SYED AMMAR HASAN NAQVI

ML Based Anomaly Detection in VSC

Supervised Machine Learning Based Anomaly Detection in Voltage Source Grid Converter

School of Technology and Innovation,
Master's Programme in Smart Energy

Vaasa 2025

UNIVERSITY OF VAASA
School of Technology and Innovation
Author: SYED AMMAR HASAN NAQVI
Title of the thesis: ML Based Anomaly Detection in VSC: Supervised Machine Learning Based Anomaly Detection in Voltage Source Grid Converter
Degree: Master of Science in Technology
Degree Programme: Master's Programme in Smart Energy
Supervisor: Mazaher Karimi
Year: 2026 **Pages:** 71

ABSTRACT:

The pressing need of securing smart grids against silent intrusions requires the implementation of cyber security at modular level. However, using classical rule base intrusion detection system can be less effective as compared to the system which can detect the intrusion based on the behavioural changes of device under consideration and can keep providing protection even if the device is installed in a different plant. In this regards use of machine learning for pattern tracking and understanding the routine operational variables of a voltage source converter by linking its parameter to the physical response of VSC installed in a plant is studied in this thesis. The thesis does not investigate how the intrusion is made, rather it focuses on finding the link between the tampering in operating electrical quantities and changes in response of converter thereby exposing the subtle actions taken after undetected intruder attempt to manipulate the converter outputs.

To build a foundational level understanding this thesis first focuses on literature review that discuss the in-depth working and control of voltage source converter. This review shed light on electrical response characteristics of voltage source converter and define how the manipulation of basic electrical quantities i.e. DC-link voltage/current, grid frequency and voltage/current can be reflected by the analysis of VSC advance electrical features. The later sections of literature review also discuss the techniques of feature extraction for use by ML classifiers, construction of optimized data sets, approaches used to clean and normalize data, followed by theoretical reflection of the types of classifiers used in study namely Random Forest method and Support Vector Machine.

After the literature review the knowledge is applied on an actual setup consisting of commercially available controller, and a plant emulated by Hardware in Loop device. For emulating intrusion multiple scenario files are created through MATLAB script, having time stamped signals which are feed to the setup through a robot framework pipeline. The same robot framework is used to perform test repetitively on the setup and simultaneously recording the outputs for analysis by the RF and SVM classifiers scripts. Lastly the results are analysed and presented though confusion matrix with metrics like F1 score and recall score, that help to gauge the performance of both classifiers based on speed, and accuracy.

This thesis provide novelty by establishing simple and iterative workflow which can be further optimized to be adopted in actual site operation for achieving an extra layer of safety in a VSC operating in smart grid. The utilization of RF and SVM classifiers for analysing data yielded by emulation of actual hardware also showcase the constraints that are not directly related to concurrent ML technology but can prove to be the limitations for adoption of discussed study in real time system and are discussed accordingly in the implementation section. Finally, this thesis is concluded by reporting the advantages of SVM over RF observed through the set performance indicators and some areas where RF classifier outperforms the SVM ML model outputs.

KEYWORDS: Voltage Source Converter, Support Vector Machine, Random Forest, False Data Injection, Denial of Service, Phase Lock Loop, Hardware in loop, cyber-physical intrusion, Droop mode of VSC, Harmonics

Contents

Figures

Tables

Abbreviations

AC	Alternating Current
AI	Artificial Intelligence
DC	Direct Current
DoS	Denial of Service
Dq	Direct – Quadrature Axis
FDI	False Data Injection
GF	Grid Forming
HIL	Hardware In Loop
IDS	Intrusion Detection System
LSTM	Long Short -Term Memory
ML	Machine Learning
PCC	Point of Common Coupling
PLL	Phase Lock Loop
RF	Random Forest
SRF	Synchronous Rotating Frame
SVM	Support Vector Machine
THD	Total Harmonic Distortion
VSC	Voltage Source Converter

.

1 Introduction

During recent years, an increased penetration of renewable energy sources in the power system has expanded the role of power electronics in modern grid infrastructure. Although this trend was initially driven by concerns towards environmental issues, but now it is reinforced by geopolitical interests that strongly demands the need of energy security in smart grids. One of the most critical component in smart grid is Voltage Source Converter (VSC) as it is responsible for the conversion of power into required form, thereby regulating desired amount of power flow between varying load and source; therefore like any other indispensable equipment of constantly developing industry the VSC have been evolving with time to incorporate features like drive to drive communication, parallel operation, remote support and on fly configurational changes capabilities. Although these features enhance the overall capability of smart grid by flexibly conducting grid operations via real time system supervision and configuration on the fly, but an underexplored opportunity also lies in leveraging the same data to detect cyber intrusion – thus, using existing monitoring infrastructure to create additional layer of security, by constantly learning the operation of device on site and then detecting anomaly.

Furthermore, owing to the decentralized environment of a microgrid which tends to have distinct communication protocols, operational hierarchy and hardware implementation makes it complex to guarantee the susceptibility against intrusion recognition by just designing an Intrusion Detection System (IDS) using a rule based method. Thus, a practical approach to achieve a more secured system is to have an adaptive learning algorithm imbedded inside the VSC that apart from traditional cyber security system learn the routine and fault behaviour of the converter in the given microgrid architecture. Such algorithm can easily model the dynamic behaviour of the plant and DUT, which could then be translated into secure boundaries encircling the consistent electrical and physical response of converter under normal as well as fault conditions separately. An efficient tool in marginalizing the cyber threats by creating such adaptive boundaries is Machine Learning, which have the capacity to assess the

nonlinear patterns between VSC signals like THD, PLL Drift, frequency and voltage to autonomously raise a flag if some suspicious activity is observed in the system.

Therefore, this thesis will provide a review about the gaps in existing literature regarding the possible implementation of Machine Learning Algorithms in assisting the IDS that are available in market to find the best working model and then do a small test to check the working of such model.

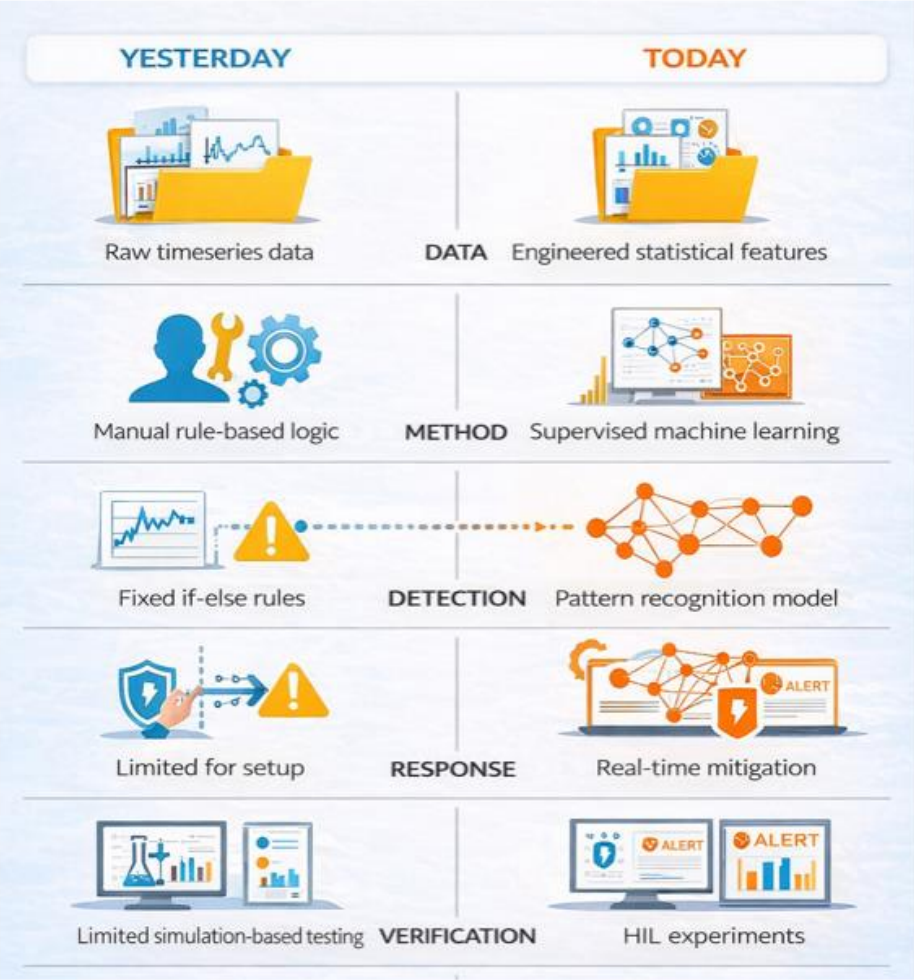

Figure 1. ML based IDS, (Generated by AI Tool Open AI Chat GPT)

1.1 Background and Research Motivation

In last decade investments in clean energy segments has surged nearly 10 times rising from USD 0.27 trillion to USD 3.4 trillion that drive a paradigm change of traditional power infrastructure from centralized to distributed generation and transmission

(REN21, 2015, slide 6; International Energy Agency [IEA],2025). As per IEA 2023 highlights this shift is primarily based on advances in power electronic, specially VSC being a key element in integration of renewable energy in microgrids, HVDC transmission and smart energy trading (International Energy Agency 2023, pg.18.). This means that the role of these converters is not only limited to DC-AC or AC-DC conversion, rather they are now enabling participation of renewables in voltage stabilization, dynamic support via fault ride through and other grid support functions by controlling flow of reactive power. The Ember's Global Electricity Review 2025 states that renewable sources generated 858 TWh electricity to aid 1,172 TWh total increase in electricity as of 2024. Furthermore, the participation by solar energy has increased by 29% as compared to 2023 thus providing total of 40% share in increase of renewable generation, while wind energy share addition of 7.9% (Graham et al., 2025, pp. 9-11).

However, integration of renewable energy sources through smart equipment like VSC for advance grid support brings new challenges for engineers pertaining to security and stability. A simple use case can be destabilisation of VSC control loops by false data injection, as with enhancement of technology the control loops are now not restricted to electrical regulations only - rather they expand to system level coordination and customizations through cascaded control (Sahoo et al., 2021, pp.5327-5329). A possible approach of dealing with such security related obstacles is to implement adaptive learning, therefore understanding system specific behaviour of VSC and then to predict intended anomaly in converter to detect intrusion (Sadi et al., 2023).

1.2 Problem Statement and Scope of Thesis

This thesis serves the purpose of researching the literature that discuss possibility of using converter core signals i.e. voltage, current and frequency for anomaly detection using supervised machine learning models. These models will be trained on processed electrical signals like Total Harmonic Distortion, PLL drift and di/dt as they provide a clear distinction between normal, fault and intruded state of VSC. The scope of this thesis will be to find the research gap in existing literature based on their research methodology, models of supervised ML used and scenario in which VSC data is extracted. This thesis is

aimed to yield the best ML model that can be provide accuracy, efficiency and simplicity. The scope of this thesis is limited to operationality of voltage source converter and selection of machine learning models, however the cybersecurity methods and rule base intrusion detection methodology for anomaly detection is out of scope of this thesis.

1.3 Research Gap

The current developments in the field of power conversion drives that utilizes machine learning for cyber security support is primarily performed on simulation level (Parvizi et al., 2025, p. 19). Furthermore, utilization of standard linear models does not provide ample information to understand complex VSC behaviours that usually involves frequency coupling, DC-link stability, and decoupled harmonics. These behaviours are paramount to study because converters actually exhibit them in the field when multiple converters are interacted together to perform a large-scale operation (Cai et al., 2024, p. 8646). In such situations the behaviour of VSC for faults like voltage sags, IGBT switching anomalies or DC link unbalancing cannot be captured truly using linear time invariant models. Thus, utilization of real hardware to understand coupled harmonic responses, control parameterization for precise operation for acute frequency and voltage generation has to be understand completely before implying ML models for intrusion detection in real VSC dominated grids.

Moreover, the architecture of a VSC controller is designed in such a way that it will be completely depending on its high sampling rate sensor feedback as baseline to synthesis correct references based on control mode along with filtering of basic current and voltage harmonics (Beikbabaei et al., 2025, p. 14). The studies conducted by Khaleghi et al. (2025, pp. 2–4) interprets that mitigation of harmonics, power quality requirements, and dynamic support during fault in VSC dominated smart grid is performed at individual level of converters, thus each converter is unaware of the system level impact in case of minor drifting at its terminal level, but the outputs it synthesized can sabotage the grid system without being detected at system level. Whereas most of the cyber intrusion detection systems are implemented at system level and does not consider the vulnerabilities hiding at control level of VSC e.g. checking of FDI at converter control

communication level. Therefore, this structural gap between the commercial level control strategy of VSC and short comings of using IDS at plant level can be exploited by intruders to perform silently enter the system for malicious activities.

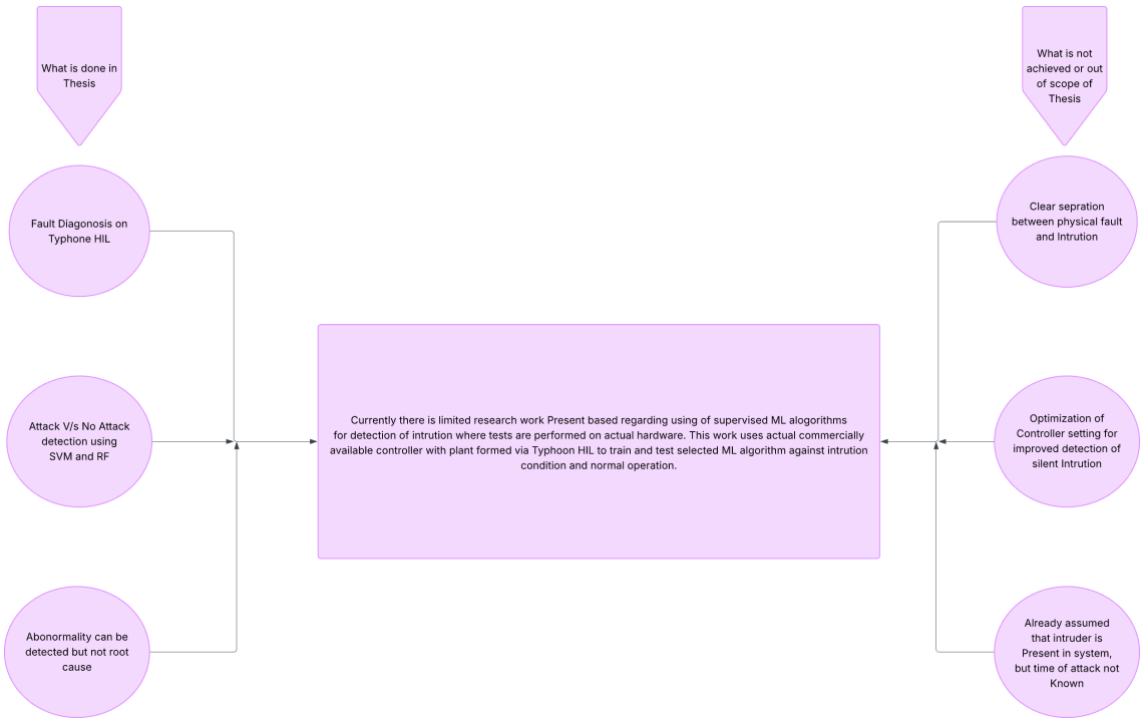

Figure 2. Research gap overview (generated with Lucid web application)

This background highlight the need of using actual VSC converter hardware that is equipped with an efficient, accurate, light weighted supervised ML based ID model which can map the operational behaviour of the VSC on which its planted, thereby providing it the intelligence to detect an intrusion at modular level by observing behavioural changes in DC-link quantities, PLL variables and harmonics. This thesis will position its contribution by conducting the research on actual hardware generated data after developing a thorough understanding of its behaviour and by evaluating the performances of Random Forest Method and Support Vector Machine on this hardware under different attack scenarios.

In summary, this thesis will assist existing research by determining the efficiency of RF and SVM ML models in detection of intrusion using commercially available hardware.

1.4 Structure of Thesis

This document comprises of five sections, where first chapter familiarize the reader with requirement of ML in VSC to detect anomaly. The same chapter educate how much investment is being poured in renewable energy market based on 2025 reports to motivate the need of advance research in the field that can be shaped into commercial level projects. Finally, chapter 1 clearly state the scope and limitation of this work.

A detailed overview of the concepts and technical knowledge is shared in chapter 2. In these topics voltage source converter operationality brief overview, control level understanding of VSC, Supervised Machine Learning methods and model training methods will be discussed. The following chapter 3 will be focused on research methodology, where simulations, feature extraction, model comparison and result assessment will be discussed. The final chapter 4 then provide the conclusion based on research gap found through hardware base implementation and future recommendation.

2 Literature Review

The previous section showcases that how the protection of Voltage Source Converter against critical cyber threats has become the focus of new industrial development, where the traditional threshold based and rule-based protection is not sufficient to protect power system against evolving cyber threats. Modern studies highlight that measurement streams used in smart grid converters are much more susceptible to the cyber threats. This means that PLL signals, dq-frame voltages and currents, switching states, or reactive power commands are like primary entrance points for attackers since the high frequency telemetry use for the discussed purpose is solely dependent on communication network. It is quite possible for attackers to use subtle and time dependent anomalies which are very difficult to differentiate from normal disturbances.

The work of Sadi et al. (2023, p. 4) has shown that how time sequence ML models are proved to be effective in identifying such attacks because these models capture the temporal behaviour of inverter and then identifies the attacks like slow drift, false data injection, and coordinated manipulation, these attacks are usually missed by classical relays. Further conventional cyber security mechanism operates on static rules; however, the cyber attackers study the system and then launch the model aware attacks which distort the behaviour without crossing the threshold value of system. The same study shows that long-term short-term intrusion detection model detects the micro level variation in the system and with high accuracy identifies the intrusion in the system. Therefore, recent research consensus concludes that data driven, machine learning based intrusion detection make the classical protection system fail especially for facilities having outdated systems, low latency networks and measuring tools with high level of noise or poor calibration.

