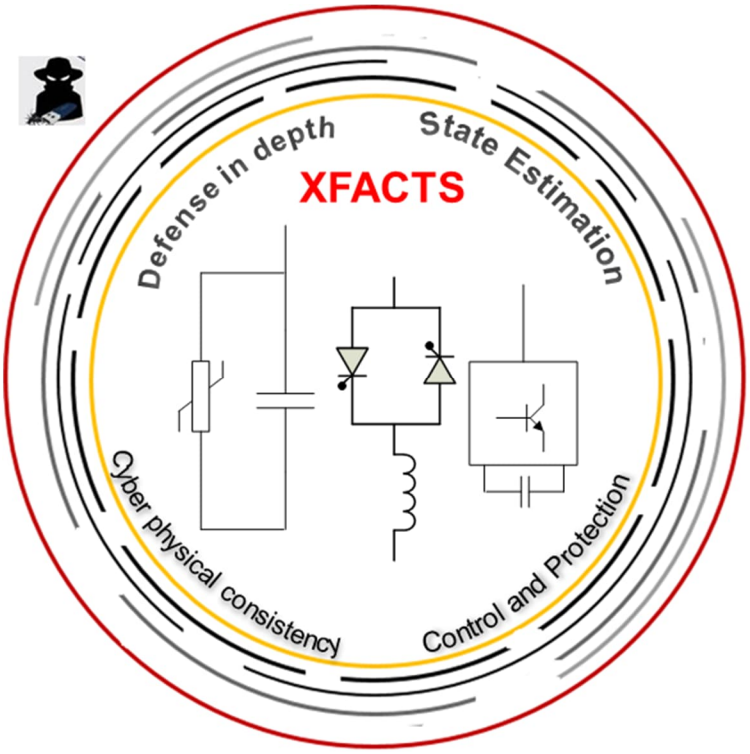
FINAL SCIENTIFIC/TECHNICAL REPORT



Cyber Resilient Flexible Alternating Current Transmission Systems (XFACTS)

DE-OE0000897

Award	DE-OE0000897
Lead Recipient:	ABB Inc.
Project Title:	Cyber Resilient Flexible Alternating Current Transmission Systems
Principal Investigator:	Reynaldo Nuqui
Team Members Organizations	Hitachi Energy Bonneville Power Administration University of Illinois at Urbana Champaign Iowa State University University of Idaho
Date of Report:	March 31, 2022
Reporting Period:	October 1, 2018 – December 31, 2021

Notice(s):

Distribution of information contained in this report is not restricted

ACKNOWLEDGEMENTS

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000896

We acknowledge the support of the BPA Office of Technology Innovation (Project No. 443, Technical Point of Contact: Aaron Martin); the DOE CESER Cyber Security for Energy Delivery Systems R&D Program (Program Manager: Mr. Akhlesh Kaushiva), and NETL (Robert Hayes). We also express our sincere gratitude to the BPA staff who have provided us with valuable guidance, advice, and logistics support throughout the demonstration phase of the project: Ms. Cynthia Polsky, Ms. Lori Bonn, and Dr. Judith Estep. Special mention and deep appreciation to Mr. Warren Reese who provided the day-to-day logistics support at BPA. Finally, we wish to recognize the technical support and contributions of our university partners: University of Illinois at Urbana Champaign (co-PIs: Mr. Al Valdes and Professor Peter Sauer), Iowa State University (co-PI: Professor Manimaran Govindarasu), and University of Idaho (co-PIs: Professors Brian Johnson and Dakota Roberson). Contributions by their PhD students who performed the academic tasks resulting in dissertation, publications, and an award-winning paper is appreciated.

EXECUTIVE SUMMARY

This report summarizes the activities conducted under the DOE-OE funded project DE-OE0000897, Cyber Attack Resilient Flexible AC Systems – XFACTS. Hitachi Energy (HE), in collaboration with ABB Inc. (ABB), Bonneville Power Administration (BPA), University of Illinois at Urbana-Champaign (UIUC), Iowa State University (ISU), and University of Idaho (UI) pursued the development of a system of defense for Flexible Alternating Current Transmission Systems against cyber-attacks (XFACTS). A FACTS substation enhanced with XFACTS defense mechanisms will be capable of mitigating cyberattacks especially those that seek to control electrical parameters like voltage or current and interrupt the power flow in AC lines. It empowers existing FACTS controllers and associated intelligent electronic devices to detect and mitigate malicious intents to depress system voltages, destabilize power flows, trip AC circuit breakers, corrupt currents, and voltages, even if the malicious commands and the measurements have correct syntax. The XFACTS functions utilize the physics of active power electronic systems, control and protection, electric power engineering principles, and state estimation to bring more in-depth cyber defense closer to the protected FACTS substation devices.

The team developed and demonstrated the XFACTS system in an AC substation environment, via functional upgrades to existing firmware of commercial off-the-shelf FACTS station devices, and/or embedded hardware, without the need for additional instrumentation nor new instrumentation technologies. This is to ensure that the developed solutions will support the FACTS devices currently installed in the US electricity delivery infra-structure.

The team focused first on developing a hardware-in-the-loop test bed representing an alternating current electrical substation equipped with FACTS devices and relays utilizing the EtherCAT protocol and IEC 61850. At Hitachi Energy this test bed consisted of a Real Time Digital Simulator, HE MACH PS 700 main computers, HE MACH PS 741 analog I/O, and HE Relion 670 transmission relays. Then, focus shifted to advancing the state of the art in cyber defense of FACTS equipped substations, namely secure FACTS data communication system; secure FACTS circuit breaker control commands; secure FACTS switch bypass commands; secure control device configuration change. This effort was preceded by identification of credible threats to FACTS control devices through simulated cyberattacks and evaluation of their feasibility and severity in a cyber physical test bed. The cyber threats and attack cases formed the basis for the development of the cyber security algorithms.

An independent red team analyzed the designs of XFACTS with the objective of exposing vulnerabilities in the defense mechanisms. The project team then emulated adversarial actions identified by the red team and evaluated performance in the face of identified cyberattacks. The team subsequently recalibrated the functions to a higher level of resilience against discovered vulnerabilities.

XFACTS final test for deployment readiness was staged at a 230 kV AC substation within the Bonneville Power Authority service area. BPA and HE demonstrated the field performance of

XFACTS in a substation environment, with staged cyberattacks on the control system and successful defense from the security functions.

The tasks developed during the project followed the project plan and consisted of: threat model specification for FACTS stations, wide area measurement systems controlling FACTS and SCADA systems controlling FACTS; development of control logic extensions that detect intrusion on normal and emergency FACTS control commands; design of a streaming state estimator that detects false measurement injection attacks on the FACTS communication system; FACTS control devices; validation of the FACTS security algorithms in a hardware-in-a-loop laboratory setup at Hitachi Energy; and field demonstration of the developed system of FACTS cyber security functions and devices at Bonneville Power Administration (BPA) within their Ross AC substation.

The Hitachi Energy Research team transferred the developed technology to HE FACTS product groups for inclusion into their product roadmap.

The accomplishments of the FACTS project have advanced the state of the art in cyber security of FACTS substations by adding intelligence to existing devices that is based on the underlying physics of the protected electrical system, as summarized in the next section.

The project is a successful example of a government-sponsored, industry/academic partnership. BPA, University of Idaho, Iowa State University, the University of Illinois, and Hitachi Energy established a collaboration that enhanced each organization’s strengths.

.

ACCOMPLISHMENTS AND COMPARISON TO OBJECTIVES

Objectives	Accomplishments
Design, prototype, and test secured FACTS real time data communication system	Designed, and prototyped a streaming three-phase state estimator function in a Hitachi Energy (HE) PS700 server. Tested in an HE MACH control system-based hardware-in-a-loop test bed with BPA RTDS system and BPA SVC station model
Design, prototype, and test a FACTS cyber physical system defender (MACHGUARD)	Designed, and prototyped a FACTS cyber defender system in a PS700 server. Tested in an HE MACH control system hardware-in-a-loop test bed with BPA RTDS system and BPA SVC station model
Design, prototype, and test secured FACTS collaborative defense system in an IEC 61850 substation against cyber attacks	Designed, and prototyped a collaborative defense system embedded in Hitachi Energy's IEC 61850 compatible RED670 and RET670 protection relays, and PS700 control devices. Tested in a hardware-in-a-loop test bed with BPA RTDS system and BPA SVC Station model
Design, prototype, and test secured FACTS series capacitor defense system against cyber attacks	Designed, and prototyped a series capacitor defense system in HE RTDS. Tested in a hardware-in-a-loop test bed with BPA RTDS system and BPA Micro-WECC system model
Design, prototype, and test secured FACTS STATCOM (static compensator) defense system against measurement attacks	Designed, prototyped, and tested a STATCOM measurement defense system in MATLAB Simulink.
Build, configure and test a cyber physical system (CPS) test bed embodying a FACTS SVC station with protection and control	Hitachi Energy built, configured, and tested a CPS test bed representative of a Static Var Compensator system in a 230 kV substation running on EtherCAT, IEC 61850, Syslog, and TCP/IP with Hitachi Energy's commercial IEDs in the Raleigh office.
Deploy and demonstrate the power system domain-based cyber security functions at a high voltage substation	Deployed and successfully demonstrated the XFACTS cyber security functions at BPA substation in Vancouver, WA, in a hardware-in-the-loop connection with BPA RTDS system.
Transfer knowledge gained in the project	BPA, UIUC, ISU, UI and Hitachi Energy presented conference papers and organized participated panel sessions in industry focused conferences to disseminate knowledge.
Chart a path to commercialization of developed technologies	Hitachi Energy business units has received the developed technologies and currently undergoing a product road map exercise to chart the commercialization of XFACTS

DETAILS OF PROJECT ACTIVITIES

Details of Project Activities are presented in Appendix A (Hitachi Energy Report), Appendix B (UIUC Report), Appendix C (ISU Report), and Appendix D (University of Idaho Report).

Highlights:

The project partner tasks encompassed:

UIUC

The University of Illinois at Urbana-Champaign (UIUC) supported the project by developing cyber-physical security solutions against threats to Flexible Alternating Current Transmission Systems (FACTS) integrated and controlled by Wide Area Measurement/Wide Area Control Systems (WAM/WACS). Such an ecosystem can benefit from advantages enabled by the ability of FACTS to enhance resiliency and robustness of transmission system. For this system to inter-operate, there must be communication over networks, currently using the IEEE C37.118 protocol. UIUC examined this wide area communication as a potential cyberattack surface.

With state-of-the-art technology, it is possible to implement communication network control host defenses in such an integrated system. These defenses potentially detect and block attacks against C37.118 as well as violations of communication and protocol whitelists.

UIUC advanced the state-of-the-art when they developed physics-informed defense that examined system behavior in response to a disturbance and in the presence of an adversary with capability to corrupt the modulation signal from the WAM/WACS to the FACTS. A successful attack of this type can result in destabilizing system conditions. The physics-based defense is based on extensive system analysis and simulation to rapidly identify when the modulation fails to achieve the expected result (for example, successfully damping an inter-area oscillation).

