 4
        ndsCom: False
        numDatSetEntries: 11
        allData: 11 items
            Data: boolean (3)
            Data: bit-string (4)
            Data: boolean (3)
            Data: boolean (3)
            Data: boolean (3)
            Data: boolean (3)
            Data: bit-string (4)
            Data: boolean (3)
            Data: boolean (3)
            Data: boolean (3)
            Data: boolean (3)
                boolean: False
[BER encoded protocol, to see BER internal fields set protocol BER preferences]
```

Real GOOSE
Trip value

```
Frame 132828: 172 bytes on wire (1376 bits), 172 bytes captured (1376 bits) on [redacted]
Ethernet II, Src: [redacted], Dst: IecTc57_01:00:20 (01:0c:cd:01:00:20)
GOOSE
    APPID: 0x8000 (32768)
    Length: 158
    Reserved 1: 0x0000 (0)
    Reserved 2: 0x0000 (0)
    goosePdu
        gocbRef: [redacted]/LLN0$GO$gcb01
        timeA[redacted]
        datSet [redacted]m/LLN0$OPGOOSEDataset
        goID:
        t: Jul  5, 2024 09:18:09.400999963 UTC
        stNum: 773
        sqNum: 0
        simulation: False
        confRev: 4
        ndsCom: False
        numDatSetEntries: 11
        allData: 11 items
            Data: boolean (3)
            Data: bit-string (4)
            Data: boolean (3)
            Data: boolean (3)
            Data: boolean (3)
            Data: boolean (3)
            Data: bit-string (4)
            Data: boolean (3)
            Data: boolean (3)
            Data: boolean (3)
            Data: boolean (3)
                boolean: True
[BER encoded protocol, to see BER internal fields set protocol BER preferences]
```

Malicious GOOSE
Trip value

Fig. 8. Packets captured in Wireshark showing the real vs manipulated GOOSE packets.



```
Frame 49652: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface ens19, id 0
Ethernet II, Src: [redacted], Dst: IecTc57_04:00:00 [redacted]
IEC61850 Sampled Values
    APPID: 0x4001
    Length: 108
    Reserved 1: 0x0000 (0)
    Reserved 2: 0x0000 (0)
    savPdu
        noASDU: 1
        seqASDU: 1 item
            ASDU
                svID: 0000MU0101
                smpCnt: 0
                confRev: 1
                smpSynch: local (1)
                PhsMeas1
                    value: 123024
                    quality: 0x00000000, validity: good, source: process
                    value: -488281
                    quality: 0x00000000, validity: good, source: process
                    value: 366211
                    quality: 0x00000000, validity: good, source: process
                    value: 954
                    quality: 0x00000000, validity: good, source: process
                    value: -531037
                    quality: 0x00000000, validity: good, source: process
                    value: -24125583
                    quality: 0x00000000, validity: good, source: process
                    value: 24656621
                    quality: 0x00000000, validity: good, source: process
                    value: 1
                    quality: 0x00000000, validity: good, source: process
```

Real SV
Measurement

```
Frame 49626: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface ens19, id 0
Ethernet II, Src: [redacted], Dst: IecTc57_04:00:00 [redacted]
IEC61850 Sampled Values
    APPID: 0x4001
    Length: 108
    Reserved 1: 0x0000 (0)
    Reserved 2: 0x0000 (0)
    savPdu
        noASDU: 1
        seqASDU: 1 item
            ASDU
                svID: 0000MU0101
                smpCnt: 0
                confRev: 1
                smpSynch: local (1)
                PhsMeas1
                    value: 9999999
                    quality: 0x00000000, validity: good, source: process
                    value: 9999999
                    quality: 0x00000000, validity: good, source: process
                    value: 9999999
                    quality: 0x00000000, validity: good, source: process
                    value: 9999999
                    quality: 0x00000000, validity: good, source: process
                    value: 9999999
                    quality: 0x00000000, validity: good, source: process
                    value: 9999999
                    quality: 0x00000000, validity: good, source: process
                    value: 9999999
                    quality: 0x00000000, validity: good, source: process
                    value: 9999999
                    quality: 0x00000000, validity: good, source: process
```

Manipulated SV
Measurement

Fig. 9. Packets captured in Wireshark showing the real vs manipulated SV packets.