2.1 Voltage Source Converter: Physical Fault versus Intrusion based Faults

In simple words a voltage source converter is a set of controlled switches (Thyristors or IGBTs) that are operating at a specified switching frequency to generate AC voltage of

desired magnitude and frequency using the DC energy source or vice versa. Now there exist multiple operation topologies involving operating of a VSC at referenced current or power level, but at application level it can be exemplified as a control valve that routes the electrical power flow from AC to DC or opposite using the buffer of available energy.

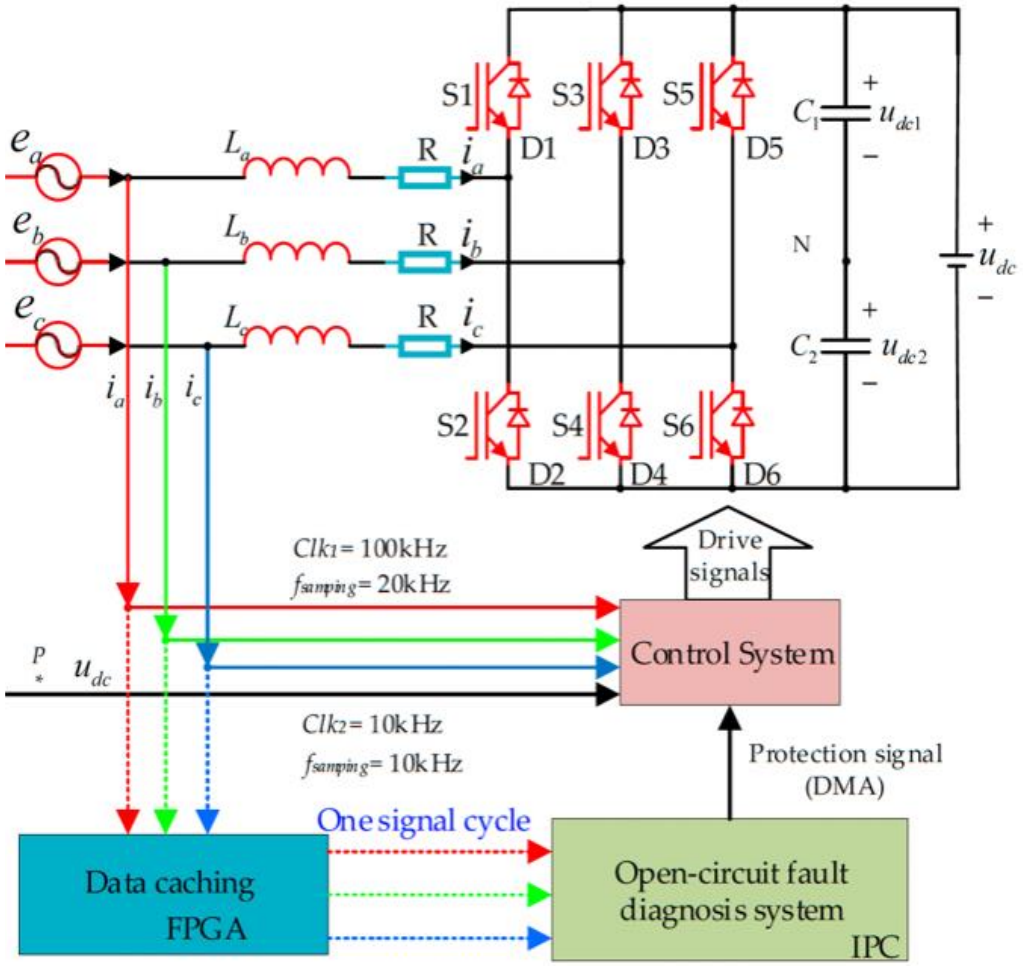

Figure 3. Control System of three phase VSC, Qiu et al., 2022, p. 4

The basic working phenomena of a VSC is based on controlling the switching of connected IGBTs in a coordinated way such that DC voltage can be made to oscillate between zero voltage and actual DC voltage along with alternation of polarities. The duration of this switching is defined as **Duty Cycle**, and it plays role in setting up the magnitude of voltage during the switching instant, whereas the final desired voltage level can be calculated by **Modulation Index**. To simplify these phenomena, assume a system having 1075 volts DC link, targeted to have grid side connected with 690 volts AC.

In this case modulation index of 0.907 shows that the amplitude of AC is 90% of the relative DC voltage. Mathematically,

$$Modulation\ Index = \frac{\sqrt{2}\ \times 690\ V_{AC}}{1075\ V_{dc}} \qquad (1)$$

So, we are generating 690 volts AC (which is 90% of 760 Volt AC) from 1075 Volts DC. The modulation index gives us the information about the available headroom after the conversion from DC/AC or AC/DC. The only thing needed to be taken care of during parameterization is that drive cannot have modulation index greater than 1, which mean the power conversion from AC to DC using 690 Volts cannot yield DC smaller then 975 Volts by just using switching, because the IGBT will saturate. Similarly, if DC/AC conversion is done using 1075 volts DC then AC voltage greater than 760 volts is not possible to generate as switches will have saturation.

The **Switching Frequency** is another parameter that defines the number of times switching device will be operated i.e. it shows how many switching operations are performed per fundamental frequency of power signal. For example, in above example the modulator switching frequency can be 8 KHz i.e. it will help to perform the switching operation 160 times for a 50 Hz power signal. Putting things simply, if same VSC have a sine wave of function V = Vmax * Sin(2*pi*F*t) where t is the ever increasing time but due to rotational nature of sine wave "F" - the function's instantaneous value increase and decrease in a defined range. So, in every 0.2 sec (50 Hz) magnitude of sine wave "V" oscillate in-between -975 to +975. If this 0.2 sec long single wave of voltage is created by a constant 975 volts DC through switching device that is operating at rate of 125 uSec (8 KHz), then we will be operating the switching device at 160 different voltage level of the sine wave. i.e.

$$\frac{Carrier\ Wave\ Frequency}{Power\ Wave\ Frequency} = \frac{8000\ Hz}{50\ Hz} = 160 \qquad (2)$$

2.1.1 DC-link Bus of VSC

One of the most important hardware that serve as a stable buffer for the transfer of energy across the voltage source converter is DC-link bus. At system level it behaves as an interconnection between inverter stage and rectification stage so that different elements of the system can be easily decoupled without affecting the operation of the system or grid. The working principal of DC-link bus is hugely dependent on DC-link capacitor which being an active element maintains a smooth DC voltage supply as its connected in parallel configuration with the switching assembly of inverter, therefore assist the flow of electrical power between AC and DC by damping the small variation in DC link voltage, thus regulating the smooth operation of converter in different operating modes. (Rodríguez et al., 2007, pp. 2930-2931).

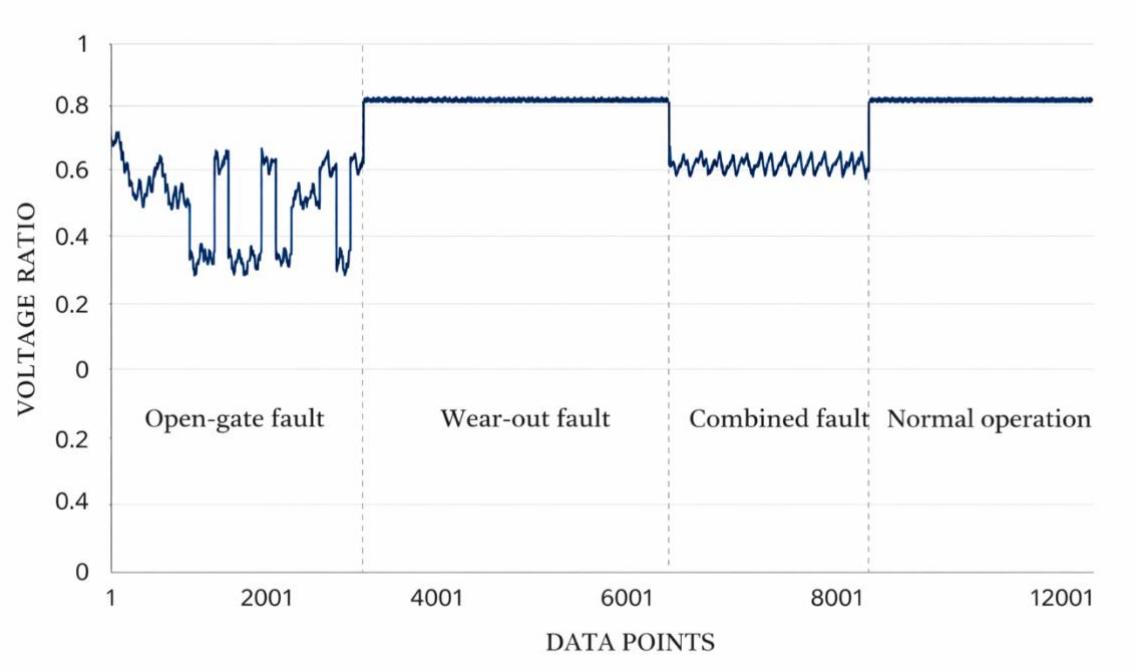

Figure 4. Voltage ratio v/s type of faults, Debnath et al., 2025, p. 174215. The picture is improved by AI using prompt "Improve the picture"

In most industrial applications the DC-link of the VSC is required to be a stable against minor fluctuation thus DC-link should remain stiff against minor power variations. This implies due to the fact that any deviation of DC-link voltage from the base values will largely impact the current controller performance and tunning done for AC voltage

generation. This is very critical during grid code compliance testing as even small volatility in DC-link can compromise the stability of whole system by creating huge harmonics and ripples during the inverter action the VSC (Du et al., 2018, p. 547).

Mathematically the amount of energy being handled by DC-link is the quadratic product of its voltage and the size of capacitor. The energy stored in the capacitor is given as,

$$E_{dc} = \frac{1}{2} \times C_{dc} \times V_{dc}^2 \quad (3)$$

Here the DC-link voltage variation will impact quadratically to the energy being transferred across the VSC, this mean that strict voltage regulation should be in place for ensuring the current controller operation and even a small DC-link voltage delta can result in tripping of system as the fine-tuned KP and KI DC-link voltage gains can generate current which if increase on sharp ramp can cause false tripping. This happen because during inverter operation the DC-link voltage is used to synthesize right amount of active power by regulating d-axis current reference. Similarly, during the active front end operation when the target is to form DC-link voltage the control is being implemented by regulating flow of active power through control of d-axis current reference (Huang et al., 2016, pp. 446-447). This dependency of DC-link voltage on power balance between AC and DC can be further explained mathematically based on power balance perspective given as,

$$C_{dc} \times V_{dc} \frac{dV_{dc}}{dt} = P_{in} - P_{out} \quad (4)$$

As discussed previously the integration of VSC in a weak grid that have very low level of short Circuit ratio demand interaction between DC-link with AC control, PLL dynamics and current control, this interaction can easily bring high level of oscillation of low frequency components that's why the DC-link cannot be studied in isolation. Furthermore, the DC-link voltage control strategy can translate into effective negative resistance at the point of common coupling of inverter.

This relation can be further explored by interpretation of impedance circuit modeling where each control loop of VSC is realized as active circuit element and connected

together to emulate the electrical elements of VSC, theses controls are then observed under different setpoints when grid is disturbed. So, when current controller is emulated as resistor, PLL like a frequency dependent impedance then DC-link control can be analyzed like a voltage single impedance in parallel with voltage source. This technique provide leverage to observe DC link instability in similar way how resonance of a RLC circuit is calculated. Thus, all possible behaviors of the DC link can be visualized to see possible points of disability by a system (Wang et al., 2025, pp. 2971) .

2.1.2 Switching Methodologies and Control of VSC

In any Voltage Source Converter the implementation of correct control strategy is a crucial scheme as it defines the performance by producing current output signals based on correct level of filter values thus supporting stability , efficiency of a converter in define range of modulation index. For industrial practices the most commonly employed strategy for VSC is Sinusoidal Pulse Width Modulation (SPWM) and Space Vector Pulse Width Modulation (SVPWM) specifically for application like renewable energy interfacing, battery energy storage system (BESS), active power filtering, microgrid formation specially in grid following mode (Wu et al., 2022, pp. 7253-7255).

The purpose behind selection of correct switching methodology is optimize the operation of IGBT or MOSFET in such a way that the desired level of grid side voltage or DC-link side voltage can be generated without compromising on switching losses, higher frequency distortion and creating a high level stress on filters due to these frequency distortion due to this reason the it is a common understanding to score both switching methodology and control strategy as a same optimization parameter.

When the industrial applications are considered and as discussed in detail the research of (Wu et al, 2022) it is observed that SPWM is used to calculate the correct switching state at given instant so that RMS value of instantaneous output voltage is in accordance with the given grid voltage reference with filter losses compensated. To perform such operation the power signal is compared with very high frequency triangular carrier

waves as defined in equation 2, therefore the output voltage can be calculated by equation 5,

$$V_{Input} \times duty\ Cycle = V_{out} \quad (5)$$

The operation can be easily implemented digitally in the converter using firmware level coding, off course some other variables will also be used to take dead time into account so there is no case of short circuit, but this feature makes SPWM most adoptable control strategy in industry. However, as seen from the Equation 2 and 5 the factor of carrier frequency can highly impact the operation and produce switching harmonics consequently leading to high DC-link current ripples. This issue has direct impact on sizing of DC-link capacitor as it will face large stress since the changes in spectral distribution require large sizing (Bierhoff & Fuchs, 2008, pp. 2086-2087).

In space vector modulation technique (SVPWM) the switching states are calculated by using alpha-beta plane references, then the correct switching signals are chosen based on sectors in which the voltage reference V_d is present. These signals for reference voltage are time weighted, means that angular position of space vector is controlled by switching time between basic vectors i.e. V1, V2, V3, V4, V5, V6, whereas the magnitude of space vector is controlled by switching between Null vectors i.e. V0 and V7. This relation can be easily explained by equation 6 give as,

$$V_{ref} \times T_s = V_1 \times T_1 + V_2 \times T_2 + V_0 \times T_0 \quad (6)$$

Here T_s is the complete switching period discussed previously, however the important point to note here is that by using SVPWM the converter can utilize maximum DC-link voltage to generate required Grid side voltage, while in case of SPWM only 85.5 % voltage of DC-link can be used for inversion process. Thus, SVPWM is very efficient as it provides high DC-link voltage head room and less harmonics due to faster change of state during null vectors as compared to SPWM making it more efficient (Jana & Biswas, 2015, p. 2378).

The mathematical relation between AC voltage synthesized from the DC-link voltage through a given switching technique are creating strong impact on stability of the converter, when considering synchronous reference frame of dq the relationship can be defined as,

$$v_d = Ri_d + L\frac{di_q}{dt} - (\omega \times L \times i_q) + v_{gd} \quad (7)$$

$$v_q = Ri_q + L\frac{di_d}{dt} + (\omega \times L \times i_d) + v_{gq} \quad (8)$$

Here the modulation process creates the v_d and v_q the relation between these two with the indices of d and q reflects the impact of switching on the AC-side filter and thus drive the harmonic behavior, flow of power and dynamics of current. Finally, from this mathematical equation it can be observed that digital computational delays can critically jeopardize the stability of VSC, and this can be unintentional fault if the VSC is connected to weak grid or can be result of intentional false data injection (Zhang et al., 2022).

When considering industrial application it should be noted that there are two level of controls that are implemented to make voltage source converter work in desired level the fastest loop is called the current control loop which is inner loop and is fastest as the reference is given in current form and the system just have to break it into d and q components using Clarks and Parks method after which the above explained methodology is implemented to generate the switching option. The inner loop is use for fast dynamic options like for using with current reference and fault ride through, it helps to provide over current protection. The other control loop is called outer loop and it is slower, this loop basically takes into account d and q voltage components and its use for slower task and involves references like P and Q reference as it will first be broken down into vd and vq and then from it the iq and id will be calculated and product of v and I will be used to calculate the power.

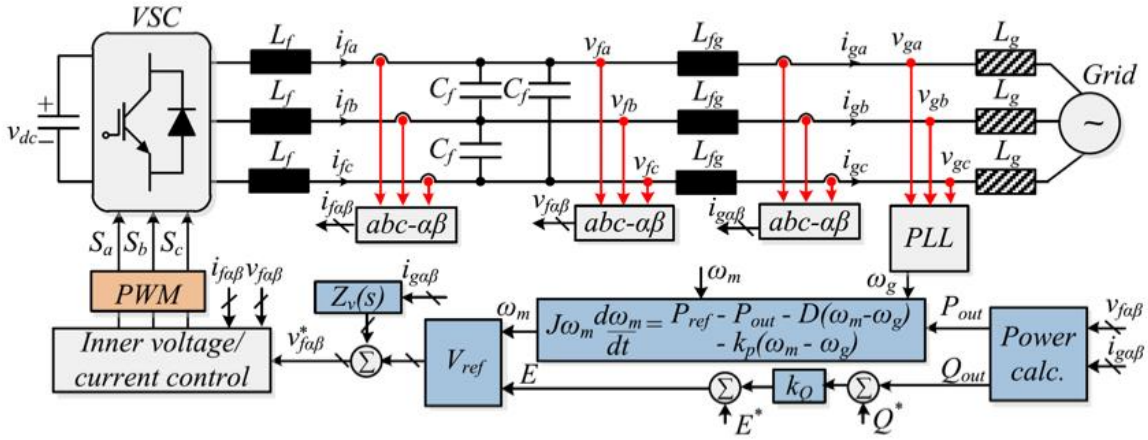

Figure 5. Voltage Source Converter Control loop, Sahoo et al., 2021, p. 5328

It should be noted that the inner control loop behave as a virtual impedance added to the system therefore it damp out the change in voltage causing change in reactive power but again if the switching frequency of the control system is made lower or there are large digital delays then the damping can become negative causing a small change of voltage to draw or inject large amount of reactive power in the system creating a loop to start and causing the VSC to trip during synchronization or it can initiate short term current injection in the system that can trip the inverter on over voltage fault. Therefore, this will be a false fault tripping which again can be caused by improper parameterization of the VSC virtual impedance parameter or by actual delay created in control system (Sun et al., 2011, pp. 1776-1777).