UIUC solutions were deployed in near real time environment using MATLAB Simulink with Power Systems toolbox. Their protypes were subjected to analysis and evaluation by the Red Team. UIUC prepared a response to the Red Team findings. They also executed an attack suite in which a simulated attacker can set parameters for the various attacks considered. Subsequently, they ran a number of attacks sampling the space of attack parameters. UIUC verified that all significant attacks were detected and mitigated. The attacks that evaded detection were all of acceptably low impact in terms of system stability.

UIUC published two conference papers based on this work, both co-authored with Hitachi Energy. One of these won the Best Student Paper award in the Power Tech Conference.

BPA

The Bonneville Power Administration hosted the demonstration of the XFACTS cyber security functions developed for Flexible AC Transmission Systems. Leading to this event, BPA provided real time digital simulation models of representative 230 kV FACTS device with the power system to which the device is connected. This allowed the BPA and Hitachi Energy team to build a hardware-in-the-loop (HIL) system that mimics near field conditions within a FACTS station. BPA provided access to the RTDS system that drives the power system models and feeds

measurements into the security enhanced controllers and IEDs. They also provide technical support in configuring the RTDS system as well as operational insights into their FACTS system. It allowed the project team to grab insights into the operations and retuning the functions developed in the R&D phase.

BPA reviewed the threat models to ensure that they are representative vulnerabilities in FACTS operations.

BPA ensured a secure and safe environment during the demonstration phase and extended logistical support of the day-to-day activities in their substation complex.

BPA is engaged in the dissemination of knowledge by sharing the project results with their cyber security and operation control personnel. They will support various panel sessions organized to discuss the new technologies developed in the project.

BPA's effort is supported by their Technology Innovation Office R&D project, TIP 443 - "XFACTS Cyber Resilient Flexible AC Transmission Systems."

ISU

ISU supported the project through the development of cybersecurity solutions for wide area-controlled FACTS devices. ISU focused on control platforms dedicated to wide-area voltage control systems (WAVCS). With the increasing deployment of FACTS for achieving improved voltage stability of bulk power systems, ISU determined that vulnerabilities exist on these systems that can exploited by cyber-attackers. They concluded that successful stealthy cyber-attacks on WACVS systems, that are difficult to detect by traditional IT-based cybersecurity solutions or threshold-based bad data detectors, can lead to a voltage collapse in power grid.

ISU developed a data-driven attack-resilient system against different classes of data-integrity attacks. It integrates machine learning-based anomaly detection system with rule-based attack mitigation to detect data integrity attacks and provide mitigation actions to quickly restore the normal operation after disturbances. The system applies variational mode decomposition technique to extract sub-signal modes, and computes statistics-based features, such as instantaneous amplitude, relative mode energy ratios, zero crossings, etc., for detection of attacks on measurement and control signals using decision trees.

ISU built a hardware-in-the-loop test bed for WAVCS with security enhancements embedded in the controllers, prototyped for real time simulation. This was used to evaluate the real time performance of ML-based ADM to ensure that the timing requirements of voltage control are met. Data integrity attacks were staged as injections in real-time over the wide-area network (WAN) within the testbed. The same test bed was used to test the attack scenarios put forth by the Red Team. Test results showed accurate and effective performance of ADM system in detecting and mitigating anomalies/attacks while keeping the grid stable and within the System Operating Limits (SOL), defined by the North America Electric Reliability Corporation (NERC).

ISU has produced three conference publications based on this work, all co-authored with Hitachi Energy, and a PhD thesis. ISU will also participate in planned panel sessions to disseminate their knowledge to IEEE and other standard making bodies, and cybersecurity stakeholders.

UI

University of Idaho supported the project by developing a cyber defense mechanism to detect power system oscillations triggered by attacks on generator exciters or power system stabilizers, locate the source of the oscillations and use a damping control scheme implemented in a shunt connected flexible ac transmission systems (FACTS) device. The team also included subsynchronous control interactions between type-3 wind turbines and series compensated transmission lines.

UI performed a threat analysis looking at vulnerabilities in synchronous generator controls that could lead to triggering forced oscillations. In addition, the threat analysis also explored approaches an attacker could use to create subsynchronous oscillations in systems with high penetration of wind generation.

UI tested the defense mechanism in a real time digital simulation environment. Tests were performed on a modified IEEE 12-bus dynamic test that included a large wind farm installed near a long transmission line. Series capacitor compensation was added to the transmission line. The damping control scheme was designed and subsequently implemented using a static VAR compensator. Cyberattack scenarios were created based on the threat analysis document, and the damping controller was tested against these scenarios.

The **Hitachi Energy** tasks encompassed:
a) Building the XFACTS hardware in the loop testbed. To demonstrate a successful cyberattack on an electrical substation and the mitigation methods against such attacks, validation with actual power system or using hardware-in-the loop (HIL) simulation testbed was built. HIL simulation offered the controlled test environment to evaluate power system operating conditions with the same hardware setup that can be found in the field. The HE testbed is composed of three major parts – a power system simulator, FACTS I/O devices, FACTS control devices, and a FACTS station communication network to interface the protection and control hardware with a time synchronized simulated environment. It was built with the following commercially available substation protection and control devices: four PS700-HE FACTS control and protection main computers; one PS741-ABB HVDC analog input devices, one PTP Ethernet managed switch; one Meinberg GPS; three unmanaged network switches, and one managed switch. These control and communication field devices were integrated into a power system model running in a real-time simulated environment.
b) Specifying, validation, and assessment of the threat models. All electrical substation data communication networks have cyber vulnerabilities. In the interests of security, these vulnerabilities will not be mentioned explicitly here but suffice it to say that vulnerabilities were attributed to infected external IEDs interacting with the FACTS controller. Additionally, by insider threats that has exploited the vulnerabilities associated with direct commands to control FACTS station power electronics via malicious voltage set point orders, unauthorized login attempts, and device

configuration changes. All the documented vulnerabilities were verified in the emulated test environment as feasible and credible. In the former, we conducted real time simulations with actual commercial hardware and the impact of such attacks on the operations of a HVDC station equipment were found to be detrimental to grid operations.

c) Design and validation of physics-based domain layer security functions for FACTS stations.

i. FACTS control and protection measurement security. A three-phase streaming AC state estimator (XSE) is prototyped to secure the sensor data in the communication data network. XSE imposes the FACTS system power flow equations into the AC measurements at fundamental frequency. The voltages and current measurements digitized by the field sensors located in the FACTS switchyard, were converted to phasor measurements at fundamental frequency, and time-synchronized by the MACH control system at the substation control room. The voltage and current phasor phasors were correlated by using Kirchhoff's laws for each of the FACTS active electronic circuits including thyristor-controlled reactor (TCR), thyristor switched capacitor (TSC), FACTS three phase transformer, and AC filters. The three phase AC state estimation model is designed to continuously estimate the state variables composed of grid side station voltage, FACTS busbar voltage, and voltages across the thyristor valves, and the thyristor firing angle. in a streaming fashion. The state estimator is designed to identify measurement points that potentially could be communicating erroneous AC measurements, either due to hardware failure or cyber intrusions. It could also provide estimates of these erroneous measurements or missing measurements caused by sensor outages. It calculates measurement residuals that indicates the distance between the measurement and its estimated value. The estimation is performed in a streaming fashion with high sampling rate to capture any abnormal residuals in real time. The XSE was designed for a FACTS station or for dedicated sub-systems within the FACTS station such as a Static Var Compensator containing TCR, TSC, and AC filters.

ii. Collaborative defense of FACTS controller and substation IEDs (CODEX). The CODEX security function is prototyped to add a security layer to a FACTS controller and the system of external IEDs interacting with the controller in an IEC61850 substation. The current and voltage measurements were digitized and converted to sampled value streams (SV or IEC61850-9-2) by a merging unit to an IEC61850 process bus. The FACTS controller received these SV and utilized by the CODEX security functions embedded within. The CODEX security function monitors the FACTS system for disturbance such as faults just like the external IEDs and perform a consistency check between the IED status changes with its own security features. When a malicious GOOSE message is sent to the FACTS controller, CODEX will determine its consistency with its own evaluation. The GOOSE message is ignored if it is malicious. In another case during an event, a GOOSE message may be suspended by a denial of service. In this case, CODEX will take over control and send the correct status to the FACTS controller. CODEX enables IEDs and the FACTS controller in a FACTS substation to collaboratively defend against cyberattacks.

iii. Series Capacitor security. A security enhancement to series capacitor controllers, called CAPX, was prototyped to secure high voltage series capacitor devices from malicious commands coming from external protection systems. A malicious command coming from a rogue external device can block or suspend the closing or opening of series capacitors potentially damaging high voltage apparatus such as circuit breakers, and worse can introduce loop flow disturbance into the power grid. CAPX works by internalizing the high voltage line and system protection into the controller. With the increasing use of series capacitors in high voltage systems to support renewable integration securing these devices from malicious control from external IEDs becomes a critical requirement to preserve grid resilience.

iv. STATCOM security. A security enhancement to STATCOM, called XDSE, is used to secure its controller from attacks on its measurements of DC and AC voltage, AC currents, and device setpoint. XDSE is composed of non-linear dynamical estimator, observer, residual calculation, and intrusion detection modules, that run in parallel with the STATCOM primary controller. Intrusion is detected if residual of the estimated states and the measurements exceeds a preset threshold.

v. FACTS Cyber Physical Security platform. We prototyped a cyber physical security platform called MACHGUARD geared for FACTS devices. It is designed to complement SIEM systems to protect against threats that penetrated deep into the control system. MACHGUARD is tightly embedded in the FACTS control system but does not impede its timely and proper operation. It provides situational awareness of the control system network and its devices as well as a cyber risk monitoring system based on Advanced Time Failure Propagation Graph (ATFPG).

d) Set up and Demonstration of XFACTS at BPA. The Hitachi Energy team made several trips to the Ross Complex substation in Vancouver, Washington and worked with BPA to set up the field demonstration testbed for XFACTS. The BPA-RTDS system was configured to run a model of BPA's Keeler 230 kV Static Var Compensator and a transmission network around the SVC to emulate the power system near field conditions required to test the security prototypes. We have configured: 1) analog-based communication for data transmission from BPA-RTDS to a PS741; 2) synchrophasor communication between BPA-RTDS and PS700 compatible server (SCM); 3) RTDS GTNET-SKT socket protocol-based communication between a PS700 compatible device and BPA-RTDS; 4) BPA-GPS time server communicating time stamps to BPA-RTDS and SCM, and three PS700. For demonstrating the XFACTS cyber security functions, two PS700 controllers were programmed with the MACHGUARD functions running at SCM; SCM running the AC state estimator; IEC 61850 compatible RED 670 relays subscribing to 9-2 sampled values and GOOSE messages; an emulated IEC61850 based SVC station; and BPA-RTDS as platform for the series capacitor security function. EtherCAT was used to coordinate the required information exchange between the PS700 and PS741. Syslog utilized the BPA-GPS server signal to support the communication network information to the SCM server.

PRODUCTS DEVELOPED UNDER THE AWARD

Conference papers

[1] Abhiroop Chattopadhyay, Alfonso Valdes, Peter W Sauer, Reynaldo Nuqui, *A cyber threat mitigation approach for wide area control of SVCs using stability monitoring*, 2021 IEEE Madrid PowerTech, Madrid, Spain, 28 June-2 July 2021. Recipient of the Basil Papadias Student Paper Award.