malicious closure or opening of the controlled CB. Fig. 7 demonstrates the case with forced CB opening for over 1 minute before the CB is closed again due to the injection of a malicious GOOSE packet with the trip value forced at 'True'. Given that the CB is actuated from either the virtual or physical GOOSE trip signal, a compromised v(IED) GOOSE packet is sufficient to force such behaviour.

On the other side, SV-based attacks are aimed at simulating faulty or normal operating conditions. Also, as part of the SV injection attacks, the malicious data injected in the test included extremely abnormal values that represent a simulation case beyond a single phase fault (seen in the Wireshark capture in Fig. 9). For example, in the injected SV packet shown in Fig. 9, the three-phase voltage and current values were manipulated and forced to an erroneous value of 9,999,999. This malicious act aims to confuse the governing protection (v)IEDs due to the abnormal measurement readings.

In this case, distinctly different behaviours have been observed between physical and virtual IEDs due to their implementation differences. Whereas the virtual IED was still able to react and clear the fault while normal conditions were maliciously injected during a fault, the physical IED entered a 'blocked' state, stopped working properly, and didn't send any trip signal to clear the fault.

A possible explanation for this undesirable behaviour is that the physical IED is not able to process the two conflicting SV streams received from the RTDS and the machine compromised by the attacker, as it has also been shown in [18]. In addition, the IED implements a distance protection that works by measuring a power line's impedance and comparing it to a preset characteristic value. In the case of an injection attack, the line's impedance value is also miscalculated and falls outside the normal values when a fault occurs. These behaviours of the virtual and physical IED are also observed when faulty measurements are replayed during normal conditions. Unlike the previous case, the physical IED's 'blocked' state prevents the IED from sending unintentional commands to the CB, whereas the virtual IED reacts to the maliciously injected faulty measurements to force open the CB.

5. Conclusions and perspectives

Following the recent trend of digital substation virtualization, it is essential to be able to investigate the integration and security of new virtualized solutions with legacy physical environments. In this study, a real-time, hybrid physical and virtual IED protection architecture was set up, and its cybersecurity assessment was performed.

Different attacks were identified and tested for both the physical and virtual environments in both normal and faulted grid conditions. The simulated cyber attacks included port scanning, resource exhaustion, and injection of spoofed GOOSE/SV messages. The feasibility of a hybrid protection selectivity scheme was validated by observing the cyber attack mitigation thanks to the timely tripping of the non-attacked (physical or virtual) IED. The demonstrated concept can be mapped and tested with other (virtual/physical) protection IEDs and setups with other attacks following the hybrid selectivity design.

During 27 test runs of the resource exhaustion attack (with different priorities) on the virtual IED virtual machine, three primary observations of its tripping signals were noted: (1) signal delays; (2) signal latches at 'True'; (3) signal drops. Such behaviours can have an important impact on the physical grid, especially in the case of a real fault, which may eventually lead to instability and cascading blackouts.

As for the GOOSE and SV injection attacks, both virtual and physical IEDs were forced to operate unintentionally following maliciously reported faulty or normal grid conditions. The security issue resides in the lack of message authentication and encryption, which can equally have critical impacts on the physical grid with forced breaker openings and disconnected lines.

The study thus emphasizes the importance of implementing prevention strategies and *cybersecurity by design* for hybrid virtual and physical IED environments. Some possible prevention approaches include ensuring robust cybersecurity for VMs by implementing strong access controls, secure configuration practices, network segmentation, and continuous monitoring to detect and mitigate potential threats or malicious firmware changes [55]. Consequently, both virtual and physical IEDs, need to be regularly updated with the latest security patches to protect against known vulnerabilities along with device hardening, network segmentation, and eventual intrusion detection systems. Due to the IEC 61850 protocols' security concerns, the IEC 62351 standard recommends the adoption of security event logging, and the implementation of message authentication codes for GOOSE and SV message authentication.