The research done by Raeispour et al. (2021) reflect that modern microgrid and industrial operations inherently require advance VSC in which multiple layers of control is implemented, this architecture require communication interfacing between multiple segments e.g. drive to drive or PLC to drive communication, thus introducing exposure points for potential cyber-attacks. These attacks can take shape of control destabilization, because to have stable modulation, the VSC needs feedback of concurrently generated voltage and current.

Furthermore, a reference is required to keep output at a specific point mostly this reference is provided via PLC using Modbus or ProfiNet or some other communication

protocol, these communication interfaces can be compromised as well and the intruder can quietly enter the system, later manipulating the feedback or reference to destabilize the system which on surface might appear as the power quality issue or control system malfunctioning.

2.1.3 Phase Lock Loop

When grid converters are operating in parallel with other units or with a stiff voltage source forming the AC side, they need to have same frequency and phase angle to operate synchronously. To achieve frequency and phase angle within acceptable range the VSC needs to lock its frequency and phase angle similar to the main source which form AC grid, this is done by the Phase Lock Loop (PLL) system. PLL consists of complex logic and hardware that serve to retain synchronization during modulation and thus maintain stable operation of voltage source converter during normal and transient operation (Teodorescu et al., 2011, p. 51).

Due to financial benefits and ease of implementation the technique uses to implement PLL in most of the marketed VSC is Synchronous Reference Frame PLL (SRF-PLL). it uses a phase detector component that tracks and align the instantaneous AC voltages to the reference voltage using the Parks transformation, in essence it checks by how much degree the calculated phase angle "Ø" is in error with respective grid phase by gauging magnitude of quadrature axis component. When the phase angle is locked between the grid and VSC, the grid voltage is aligned with direct component of phase lock loop SRF and v_q becomes zero. The output of phase detector is then feed to a PI controller that process the v_q error thereby synthesizing deviation in angler frequency required to be integrated by voltage controlled oscillator to achieve the required frequency.

Furthermore, depending upon the mode of operation of VSC the criticality of PLL can be distinguish. If the VSC is operating in grid following mode, then PLL is indeed very critical in maintaining synchronization with grid forming units as discussed above. In the preceding case the VSC is being use as controlled current device, this means that the system operator requires VSC to follow the given Active and Reactive current/ power

reference. Thus, an intentional alignment of d and q axis electrical quantities is required for having current/power control via decoupled current elements (Bahrani et al., 2013, p. 1357).

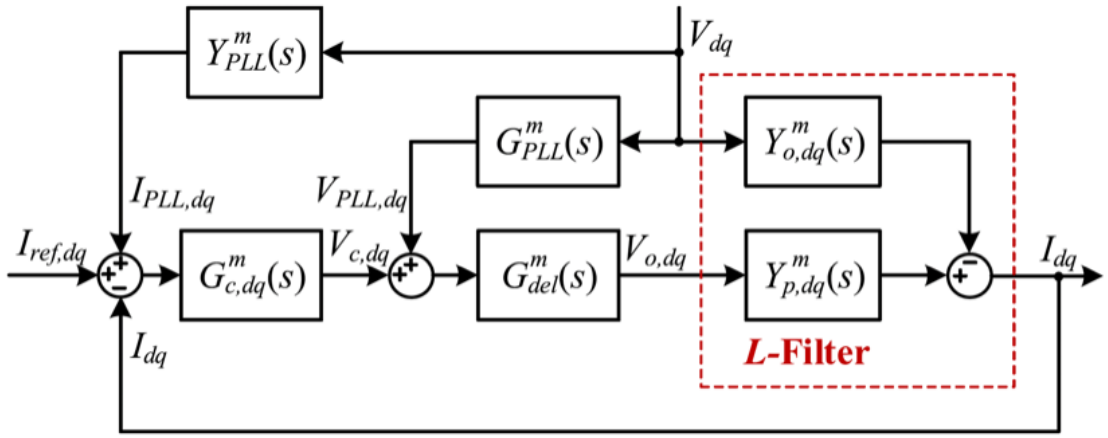

Figure 6. Block diagram of small signal dynamics of PLL, (Wang et al., 2018, p. 1778)

This alignment is achieved by calculating correct value of ø that is strongly linked to instantaneous values of phase angle and frequency, consequently the frequency synthesized by VSC via SRF-PLL is coupled with converter power quality and this close looping mechanism is a sensitive part that is responsible in preventing power oscillations or degraded current tracking. It's important to recall from previously established concepts in equation 6 and equation 7, that correct calculation of d and q elements is dependent on correctly evaluated "ω", given as,

$$\omega = 2\pi f \tag{9}$$

$$\Delta\omega = ({K_p}^{pll} \times v_q) + ({K_i}^{pll} \int v_q \, dt)$$

$$\emptyset = \omega_0 + \Delta\omega \tag{10}$$

On the other hand, when VSC converter is operating in grid forming mode it does not require fast SRF-PLL implementation as it is responsible to create its own frequency and voltage , rather droop control or synthetic inertia is required to maintain required supply of current (Zhong & Weiss, 2011, pp. 1262 - 1263).

The working of PLL highlight one big issue which can be exploited to have controlled attack on power system or digital grid. Since the synchronization process depends on PLL, which in turn depends on grid voltage feedback received either by internal voltage sensing hardware (commonly used hardware is Hall effect sensor), these sensors can be exploited by an intruder to create the instability by using man in middle or false data injection since these feedback are often received from external hardware through e.g. fieldbus can be used to provide external voltage feedback to have close loop control for synchronization as supported by Danfoss Drives IC7 series extended option board (Danfoss A/S, 2023). The fieldbus can be a hot spot for data spoofing in this case, because injecting a false data series through long time intruded can be a simple task using gaps in communication protocol. This pulse of injected data can break lock of PLL momentarily and create oscillation ultimately collapsing the system without leaving any hint of cyberattack.

A similar case study can be made from Stuxnet intrusion in Iran ICS network, where the intruder was hidden inside the system for months, the target was to slowly destroy the nuclear facility centrifuge by transmitting wrong parameters showing it as a hardware fault rather than cyber-attack, since the Iran information monitoring system does not detect breach due to lack of expertise in filtering digital intrusion, so the attackers successfully destroyed over thousands of centrifuge (Vanlyssel, 2024, p. 17). This case can be implemented in grid environment where the false data injection in context of frequency feedback to PLL can slowly drift the VSC out of PLL capturing range, thus causing loss of synchronization, large power swings, or power angle instability.

VSC can be vulnerable for intrusions that are difficult to detect because contemporary cyber intrusion detection systems are mostly related to software level monitoring and for legacy systems which have outdated hardware technology, can prove to be an easy access point for system level attacker who intent to cause slow damage.

2.1.4 Harmonic Behavior of VSC

In electrical network harmonics are like the additional sinusoidal sources that are existing the system and exist at the integer multiple of fundamental frequency. To put it simply if a 50 Hz power signal is supplied to a network where the load is nonlinear or the network impedance have high level of inductance or capacitance then the system will observe the development of alternative sources that have frequency equal to the integer multiple of 50 Hz. The development of these harmonics is damaging to the system as they introduce heating effects and degradation of the system current. In VSC the switching action of high power switches e.g. IGBT and Thyristor alongside connected inductors and capacitors cause the current source harmonic to develop (Abu-Rub et al., 2014, pp. 535-537). It's important to understand that harmonics are different from disturbances that are observed in transient state like faults and voltage sags, the harmonics do exist in steady state are more dependent on the source side impedance and the linearity of the load. Therefore, for weak grids the voltage source harmonics are high and for nonlinear load the current source harmonics are high.

The VSC of advance level are designed to suppress the harmonic disturbances in transient state, as well as in steady state. For example, the IC7 series grid converter application of Danfoss drives retain high quality of current even during fault ride through state when the dynamic support is being provided during the voltage sags. This means that it's the responsibility of a VSC to retain low value of Total Harmonic Distortion (THD) to a very low level during normal operation as well as during fault support state. THD is the ratio of RMS integral of voltage or current harmonics of all present integers of fundamental frequency and magnitude of fundamental frequency voltage or current respectively. Based on this conventional definition the Abdel Aleem et al. (2016, p. 65) provided the harmonic adjusted THD that reflects the dependency of these harmonics on frequency based impedances, which means that by observing harmonic adjusted THD the system can get insight of losses, thermal stresses and current derating in a better way, the mathematical relation is given as,

$$THD\ V_{HA} = \frac{\sqrt{\sum_{h>1}\left(K_h{}^{v} \times V_h{}^{2}\right)}}{V_1}$$

$$THD\ V_{HA} = \frac{V_H}{V_1} \quad (11)$$

As per IEEE-519 standard there are strict limits on allowed harmonic distortion at the point of common coupling (PCC). For low-voltage systems which means that AC side voltage is $\leqslant$1 kV, the IEEE-519-2014 imposes limits on both individual harmonic magnitudes and total demand distortion (TDD). For example, in such system the high order current harmonics must be smaller than 0.3% of the fundamental current, this shows the need to virtually eliminate high-frequency harmonics like 3rd, 5th and 7th order. Ensuring to maintain these limits is very difficult for converters under fluctuation or transient state, so VSC design engineers usually oversize filters or employ advanced modulation to keep harmonics in check, one of them is like switching between SVPWM and SPWM based on operation. Finally, minimizing harmonics is crucial for smooth current delivery necessary for grid code compliance, avoiding utility penalties, and ensuring reliable operation of both the converter and neighboring equipment, to avoid damaging neighboring equipment.

The most commonly employed VSC in industrial application and power distribution system are two level VSC, which uses the high frequency switching to convert it Dc-link voltage to an alternating output, this process introduces an output waveform which consist of fundamental frequency wave and a lot of harmonics when analyzed from Fourier Series. As per this analysis the output of VSC consist of following three groups of periodic sinusoidal output: The first group consist of integer multiple of base band frequency also termed as fundamental harmonics, the second group consist of harmonics at switching frequency, finally the third band consist of harmonics that are multiples of carrier frequency and shifted by fundamental frequency.

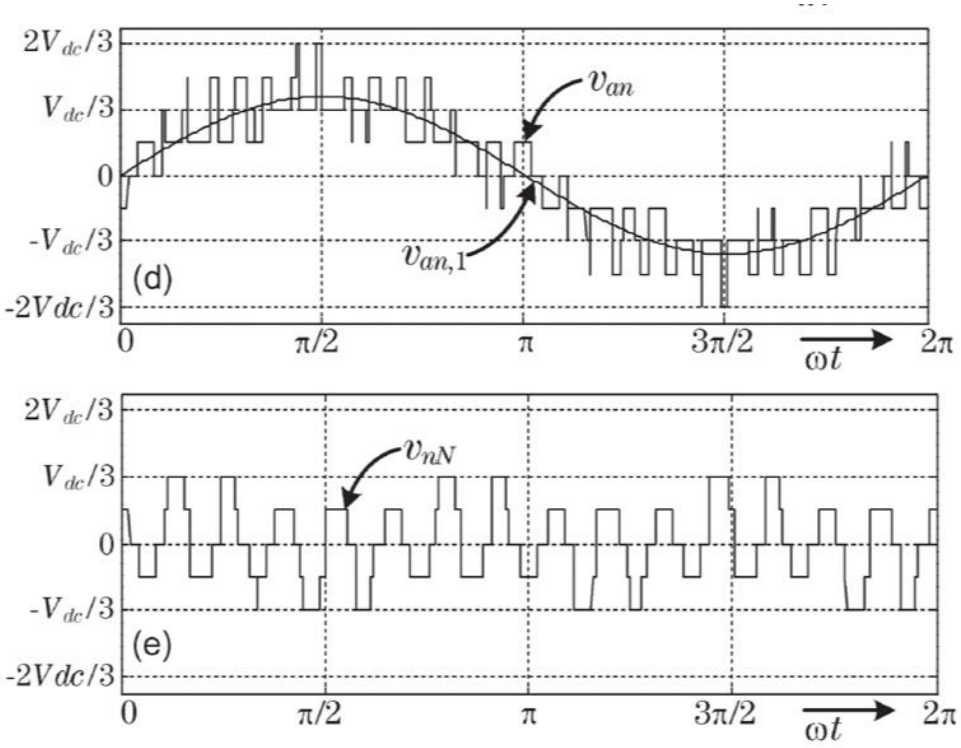

Figure 7. Third level voltage harmonic, (Rodríguez et al., 2007, p. 2934).

As discussed previously the most commonly used modulation is SPWM in industrial practice so as per the concepts established the SPWM have the modulation with high carrier ratio generating harmonic distortion around the carrier frequency and its side band, furthermore it helps to keep the low frequency harmonics (3rd, 5th and 7th) to a much small magnitude given that the power modulation signal are balanced. This indicates that harmonics induced in power system is unintentional byproduct of VSC modulation process and the commercially available converters have deliciated techniques to damp out these harmonics while functioning.

Although, the generation of harmonics and their mitigation are the part of process when generating desired power using VSC, but these phenomena can be exploited by the cyber intruder to inject abnormal harmonics in system that are not suppressible by implemented technology. This can be possible if the attacker somehow compromises the intrusion system of Grid converter, later on altering the gate timing signal in a way that switching IGBTs inject abnormal harmonics in the grid side of power system.

An example of such intrusion scenario can be understood by studies done by Park et al. (2019, pp. 4908-4909) about stealthy zero dynamic attack, in this attack the internal unstable modes of converter were excited by the intruder, but the output used for monitoring and system supervision of converter e.g. current harmonics or voltage harmonics remain close to standard values. This attack diverges the internal states in such a way that output manifest physically as abnormal dc-link stress, switching harmonics or oscillatory current components, however the standard THD does not indicate any abnormality. The interesting thing about such attack is their ability to remain undetected by output based anomaly detection system since the measured output remain close to nominal and only become visible when damage has already occurred by sudden increased instability.

Another example is the research conducted by Wu et al. (2018, pp. 4492-4493) about the stealthy injection of false data to destabilize load frequency control that can be correlated to frequency harmonics. The injected data can be delicately perturbating with the measurable outputs in such a that the total harmonic distortion remain within plausible operating bound, whereas specific harmonic components can be amplified beyond limits that can cause disturbance to the fast control dynamics thus jeopardizing the whole operation by using its own harmonic suppression control loop.

An effective solution to identify such intrusions is to measure the temporal correlation of signals like voltage source harmonic distortion or current source harmonic distortion rather than just have single instant set point monitoring of these signals. Another more practical way to look into this solution is to have wavelet analysis to monitor in a short time for filtering out sudden changes, this window can be use by ML algorithm for separating slow trend from fast changes as repeated sudden spikes of harmonics during normal operation resembling the transient state behavior can be a prominent signal of some un identified intruder in the system.

The study conducted by Kou et al. (2020) shows that supervised machine learning can be helpful in analyzing transient voltage and current signals to understand the fault behavior of a system, as wavelet based analysis combined with Deep Feed Forward

Network (DFFN) has shown to identify correctly the normal operation pattern versus fault pattern with an accuracy of 97 % (Kou et al., 2020, p. 1). This work can be further extended to learn the normal and then faulty behavior of a system caused by various harmonic based expected causes, later to use this learning for differentiating aforementioned scenarios from a malicious activity conducted by manipulating the intentional changes in VSC control dynamics for controlled spiking of harmonics.

2.2 Machine Learning application In Anomaly Detection

Machine learning is a rapidly growing field that involves the use of available data to form patterns and statistical models, which are then used to that synthesize specific boundaries and functions defining the logical behavior about how the system in question operate. The strong point of machine learning is the mapping of system it creates and forms the understanding of how system will be creating an output based on input, so basically creating a transfer function of the system. Thus, there is no need to program the system again and again to get the desired output, rather the algorithm will interpret the output based on the functionality of system. The ML can be categorized into three branches, namely supervised machine learning, unsupervised machine learning and reinforcement learning (Oelhaf et al., 2025, pp. 3-5).

The focus of this research will be exploring supervised machine learning and using gained understanding to find out which supervised ML method is best in distinguishing between the intrusion based anomaly and actual fault present in VSC. Supervised machine learning is about using the labeling of data which are termed as feature and cluster them into corresponding groups so that a relationship between features and labels can be established. It requires large amount of dataset to fetch corresponding input and categorizing them based on their properties which the system learn by training itself again and again and reducing the error while learning during testing in order to identify correct statistical model of give data set.

As discussed by Hernandez-Matheus et al. (2022, p. 6) there are two methods of labeling the inputs, one is using regression which is very beneficial in case of prediction of output

e.g. in case of forecasting demand of load based on consumption pattern or other variables like events, wind and solar prescience, load current profile the regression method can be useful. The other method is categorizing the inputs into specified outputs that are already sort of classified during past data examples. A good example of it can be use of data sets for inputs like THD results, PLL output values and Modulation signal output during category of Natural Fault, Intentional Fault and normal operation.

As discussed in Chapter 2.1 voltage source converter have multiple input variables in form of measurements that can be PLL angles, DC-link voltage peak to peak values, current harmonics dq voltage and current values, these can be used by supervise ML model to first train the system for mapping their statistical behavior under normal condition, then emulated fault condition, and then using perturbed values to mimic false data injection for parameter that impact the performance PLL, DC-link controller and AC side harmonics.

The collection of above discussed inputs can be segregated into several steps to clarify the working of supervised machine learning (Kumbhar et al., 2021, pp. 5470-5471). the first step is to gather data, as this data will be in raw format so to turn this data in useable format some cleaning is required so to remove out liars and noise. The second step is to convert that data into some understandable or relatable format like raw voltage and current should be converted to THD or PLL angle variation format to gain understanding of data and to check their relatability. Third step is to find pattern in that data using available supervised ML techniques and to create boundaries so to segregate data in mapping came out as result of categorization, this step is made robust by the process of testing the algorithm between different sets of training sets and test sets. Finally, the actual process is tested by placing the ML algorithm in the actual system and verifying its efficiency.