[2] Vivek Kumar Singh, Manimaran Govindarasu, Reynaldo Nuqui, *Impact Analysis of Data Integrity Attacks on FACTS- based Wide-Area Voltage Control System* 2021 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 16-18 Feb. 2021

[3] Abhiroop Chattopadhyay, Alfonso Valdes, Peter W Sauer, Reynaldo Nuqui, *A Localized Cyber Threat Mitigation Approach for Wide Area Control of FACTS*, 2021 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Aachen, Germany, 25-28 Oct. 2021

[4] B. Hyder, V.K. Singh, M. Govindarasu, and R. Nuqui, *Machine Learning-based Cyber-Physical Anomaly Detection in Wide Area Voltage Control Systems*, accepted for publication at the IEEE PES ISGT NA 2022, New Orleans, LA, Aril 22-28, 2022
[5] B. Hyder, V.K. Singh, M. Govindarasu, and R. Nuqui, *Anomaly Detection and Mitigation in FACTS-based Wide-Area Voltage Control Systems using Machine Learning*, accepted for publication at the IEEE PES General Meeting, Denver, CO, July 17 - 21, 2022

Status Reports
Quarterly Status Reports were regularly submitted to NETL as required.
Invention Disclosures
Two Invention Disclosures reported to DOE NETL.

APPENDIX A: HITACHI ENERGY FINAL REPORT

HITACHI
Inspire the Next

Final Technical Report

Cyberattack Resilient Flexible AC Systems - XFACTS

Acknowledgement of Government Support and Government License
This work was generated with financial support from the U.S. Government through Contract/Award No. DEOE0000897, and as such the U.S. Government retains a paid-up, nonexclusive, irrevocable, world-wide license to reproduce, prepare derivative works, distribute copies to the public, and display publicly, by or on behalf of the Government, this work in whole or in part, or otherwise use the work for Federal purposes.

Summary:

This report summarizes the activities conducted under the DOE-OE funded project DE-OE0000897, Cyberattack Resilient Flexible AC Systems – XFACTS. Hitachi Energy (HE), in collaboration with ABB Inc. (ABB), Bonneville Power Administration (BPA), University of Illinois at Urbana-Champaign (UIUC), Iowa State University (ISU), and University of Idaho (UI) pursued the development of a system of defense for Flexible Alternating Current Transmission Systems against cyber-attacks (XFACTS). A FACTS substation enhanced with XFACTS defense mechanisms will be capable of mitigating cyberattacks especially those that seek to control electrical parameters like voltage or current and interrupt the power flow in AC lines. It empowers existing FACTS controllers and associated intelligent electronic devices to detect and mitigate malicious intents to depress system voltages, destabilize power flows, trip AC circuit breakers, corrupt currents, and voltages, even if the malicious commands and the measurements have correct syntax. The XFACTS functions utilize the physics of active power electronic systems, control and protection, electric power engineering principles, and state estimation to bring more in-depth cyber defense closer to the protected FACTS substation devices.

The team developed and demonstrated the XFACTS system in an AC substation environment, via functional upgrades to existing firmware of commercial off-the-shelf FACTS station devices, and/or embedded hardware, without the need for additional instrumentation nor new instrumentation technologies. This is to ensure that the developed solutions will support the FACTS devices currently installed in the US electricity delivery infrastructure.

PROJECT NAME	PROJECT ID	RECEIVER		
Cyber Resilient Flexible AC Transmission Systems	PRJ-7710	Department of Energy		
PREPARED		STATUS	SECURITY LEVEL	
2022-03-31 Reynaldo Nuqui		Final	External	
APPROVED		DOCUMENT KIND		
2022-03-31 Debrup Das		Technical publication		
AUTHORS				
Reynaldo Nuqui, Jiuping Pan, HyoJong Lee, Anil Kondabathini, Liqi Zhang, Ghanshyam Gohil				
TITLE				
Final Technical Report: Cyberattack Resilient Flexible AC Systems				
OWNING ORGANIZATION		DOCUMENT ID	REV.	LANG.	PAGE
Hitachi Energy		8DAB002343	A	en	1/45

Hitachi Energy

The team focused first on developing a hardware-in-the-loop test bed representing an alternating current electrical substation equipped with FACTS devices and relays utilizing the EtherCAT protocol and IEC 61850. At Hitachi Energy this test bed consisted of a Real Time Digital Simulator, HE MACH PS 700 main computers, HE MACH PS 741 analog I/O, and HE Relion 670 transmission relays. Then, focus shifted to advancing the state of the art in cyber defense of FACTS equipped substations, namely secure FACTS data communication system; secure FACTS circuit breaker control commands; secure FACTS switch bypass commands; secure control device configuration change. This effort was preceded by identification of credible threats to FACTS control devices through simulated cyberattacks and evaluation of their feasibility and severity in a cyber physical test bed. The cyber threats and attack cases formed the basis for the development of the cyber security algorithms.

An independent red team analyzed the designs of XFACTS with the objective of exposing vulnerabilities in the defense mechanisms. The project team then emulated adversarial actions identified by the red team and evaluated performance in the face of identified cyberattacks. The team subsequently recalibrated the functions to a higher level of resilience against discovered vulnerabilities.

XFACTS final test for deployment readiness was staged at a 230 kV AC substation within the Bonneville Power Authority service area. BPA and HE demonstrated the field performance of XFACTS in a substation environment, with staged cyberattacks on the control system and successful defense from the security functions.

The tasks developed during the project followed the project plan and consisted of: threat model specification for FACTS stations, wide area measurement systems controlling FACTS and SCADA systems controlling FACTS; development of control logic extensions that detect intrusion on normal and emergency FACTS control commands; design of a streaming state estimator that detects false measurement injection attacks on the FACTS communication system; FACTS control devices; validation of the FACTS security algorithms in a hardware-in-a-loop laboratory setup at Hitachi Energy; and field demonstration of the developed system of FACTS cyber security functions and devices at Bonneville Power Administration (BPA) within their Ross AC substation.

The Hitachi Energy Research team transferred the developed technology to HE FACTS product groups for inclusion into their product roadmap.

The accomplishments of the FACTS project have advanced the state of the art in cyber security of HVDC substations by adding intelligence to existing devices that is based on the underlying physics of the protected electrical system, as summarized in the next section.

Contents

1. Introduction 5
1.1. Purpose 5
1.2. Scope 5
1.3. Definitions 5
1.4. Structure 5

2. MACHGUARD 6
2.1. Problem Description 6
2.2. Requirements 7
2.3. Solution 7
2.4. Results 9
2.4.1. USE CASE 1: Login attempts 9
2.4.2. USE CASE2: DoS attack by malicious ICMP 10
2.5. Conclusions 12
2.6. Future Work 12

3. STATE ESTIMATOR 12
3.1. Problem Description 12
3.2. Requirements 14
3.3. Solution 14
3.4. Results 16
3.4.1. Case study 1: Static Var Compensator and Anomalies on Transformer Measurements 16
3.4.2. Case study 2: Cyberattack on TCR measurement 17
3.4.3. Case Study 3: Cyberattack on TSC measurement vs. capacitor degradation 18
3.5. Conclusions 19

4. CODEX 20
4.1. Problem Description 20
4.2. Requirements 20
4.3. Solution 20
4.3.1. Test Bed Description 21
4.3.2. Realization of SVC station protection 24
4.4. Results 26
4.6. Conclusions 29
4.7. Future Work 29

5. CAPX 29
5.1. Problem Description 29
5.2. Requirements 31
5.3. Solution 31
5.4. Results 31
5.5. Conclusions 32
5.6. Future Work 32

6. XDSE 33
6.1. Problem Description 33
6.2. Requirements 33
6.2.1. STATCOM Control Structure 34
6.2.2. STATCOM Control: Vulnerability Analysis 36

6.3. Solution 40
6.4. Results 42
6.4.1. Test Bed Description 42
6.4.2. Results 42
6.4.3. Performance Validation 43
6.5. Conclusions 44
6.6. Future Work 44
7. Additional Information 45
7.1. Listing of related documents 45
8. Addendum 45
9. Revisions 45
9.1. Reviews 45

1. Introduction

1.1. Purpose

The purpose of this report is to disseminate the technical accomplishments of this RD&D project. The goal is to communicate the advancement in state of the art in cyber physical security, through the use of physical models and control and protection domains, as technical basis for cyber defense mechanisms. These defenses were conceptualized, developed, tested, and demonstrated to validate their performance in field conditions.

The target group for this report are asset owners, manufacturers, and operators of FACTS systems.

1.2. Scope

This report described the five technical functions developed in the XFACTS project in fulfillment of the scope of work laid out in the project's statement of objectives, and project plan, and technical narrative submitted to the Department of Energy.

This report does not describe security functions outside the scope of work, including but not limited to the existing cybersecurity standards or frameworks. References to such technologies are cited as appropriate.

1.3. Definitions

Cyber physical security or CPS	Methods and systems developed to address security concerns of industrial control systems controlling physical systems
MACH	Hitachi Energy control system for FACTS and HVDC
Relion	Hitachi Energy substation automation solutions for equipment and line protection
State Estimator	A CPS system used to estimate the states of FACTS operating at steady state and detect anomalies or errors in the sensor system
CODEX	Collaborative defense of protection and control devices in a FACTS station
CAPX	A defense mechanism against attacks by external systems on series capacitor controllers
XDSE	A defense system to secure STATCOM controllers from attack
MACHGUARD	A cyber physical security platform for FACTS control systems

1.4. Structure

This report has the following structure.

Section 1 Introduction (this section) describes the purpose and scope for this report as well as terms, abbreviations and acronyms used.

Section 2 MACHGUARD describes the conceptual cyber physical security platform

Section 3 State Estimator describes the novel concept for a streaming state estimator application for error and anomaly detection in a FACTS sensor system

Section 4 CODEX describes the collaborative defense on intelligent electronic devices and FACTS controllers in an IEC61850 environment

Section 5 CAPX describes the defense mechanims in series capacitor controllers against external threats

Section 6 XDSE describes the defense mechanism to secure STATCOM from attacks to its controllers

2. MACHGUARD

2.1. Problem Description

Various digital devices and control units are used to control and protect FACTS devices, such as a gateways, human-machine interfaces, controllers, and network devices as shown in Figure 1. These digital devices in FACTS provide many advantages for control and protection but could be exposed to cyberattacks.

The control and monitoring of the FACTS device is done both locally and remotely. Local control collects local sensor information into the control device as an integral part of FACTS operation. This operation does not require external input, so it is relatively secure from remote cyberattacks but vulnerable to internal attacks. On the other hand, remote control is imposed by external systems such as central dispatch, wide area system, and higher-level protection. In this case the external input could be vulnerable to cyberattacks to these external systems. FACTS stations are normally equipped with monitoring and logging software (e.g., Syslog, Firewall, Anti-virus software, etc.) to protect them from cyberattacks.