The real-world implementation and impacts of this work would be further strengthened if multiple perspectives are tackled. Some of these perspectives for future work include simulating other attacks, such as live migration with more than one server, VM escape, Denial of Service (DoS) on local network switch, or scenarios with multiple simultaneous cyber attacks. Attacks specific to containerized IEDs can also be investigated along with real-time Linux OS optimization. Focusing on various fault types/combinations for an advanced system dynamics study of the cyber attacks and their impacts on the hybrid protection scheme can be further researched. Also, benchmarking the hybrid scheme against an all-physical protection scheme with HRS/PRP network redundancy is an interesting research direction. Moreover, developing intrusion detection systems that can differentiate between a real cyber attack and system disturbances in the presence of noisy data, specifically for hybrid (physical/virtual) digital substations, is also an interesting avenue for research and can increase the hybrid scheme's applicability in real life.

CRediT authorship contribution statement

Nadine Kabbara: Writing – original draft, review & editing, Methodology, Conceptualization, Validation, Investigation, Visualization, Software, Data curation. **Nicola Cibin:** Writing – review & editing, Investigation, Conceptualization, Visualization, Software, Data curation. **Hugo Morais:** Writing – review & editing, Supervision. **Alexandru Ştefanov:** Writing – review & editing, Supervision. **Madeleine Gibescu:** Writing – review & editing, Supervision.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available upon request.

References

[1] N. Kabbara, M.O.N. Belaid, M. Gibescu, L.R. Camargo, J. Cantenot, T. Coste, V. Audebert, H. Morais, Towards software-defined protection, automation, and control in power systems: concepts, state of the art, and future challenges, Energies 15 (24) (2022) 9362.

[2] N. Kabbara, A. Mwangi, A. Ştefanov, M. Gibescu, A real-time implementation and testing of virtualized controllers for software-defined IEC 61850 digital substations, IEEE Open J. Ind. Appl. (2024) 1–12, https://doi.org/10.1109/OJIA.2024.3426321.

[3] C. Guarnieri Calò Carducci, M. Pau, F. Ponci, A. Monti, Towards the virtualization of measurements: architecture, solutions and challenges, in: 2021 IEEE 11th International Workshop on Applied Measurements for Power Systems (AMPS), 2021, pp. 1–6, https://doi.org/10.1109/AMPS50177.2021.9586022.

[4] L. Lázaro-Elorriaga, D. Guerra, I. García-Pastor, C. Martínez, E. Sanchez, E. Perea, Comprehensive analysis of smart grids functionalities virtualization, Sustain. Energy Grids Netw. (2024) 101507, ISSN 2352-4677, https://doi.org/10.1016/j.segan.2024.101507, https://www.sciencedirect.com/science/article/pii/S2352467724002364.

[5] J.A.L. Vilaplana, N. Kabbara, T. Coste, H. Morais, H. Zerriffi, M. Gibescu, Virtualized protection, automation, and control in electrical substations: an open-source dynamic cost-benefit assessment model, IEEE Access 12 (2024) 107488–107504, https://doi.org/10.1109/ACCESS.2024.3435972.

[6] W. Huang, Learn IEC 61850 configuration in 30 minutes, in: 2018 71st Annual Conference for Protective Relay Engineers (CPRE), IEEE. College Station, TX, March 2018, pp. 1–5, ISBN 978-1-5386-6127-7, https://doi.org/10.1109/CPRE.2018.8349803, https://ieeexplore.ieee.org/document/8349803/.

[7] G. Kulathu, J. Starck, Hybrid protection and control system for distribution substations in power utilities, industries and infrastructure, in: 2018 20th National Power Systems Conference (NPSC), IEEE, 2018, pp. 1–6.

[8] Cigre Study Committee B5.77, Requirements for Information Technologies (IT) and Operational Technology (OT) Managed of Protection, Automation, and Control Systems (PACS), 2026.