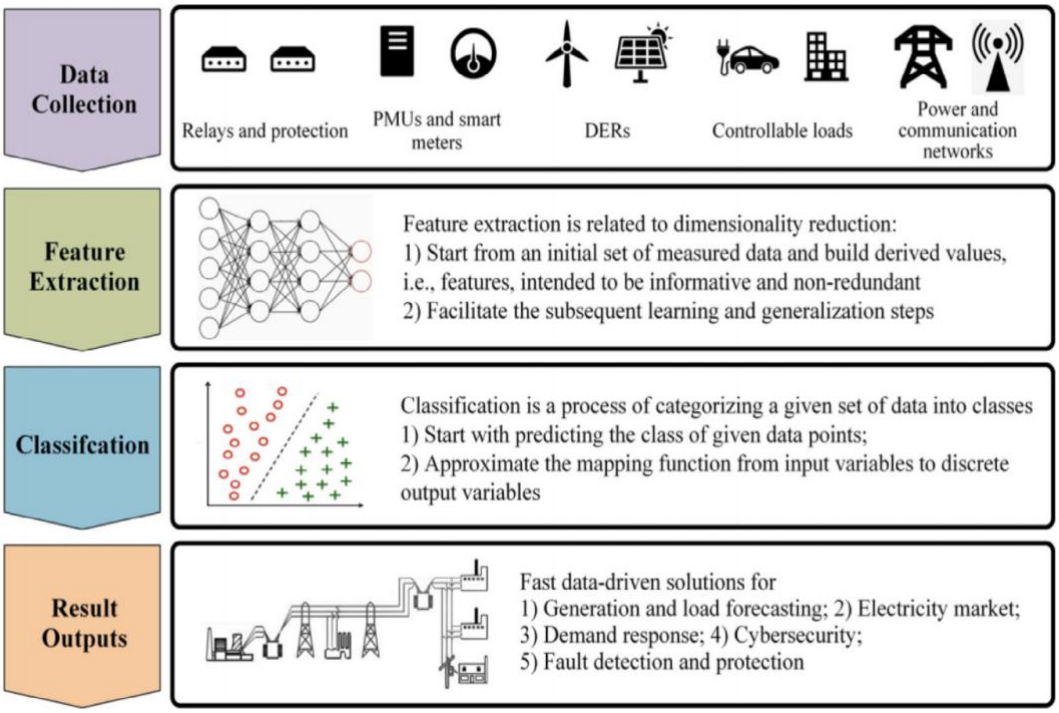

Figure 8. Machine Learning Framework, (Farhoumandi et al., 2021, p. 4)

2.2.1 Selection of models for Feature Engineering in VSC Intrusion detection

The study conducted by Rajora et al. (2024, pp. 2159-2160) reflects that Support Vector Machine (SVM) and Random Forest (RF) are two subsets of supervised machine learning models that are extensively adopted for implementation of power system security and operational improvements in power electronic devices, because of their capability to handle data that is spread across multiple dimensions that's produced by various measuring units installed in complex infrastructure of VSC interfaced advance grids. Huge data sets captured by high sampling rate data loggers, Phasor Measurement Units (PMUs), and scopes can be consumed by RF and SVM models to efficiently and precisely classify the inputs into correct labels without requirement of sophisticated physical models (Rajora et al., 2024, p.2161).

2.2.2 Analysis of Intrusion Detection Through Random Forest

Random Forest method is based on multiple decision making models; therefore, high dimensional data that can be labeled across multiple categories. The outcome of these decision models is combined based on voting done by each decision tree to get a high probability and robust result (Nivedha & Titus, 2023, p. 2304). The important thing in this multi tree modeling is special shuffling of data. it can be explained by an example where a data set of 15,000 data points, now each decision making model is supplied with some data points and out of them some are place back in the pool of 15000, in this way some models have same data sets multiple times and some don't have that exact at all. In this way each modeling tree sees the data set from slightly different perspective, creating a diversity in result. Finally, all outcomes are averaged known as voting thus causing the highly dominant attributes of input data to standout. This process is fast to operate and can be used to create labels either on basis of number or categorization as per strings. Mathematically it can be represented as follow,

$$\hat{y} = \quad mode\ (T_1(x), T_2(x), .. T_n(x)) \tag{12}$$

The study conducted by Sami & Naeini (2023, p. 3) shows that Random Forest method can be used in a hybrid way, therefore the advantages of classification method which helps to label the components of power transmission system as vulnerable or not vulnerable, and attribute of regression that calculate the score of vulnerability for transmission system components, can be combined to check how much the whole system is vulnerable to cascading failure. Based on this it can be assumed that Random Forest method has flexibility and precision to detect intrusion in a VSC based on abnormal outputs of specific system components.

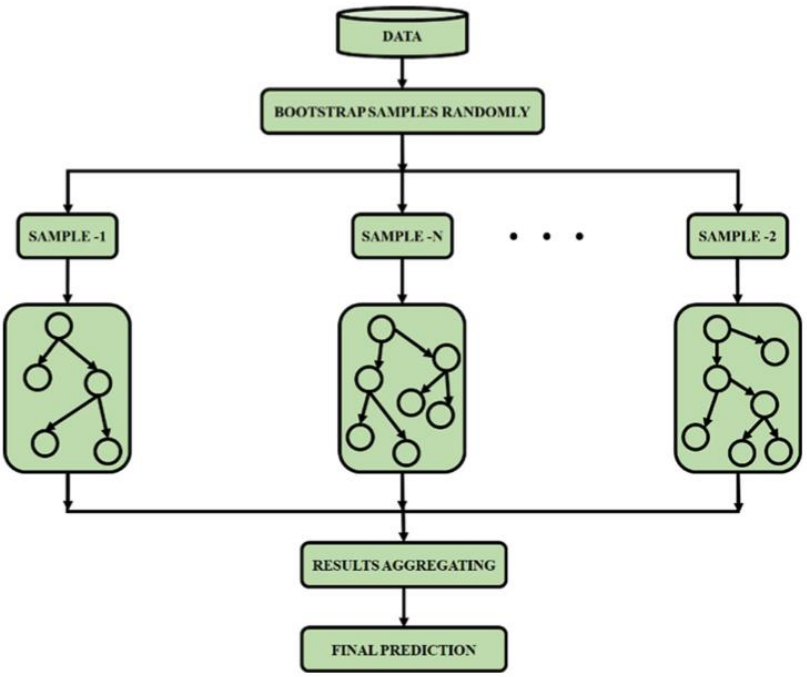

Figure 9. Random Forest Sorting Method (Nivedha & Titus, 2024, p. 2304).

2.2.3 Feature Engineering for Intrusion Detection using SVM

Another method that will be evaluated in this thesis is the use of Support Vector Machine (SVM), as it operates by creating the boundary plane between data samples pertaining to different labels. The division of data into separate categories for complex plane is done using kernel function that map the available data points into high dimensional plane in order to analyze the relation between samples through maximum margin that's defined by sample points at boundary also known as Support Vectors . (Debnath et al., 2025, pp. 174213 - 174215).

The study conducted by Debnath et al. (2025, pp. 174216-174217) reflects that SVM underperformed in-terms of accuracy (68.05%) and consumed large computational time of 12.897 second when competed against K-Nearest Neighbours (KNN) and Naïve Bayes (NB) methods. However, this research was conducted on SCR based rectifier and not a VSC. As discussed in previous sections for case of grid following VSC the anomalies are created via manipulation of complex signals like PLL angle variation or controlled

disturbance in harmonic patterns, which is not detectable by simple models of KNN and NB. Thus, providing gap to reanalyze SVM model for grid following VSC with previously described condition for intentional and unintentional unit level disturbances.

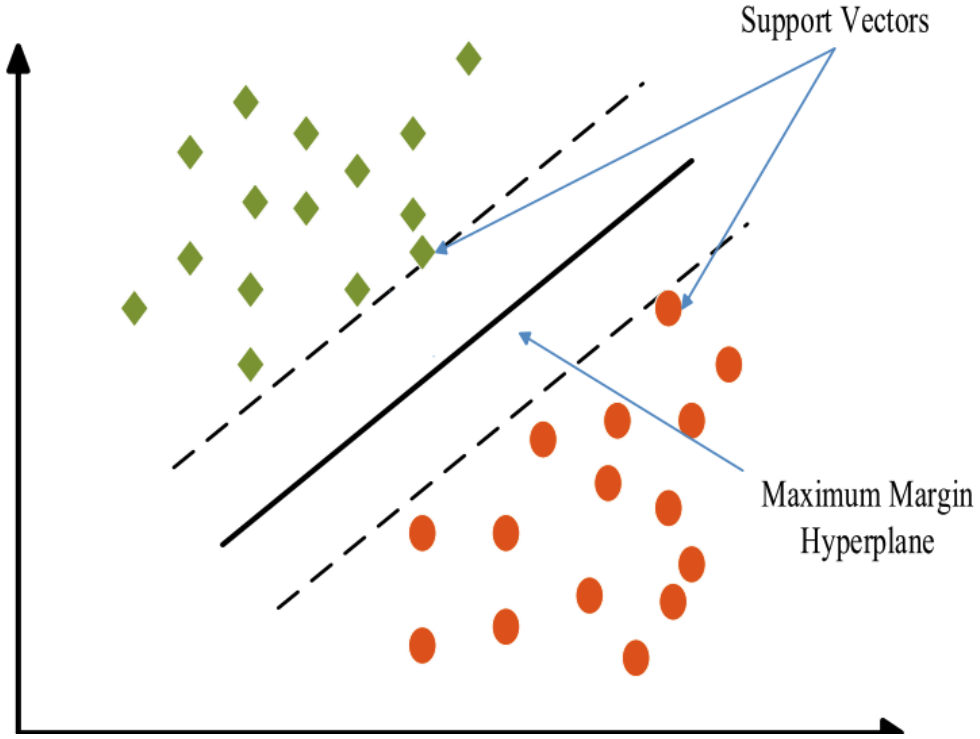

Figure 10. Hyper Plane of SVM (Debnath et al. 2025, p. 174215).

Furthermore, the review conducted by Farhoumandi et al. (2021, p. 6-7) indicates that SVM provide robust categorization owing to its inherent feature of building controlled margin. Specially for nonlinear dynamics of converter during an intrusion, where differentiating between a fault and intentional anomaly can be subtle and rare, a SVM model combined with wavelet analysis technique can prove to be competitive against other models since large amount of data is available for its training during normal operation.

Although the research in this regard by using actual hardware or HIL models is not available, but as explored by Babakmehr et al. (2021, pp. 5290-5291) using

MATLAB/Simulink simulation of IEEE-34 Bus distribution system for categorizing intrusion based faults in power converters, the Radial basis Function (RBF) SVM model achieved 92.25% accuracy for detecting cyber physical events. In section of 5-C a comparison is created between RBF based artificial neural network, RBF-SVM and Time-Frequency based sparse classifier (TISC) for single phase event detection using 150 machines and tabulated results like in table 3 show casing 92-93% accuracy for SVM method, thus a strong simulation based recommendation to employ SVM for detection of high dimensional overlapping signatures in time-frequency domain (Babakmehr et al., 2021, p. 5291).

This literature indicates that the performance of SVM for non-liner feature categorization like frequency jumps, switching harmonics or DC-link spiking is still under evaluated and strong research is needed by using actual Hardware based emulation to evaluate the accuracy and performance speed of SVM and RF models in detection of intrusion for VSC.

2.2.4 Utilization of VSC Signals for Constructing Supervised Datasets

The study conducted by Eswaran et al. (2025, pp. 3, 12) discuss in detail about the selection of voltage and current signals to form a data set that can be used to supervise a ML model to segregate a cyber-attack from a normal operation. The authors make use of Simulink for simulation of a Microgrid that operate in islanded mode and modeled an islanded setup through battery connected string converter, DCDC converters and DC to AC inverters which are interfaced with variety of conditions based on normal operating use cases and cyber attack condition. For creating attack scenario, some mathematically calculated data matrices are used to emulate False Data Injection (FDI) and Denial of service models. These models are then feed in place of controller signal for a defined period of time to create abrupt changes in converter output mimicking manipulation in sensor measurement in a real time condition. The detection of attack is classified in binary terms; therefore, data set is label 1 or 0 if its cyber-attack or normal operation respectively. Although this study is done for deep learning models, but this data set formation method can be understood to perform same task for Random Forest and Support Vector Machine at principal level. So, to put the process in simple words the raw

data of voltage and current measurement is collected under defined scenarios, after which the process of normalization and removal of noise is done by eradicating outliers (Hassan et al., 2025, p. 14). To make sample batch a sliding window style in employed where a data frame of 10 rows containing 09 features in each raw is focused on each time stamp and in the next step the window slid by one row, making steps till all the data rows are covered. Here each window is marked with a label depending on how many times a specific feature has appeared in that window. Finally, these label windows are feed to the ML models to get it informed about the system and its behavior in a specified scenario. The detail of labeling data as normal or Attack can be observed through Table 1, whereas Table 2 show the classification of attack data into attack type.

Table 1. Extracted Features Structure (Eswaran et al., 2025, p. 13).

Time Stamp	Feature 1	Feature 2	……. Feature 9	Truth Condition
T_n	Voltage-1, Current-1	Voltage-1, Current-1	Voltage-1, Current-1	Normal
T_{n+1}	Voltage-1, Current-1	Voltage-1, Current-1	Voltage-1, Current-1	Normal
T_{n+2}	Voltage-1, Current-1	Voltage-1, Current-1	Voltage-1, Current-1	FDI
…….	…….	…..	……	…..
T_{n+10}	Voltage-1, Current-1	Voltage-1, Current-1	Voltage-1, Current-1	Normal

In the above mentioned table, the feature 1 till feature 9 can be measurement of voltage and current that are received at nine different locations of the converter like phase A, B, C voltages and currents extracted at converter's output before the point of common coupling and after the point of common coupling. Also, the DC link measurements can be considered in-terms of voltage and current.

Table 2. Window Labeling Rules (Eswaran et al., 2025, p. 13).

Window Rows	Condition for labeling window	Assigned Label
1-10	All normal	0 (No attack)
2-11	Majority Attack row	1 (Attack)
3-12	Majority normal row	0 (No Attack)
14-23	Majority attack row	1 (Attack)

After labeling the data set inside a specified window of 10 rows, the data is classified based on type of attack done. To do this classification the nature of data that is received is analyzed and then label shown in Table 3 are assigned. Therefore, if all or majority of signals in a window for an attacked sample are different from normal signals by a scaled value then the attack can be classified as False Data Injection (FDI) attack. However, if some signals have dropped to zero and some have changed abnormally then the attack can be classified as a Denial of Service (DoS) attack (Eswaran et al. ,2025).

Table 3. Fault Classification (Eswaran et al., 2025, p. 13).

Window Rows	Condition for classifying window	Assigned Label
1-10	No Attack	Class 0
2-11	Attack : Signals dropped to zero. (This is Emulated by droping to zero in majority features in window)	Class 1 (DoS)
3-12	Attack (Signal changes by a bias or scaling)	Class 2 (FDI)
14-23	Attack (Signal changes by a bias or scaling)	Class 2 (FDI)

2.2.5 Challenges in deploying supervised Intrusion Detection in real VSC

One of the critical issues that can be observed from discussions done in previous topics is the collection of correct data for training the models that can distinguish between the case of normal operation, actual fault in converter and silent intrusion actions done in system. However, collection of data for field implemented voltage source converter can be a difficult task involving issues related to data privacy and extending to gathering of correct data with minimal noise suppression needed. Some interesting points can be fetched from study done by Pan et al.(2025) where he used actual TI C2000 inverter to study the use of ML for detection cyberattack on VSC. In this study it was observed that collection of data in physical converter affected by variating environment and its limitation at digital signal processing level can greatly impact the possibility of doing feature extraction and processing of data by the VSC unit (Pan et al., 2025, pp. 3228-3229). This directly point to the fact if controller memory and performance is not compatible to provide fast enough data extraction and rendering then use of ML cannot be done in real time converter.

Another challenge associated with current research done via model simulation versus actual hardware implementation is related to label designing and categorization itself. Currently the available research work does not provide readily available schemes or labels that can help to distinguish between normal operation, physical fault and fault triggered by intrusion. One such example can be extracted from the work of Yang et al. (2025, pp. 3-4) where a study involving 07 different commercial PV inverters is done in real time to explore limitations observed by such system under variable conditions. The paper reflects that a system which is trained with specific data sets intended to detect intrusion detection using supervised ML models, when placed in actual field with diversified hardware portfolio the converter fails to successfully detect the intrusions. This happens as a lot of environmental factors specifically involving but not limited to EMI signals can change the operational behaviour of device, therefore the device trained on one specific setup cannot be utilized on all site locations as being a generic intrusion detection mechanism.

Furthermore, the integrity and robustness of the models evaluated in multiple research papers is also questionable. As observed in most of the research paper reviewed in this section often times the model is trained and then tested on a data set that is constructed using limited number of runs thus generating a small data set. Also, it seldom that the models are trained with data sets of strong class imbalance, which is contrary to actual site situations where majority of time the device operate under normal condition and occasionally going to faults or very rare to interact with intrusion case (Zhang et al. ,2023, p. 1). This can be observed in studies reviewed in section 2.1 about the Intrusion detection and fault detection done for Voltage Source Converter, where it's evident that within the simulation the anomalies are added repetitively multiple times so that the model can learn pattern and form clearly separated boundary.

However, as reviewed previously the strategy of training models on a carefully formed data set is not suitable when implementation is targeted in a variety of actual fields, because a generic training is not sufficient to cater for variable field situation. In actual cases some outliers may become the misleading factor to provide ML model the required data for making decision for declaring a scenario as Cyber Intrusion or fault. This issue can be further realized by the work of Poudel et al. (2022, pp. 66635-66636) in which the tree-based decision making classifier is used for detection of physical faults. The results of his research showed that the classifier detected the unbalance faults with great accuracy, but the work framed prespecified faults, also it reflects the insufficiency to detect if there exist a silent attacker in the system who imitate intentional changes as faults. Furthermore, there are numerous deep learning methods that are adopted in studies but due to their intensive CPU load they are more compatible for offline modelling rather than being use as real time anomaly detection classifiers.