Figure 1 shows the overall network diagram of the FACTS control system that includes network security. The FACTS control system consists of operation workstation (OWS) for HMI, gateway for external connection, GPS for time synchronization, anti-virus system (AVS) for detecting malware/virus, firewall for detecting unauthorized access, system management control (SMC) for collecting system information, and control units for control/protection of FACTS devices. The firewall, AVS, and SMC devices in the aim to detect and mitigate the external cyberattacks such as Man-in-the-middle attack, DoS attack by remote access, injection attack from the remote access point, etc. A generic FACTS system is generally secured by a Security Information and Event Management (SIEM) system from cyberattacks.

However, cyberattacks are not limited to the external attacks. They are also caused by illegitimate access or insider threats. For example, an insider can insert an infected USB into an operation computer in substation that could deploy a malware so as to cause a malicious command or a DoS attack.

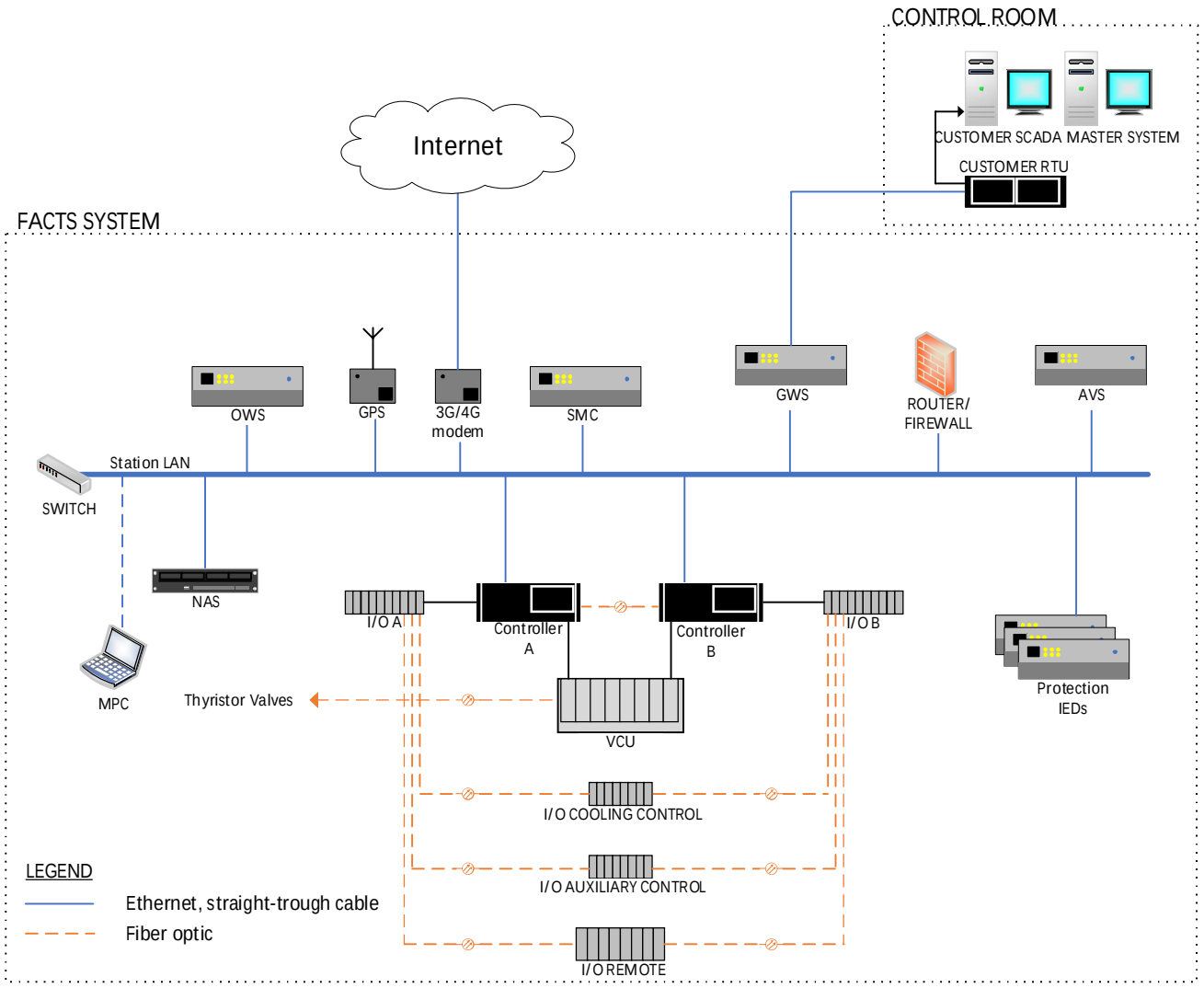


Figure 1 overall network diagram of FACTS control system

2.2. Requirements

SIEM systems described prior are not sufficient to protect against insider threats. What is required is a security system that is deeply embedded in the FACTS control system with the ability to monitor the control and protection devices in real time for anomalies. Obviously, this system must not impede the timely and proper operation of the control and protection system but has situational awareness beyond what is provided by SIEM. Ideally, this system must possess its own HMI to allow network security personnel and FACTS operator to make timely decisions in case of a cyberattack. Additionally, such system must also provide the security state of the controller, that is, some level of security risks depending on the network condition.

2.3. Solution

To defend against internal cyberattacks, a conceptual security risk monitoring system is proposed and is called MACHGUARD. It uses a multiple classifier security risk monitoring systems based on Advanced Time Failure Propagation Graph (ATFPG). The ATFPG is a graphical model that contains the cause-effect relationship between (1) failure modes, (2) system behavior discrepancies, and (3) failure propagations. When a fault occurs in a system, discrepancies appear between normal and abnormal behavior. Once the abnormal behavior is observed, it may trigger other discrepancies, and then the system will reach a steady-state status after some time window. Since each failure mode can create a specific propagation path to the final status of a system, the

attack sequence and anomalies can be regarded as the propagation path and discrepancies in the cyber system of FACTS, respectively. A coordinated cyber-attack should follow the specific attack sequences to reach an ultimate goal (e.g., change voltage set points or control FACTS switches). Thus, a coordinated cyber-attack can be identified by analyzing the attack sequences of the FACTS system.

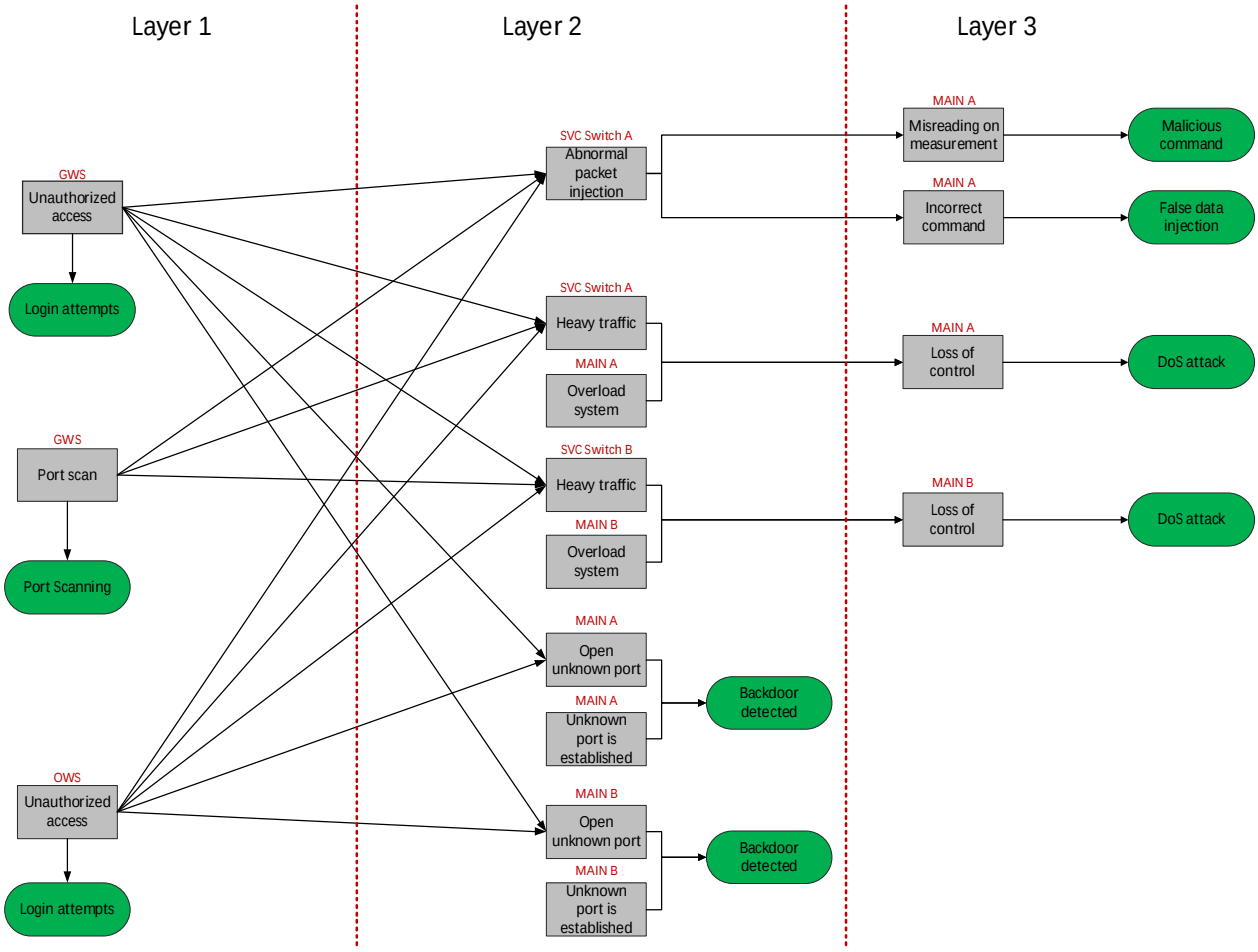


Figure 2 An Example of the advanced timed failure propagation graph model for FACTS control system

The principle of this method is that the attacker should successfully perform a series of sub-goals to achieve the final goals such as DoS, injecting malicious commands, and/or false data injection. The ATFPG uses evidence such as monitoring data, logging data, and sensor measurements to identify the current cyber-attack activities and the potential risk. Note that ATFPG can expand its model based on the extra monitoring features from security information and event management (SIEM) or external monitoring tools.