[9] A.R. Haron, A. Mohamed, H. Shareef, Coordination of overcurrent, directional and differential relays for the protection of microgrid system, Procedia Technol. 11 (2013) 366–373, ISSN 2212-0173, https://doi.org/10.1016/j.protcy.2013.12.204, https://www.sciencedirect.com/science/article/pii/S2212017313003587, 4th International Conference on Electrical Engineering and Informatics, ICEEI 2013.

[10] R.J. Best, D.J. Morrow, P.A. Crossley, Communication assisted protection selectivity for reconfigurable and islanded power networks, in: 2009 44th International Universities Power Engineering Conference (UPEC), IEEE, 2009, pp. 1–5.

[11] Defense Use Case, Analysis of the cyber attack on the Ukrainian power grid, Electricity Information Sharing and Analysis Center (E-ISAC) 388 (1–29) (2016) 3.

[12] P. Kozak, I. Klaban, T. Šlajs, Industroyer cyber-attacks on Ukraine's critical infrastructure, in: 2023 International Conference on Military Technologies (ICMT), IEEE, 2023, pp. 1–6.

[13] ZD NET, UK Electricity Middleman Hit by Cyber-Attack, 2020, https://www.zdnet.com/article/uk-electricity-middleman-hit-by-cyber-attack/ (Accessed: 2024-07-31).

[14] J. Gaspar, T. Cruz, C.-T. Lam, P. Simões, Smart substation communications and cybersecurity: a comprehensive survey, IEEE Commun. Surv. Tutor. 25 (4) (2023) 2456–2493, https://doi.org/10.1109/COMST.2023.3305468.

[15] D. Agnew, S. Boamah, A. Bretas, J. McNair, Network security challenges and countermeasures for software-defined smart grids: a survey, Preprints (March 2024), https://doi.org/10.20944/preprints202403.1701.v1.

[16] S. Abdelkader, J. Amissah, S. Kinga, G. Mugerwa, E. Emmanuel, D.-E.A. Mansour, M. Bajaj, V. Blazek, L. Prokop, Securing modern power systems: implementing comprehensive strategies to enhance resilience and reliability against cyber-attacks, Results Eng. 23 (2024) 102647 ISSN 2590-1230, https://doi.org/10.1016/j.rineng.2024.102647, https://www.sciencedirect.com/science/article/pii/S2590123024009022.

[17] V.S. Rajkumar, M. Tealane, A. Ştefanov, P. Palensky, Cyber attacks on protective relays in digital substations and impact analysis, in: 2020 8th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems, 2020, pp. 1–6, https://doi.org/10.1109/MSCPES49613.2020.9133698.

[18] V.S. Rajkumar, M. Tealane, A. Ştefanov, A. Presekal, P. Palensky, Cyber attacks on power system automation and protection and impact analysis, in: 2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe), IEEE, 2020, pp. 247–254.

[19] S. Hussain, S. Hussain, M. Hemmati, A. Iqbal, R. Alammari, S. Zanero, E. Ragaini, G. Gruosso, A novel hybrid cybersecurity scheme against false data injection attacks in automated power systems, Prot. Control Mod. Power Syst. 8 (2023) 08, https://doi.org/10.1186/s41601-023-00312-y.

[20] M.M. Roomi, S.S. Hussain, D. Mashima, E.-C. Chang, T.S. Ustun, Analysis of false data injection attacks against automated control for parallel generators in IEC 61850-based smart grid systems, IEEE Syst. J. 17 (3) (2023) 4603–4614.

[21] M. Teresa Villén Martinez, M.P. Comech, A.A.P. Hurtado, M.A. Olivan, D.L. Corton, C.R.D. Castillo, Software-defined analog processing based on IEC 61850 implemented in an edge hardware platform to be used in digital substations, IEEE Access (2024).

[22] A.T.-R. Oscar, A.-R.-R. Omar, G.D. Rueda-Carvajal, A. Leal-Piedrahita, F.B.-V. Juan, A.G.-B. Sergio, W.-B.-B. John, G.D. Zapata-Madrigal, Goose secure: a comprehensive dataset for in-depth analysis of goose spoofing attacks in digital substations, Energies 17 (23) (2024). ISSN 1996-1073, https://doi.org/10.3390/en17236098, https://www.mdpi.com/1996-1073/17/23/6098.