3 Hardware Level Implementation

This chapter will share information regarding the structured approach used to perform hardware in loop (HIL) based detection of intrusion in the system. The use of actual controller hardware which is connected with the grid environment emulated by the use of Typhoon HIL make this research different from the literature reviewed in previous section, as this research uses actual hardware based responses to train the ML models and to calculate the operational efficiency of RF and SVM models. In this case study supported by literature review a combination of MATLAB scripts and robot test is used to generate csv based files that represent multiple scenarios i.e. normal, fault case and recovery phase which in fact is an actual fault case.

Followed by this a robot test is used to first run the drive via pipeline and later on injecting synthetic anomaly, this anomaly is the offsetting of the DC-link feedback voltage so as to mimic the intruder who is changing the measurement feedback provided to the converter by the measuring device. The target of this operation is to use windowed features as showed in the work of Eswaran et al. (2025, p. 13). In this work the classifier will be judged on models' ability to detect the intrusion before, during and after the disturbance is injected in to control loop of controller. The Figure (11) shows the process flow, highlighting how the two different models therefore SVM which as per Bairagi & Munot (2019, pp. 181-183) will define the hyperplane to separate the extracted features and RF which will focusing on dynamic signatures.

For this thesis a commercially available grid converter controller is used. It is then integrated with a free licensed Typhoon HIL environment to model the DC-link management and Grid management system. The commercially available controller was communicated with system PC on which HIL was operated using two distinctive IP end points i.e. 192.167.3.302 and other one is 192.167.3.307. The advantage of using this configuration is to have a consolidated closed loop environment where the behavior of controller, plant and attacking sequence can be studied together. The importance of using real time data for fault detection is to understand how the industrial controller

process different signals and how the labeling can be in case of real controller (Upal et al., 2023, p. 2).

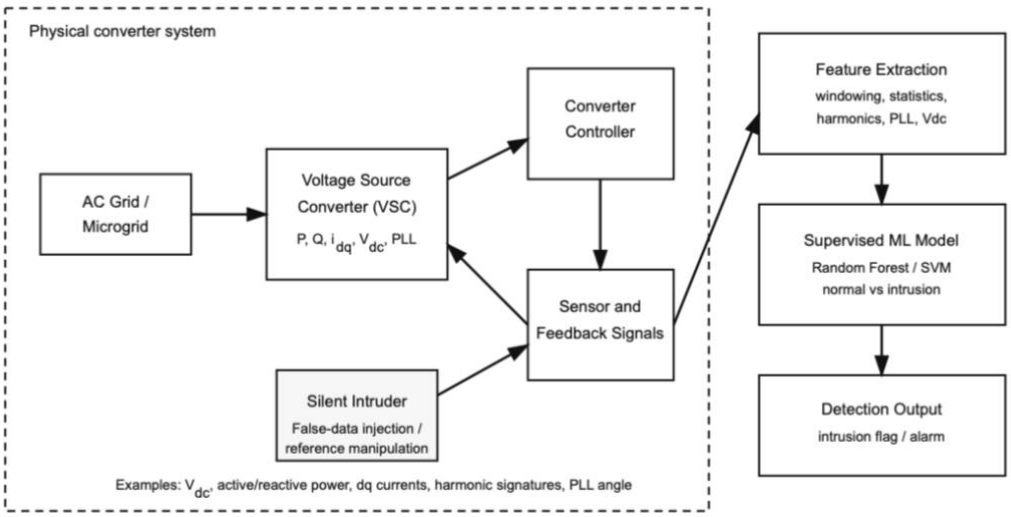

Figure 11. Workflow of State Detection (Open AI Chat GPT and Canva).

3.1 Data Acquisition and Data Engineering

The formation of data set for this thesis is achieved by use of a MATLAB script that generate 50 different scenarios realized through csv files, this script is named as `01_generate_scenarios.m` and is provided in appendix A for curious readers. The data inside the files generated by this script was intended to be use by repetitive test pipeline therefore a huge data set was created. In each scenario file there are 1000 rows of signals, where each row comprises of signal time stamp, active power reference command P_ref_cmd, reactive power reference command Q_ref, applied active power reference P_ref_applied, true DC-link voltage Vdc_true, and measured DC-link voltage Vdc_meas. The detail of each signal is listed below,

1- *time* = The values under this header provide time stamp for signal in specified scenario.
2- *P_ref_cmd* = It's the actual active power reference which the control hardware is supposed to receive. It's the active power reference without any tempering of data.

3- *Q_ref_cmd* = It's the actual reactive power reference which the control hardware is supposed to receive. It's the active power reference without any tempering of data.
4- *P_ref_applied* = This a signal which will reflect tempering of active power reference. Therefore, in normal condition the P_ref_applied will be equal to the P_ref_cmd, however in case of attack the value of P_ref_applied may be tuned to mimic an attack.
5- *Vdc_meas* = This signal is the value of DC-link voltage measured which can be impacted by noise or can be distorted as a result of silent intrusion at sensor level.
6- *Vdc_true* = This value provides actual measurement that the plant should have as per the normal operating setup.
7- *Attack_flag* = This value is critical for training purpose as it provide information if the data series at a specific time stamp is a normal value or attack value.

This data stream was imported to the robot test which holds the responsibility to perform the startup sequence of the converter, setup the plant model and DC-link energization in HIL emulator and allocation of different IP end points for delivering the controller required references, along with handling of Typhon HIL emulator for injecting offset of DC-link voltage to distort the Vdc_true readings. After running the system at a bounded frequency of 50 Hz the test pipeline is feed with three different phases i.e the normal state where the DC-link voltage delivered by sensor is not offset by any value, the state where derive is in attack phase i.e. the DC-link voltage delivered by sensor is offset by a specific value by robot test through feeding a different value to analogue input, and finally the recovery state where the offset is made zero and the behavior of system because even if the offset is made zero but still the system carries the impact of attack and this portion is very useful for training of model. Therefore, although the data samples generated in initial script were only segregated as attacked and no attacked but division of before mentioned sequence in test captured a more realistic behavior of the system.

Once the robot test was completed and output for each scenario logged by controller was moved to CSV files on HIL agent PC, then the analysis of data was performed offline on MATLAB, by using overlapping window so that the classifiers can correctly marginalize the difference between different states by recording their dynamic behavior making the ML model smart enough to capture the short term responses and causes of the system, otherwise the feed of clearly separated data points to classifier will result in poor training of ML models. The process of labeling and analysis was performed by a MATLAB script name as `train_rf_intrusion_detector.m`, the length of the single window that records the state was 0.2 seconds long and the overlapping time of window was 0.1 seconds, and total windows evaluated are 990, these values are hardcoded in the script. Also, the labeling of each window was done on the basis of the attack flags that were active and to obtain engineered features the script processes the data to have mean values , standard deviation values , kurtosis values, skewness, root mean square, and high pass variance. The selection for calculation of these properties of the output data was done to extract the response of converter in transient changes as well as steady state operation. By doing so the changes at signal level can be observed by model using root mean square and mean values, whereas the shape of waveform can be analyzed better by using skewness and kurtosis.

Therefore, all these mathematical properties evaluated helped to observe the temporal pattern of the VSC response inside the given plant model without losing the difference between numerical description of healthy and attacked system behavior.

Table 4. List of Features Extracted

No.	Feature	Description
1	mean(P)	Arithmetic mean of active power
2	std(P)	Standard deviation of active power

3	rms(P)	Root-mean-square of active power
4	skew(P)	Skewness — asymmetry of the power distribution
5	kurt(P)	Kurtosis — tail weight of the power distribution
6	var(P_hp)	Variance of high-pass filtered power
7	std(dP/dt)	Std of power derivative (rate of change volatility)
8	rms(dP/dt)	RMS of power derivative
9	mean(Vdc)	DC-link voltage mean
10	std(Vdc)	DC-link voltage standard deviation
11	rms(Vdc)	DC-link voltage RMS
12	p2p(Vdc)	Peak-to-peak range: max(Vdc) − min(Vdc)
13	std(dVdc/dt)	Std of DC-link voltage derivative
14	rms(dVdc/dt)	RMS of DC-link voltage derivative
15	var(Vdc_hp)	Variance of high-pass filtered DC-link voltage
16	mean(ΔP_ref)	Mean command mismatch

17	std(ΔP_ref)	Std of command mismatch
18	rms(ΔP_ref)	RMS of command mismatch
19	var(ΔP_ref_hp)	Variance of high-pass filtered command mismatch
20	time	Window end timestamp (temporal feature)

3.2 RF Model use in Grid Forming and DC-link Forming Mode

In grid forming mode the grid converter takes on the responsibility to retain the grid voltage and frequency with in the define limits as there is no utility present to provide constant voltages and frequency to the system. To achieve this control the VSC regulate the flow of Active power (or current) and Reactive power (or current) in order to keep the power equation balance on AC and DC side. For case of Droop mode, the VSC connected in parallel share the load base on dropping curve and voltage/frequency of the grid is maintained at reference voltage and frequency while dropping across a predefine slope at a specified rate of change of voltage for reactive power and rate of change of frequency for active power. Moving toward Droop mode with a base reference of active power reference and reactive power reference, the voltage drooping curve and frequency drooping curve is offset by a referenced amount active power and reactive power respectively.

Therefore, the data generated for model training in this operation mode reflect the system behavior on basis of how the Active power reference and Reactive power reference spoofed by the attacker. The training set consist of the data which have denial of service by putting the value of P_ref_applied to zero and then in some scenarios the false data injection is created by changing P_ref_applied from the P_ref_cmd by a small value, same is done for Q_ref_applied. The quantitative research conducted on the

commercial controller operating in Droop mode with P an Q references being active, generates 50 scenario specific log files from time stamped data frames inputs. The confusion matrix formed after training of Random Forest classifier on this data shows that 190 overlapping windows were identified incorrectly as attacked scenarios by the RF model, also 280 actual attacked windows were missed by classifier after training was completed which makes up to 18.85%. This show that RF model proves to be fairly accurate, preventing the controller from getting interrupted by a false alarm with an accuracy of 65.2%.

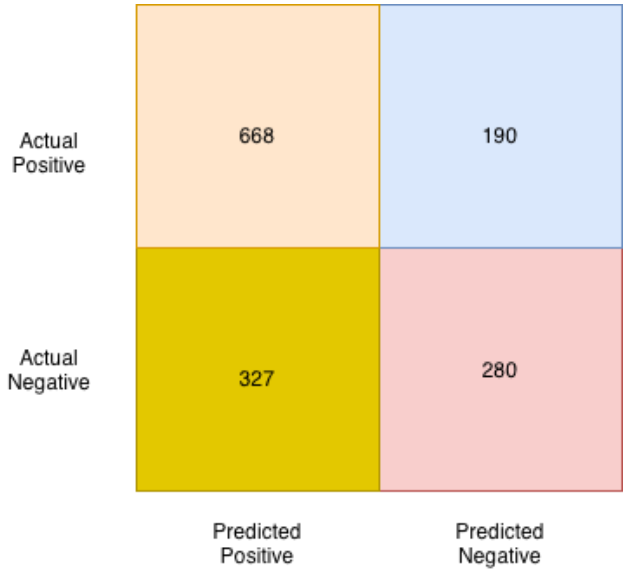

Figure 12. Confusion Matrix of RF output

The matrices evaluated from the truth table are tabulated in Table 5. Having a precision of 59.6 % indicates that after training when injected data series was injected to test normal operation - the system was getting a significant quantity of false flag indicating intrusion thus reflecting that classifier was not able to completely understand the temporal behavior of the VSC controller when it was operating normal, versus the behavior when it was under attack or its feedback loop is manipulated during the training.

Table 5. Random Forest Scores

Total evaluated Windows	**1485**
F1 Score	0.520

Specificity	0.784
Recall	0.461
Precision	0.596
Accuracy	0.652

The Figure 13 shows the first ten scenarios, illustrated with ground truth table (continues red lines) based on flag provided in time series data and the decision boundary (dashed blue lines) made by RF method. As the scenarios progressed from scenario 1 to scenario 38 it can be observed that the model improve its performance by not only detecting the start of attack within a duration of 100 msec, but it also detects the change in response when the offsets were removed from feedback during the recovery phase making the overall attack window visible during the disturbance. As indicated by F1 score and visualized through the plots it can be described that success of detecting the intrusion by RF model greatly depends upon difficulty level of tested scenario.

As an example, Appendix A provide the meta data for all the scenarios and out of them the scenario_035 is the trickiest scenario due to is fast attacking time and slight offset in reference values, the RF model completely failed to recognize the events where the attack initiated, because of this reason the scenario wise matric present in Appendix A shows that RF model attain zero value in F1 score for this scenario. This failure can be explained by research work of Cantor et al. (2024, p. 2) where the authors claim that RF model performance degrade when high dimensionality data is used to model the behavior of a system, calling these phenomena as curse of dimensionality. Similarly, scenario_016 shows that the model manages to detect an attack after a delayed period but then lose the precision causing a wrong window size in attack identification.

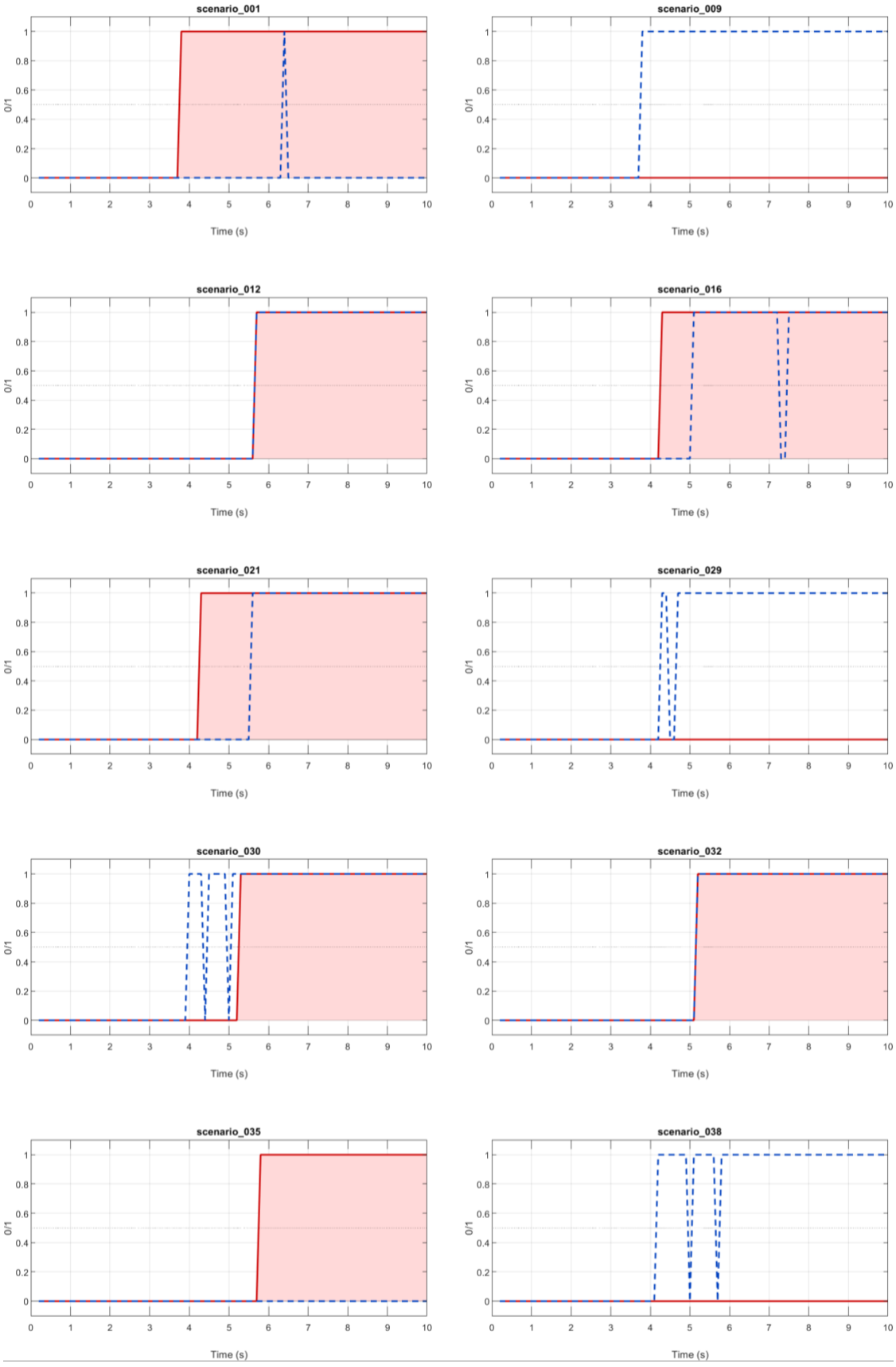

Figure 13. RF Detection V/S Ground Truth Scenario

One of the most interesting windows in panel of Figure 13 is Scenario_012 which is shown in Figure 14 with detail. From the time axis it can be observed that the attack duration is about 45% of the total scenario time, although the recognition of attack has a high precision of 1 with F1 score of 0.962 but due to False Negative of 05 windows the recall rate dropped to 0.937. Even though with these scores the model has shown good response in understanding the controller behavior and validate the fact that model is detecting the intrusion in the system on the basis of DoS or offset to measurements (FDI) rather than just memorizing the scenario attack flag.