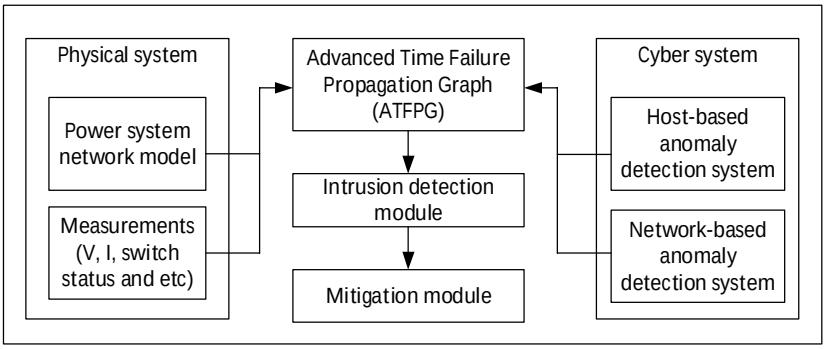


Figure 3 The proposed multiple classifier security risk monitoring system

Figure 3 shows an overall design and structure of the multiple classifier security risk monitoring systems (MCSRM), which is an analytical engine of MACHGUARD. The ATFPG module receives both physical system and cyber system data to process the probability of cyber intrusion, and the results will be sent to the intrusion detection module to identify the cyberattacks in the FACTS system. Due to the connectivity of the cyber and physical system, any control actions should be initiated from a cyber system, and the result of the control action needs to follow the designated ICT structure. Meanwhile, the result of control action will impact the physical system, and the impact can be estimated by the measurements from the physical system. For instance, if an Energy Management System changes the set point of bus voltage of the FACTS system due to a voltage instability issue, the command should come from the control center to the substation gateway where the FACT system is installed. Then the command will be forwarded from the gateway to the FACTS controller, and then the controller will issue the switching commands to the appropriate devices. After successfully finishing the switching action, the changed switch status and measurements can be reported to the controller. However, if the command is not issued via substation gateway but rather from a station communication bus to the FACTS controller, it will generate a discrepancy between normal operation and cyber intrusion. Then the proposed MCSRM can identify the intrusion even though the HADS and NADS can't detect it (since the command is valid).

The concept of MACHGUARD as implemented in this project consisted of the following hardware and software

- Hardware
    - FACTS controller
    - Data collector
    - Time synchronization device (GPS and PTP switch)
    - Managed network switch (SVC LAN switch)
- Software
    - Windows operating system (Windows 10 or Linux)
    - System event loggers
    - Event forwarder
    - SQL server

The MACHGUARD collects system information using the Syslog protocol (RFC 3164). The collected Syslog data is stored in the database to avoid unauthorized modifications. Additionally, it requires installing the event logger forwarder provided by a vendor or 3rd party's forwarding software if the operating system does not have the event log forwarder

2.4. Results

MACHGUARD uses a testbed which consists of two MACH controllers, one SCM server, and one SVC LAN switch. The method uses the event logs on these devices to determine the type of attacks and potential risk level of the FACTS control and protection system. This report addresses two use cases; 1) Login attempts on MACH controller and 2) malicious ICMP packet injection.

2.4.1. USE CASE 1: Login attempts

The login attempts case is simulated using Kali Linux which has a tool to generate fake login packets via the remote desktop protocol (RDP) with various combinations of username (ID) and password (PW). The failures of

login attempts are captured in the target device (in this case, FACTS controller) and transferred to SCM DB and MIMS DB in form of Syslog format every 10 seconds as shown in Figure 4.

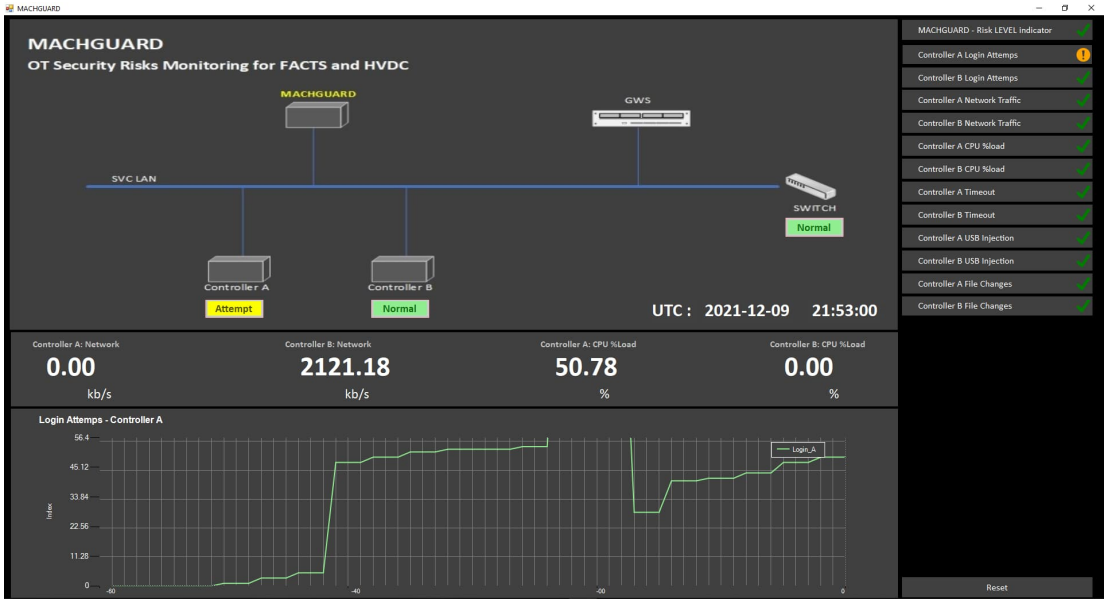


Figure 4 An HMI of MACHGUARD for login attempt case

Table 1 Average detection time for Login attempt case

Target device	Detection time
Controller A	21 sec
Controller B	19.6 sec

The login attempts are captured by the standard monitoring feature in the controller. Therefore, any failures of login attempts are detected by MACHGUARD.

2.4.2. USE CASE2: DoS attack by malicious ICMP

In general, the Internet Control Message Protocol (ICMP) is used to check the availability (heartbeat) of the target device. However, a cyberattacker can also use it as the DoS attacking tool by sending a large number of ping packets to the target device. Figure 5 shows both cases of normal and abnormal ICMP sequences between individual and target.

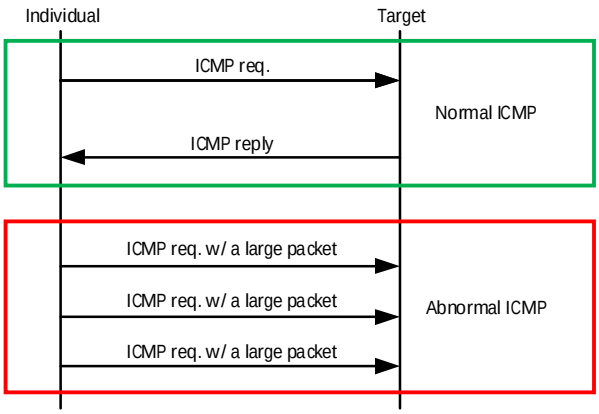


Figure 5 An example of sequence of both normal and abnormal ICMP

As illustrated in Figure 5, this malicious ICMP can generate a large number of packet and transmit it to the target device – in this case to the FACTS controller A/B continuously. The target device responses to the individual by replying ICMP replay but the individual ignores the reply signal as abnormal case. As a result, the target device eventually timed out the connection. However, this ICMP DoS case does not interrupt the CPU of the target device, so it does not slow down the FACTS controller. The figure below illustrates how MACHGUARD detects the DOS attack

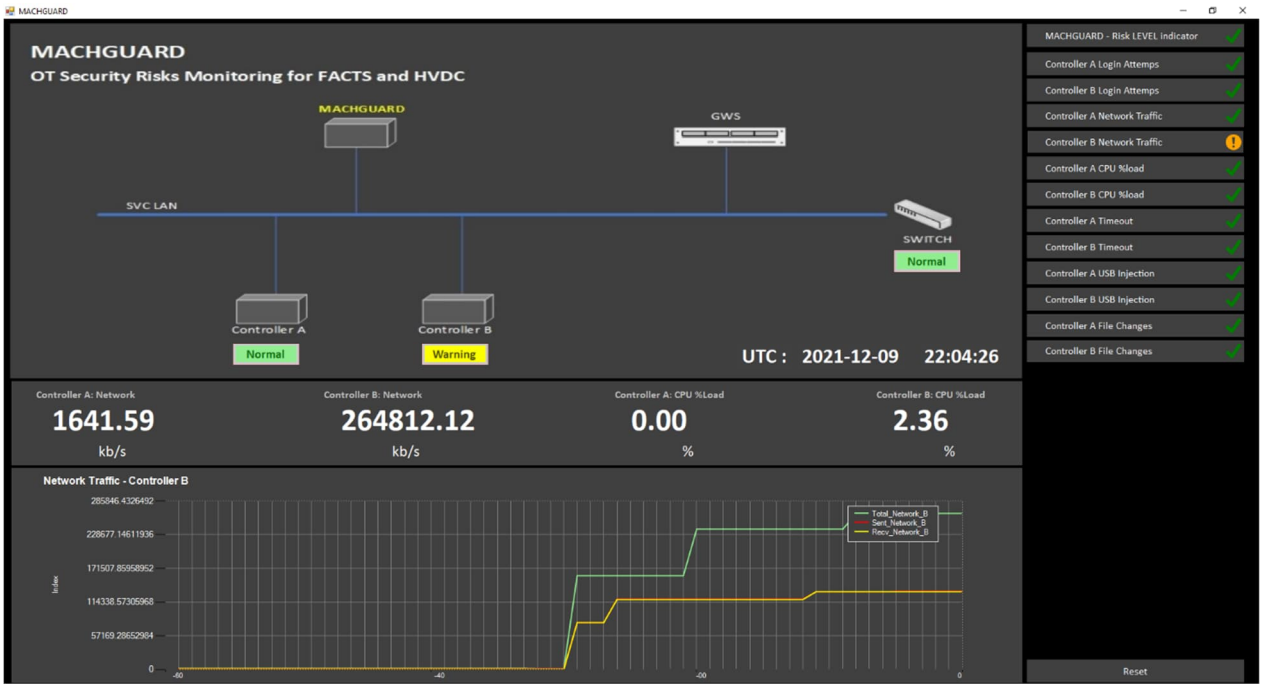


Figure 6 An HMI of MACHGUARD for DoS case using ICMP

Table 2 shows the average detection times for the ICMP cases where both DoS and DDoS cases were detected.

Table 2 Average detection time for ICMP case

		Detection time in sec
Denial of Service	1	32.8
	2	25.2
	3	25.3
	4	26
	5	25.5
Distributed Denial of Service	6	25.3
	7	20.3
	8	23.1
	9	22.3
	10	25

2.5. Conclusions

MACHGUARD uses the internal system information collected from FACTS controllers and internal network devices directly. Based on the collected data, MACHGUARD can detect abnormal activities in the system and identify the location of the attacker and device/system-level risk. The performances of MACHGUARD are discussed in Section 2.4 along with its detection time. Due to the limitations of the XFACTS testbed, the detection time has a little lag of about 20 – 40 seconds from the actual event. However, MACHGUARD provides a detection rate of 100% once it received system information from its database at given tests. Even though MACHGUARD is specially designed to defend against attacks that have penetrated the SIEM layer in FACTS control and protection system, it uses a standard system information technique called Syslog protocol (RFC 3164). Therefore, the MACHGUARD concept is not vendor specific. Similarly, MACHGUARD can also be deployed to HVDC systems.

2.6. Future Work

In MACHGUARD, the ATFPG model has been used to check the potential attack path and risk level for the FACTS control system. This model only covers the known attack path that has been encountered in the ATFPG model. In other words, the ATFPG model should be developed with extra caution. To deal with novel attacks, the ATFPG model can replace with Hidden Markov Model (HMM). Especially, profile HMM is developed to find the potential sequence from the series data.

3. STATE ESTIMATOR

3.1. Problem Description

With a high-level integration of power system networks, and the emerging digital technology which connects such big networks, control systems of FACTS could be a potential target for cyber-attack, which would cause short-term system shutdown or long-term system failure. This poses challenges and threats to the goal of providing resilient power supply to the customers.