[23] S. Zemanek, I. Hacker, K. Wolsing, E. Wagner, M. Henze, M. Serror, PowerDuck: a GOOSE data set of cyberattacks in substations, in: Proceedings of the 15th Workshop on Cyber Security Experimentation and Test, ACM, Virtual CA USA, August 2022, pp. 49–53, ISBN 978-1-4503-9684-4, https://doi.org/10.1145/3546096.3546102, https://dl.acm.org/doi/10.1145/3546096.3546102.

[24] M. Hasan, A. Kashinath, C.-Y. Chen, S. Mohan, SoK: security in real-time systems, ACM Comput. Surv. 56 (9) (Apr 2024), ISSN 0360-0300, https://doi.org/10.1145/3649499.

[25] M. Hasan, S. Mohan, R. Pellizzoni, R.B. Bobba, Contego: an adaptive framework for integrating security tasks in real-time systems, 2017, CoRR arXiv:1705.00138.

[26] S. Singh, A systematic review on security aware real-time task scheduling, Sustain. Comput. Inf. Syst. 38 (2023) 100872, ISSN 2210-5379, https://doi.org/10.1016/j.suscom.2023.100872, https://www.sciencedirect.com/science/article/pii/S2210537923000276.

[27] S. Banik, T. Banik, S. Banik, Using virtual environment to analyze cyber-attacks on smart grid protocol, Preprints (September 2023) https://doi.org/10.20944/preprints202309.0984.v1.

[28] P.P. Biswas, H.C. Tan, Q. Zhu, L. Yuan, D. Mashima, B. Chen, A synthesized dataset for cybersecurity study of IEC 61850 based substation, in: 2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), IEEE, Beijing, China, October 2019, pp. 1–7, ISBN 978-1-5386-8099-5, https://doi.org/10.1109/SmartGridComm.2019.8909783, https://ieeexplore.ieee.org/document/8909783/.

[29] International Electrotechnical Commission, IEC 61850-4: 2011 communication networks and systems for power utility automation - part 4: system and project management, 2011, https://webstore.iec.ch/publication/6011 (Accessed: 2024-10-21).

[30] R.E. Mackiewicz, Overview of IEC 61850 and benefits, in: 2006 IEEE Power Engineering Society General Meeting, IEEE, 2006, pp. 8.

[31] R. Hat, What is virtualization? 2024, https://www.redhat.com/fr/topics/virtualization/what-is-virtualization (Accessed: 2024-10-21).

[32] H.F. Gary, Power system selectivity: the basics of protective coordination, 2010, https://api.semanticscholar.org/CorpusID:115016687.

[33] J. Robert, D.J.M. Best, A.C. Peter, Communication assisted protection selectivity for reconfigurable and islanded power networks, in: 2009 44th International Universities Power Engineering Conference (UPEC), 2009, pp. 1–5.

[34] J.L. Blackburn, T.J. Domin, Protective Relaying: Principles and Applications, CRC Press, 2006.

[35] P. Barham, B. Dragovic, K. Fraser, S. Hand, T. Harris, H. Alex, R. Neugebauer, I. Pratt, A. Warfield, Xen and the art of virtualization, ACM SIGOPS Oper. Syst. Rev. 37 (5) (2003) 164–177, https://doi.org/10.1145/945445.945462, https://dl.acm.org/doi/10.1145/945445.945462.

[36] RTDS Technologies, Rscad® fx: all-in-one real-time simulation software, 2024. https://www.rtds.com/technology/graphical-user-interface/ (Accessed: 2024-10-21).

[37] MZ Automation, libiec61850, 2024. https://github.com/mz-automation/libiec61850 (Accessed: 2024-10-22).

[38] Robidev, IEC61850_open_server: an open source implementation of an IEC61850 ied using lib61850, 2025, https://github.com/robidev/iec61850_open_server (Accessed: 2025-05-20).

[39] National Institute of Standards and Technology, CVE-2023-28766 detail, 2023, https://nvd.nist.gov/vuln/detail/CVE-2023-28766 (Accessed: 2024-07-31).