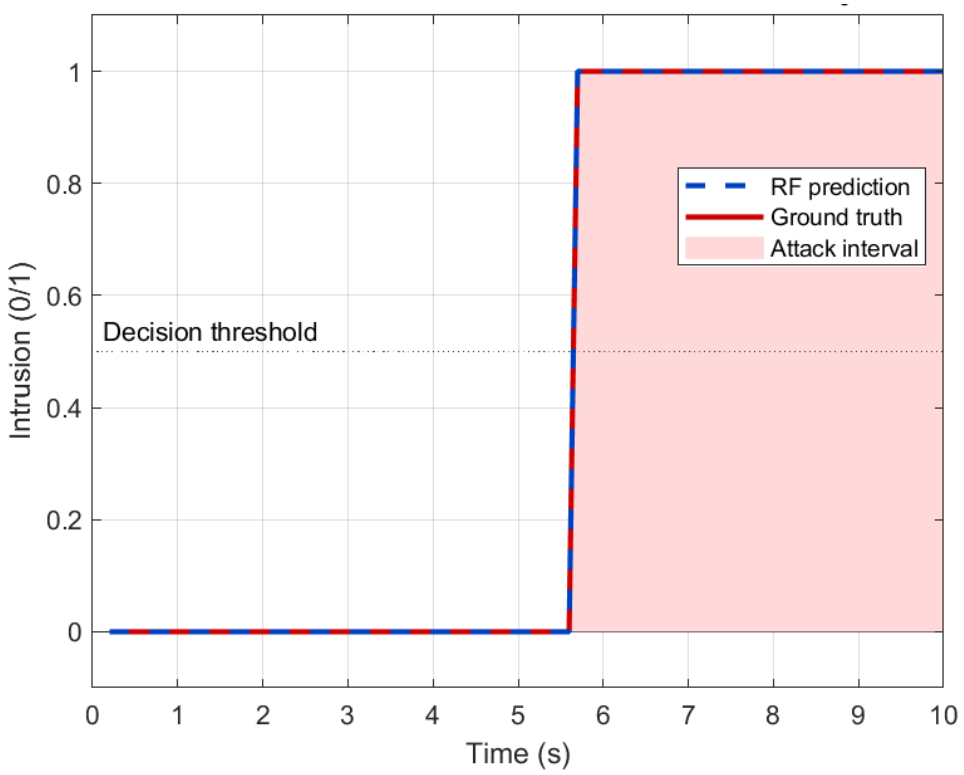

Figure 14. RF Intrusion Detection scenario 12

In grid following mode the VSC follows the grid voltage and frequency by locking to it using synchronous PLL as discussed in literature review chapter. This mode used in the commercially available controller use a DC-link voltage reference and the feedback through the sensor to regulate the DC-link at the specified value. When this method was adopted as mode of operation in current experimentation then training set was mimicking the data which have denial of service by putting the value of *Vdc_true* to zero and then in some scenarios the false data injection is created by offsetting *Vdc_true*

through some value called as *Vdc_meas*. When the HIL test was operated in this mode of commercially available converter the results of the Random forest yield approximately same confusion matrix as shown in Table 6 . The reason for having the similar results with two different control methods can be described from the Figure 15 which illustrate the relation developed by RF model for two features during its training.

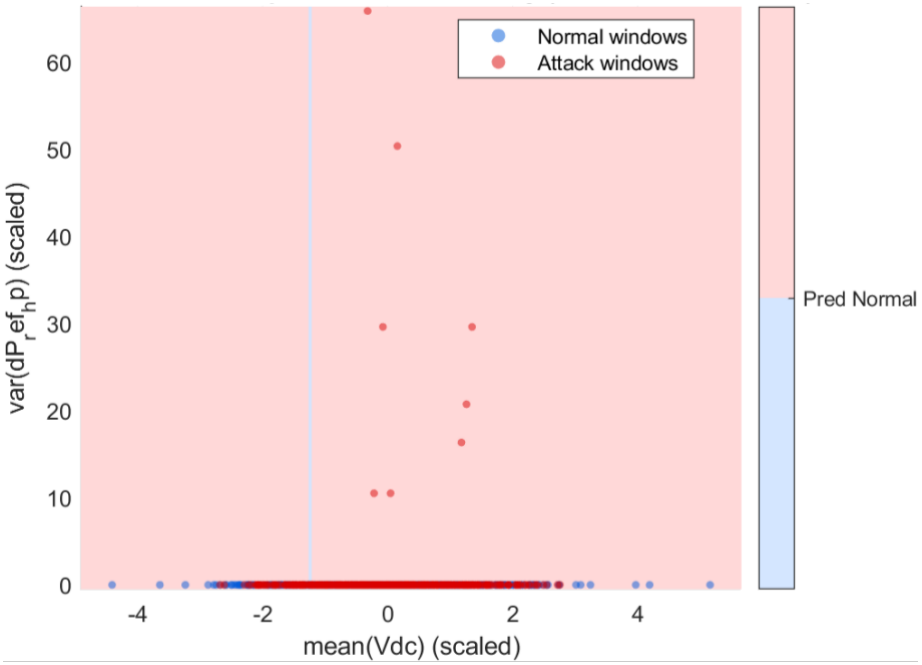

Figure 15. RF Decision boundary (held-out feature slice)

On x-axis of Figure 15 the average DC-link voltage offset is mapped which was feed to the system through *Vdc_meas,* whereas y-axis represent that how much the dynamic power related signal changed in relation to DC-link voltage within the window under consideration. The colored dots shown in legend is one data window per dot that is generated from the HIL emulation. Similarly, the side bar shows the color of state which RF model would predict in that window region. The unique thing about this plot is that RF model marks the decision map for whole relationship as Predicted attack without separating the boundaries based on windows correctly, however the confusion matrix illustrates an accuracy score of 0.652, that still is a strong diagonal element. This contrast in “2 feature slice” of RF model versus the “full feature set” training of RF model shows that RF model is making use of total information received from the temporal behavior of

system upon changing the input references or expected feedback values, rather than just relying upon some limited known relative variables.

3.3 SVM Model use in Grid Forming and DC-link Forming Mode

For this quantitative research conducted on the commercial controller operating in Droop mode with P an Q references, the 50 scenario specific log files generated as an output of robot test were analyzed by a script. The script uses kernelized SVM for mapping non-linear boundaries, that illustrate the behavior of active and reactive power responses through derivative based dispersion of frequency and voltage, furthermore the model also quantizes the disturbance affect by evaluating energy of high frequency components. All of these processed values were normalized to the same scale therefore forcing the model to provide accurate decisions, these decision planes are then further tuned by cross validating different sets of training data. At the final stage the validation datasets are used to improve the precision and accuracy of model thus finalizing decision threshold.

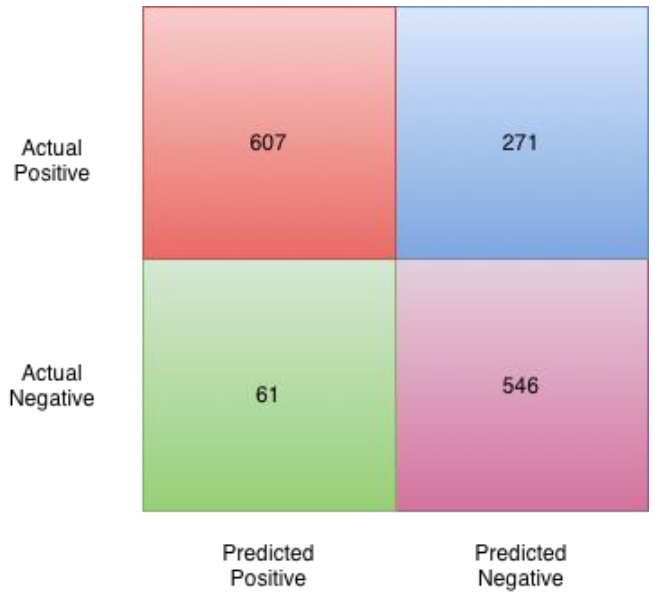

Figure 16. Confusion matrix of SVM output

The confusion matrix formed after training of support vector machine classifier on this data shows that 271 overlapping windows (18.24%) were identified incorrectly as attacked scenarios by the SVM model. However, only 61 normal windows were miss

classified as attacked after training was completed which makes only 4.1% of total windows. SVM model proves to be more precise than the RF model, preventing the controller from getting interrupted by a false alarm with an accuracy of 77.6%.

Table 6. Support Vector Machine Scores

Total evaluated Windows	**1485**
F1 Score	0.776
Specificity	0.691
Recall	0.9
Precision	0.668
Accuracy	0.776

The results from DC-link forming mode are used to analyze the decision forming pattern of SVM. Provided Figure 17 illustrate the thinking and decision making pattern of SVM, unlike the confusion matrix which shows overall performance using numbers like F1 score, this decision boundary plot shows deep insight about the categorization criteria of scenarios in SVM.

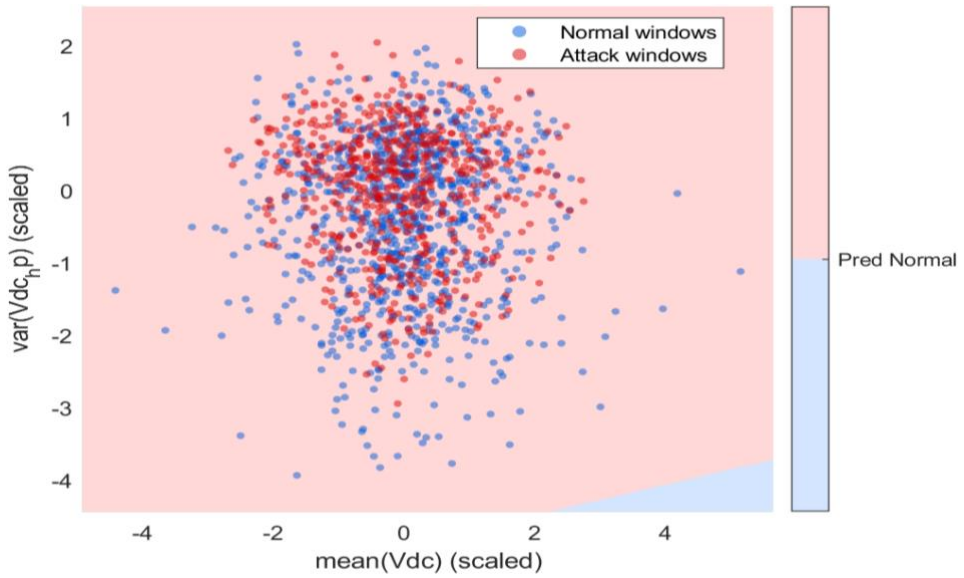

Figure 17. SVM held-out feature slice

Here the background color of plot shows the attack prediction by SVM model, where red background shows the predicted attack window and blue color shows the predicted

normal state. Also, the respective color dots represent the actual output of the typhoon HIL. To better understand the behavior the mean value of DC-link voltage is plotted against high pass variance evaluated for similar windows. These axes are physically linked to each other because if the DC-link feedback path is intruded then DC link voltage show abnormal fast fluctuations. However, in this situation the actual normal and attack windows are not separated from each other, rather they are clustered and make it difficult to form the boundary in the 2D plane. However, the SVM classifier still segregate the fault region from normal smoothly because these two features alone cannot provide the class difference shapely and the calculation done by SVM in no linear region provide the hyperplane to differentiate between the attack and normal windows.

The prove of this smooth performance can be extracted from the following panels of multiple scenario performance timeline captured in Figure 18. It shows the progressive improvement in the performance of SVM over time. Here the red shaded region represents the actual attack window bordered by continuous red line of ground truth, and dash line represent the predicted path by SVM. Here along with accuracy the speed of intrusion detection is also increased as observable in Scenario_16, and Scenario_35.

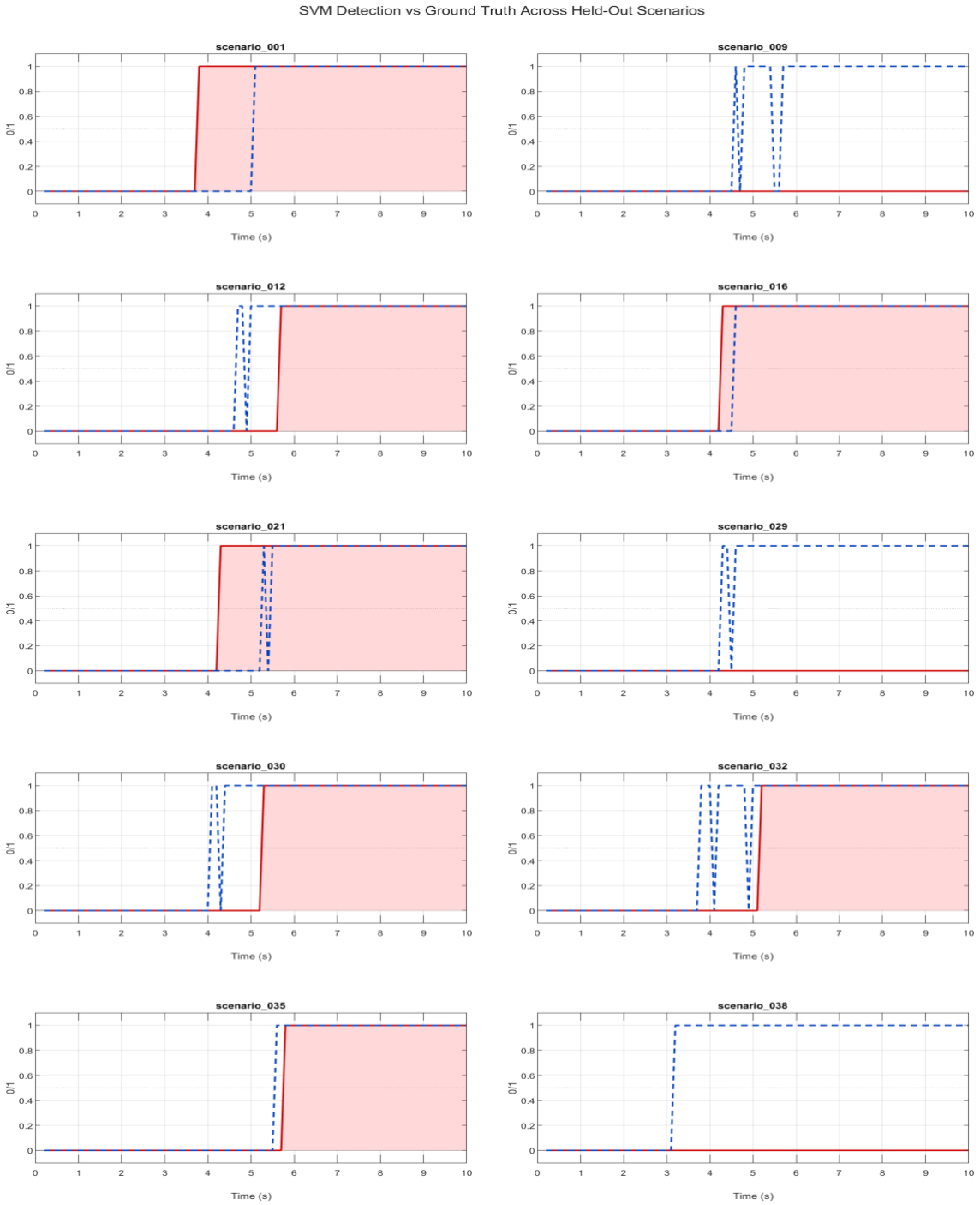

Figure 18. SVM v/s Ground Truth Scenario

The score distribution function shown below in Figure 19 helps to illustrate how the tunning of SVM model is done during training to select the correct threshold value. The threshold to declare an attack state is easy to choose if the histograms of normal and attack windows are separated themselves, however in case of overlapping as shown in

the Figure 19 it's difficult to set threshold as small difference in position can decrease the recall value or increase the number of false alarms. Therefore, use of validation style data makes it easier to select correct threshold for complex cases of VSC operating in different operation modes.

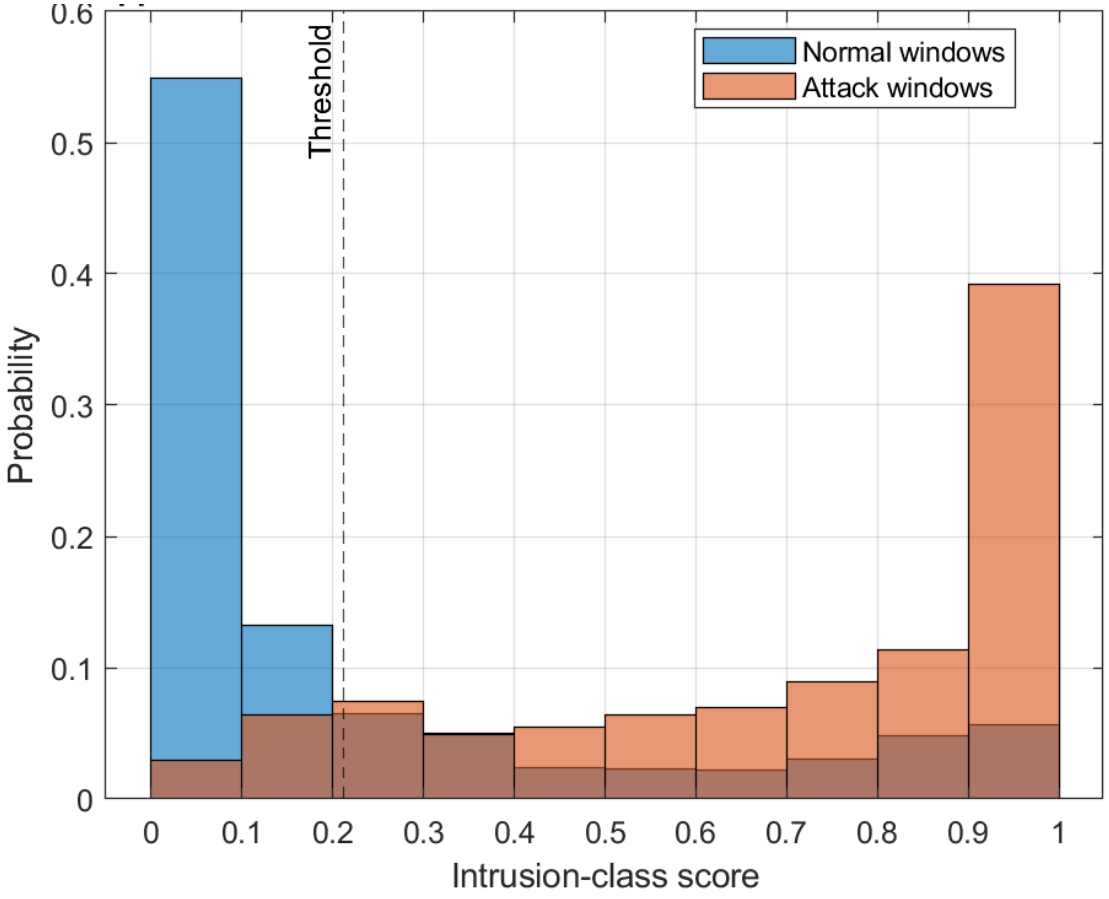

Figure 19. SVM score distribution plot

3.4 Issues in Actual Controller Implementation and Future Recommendations

The above experimentation of real time data with a commercially available hardware shows some promising results regarding detection of intrusion, however this emulation also highlights some critical issues in performing field level implementation of this work. The first thing is the memory limitation of controller which is also discussed in literature review section, but an additional difficulty observed during this work is the impact of processing data on CPU performance which can directly reduce credibility of VSC where

multiple read and write cycles are in progress from PLC for plant level control. Furthermore, the controller has to perform the triggering of protections and data logger as well which are highly impacted by the reaction time of controller when excessively heavy computational work of cyber physical intrusion detection is going on at controller level. Sometimes, the high CPU load can cause the crashing of controller and change of CPU is an architectural level of breaking change which a lot of industrial players would not support due to financial backlash. On the other hand, if this work is adopted at offline level as it is done in this experiment, then it does not yield a fruitful result since the real time protection and data privacy concept will be compromised in that case.