A potential attack can be directed towards the FACTS measurement system. A FACTS station is composed of a matching sensor system to provide the measurement needed for the control and protection functions. For example, a typical static var compensator would have its measurements installed at locations as shown in Figure 7

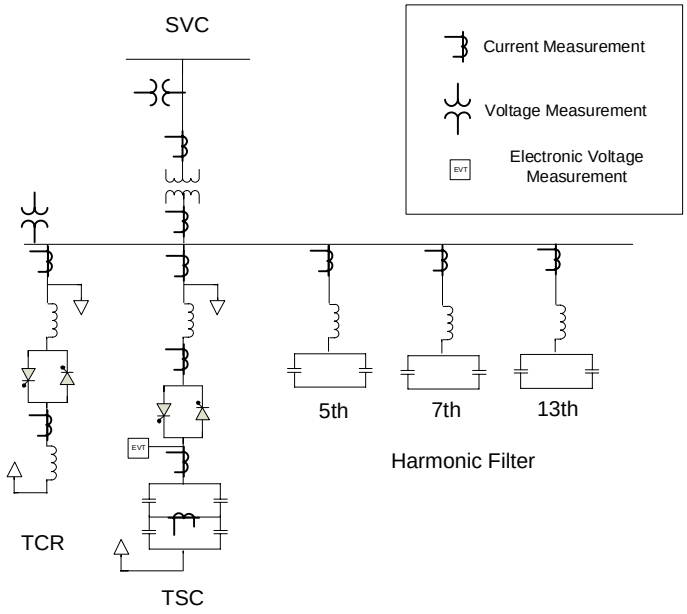


Figure 7. Typical Voltage and Current Sensor Placement in a Static Var Compensator

It is possible that one or more of these measurements could be in error. The measurement error could be caused possibly by malicious intent to falsify them including but not limited to false data injection or attack on the configurations of the sensor devices.

The errors could also result from wear and tear, aging, problems, or faults in with the signal processing unit, issues with the I/O boards, etc. It could also be caused by misconfigured devices. Sometimes the errors are not high enough to be detected by normal consistency checking and so the errors will remain undetected and uncorrected by the monitoring system. Under these conditions, it is possible that duplicate sensors on the same measuring point will not agree on the measured values, and the sensor in error will have to be identified before it creates issues such as sending the wrong measured values to the controllers or worst to the protection system causing it to mis-operate.

Being an essential part of the FACTS system, Static VAR Compensator (SVC) typically includes Thyristor-Controlled Reactor (TCR), Thyristor-Switched Capacitor (TSC), and harmonic filter. A digital control system is usually employed to receive measurements from the field, and commands from the operator and send pulses to the thyristor valve of TCR and TSC. Due to the vulnerability of the digital control system, a cyber-attack could aim at controlling the thyristors in an unwanted manner by means of attacking the measurement signals, which would result in system shutdown or failure.

The basic problem is how to identify measurements that are compromised and therefore inconsistent with the rest. Here state estimation could be a good technical basis.

State estimation has been used describe underlying behavior of a system at any point in time by taking all available measurements in real time. The overall approach is to use a model to predict the behavior in a particular state, and then compare that behavior with the actual measurements to determine which state or states would most likely describe that behavior. In that process, erroneous measurements will be identified, such as caused by cyberattacks on the measurement system.

If we define the model collectively as the function vector $\boldsymbol{h}(\boldsymbol{x})$ and the state to be the vector $\boldsymbol{x}$, then we can assume that the measurements $\boldsymbol{z}$ in the system will deviate from the model by the error vector $\boldsymbol{e}$.

$$\boldsymbol{z} = \boldsymbol{h}(\boldsymbol{x}) + \boldsymbol{e} \tag{3-1}$$

In most cases, FACTS systems operate at steady state. Hence, a logical steady state representative model could be a power flow model at fundamental frequency. In the power flow model, the states are described by

the nodal voltages in the FACTS circuit, and the currents are calculated from the state estimates and the circuit parameters, that is, resistances, inductance, capacitance, etc.

Within this context of steady state operation, state estimation could be formulated as an optimization problem that seeks to minimize the weighted average of measurement residuals - the differences between the actual measurement readings by the FACTS control system and its estimated value. If we define the j-th (current or voltage) measurement to be, z_j, then for a system composed of m number of measurements, the objective of state estimation is to minimize the function $J(x)$;

$$J(\boldsymbol{x}) = \frac{1}{2}\sum_{j=1}^{m}\left(\frac{z_j - h_j(\boldsymbol{x})}{\sigma_j}\right)^2 \quad (3\text{-}2)$$

where $h_j(x)$ is the estimated value of the j-th measurement, and $1/\sigma_j$is the weight imposed on the j-th measurement.

Here $\boldsymbol{x}$ is an n-sized system state vector, and each i-th element in the vector x_i is chosen to be the unique nodal voltages in the FACTS system. The states fully describe the power flow or current flow behavior in the circuits. The currents in the model can be conveniently described by Kirchhoff's laws with the measurement functions $\boldsymbol{h}(\boldsymbol{x})$ where each element $h_j(\boldsymbol{x})$ corresponds to each estimated measurement.

Thus, formally the measurement vector $\boldsymbol{z} = [\boldsymbol{I}\ \boldsymbol{V}]^T$ of size m is composed of both voltages set V and current set I.

3.2. Requirements

Requirements to a local FACTS station state estimator are dependent on the performance expectations. Being a novel concept, these requirements have yet to exist. However, we freely declare here what could be the specifications for a streaming state estimator when put into action.

Inputs

Being integrated with a FACTS controller, the required inputs shall be analog measurements of currents and voltage signals sufficiently digitized to the accuracy required by existing controllers.

Outputs

The output shall consist of 1) calculated errors in the measurements, also known as measurement residuals in state estimation; 2) location of compromised or erroneous sensors; 3) calculated measurements; 4) calculated states or voltages

Speed

One second scan rate shall be a minimum of one state estimation update every second.

Parameters

Circuit parameters and topology are required by the estimator. These includes such FACTS circuit parameters as TCR inductance, TSC capacitance, AC filters capacitance, inductance, resistance, transformer leakage reactance, phase shifts, tap, FACTS topology, circuit diagram,

3.3. Solution

Newton's method or more popularly known as Newton-Raphson method was used to solve the state estimation problem (3-1). In this numerical approach whose objective is to find the roots of the objective function $J(\boldsymbol{x})$, which are the states $\boldsymbol{x}$. Literature is profused with information on the iterative solution, see SE Monticello book reference for example. The specific approach taken here is presented.

Numerical iterative procedure

The state estimate $\hat{\boldsymbol{x}}$ can be obtained by the following iterative procedure:

$$(\boldsymbol{H}^T(\boldsymbol{x}^v)\boldsymbol{R}_z^{-1}\boldsymbol{H}(\boldsymbol{x}^v))\Delta\hat{\boldsymbol{x}}^v = \boldsymbol{H}^T(\boldsymbol{x}^v)\boldsymbol{R}_z^{-1}\Delta\mathbf{z}(\boldsymbol{x}^v) \quad (3\text{-}3)$$

$$\boldsymbol{x}^{v+1} = \boldsymbol{x}^{v+1} + \Delta\boldsymbol{x}^v \quad (3\text{-}4)$$

Here v is the iteration count each time (3-3) and (3-4) are solved and repeated until convergence is achieved. Convergence is achieved by the error in the state estimate becomes sufficiently small according to the convergence criterion $\Delta\boldsymbol{x}^v \leq \epsilon$.

$\boldsymbol{R_z}$ is the variance matrix corresponding to the error vector ***e*** as described in (3-1). We assume that ***e*** has a zero mean. Typically, the variance matrix is set using the accuracy of the sensors used in the measurement system.

$\boldsymbol{H}$ is the matrix of derivatives or Jacobian of the function $\boldsymbol{J(x)}$. For an m -sized measurement vector, and n sized state vector, the $\boldsymbol{H}$ matrix is an mxn.

A key challenge is to find the expressions for the derivatives. Each of these mn Jabonian elements were derived by hand here in the project as closed form expressions.

State and measurement variables

The power flow equations are expressed in polar coordinates. This coordinate system conveniently express the measurements and state variables in magnitude and angle. It puts the extra requirement of mapping the analog inputs into polar form using Fourier transform. Thus, the voltage measurements are expressed as $\boldsymbol{v} = \boldsymbol{v}\angle\boldsymbol{\theta}$ while currents are expressed as $\boldsymbol{I} = \boldsymbol{I}\angle\boldsymbol{\theta}$

Sensor Error Modeling

Sensing equipment, like the voltage and current instrument transformers are not 100% accurate. It is required to model inherent sensor errors. Here we assume that sensor errors follow a normal distribution with zero mean and a standard deviation dependent on the sensor accuracy classes.

Solution Flow

The objective of state estimation is to detect any inconsistent measurement(s) using the physical model of the FACTS system as a type of security filter. Figure 8 (also Figure 7) shows the placement of measurements in a typical FACTS station of SVC type. A cyberattack scenario could relate to spoofing one or more of these measurements. This could be achieved by man-in-the middle attacks, a malware that injects false data into the digital communication of the controller, etc.

A high-level design of the intrusion detection and mitigation system based on state estimation is shown below. It starts by receiving synchronized values of the analog measurements from the sensors, which are digitized by the field sensors. These signals are then transmitted to the control room via digital communication, where they are converted into phasors for processing by the state estimator. The measurements are continuously received by the controller. Depending on the hardware and processing capability of the host platform, the state estimator can receive the signals at the same rate or a lower rate, as indicated in the figure where FACTS control measurements are sampled between ½ Hz to 60 Hz and fed in real time to the state estimator. The estimator is composed of the digital model of the FACTS system, which include the impedances of the various components, from power electronics switches to static devices such as reactors and capacitors, connectivity of the components, and accuracy and or bandwidth of the measurement sensors. The state estimator calculates the state estimate in real time and more importantly detects erroneous measurements caused by cyber intrusions such as false data injection via man in the middle attacks. Note that state estimator is streaming continuously, and the detection and mitigation actions are happening in speeds compatible with the FACTS controller speed.