[40] National Institute of Standards and Technology, CVE-2017-8779 detail, 2017, https://nvd.nist.gov/vuln/detail/CVE-2017-8779 (Accessed: 2024-07-31).

[41] Blue Goat Cyber, Understanding VM escape: a threat to virtualized environments, 2024, https://bluegoatcyber.com/blog/understanding-vm-escape-a-threat-to-virtualized-environments/ (Accessed: 2024-07-31).

[42] H. Abusaimeh, Virtual machine escape in cloud computing services, Int. J. Adv. Comput. Sci. Appl. 11 (7) (2020).

[43] Z. Aalam, V. Kumar, S. Gour, A review paper on hypervisor and virtual machine security, J. Phys. Conf. Ser. 1950 (1) (Aug 2021) 012027, https://doi.org/10.1088/1742-6596/1950/1/012027, https://dx.doi.org/10.1088/1742-6596/1950/1/012027.

[44] R. Shea, J. Liu, Performance of virtual machines under networked denial of service attacks: experiments and analysis, IEEE Syst. J. 7 (2) (2013) 335–345, https://doi.org/10.1109/JSYST.2012.2221998.

[45] T. Zhang, Y. Zhang, R.B. Lee, DoS attacks on your memory in cloud, in: Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, ASIA CCS '17, Association for Computing Machinery, New York, NY, USA, 2017, pp. 253–265, ISBN 9781450349444, https://doi.org/10.1145/3052973.3052978.

[46] A. Bonguet, M. Bellaiche, A survey of denial-of-service and distributed denial of service attacks and defenses in cloud computing, Future Internet 9 (3) (2017), ISSN 1999-5903, https://doi.org/10.3390/fi9030043, https://www.mdpi.com/1999-5903/9/3/43.

[47] A. Choudhary, M. Govil, G. Singh, et al. A critical survey of live virtual machine migration techniques, J. Cloud. Comput. (Heidelb). 6 (23) (2017) https://doi.org/10.1186/s13677-017-0092-1.

[48] National Institute of Standards and Technology, CVE-2022-31705 detail, 2022. https://nvd.nist.gov/vuln/detail/CVE-2022-31705 (Accessed: 2024-07-31).

[49] National Institute of Standards and Technology, CVE-2024-22273 detail, 2024, https://nvd.nist.gov/vuln/detail/CVE-2024-22273 (Accessed: 2024-07-31).

[50] I. Semertzis, V.S. Rajkumar, A. Stefanov, F. Fransen, P. Palensky, Quantitative risk assessment of cyber attacks on cyber-physical systems using attack graphs, in: 2022 10th Workshop on Modelling and Simulation of Cyber-Physical Energy Systems (MSCPES), IEEE, Milan, Italy, May 2022, pp. 1–6, ISBN 978-1-66546-865-7, https://doi.org/10.1109/MSCPES55116.2022.9770140, https://ieeexplore.ieee.org/document/9770140/.

[51] S. Madabhushi, R. Dewri, A survey of anomaly detection methods for power grids, Int. J. Inf. Secur. 22 (2023) 1799–1832, https://doi.org/10.1007/s10207-023-00720-z.

[52] Wireshark Foundation, Wireshark, 2024, https://www.wireshark.org/ (Accessed: 2024-10-22).

[53] G. Lyon, Nmap: network mapper, 2024, https://nmap.org/ (Accessed: 2024-10-22).

[54] H. Teryak, A. Albaseer, M. Abdallah, S. Al-Kuwari, M. Qaraqe, Double-edged defense: Thwarting cyber attacks and adversarial machine learning in IEC 60870-5-104 smart grids, IEEE Open J. Ind. Electron. Soc. 4 (2023) 629–642, https://doi.org/10.1109/OJIES.2023.3336234.

[55] E. Krishna, S. Ethala, M. Karthik, Managing DDoS attacks on virtual machines by segregated policy management managing DDoS attacks on virtual machines by segregated policy management, 2014 Jan.