Secondly, the data used to perform the training for this evaluation is still performed on a single converter where the impact of actual site where multiple inverters are interacting under one plant level communication topology. Thus, the setup failed to be recorded at the full potential the performance of discussed ML models. The data generated from this emulation shows how the VSC would behave at software and hardware layer to perform field level protection but it is worth noting that such intrusion occur once in a while and the system would not have a separate training base to detect those attack, so a future work is still needed to devise method for generating more robust attack scenarios that could be closer to real time attack and based on larger data sets. Thereby, the test should cancel out all the possibilities that could be result in hallucination of model, like performing the FDI fault at very slow drifting rate so that it’s possible to assure that the model is not relying on the test memory and filtering out the attack cases with boundaries formed from highly dense data training.

Furthermore, as observed in section 3.1.2 and 3.1.3 the speed of detecting the intrusion was not too fast, comparing to microsecond operation taking place at Firmware level or operations taking place at application level at few millisecond rates of VSC (Sahoo et al., 2021, p. 5328). The detection of intrusion at such high latency by the discussed ML based program will fall short to create timely alert, therefore it’s recommended that future studies consider the performance of other classifiers in order to evaluate the possibility to detect the silent attack possibility in VSC.

4 Conclusion

This thesis provides a thorough hardware based quantitative analysis and literature backed qualitative review regarding performance of SVM and RF classifiers when used as ML mode in a VSC for detection of intrusion. The use of commercially available hardware integrated to a plant setup emulated by Typhoon HIL set it apart from simulation based thesis work, where time stamp data is collected by operating the control under different plant conditions and injected by well-known attacks like FDI and DoS through manipulation of DC-link voltage and Grid side feedback. The finalized scores are compared in table 7 where SVM can be seen to outperform RF in terms of accuracy and precision, reflecting its sensitivity in identification of attack scenarios. However, the RF model shows more conservative behavior in initiating false flag which can be interpreted from its higher specificity score.

Although from composite score it can be concluded that SVM is faster when it comes to training time, sensitive in missing the attack and better performance with compact feature set. However, the composite score does not capture the whole picture because the RF model proves to be less sensitive to scaling and reduced false alarms which otherwise can cause unnecessary tripping or activation of action again intrusion. So, both models present their own trade-offs, and it depends upon the nature of ID that might be expected in VSC based on its industry of application.

Table 7. RF v/s SVM Composite Score data

Model	Accuracy	Precision	Recall	Specificity	F1	Fit Time (s)	Composite Score
Random Forest	0.652	0.596	0.461	0.784	0.520	2.397	53.69
Support Vector Machine	0.776	0.668	0.900	0.691	0.767	0.891	79.04

The Figure 20 shows practicalities of these classifiers when adopted in real time controller. For a commercial grade controller its efficiency is evaluated based on its cost, responsiveness and load handling capacity. In this case it's crucial for a classifier to train itself at a fast pace and utilizing less resources to differentiate between a normal, fault or malicious situation. Although, the final work on hardware does not involve a fault state but the comparison between the SVM and RF based on its ability to make its decision boundaries and power to analyze large quantity of data it can be confidently mentioned that SVM hold strong grounds in analyzing more data than the RF and with this edge it also complete the training phase in 1.5 seconds less time than RF. Therefore, SVM is more feasible for online adaptation if the resources allow, because it will consume less CPU power and bandwidth in detection of intrusion as compared to RF model.

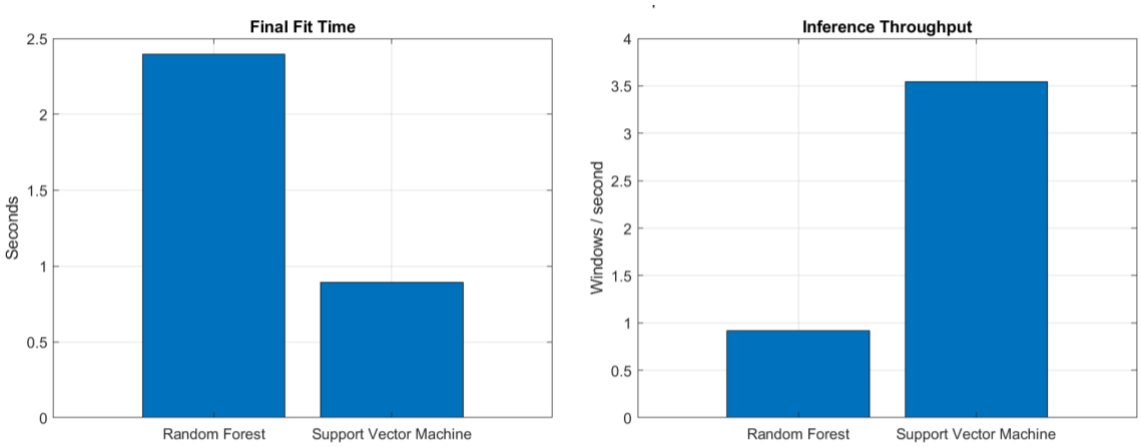

Figure 20. Model's Runtime Comparison

The Figure 21 illustrates the comparison between performance of SVM and RF models when plotted in same window but across different attack levels, i.e. Hardest attack, cases with strong false alarm pressure, and normal test cases with easy to detect intrusion signals, this distinction of different level for attacks can be analyzed further from signals provided in appendix A . From these plots it can be observed that SVM intrusion prediction rate improves over the time but during scenario of hardest data set to avoid false alarm it badly fails. Similarly, in the scenarios where detection of intrusion is fairly easy, both ML models detect the intrusion, however the performance if SVM even in

these cases outperform the RF classifier in-terms of timely detection and consistent detection.

Furthermore, for the tough cases like scenario 50 where the signals under consideration are drifted just slightly from base reference, the difference of performance between SVM and RF become more visible. For such cases as visible in plot row 2 the SVM succeeded consistently and accurately to recognize the intrusion although there was delay in detection, but RF model frequently failed to marginalize the intrusion and proves to be less reliable than SVM in this hardware level implementation.

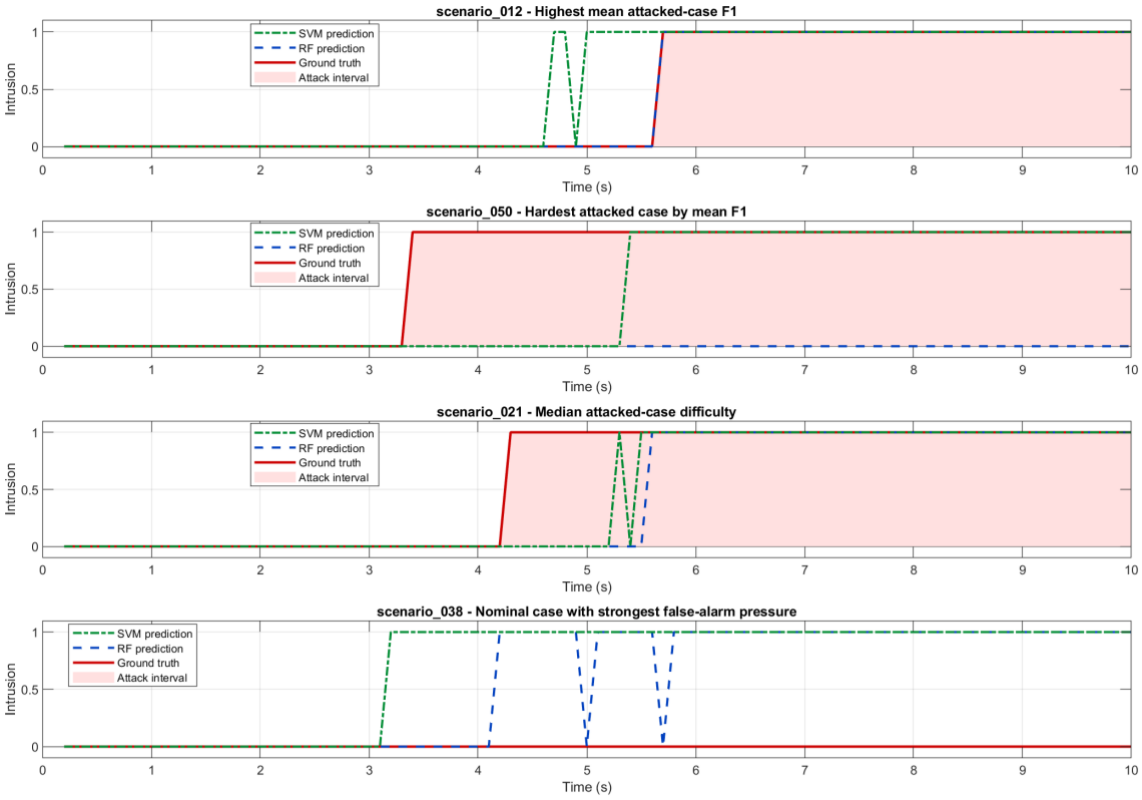

Figure 21. Representative Scenario Timeline

References

REN21. (2015). *Global status report 2015 – CESC webinar presentation.* Clean Energy Ministerial. https://www.cleanenergyministerial.org/sites/default/files/documents/gsr2015_cesc-webinar_9-10-2015.pdf

International Energy Agency (IEA). (2025, June 5). *Global energy investment set to rise to $3.3 trillion in 2025 amid economic uncertainty and energy security concerns.* IEA. https://www.iea.org/news/global-energy-investment-set-to-rise-to-33-trillion-in-2025-amid-economic-uncertainty-and-energy-security-concerns

International Energy Agency (IEA) (2023). *Electricity Grids and Secure Energy Transitions: Enhancing the foundations of resilient, sustainable and affordable power systems*, OECD/IEA, Paris, p. 18. Available at: https://www.iea.org/reports/electricity-grids-and-secure-energy-transitions

Graham, E., Fulghum, N. & Altieri, K. (2025). *Global Electricity Review 2025*, Ember, London. Available at: https://ember-energy.org/app/uploads/2025/04/Report-Global-Electricity-Review-2025.pdf [Accessed 10 Nov 2025].

Sahoo, S., Dragičević, T. & Blaabjerg, F. (2021). *Cyber security in control of grid-tied power electronic converters – challenges and vulnerabilities.* IEEE Journal of Emerging and Selected Topics in Power Electronics, 9(5), 5326-5340. https://doi.org/10.1109/JESTPE.2019.2953480

Sadi, M.A.H., Zhao, D., Hong, T. and Ali, M.H. (2023). *Time sequence machine learning-based data intrusion detection for smart voltage source converter-enabled power grid. IEEE Systems Journal,* 17(2), pp. 2477–2488. doi: 10.1109/JSYST.2022.3186619.

Rodríguez, J., Bernet, S., Wu, B., Pontt, J. O., & Kouro, S. (2007). Multilevel voltage-source-converter topologies for industrial medium-voltage

drives. IEEE Transactions on Industrial Electronics, 54(6), 2930–2945. https://doi.org/10.1109/TIE.2007.907044

Du, W., Fu, Q., Wang, X., & Wang, H. F. (2018). Small-signal stability analysis of integrated VSC-based DC/AC power systems: A review. International Journal of Electrical Power & Energy Systems, 103, 545–552. https://doi.org/10.1016/j.ijepes.2018.06.015

Huang, Y., Yuan, X., Hu, J., Zhou, P., & Wang, D. (2016). DC-bus voltage control stability affected by AC-bus voltage control in VSCs connected to weak AC grids. IEEE Journal of Emerging and Selected Topics in Power Electronics, 4(2), 445–458. https://doi.org/10.1109/JESTPE.2015.2480859

Wang, Z., Cheng, P., Pan, H., & Jia, L. (2025). *Impedance circuit model of voltage source converter with DC-link voltage control dynamics*. IEEE Transactions on Circuits and Systems I: Regular Papers, 72(6), 2970–2983. https://doi.org/10.1109/TCSI.2025.3548907

Wu, Y., Xu, J., Batista Soeiro, T., Stecca, M., & Bauer, P. (2022). *Optimal periodic variable switching PWM for harmonic performance enhancement in grid-connected voltage source converters*. IEEE Transactions on Power Electronics, 37(6), 7247–7261. https://doi.org/10.1109/TPEL.2022.3141268

Bierhoff, M. H., & Fuchs, F. W. (2008). *DC-link harmonics of three-phase voltage-source converters influenced by the pulsewidth-modulation strategy—An analysis*. IEEE Transactions on Industrial Electronics, 55(5), 2085–2092. https://doi.org/10.1109/TIE.2008.921203

Jana, K. C., & Biswas, S. K. (2015). *Generalised switching scheme for a space vector pulse-width modulation–based N-level inverter with reduced switching frequency and harmonics*. IET Power Electronics, 8(12), 2377–2385. https://doi.org/10.1049/iet-pel.2015.0101

Zhang, S., Zhao, J., Liu, K., Shi, Z., & Jin, L. (2022). *Stability enhancement and discrete-time resonant controller synthesis for voltage-controlled voltage source converters*. IET Generation, Transmission & Distribution, 16(5), 924–937. https://doi.org/10.1049/gtd2.12339

Qiu, G., Wu, F., Chen, K., & Wang, L. (2022). A robust accuracy weighted random forests algorithm for IGBTs fault diagnosis in PWM converters without additional sensors. Applied Sciences, 12(4), 2121. https://doi.org/10.3390/app12042121

Sun, J., Wang, Y., & Burgos, R. (2011). Unified impedance model of grid-connected voltage-source converters. IEEE Transactions on Power Electronics, 26(12), 3380–3391. https://doi.org/10.1109/TPEL.2011.2158582

Wang, X., Harnefors, L., & Blaabjerg, F. (2018). Unified impedance model of grid-connected voltage-source converters. IEEE Transactions on Power Electronics, 33(2), 1775–1787. https://doi.org/10.1109/TPEL.2017.2684906

Raeispour, M., Atrianfar, H., Baghaee, H. R., & Gharehpetian, G. B. (2021). Robust hierarchical control of VSC-based off-grid AC microgrids to enhancing stability and FRT capability considering time-varying delays. IEEE Journal of Emerging and Selected Topics in Power Electronics, 9(6), 7159–7171. https://doi.org/10.1109/JESTPE.2020.3017713

Teodorescu, R., Liserre, M., & Rodríguez, P. (2011). Grid converters for photovoltaic and wind power systems. John Wiley & Sons. https://ebookcentral-proquest-com.proxy.uwasa.fi/lib/tritonia-ebooks/detail.action?docID=698560

Bahrani, B., Karimi, A., Rey, B., & Rufer, A. (2013). Decoupled dq-current control of grid-tied voltage source converters using nonparametric models. IEEE Transactions on Industrial Electronics, 60(4), 1356–1366. https://doi.org/10.1109/TIE.2012.2185017

Zhong, Q.-C., & Weiss, G. (2011). Synchronverters: Inverters that mimic synchronous generators. IEEE Transactions on Industrial Electronics, 58(4), 1259–1270. https://doi.org/10.1109/TIE.2010.2048839

Danfoss A/S. (2023). Functional extension options: Installation guide (iC7 series) (Doc. No. AN389824059610en-000101). Danfoss.

Vanlyssel, J. (2024). Securing U.S. critical infrastructure: Lessons from Stuxnet and the Ukraine power grid attacks. Cybersecurity and National Security course paper. Retrieved 2024-10-08 from https://doi.org/10.48550/arXiv.2510.14185 [restricted availability].