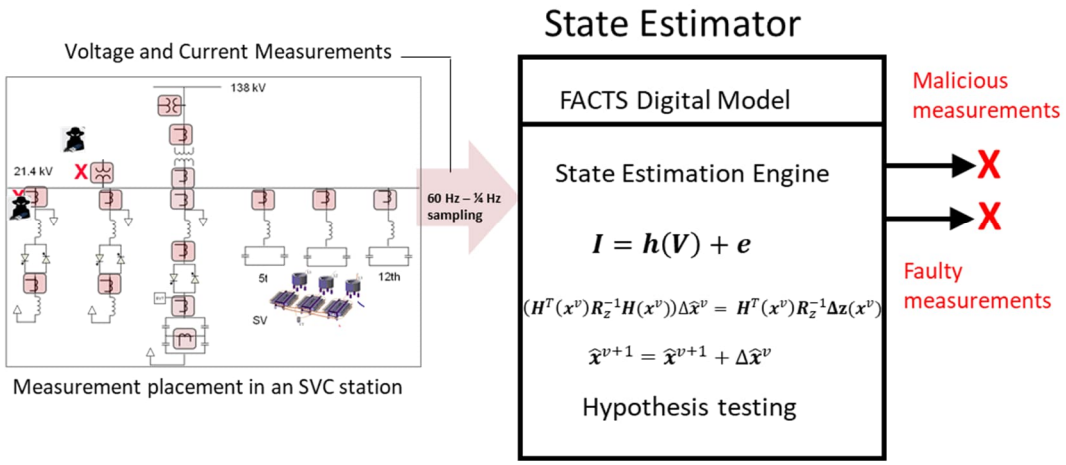


Figure 8. State Estimator Design with attack and mitigation illustration

The state estimator as a security function is a consensus mechanism by which the various sensing devices in a FACTS station collaborate to detect and mitigate a cyberattack. The improvement proposed here over the earlier methods is that the power system signals in a FACTS station exhibit different signatures due to the switching of the semiconductor devices.

3.4. Results

3.4.1. Case study 1: Static Var Compensator and Anomalies on Transformer Measurements

This function was tested in a STATIC VAR COMPENSATOR (SVC). SVC is a type of shunt connected FACTS used to support system voltage by regulating the reactive power (vars) at its terminals. The regulation is achieved by modulating the effective susceptance of the FACTS by varying the firing angle of the thyristors – the main PE device in SVC.

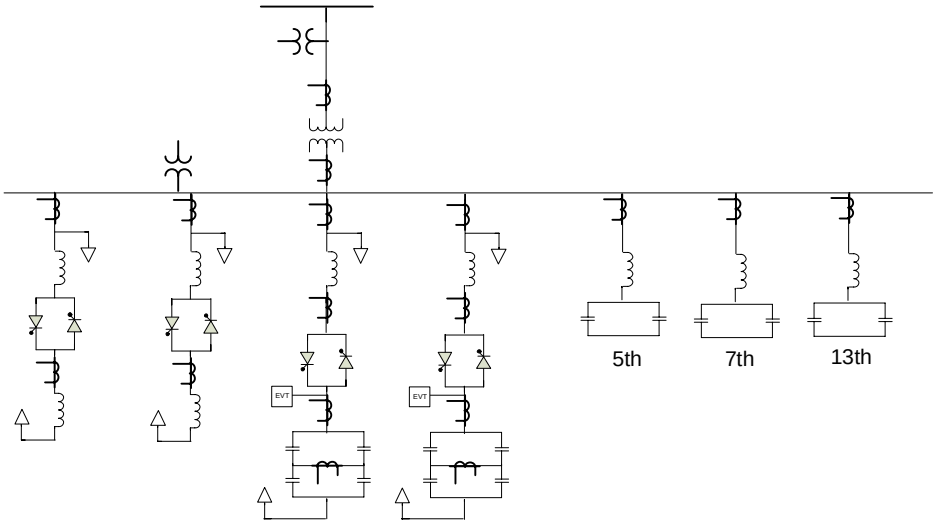


Figure 9. SVC Test System

State Vector and Measurement Vector for SVC

With reference to the measurement placement in Figure 9 and the indicated variables the state vector includes: 1) primary voltage of transformer, $\boldsymbol{V_S}$; 2) secondary voltage of transformer, $\boldsymbol{V_{AC-line}}$; 3) TCR valve voltages, $\boldsymbol{V_t}$;

4) TSC valve voltage, $\boldsymbol{V_c}$; and the thyristor firing angle, α. Note that all voltages are in phasor form with magnitude and angles. The firing angle is scalar.

$$\boldsymbol{x} = (\boldsymbol{V_S}\ \boldsymbol{V_{AC-line}}\ \boldsymbol{V_t}\ \ \boldsymbol{V_{t2}}\ \ \boldsymbol{V_c}\ \ \boldsymbol{V_{c2}}\ \ \alpha\ )^T \quad (3\text{-}5)$$

Each of the vector elements of these matrices are of size 6 representing individual phase A, B, C measurements of magnitude and angle.

The $\boldsymbol{m-vector}$ of measurements $\boldsymbol{z}$ is composed of all the available measurements, currents, and voltages. Specifically, for the measurement placement shown for the SVC

$$\boldsymbol{z} = (\boldsymbol{V_S}\ \ \boldsymbol{V_{AC-line}}\ \boldsymbol{V_t}\ \ \boldsymbol{V_{t2}}\ \ \boldsymbol{V_c}\ \ \boldsymbol{V_{c2}}\ \ \boldsymbol{I_G}\ \ \boldsymbol{I_{ac-line}}\ \boldsymbol{I_t}\ \ \boldsymbol{I_{t2}}\ \ \boldsymbol{I_c}\ \ \boldsymbol{I_{c2}}\ \ \boldsymbol{I_s}\ \ \ \boldsymbol{I_L}\ \ \ \boldsymbol{I_{F-5}}\ \ \boldsymbol{I_{F-7}}\ \ \boldsymbol{I_{F-12}}\ )^T + \boldsymbol{e}^T \quad (3\text{-}6)$$

Similar to the state vector elements, each of the vector elements of these matrices are of size 6 representing individual phase A, B, C measurements of magnitude and angle.

Sensor error modeling

Monte Carlo simulation was performed to generate normally distributed random numbers (error factors) assuming various sensor accuracies. The ideal measurements are multiplied with the generated error factors, and added with themselves, resulting in the artificial field measurements.

Measurement attack modeling

Magnitude scaling attack, typically ranging from 0.8 to 1.2 in this study, is multiplied with the artificial field measurement, which is then processed by the DFT algorithm. For simplicity, angle attack is made after the DFT data processing stage, which could also be realized by shifting the artificial field measurements.

Numerical Results

The SVC test system consisted of 120 measurement variables and 42 state variables. Following the SE run a record of the residual vector is plotted in Figure 10. A threshold of 0.1 on the absolute value of the residuals is set to detect anomalies on the data; they are plotted as red lines in the figure. In this scenario anomalies on the transformer primary current and secondary current magnitudes and angles, on all phases A, B, C were detected; they are encircled with red.

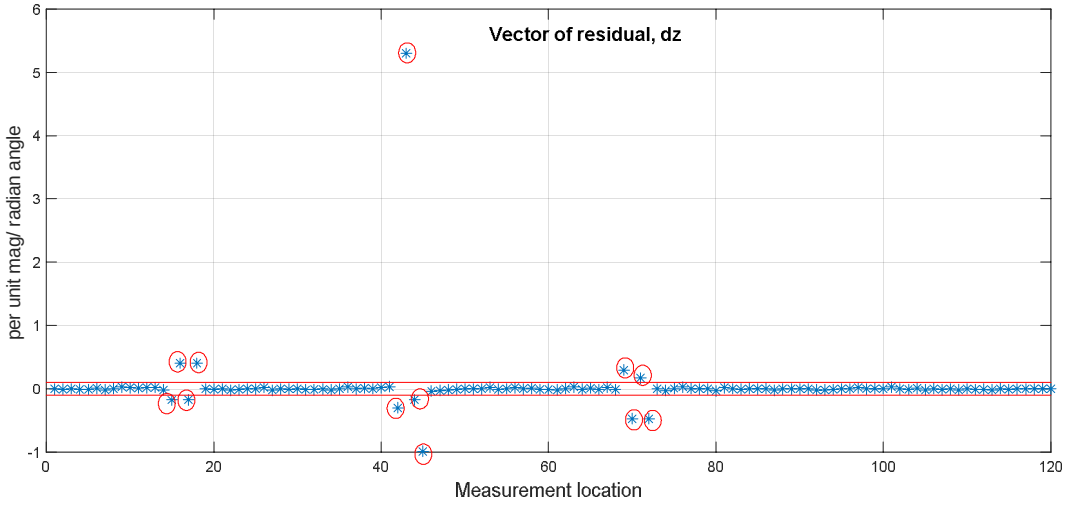


Figure 10. Residual vector following the state estimation run for the SVC test system

3.4.2. Case study 2: Cyberattack on TCR measurement

TCR consists of reactors and press-pack thyristor valves. Thyristor firing in an unwanted manner is called thyristor misfiring. It could be the result of physical failure of digital controller or driving circuit, for example, loss of reference, measurement noise, or signal pick-up on the gate lead. It could also be the result of cyber-attack, for

example, intrusion of the attacker to the digital controller and maliciously modify some of the key parameters in the control loop, either measurement processing unit or reference point.

Checking for misfiring can only be done by checking the SCR current waveform with an oscilloscope. A small misfire, or even a quite significant one, won't stop the SCR working. However, it may have a degrading effect on other equipment which may not be apparent immediately. Therefore, in order to improve asset management capability, it is essential to monitor and defend the SVC station in terms of physical-induced degradation/fault and cyber-attack-induced degradation/fault.

Cyberattack from two different levels is proposed in this study, namely, the component level attack and system level attack. Either attack will cause overcurrent or overvoltage on the SVC components. The attack could also be categorized as strong attack where protection threshold is usually exceeded and circuit breaker will trip and system will cease operation, and stealth attack where protection threshold is not met, and the system is operating in an accelerated degradation speed.

Simulation in MATLAB/Simulink is carried out to investigate impact of potential cyber-attack. An example of attack on voltage measurement data processing unit is shown below. Repetitive signal is maliciously injected to the voltage measurement processing unit that push the TSC capacitor current to just below its protection threshold. It will result in accelerated degradation TSC capacitors and shorten its lifetime, which results to capacitor bank failure before regular maintenance comes in. One indicator for the cyber-attack could be the repetitive firing angle change of the TCR, as shown in Figure 11, which could be added to the cyber-attack detection function.

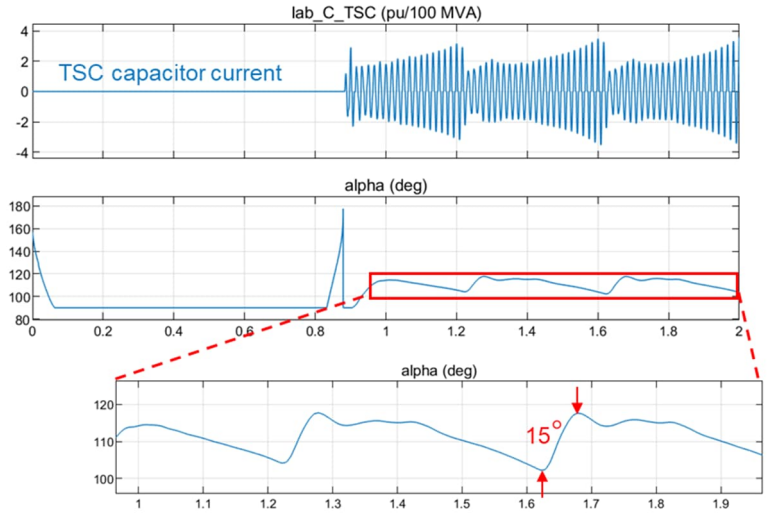


Figure 11 Simulation waveforms of stealth attack on voltage measurement

3.4.3. Case Study 3: Cyberattack on TSC measurement vs. capacitor degradation

A MATLAB test bed was used to test the security function against cyberattack on TSC measurement. The SVC is rated at+/-330 MVA (mega volt amperes) connected to the electric grid at 138. kV voltage via a three phase AC transformer rated 138 kV at the primary and 21.4 kV on the secondary. The SVC has two thyristor-controlled reactors (TCR) connected in parallel to a thyristor switched capacitor (TSC). In addition, the SVC has three shunt connected filters tuned for the 5th, 7th, an 12th harmonic. The control system is based on a generic SVC control model available in MATLAB.