Abu-Rub, H., Malinowski, M., & Al-Haddad, K. (Eds.). (2014). Power electronics for renewable energy systems, transportation and industrial applications. John Wiley & Sons / IEEE Press. ISBN 978-1-118-63403-5

Abdel Aleem, S. H. E., Ibrahim, A. M., & Zobaa, A. F. (2016). Harmonic assessment-based adjusted current total harmonic distortion. The Journal of Engineering, 2016(4), 64–72. https://doi.org/10.1049/joe.2016.0002

Park, G., Lee, C., Shim, H., Eun, Y., & Johansson, K. H. (2019). Stealthy adversaries against uncertain cyber-physical systems: Threat of robust zero-dynamics attack. IEEE Transactions on Automatic Control, 64(12), 4907–4923. https://doi.org/10.1109/TAC.2019.2903429

Wu, Y., Wei, Z., Weng, J., Li, X., & Deng, R. H. (2018). Resonance attacks on load frequency control of smart grids. IEEE Transactions on Smart Grid, 9(5), 4490–4502. https://doi.org/10.1109/TSG.2017.2661307

Kou, L., Liu, C., Cai, G.-W., & Zhang, Z. (2020). Fault diagnosis for power electronics converters based on deep feedforward network and wavelet compression. Electric Power Systems Research, 185, 106370. https://doi.org/10.1016/j.epsr.2020.106370

Hernandez-Matheus, A., Löschenbrand, M., Berg, K., Fuchs, I., Aragüés-Peñalba, M., Bullich-Massagué, E., & Sumper, A. (2022). A systematic review of machine learning techniques related to local energy communities. Renewable and Sustainable Energy Reviews, 170, 112651. https://doi.org/10.1016/j.rser.2022.112651

Oelhaf, J., Kordowich, G., Pashaei, M., Bergler, C., Maier, A., Jäger, J., & Bayer, S. (2025). A scoping review of machine learning applications in power system protection and disturbance management. International Journal of Electrical Power & Energy Systems, 172, 111257. https://doi.org/10.1016/j.ijepes.2025.111257

Kumbhar, A., Dhawale, P. G., Kumbhar, S., Patil, U., & Magdum, P. (2021). A comprehensive review: Machine learning and its application in integrated power system. Energy Reports, 7, 5467–5474. https://doi.org/10.1016/j.egyr.2021.08.133

Rajora, G. L., Sanz-Bobi, M. A., Bertling Tjernberg, L., & Urrea Cabus, J. E. (2024). A review of asset management using artificial intelligence-based machine learning models: Applications for the electric power and energy system. IET Generation, Transmission & Distribution, 18, 2155–2170. https://doi.org/10.1049/gtd2.13183

Nivedha, M., & Titus, S. (2024). IoT-based monitoring of smart grid using high-gain converter with optimized maximum power point tracking. Electrical Engineering, 106, 2297–2311. https://doi.org/10.1007/s00202-023-02070-4

Sami, N. M., & Naeini, M. (2023). Machine learning applications in cascading failure analysis in power systems: A review. Electric Power Systems Research, 223, 109630. https://doi.org/10.1016/j.epsr.2023.109630

Debnath, S., Vhakta, S., Tsui, Y. Y., & Islam, M. Z. (2025). Fault detection of three-phase controlled rectifiers using supervised machine learning algorithms. IEEE Access, 13, 174210–174218. https://doi.org/10.1109/ACCESS.2025.3618193

Farhoumandi, M., Zhou, Q., & Shahidehpour, M. (2021). A review of machine learning applications in IoT-integrated modern power systems. The Electricity Journal, 34(1), 106879. https://doi.org/10.1016/j.tej.2020.106879

Babakmehr, M., Harirchi, F., Dehghanian, P., & Enslin, J. H. (2021). Artificial intelligence-based cyber–physical events classification for islanding detection in power inverters. IEEE Journal of Emerging and Selected Topics in Power Electronics, 9(5), 5282–5293. https://doi.org/10.1109/JESTPE.2020.2980045

Eswaran, N., Sivarajah, J., Karunakaran, K., Velmanickam, L., Kumarawadu, S., & Wanigasekara, C. (2025). Cyberattack detection and classification of power converters in islanded microgrids using deep learning

approaches. Electronics, 14(17), 3409. https://doi.org/10.3390/electronics14173409

Hassan, G. F., Ahmed, O. A., & Sallal, M. (2025). Evaluation of deep learning techniques in PV farm cyber attacks detection. Electronics, 14(3), 546. https://doi.org/10.3390/electronics14030546

Pan, K., Wang, Z., Dong, J., Palensky, P., & Xu, W. (2025). Real-time estimation and defense of PV inverter sensor attacks with hardware implementation. IEEE Transactions on Industrial Electronics, 72(3), 3228–3232. https://doi.org/10.1109/TIE.2024.3436516

Yang, F., Pan, K., Yan, C., Ji, X., & Xu, W. (2025). Systematic security analysis of sensors and controls in PV inverters: Threat validation and countermeasures. Sensors, 25, 1493. https://doi.org/10.3390/s25051493

Zhang, J., Ye, J., Song, W., Lian, J., Zhao, D. & Yang, H. (2023) Hybrid cyber-attack detection in photovoltaic farms. In: 2023 IEEE Energy Conversion Congress and Exposition (ECCE). IEEE, pp. 6295–6300. https://doi.org/10.1109/ECCE53617.2023.10362667

Poudel, B. P., Bidram, A., Reno, M. J., & Summers, A. (2022). Zonal machine learning-based protection for distribution systems. IEEE Access, 10, 66634–66645. https://doi.org/10.1109/ACCESS.2022.3184865

Bairagi, V., & Munot, M. V. (Eds.). (2019). Research methodology: A practical and scientific approach. CRC Press. https://doi.org/10.1201/9780429464342

Upal, M., Gupta, D., Goyal, N., Imoize, A. L., Kumar, A., Ojo, S., Pani, S. K., Kim, Y., & Choi, J. (2023). A real-time data monitoring framework for predictive maintenance based on the Internet of Things. Complexity, 2023, Article 9991029. https://doi.org/10.1155/2023/9991029

Parvizi, P., Amidi, A. M., Zangeneh, M. R., Riba, J., & Jalilian, M. (2025). A taxonomy of robust control techniques for hybrid AC/DC microgrids: A review. Eng, 6(10), 267. https://doi.org/10.3390/eng6100267

Beikbabaei, M., Kwiatkowski, B. M., & Mehrizi-Sani, A. (2025). Model-free resilient grid-forming and grid-following inverter control against cyberattacks using reinforcement learning. Electronics, 14, 288. https://doi.org/10.3390/electronics14020288

Cai, Y., He, Y., Du, H., & Liu, J. (2024). Harmonic state-space modeling and system characteristic analysis of grid-connected inverter parallel-operation system considering asynchronous carriers. IEEE Transactions on Power Electronics, 39(7), 8645–8659. https://doi.org/10.1109/TPEL.2024.3381813

Khaleghi, A., Oshnoei, S., & Mirzajani, S. (2025). Federated learning detection of cyberattacks on virtual synchronous machines under grid-forming control using physics-informed LSTM. Fractal Fract., 9, 569. https://doi.org/10.3390/fractalfract9090569

Cantor, E., Guauque-Olarte, S., León, R., Chabert, S., & Salas, R. (2024). Knowledge-slanted random forest method for high-dimensional data and small sample size with a feature selection application for gene expression data. BioData Mining, 17, 34. https://doi.org/10.1186/s13040-024-00388-8

AI has been used to spread ideas, make technical understanding clear and style of delivering knowledge in better way. The tool used for translating research papers into easily understandable examples is Chat GPT “Thinking version 4.3”. For making the Json scripts correct to and improving robot tests for more result-oriented approach the copilot is used having Claude 4.6 sonnet.

Appendix A

scenario_id	scenario_file	duration_before	duration_attack	duration_after	p_ref_normal	p_ref_attack	vdc_offset_attack
scenario_001	scenario_001_inputs.csv	3.772	6.228000000000001	0.0	0.2403944939235236	0.12227765288001254	-17.665530145319035
scenario_002	scenario_002_inputs.csv	5.375	4.625000000000001	0.0	0.3048977310157724	0.42351558649261284	0.016560134340936103
scenario_003	scenario_003_inputs.csv	3.367	6.633000000000001	0.0	0.6888847098348762	0.7110406245062787	-23.144511170310782
scenario_004	scenario_004_inputs.csv	5.578	4.422000000000001	0.0	0.8412223922605251	0.7455668883791249	-0.013016330440570486
scenario_005	scenario_005_inputs.csv	5.566	4.434000000000001	0.0	0.10000000000001043	0.16224934056553758	0.010598012687149105
scenario_006	scenario_006_inputs.csv	5.637	4.363000000000001	0.0	0.2674146746594527	0.32687925041499305	-0.001449170182044047
scenario_007	scenario_007_inputs.csv	3.235	6.765000000000015	0.0	0.9000000000000533	0.9868588322246841	2.435860714743348
scenario_008	scenario_008_inputs.csv	4.364	5.636000000000001	0.0	0.45574766884755197	0.4813599299814409	-24.061206255419616
scenario_009	scenario_009_inputs.csv	9.999	0.0	0.0	0.392878955006823	0.392878955006823	0.0
scenario_010	scenario_010_inputs.csv	5.718	4.282000000000001	0.0	0.3157003346095242	0.2681186993513124	0.017132973883035776
scenario_011	scenario_011_inputs.csv	9.999	0.0	0.0	0.1	0.1	0.0
scenario_012	scenario_012_inputs.csv	5.622	4.378000000000001	0.0	0.4279618207594221	0.28844958604755006	0.032617120511791906
scenario_013	scenario_013_inputs.csv	9.999	0.0	0.0	0.269889548794584	0.269889548794584	0.0
scenario_014	scenario_014_inputs.csv	5.203	4.797000000000001	0.0	0.9040564946102073	0.9132575009149345	-0.002141938939115729
scenario_015	scenario_015_inputs.csv	3.928	6.072000000000001	0.0	0.24742159606516617	0.14602362898790444	21.235595026629486
scenario_016	scenario_016_inputs.csv	4.278	5.722000000000001	0.0	0.5334132284759395	0.4548343218569166	25.43751445845841
scenario_017	scenario_017_inputs.csv	3.511	6.489000000000001	0.0	0.7095863528861636	0.643150121759251	-30.363934850236816
scenario_018	scenario_018_inputs.csv	4.301	5.699000000000001	0.0	0.9000000000000626	0.9611381858552305	-0.017325536183376344
scenario_019	scenario_019_inputs.csv	5.783	4.217000000000005	0.0	0.8999999999999973	0.9408233881843099	-0.017042207370940567

scenario_020	scenario_020_inputs.csv	3.763	6.2370000000000001	0.0	0.6311806774312315	0.494289978301925	9.846479235686404
scenario_021	scenario_021_inputs.csv	4.268	5.7320000000000001	0.0	0.11030143228217687	0.26046172620550767	-20.375427562292927
scenario_022	scenario_022_inputs.csv	9.999	0.0	0.0	0.761218166812684	0.761218166812684	0.0
scenario_023	scenario_023_inputs.csv	5.797	4.2030000000000001	0.0	0.6203161444310387	0.6627299097658259	-0.0047452981888984
scenario_024	scenario_024_inputs.csv	9.999	0.0	0.0	0.650057335765126	0.650057335765126	0.0
scenario_025	scenario_025_inputs.csv	4.806	5.1940000000000001	0.0	0.693995788191003	0.647084995869563	-2.9060598172579484
scenario_026	scenario_026_inputs.csv	5.092	4.9080000000000001	0.0	0.7669020878806249	0.7638584297901678	0.022672511919690903
scenario_027	scenario_027_inputs.csv	5.824	4.1760000000000001	0.0	0.4484351263120888	0.6120309405105934	-0.0030678715369111165
scenario_028	scenario_028_inputs.csv	9.999	0.0	0.0	0.153267305924001	0.153267305924001	0.0
scenario_029	scenario_029_inputs.csv	9.999	0.0	0.0	0.58381629998515	0.58381629998515	0.0
scenario_030	scenario_030_inputs.csv	5.208	4.7920000000000001	0.0	0.5773996606223953	0.38751445904704446	-0.018465371445530634
scenario_031	scenario_031_inputs.csv	5.947	4.0530000000000001	0.0	0.10066153764351551	0.10432801360394685	0.015158365747014452
scenario_032	scenario_032_inputs.csv	5.187	4.8130000000000001	0.0	0.7383112752787374	0.7248816413953469	-0.00316944626686797
scenario_033	scenario_033_inputs.csv	9.999	0.0	0.0	0.113424393436396	0.113424393436396	0.0
scenario_034	scenario_034_inputs.csv	5.759	4.2410000000000005	0.0	0.8066302905116671	0.9112043721534063	0.008762404653005073
scenario_035	scenario_035_inputs.csv	5.791	4.2090000000000005	0.0	0.0806423761008 5265	0.0	0.0032104598796653086
scenario_036	scenario_036_inputs.csv	5.013	4.9870000000000001	0.0	0.20890441171590352	0.29497779140426006	0.006994632169341401
scenario_037	scenario_037_inputs.csv	5.854	4.1460000000000001	0.0	0.5926044581700891	0.6269256217883152	-0.0008986316854523139
scenario_038	scenario_038_inputs.csv	9.999	0.0	0.0	0.9	0.9	0.0
scenario_039	scenario_039_inputs.csv	4.09	5.9100000000000001	0.0	0.9000000000000612	0.8474911852224186	31.33715516525942
scenario_040	scenario_040_inputs.csv	3.747	6.2530000000000001	0.0	0.18800182274973554	0.07937836207776469	8.470496218813492
scenario_041	scenario_041_inputs.csv	4.623	5.3770000000000001	0.0	0.4238898006226011	0.2857508074001439	-31.078314650336342

scenario_042	scenario_042_inputs.csv	9.999	0.0	0.0	0.501315132611982	0.501315132611982	0.0
scenario_043	scenario_043_inputs.csv	9.999	0.0	0.0	0.1	0.1	0.0
scenario_044	scenario_044_inputs.csv	4.726	5.2740000000000001	0.0	0.6493489148600018	0.7248193340464179	-0.01598239110872687
scenario_045	scenario_045_inputs.csv	4.004	5.9960000000000001	0.0	0.9000000000000605	0.8832784551180547	-35.04776265135181
scenario_046	scenario_046_inputs.csv	3.616	6.3840000000000001	0.0	0.3763355107438873	0.34775904003998737	-12.367834233398868
scenario_047	scenario_047_inputs.csv	3.916	6.0840000000000005	0.0	0.9000000000000599	0.723886814172178	-34.73665787598434
scenario_048	scenario_048_inputs.csv	3.386	6.6140000000000001	0.0	0.30692739298435723	0.19588981038144718	8.10777248634915
scenario_049	scenario_049_inputs.csv	4.117	5.8830000000000001	0.0	0.86005404863138	0.7072150613374775	0.012738417261751383
scenario_050	scenario_050_inputs.csv	3.308	6.6920000000000001	0.0	0.10000000000000203	0.017319187089061 22	-37.31126190970005

RF scenario wise matrix

ScenarioID	TN	FP	FN	TP	Accuracy	Precision	Recall	F1	AttackWindowRate
scenario_001	36	0	62	1	0.373737373737374	1	0.0158730158730159	0.03125	0.636363636363636
scenario_009	36	63	0	0	0.363636363636364	0	0	0	0
scenario_012	55	0	0	44	1	1	1	1	0.444444444444444
scenario_016	41	0	10	48	0.898989898989899	1	0.827586206896552	0.90566037735849	0.585858585858586
scenario_021	41	0	13	45	0.868686868686869	1	0.775862068965517	0.87378640776699	0.585858585858586
scenario_029	43	56	0	0	0.434343434343434	0	0	0	0
scenario_030	40	11	0	48	0.888888888888889	0.813559322033898	1	0.897196261682243	0.484848484848485
scenario_032	50	0	0	49	1	1	1	1	0.494949494949495
scenario_035	56	0	43	0	0.565656565656566	0	0	0	0.434343434343434
scenario_038	42	57	0	0	0.424242424242424	0	0	0	0
scenario_040	36	0	63	0	0.363636363636364	0	0	0	0.636363636363636

scenario_043	99	0	0	0	1	0	0	0	0
scenario_044	43	3	51	2	0.454545454545455	0.4	0.03773584905660377	0.06896551724137931	0.5353535353535335
scenario_047	38	0	18	43	0.818181818181818	1	0.704918032786885	0.826923076923077	0.616161616161616
scenario_050	32	0	67	0	0.323232323232323	0	0	0	0.676767676767677

SVM scenario wise matrix

ScenarioID	TN	FP	FN	TP	Accuracy	Precision	Recall	F1	AttackWindowRate
scenario_001	36	0	13	50	0.868686868686869	1	0.793650793650794	0.884955752212389	0.6363636363636363
scenario_009	47	52	0	0	0.474747474747475	0	0	0	0
scenario_012	46	9	0	44	0.909090909090909	0.830188679245283	1	0.907216494845361	0.4444444444444444
scenario_016	41	0	3	55	0.969696969696967	1	0.948275862068966	0.973451327433628	0.5858585858585856
scenario_021	41	0	11	47	0.888888888888889	1	0.810344827586207	0.895238095238095	0.5858585858585856
scenario_029	42	57	0	0	0.424242424242424	0	0	0	0
scenario_030	40	11	0	48	0.888888888888889	0.813559322033898	1	0.897196261682243	0.4848484848484845
scenario_032	38	12	0	49	0.878787878787879	0.803278688524459	1	0.890909090909091	0.4949494949494945
scenario_035	54	2	0	43	0.979797979797978	0.955555555555556	1	0.977272727272727	0.4343434343434344
scenario_038	30	69	0	0	0.303030303030303	0	0	0	0
scenario_040	36	0	14	49	0.858585858585859	1	0.777777777777778	0.875	0.6363636363636363
scenario_043	55	44	0	0	0.555555555555556	0	0	0	0
scenario_044	38	8	0	53	0.919191919191919	0.868852459016393	1	0.929824561403509	0.5353535353535355
scenario_047	31	7	0	61	0.929292929292929	0.897058823529412	1	0.945736434108527	0.6161616161616166
scenario_050	32	0	20	47	0.797979797979798	1	0.701492537313433	0.824561403508772	0.6767676767676767

First 12 raw scenarios

time	P_ref_cmd	Q_ref_cmd	P_ref_applied	Vdc_true	Vdc_meas	attack_flag
0	0.240394493923504	0	0.240394493923504	1100	1098.4539410375	0
0.001	0.240394493923504	0	0.240394493923504	1100.12566039883	1099.36720710155	0
0.002	0.240394493923504	0	0.240394493923504	1100.25130095443	1099.14168791593	0
0.003	0.240394493923504	0	0.240394493923504	1100.3769018267	1099.53135058669	0
0.004	0.240394493923504	0	0.240394493923504	1100.5024431818	1099.92977831534	0
0.005	0.240394493923504	0	0.240394493923504	1100.62790519529	1100.06922443082	0
0.006	0.240394493923504	0	0.240394493923504	1100.75326805528	1100.93164828113	0
0.007	0.240394493923504	0	0.240394493923504	1100.87851196551	1100.68165051903	0
0.008	0.240394493923504	0	0.240394493923504	1101.00361714851	1101.59005977018	0
0.009	0.240394493923504	0	0.240394493923504	1101.12856384873	1100.27667687911	0
0.01	0.240394493923504	0	0.240394493923504	1101.25333233564	1102.05365304544	0
0.011	0.240394493923504	0	0.240394493923504	1101.37790290685	1099.86849818211	0
0.012	0.240394493923504	0	0.240394493923504	1101.50225589121	1102.37813003904	0