Test use cases can be categorized into 5 groups are listed below:

1. Base cases where there is no degradation or attack
2. TSC capacitor degradation
3. Scaling attack on TSC current measurement

4. Bias attack on TSC current measurement
5. Signal delay attack on TSC current measurement

Table 3 summaries the performance of the SE defense mechanism. The dependability metric is defined as the percentage of cyberattack cases that were detected. On the other hand, false negative is the misclassification rate defined as the percentage of cyberattack cases that were not detected. The calculation can be illustrated using the below equations, where Q1 refers to the case numbers in quadrant 1, while Q4 refers to the case numbers in quadrant 4.

False positives is a misclassification rate that is the percentage of non-attack cases incorrectly classified as cyberattacks. The security metric is defined as the percentage of non-attack cases that did not trigger the SE security function. Similarly, the below equations illustrate the calculation, where Q2 refers to the case numbers in quadrant 2, while Q3 refers to the case numbers in quadrant 3.

Table 3 Figure of merit of the SE defense mechanism

Performance metrics	**Percentage**
dependability in terms of detection percent	91%
misclassification in terms of false positives	18%
misclassification in terms of false negatives	9%
security in terms of not detecting a cyberattack during a physical event	82%

We needed to understand how the SE security function will perform during equipment degradation cases. Degradation masks itself as an inconsistent measurement due to change in the impedance of the monitored circuit element. Figure 12 shows TSC unequal degradation cases, where the red line marked are the threshold of criteria 1 (left) and 3 (right). In those cases, 8 out of 10 test cases are categorized correctly as physical event, while 2 out of 10 test cases are categorized as false positives. Here a threshold of 2% error in TSC current magnitude is chosen to represent threshold of 100A as defined in criteria 1. Results show a few tests use cases of unequal capacitor degradation may lead to misclassification of physical degradation as cyberattack events (false positives). Major reason behind the false positives: capacitor degrades simultaneously which leads to similar ratio of C_{top}/C_{bottom} of two paralleled capacitor branches, therefore middle line currents is negligible.

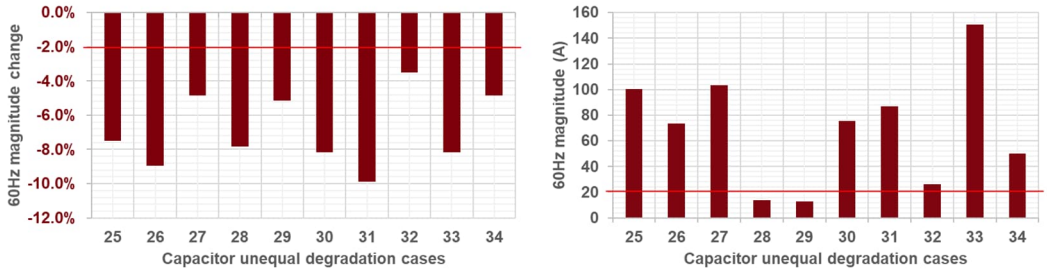


Figure 12 TSC current change (left) and TSC current unbalance (right) between capacitors in capacitor unequal degradation (test cases 25~34)

3.5. Conclusions

The concept of state estimator for FACTS devices with particular attention to SVC devices is introduced. Initial test results proved that it could detect both cyberattack on the measurement and physical degradation event. Testing in a non-real time environment revealed promising results towards advancing the security of the

measurement system in FACTS device. The state estimator was deployed in the MACH system as a research grade firmware and validated its performance in the near field conditions during the utility demonstration. Based on the exhaustive tests in an off-line environment it exhibited performance in detecting false data injection at 91% dependability, on test cases the includes a mix of cyberattack and noncyberattack cases, including equipment degradation.

4. CODEX

4.1. Problem Description

The current state of the art is FACTS substation protection and control dependent on interactions and coordination of multi-object protection IEDs with FACTS controller device. In near future these interactions are expected to be realized heavily on Cyber/IT (Information Technology) based communications, similar to digital substations. This will pose risk of cyber security i.e., once it is breached an attacker immediately assumes the position where FACTS substation equipment protection devices and can be directly control and interrupt normal operation.

4.2. Requirements

To address some of these cyber vulnerabilities, the concept of *CODEX - Collaborative Defense of FACTS and IEDs* provides added security layer in FACTS controller to act against direct attacks on the FACTS substation's protection IEDs and controller. As of part of this concept FACTS controller is equipped with added security layer, that would collaborate with installed field IEDs to defend and report the existence of cyber-attack inside the station and block malicious attempts from controlling these devices. Information that is being exchanged among devices and security features based on first principles of circuit theory, protection coordination, and power system dynamics are implemented in realizing security function inside the FACTS controller. Confirmation and/or blocking of attacks are based on violation or inconsistencies of the state of the system with these principles.

In summary this concept enables IEDs (Protective Relays) and MACH3 (FACTS controller) in a FACTS substation to collaboratively defend against cyberattacks. The technology will demonstrate firmware enhancements in the controller and communication capabilities with IEC61850 compliant IEDs, its performance will be validated in a FACTS substation test environment.

NOTE: CODEX does not supersede IEC62351 extensions of IEC61850. The primary objective of CODEX functionality is to address security against connected IEDs, that externally communicates with the FACTS controller, and may send malicious commands either due to a malware or incorrect operation.

4.3. Solution

The protection in FACTS substation in general is realized by various IEDs with multiple protection functions described in [1] such as: (1) current differential protections with overlapping protection zones and over current protections are used as short circuit protection for all substation components. (2) Time delayed residual overvoltage protection is used as earth fault protection for the SVC busbar and all SVC medium voltage components. (3) Current unbalance protection is employed for the capacitor banks in TSCs and filters. (4) A special capacitor overload protection is used on the filters to protect against low order harmonics from the system. The above-mentioned protection functions interact with FACTS controller to isolate the SVC from the network by tripping SVC main circuit breaker.

The function design of *CODEX* is essentially consisting of a security layer which is an add-on hardware and/or add-on software module. The security add-on can be realized like other protection IEDs and can be hosted as a part of FACTS controller and should be able to: (1) obtain and process field measurements i.e., analog input, (2)

Perform signal processing algorithm on the analog data, (3) detect the fault or abnormality and (4) send and receive control signals in real time. The methodology employed is a measurement-based approach, where dynamic operating state of the substation from analog measurement inputs (IEC61850-9-2 Sample Value (SV) streams transmitted on the process bus) and status information from the field devices and IEDs are used to develop additional security measures.

Figure 13 shows the high-level design of the add-on security function *CODEX* that would host *collaborative defense algorithms.* The add-on layer also enables flexible security algorithm development or deployment that would serve as an extension to FACTS protection functionalities and collaborate with other IEDs for enhanced security. The other aspects of this function that are considered during the implementation phase are the functionality interactions and interoperability with the IEDs. Ideally, it will take advantages of IEC61850 interoperability, and work with the IEDs via the exchange of substation SCD files. The core function of the module is to validate an issued command from IEDs by validated against the statuses derived from field measurements. The module then publishes a warning/alert status and block the command if any disparities in the normal operating conditions are detected.

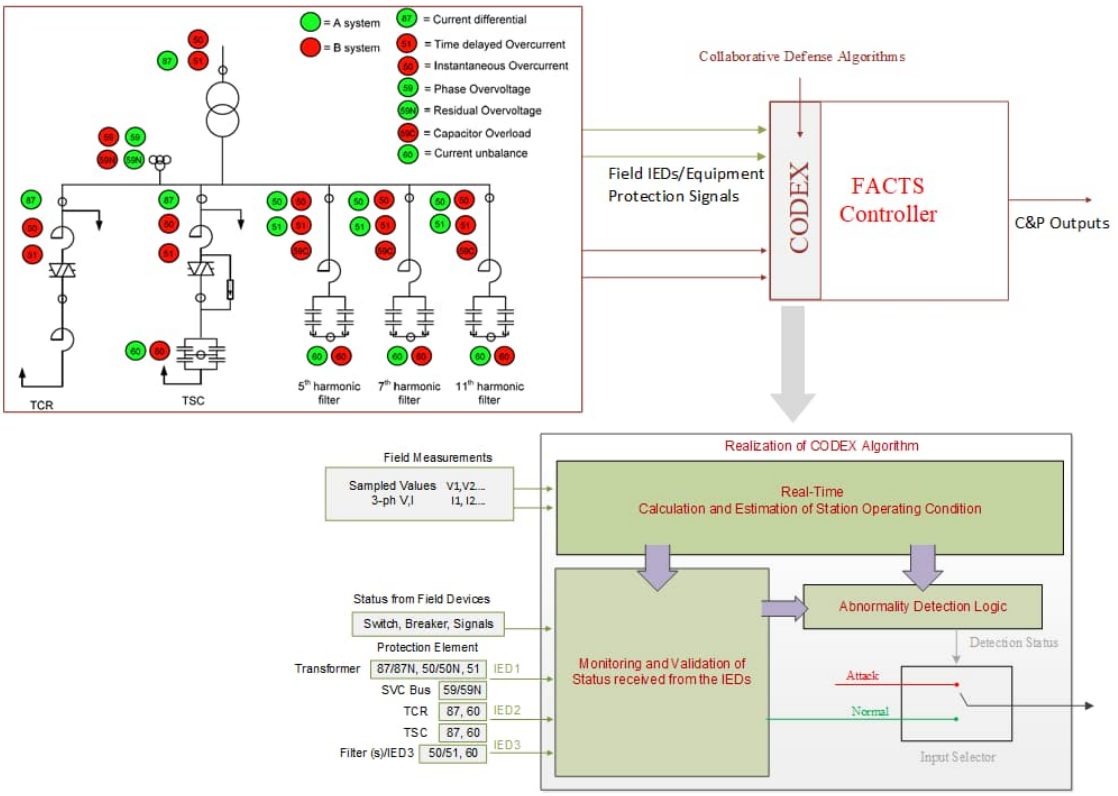


Figure 13 Overview of functional design for realizing CODEX

4.3.1. Test Bed Description

To test and validate the *CODEX* functionality in a FACTS substation, either an actual power system or using hardware-in-the loop (HIL) simulation testbed is required. Here, the project team has chosen HIL approach. HIL simulation offers a controlled test environment to evaluate power system operating conditions with the same hardware setup that can be found in the FACTS substation. The XFACTS demonstrator is cyber-physical HIL simulation testbed built with commercially available FACTS controller, substation protection devices (IEDs), and communication equipment that are integrated into a power system model running in a real-time simulated environment. The planned demonstrator is composed of three major parts – a power system simulator, FACTS substation protective and control devices, communication interfaces as shown in Figure 14 and includes RTDS racks, and Hitachi ABB's control and protection system MACH.

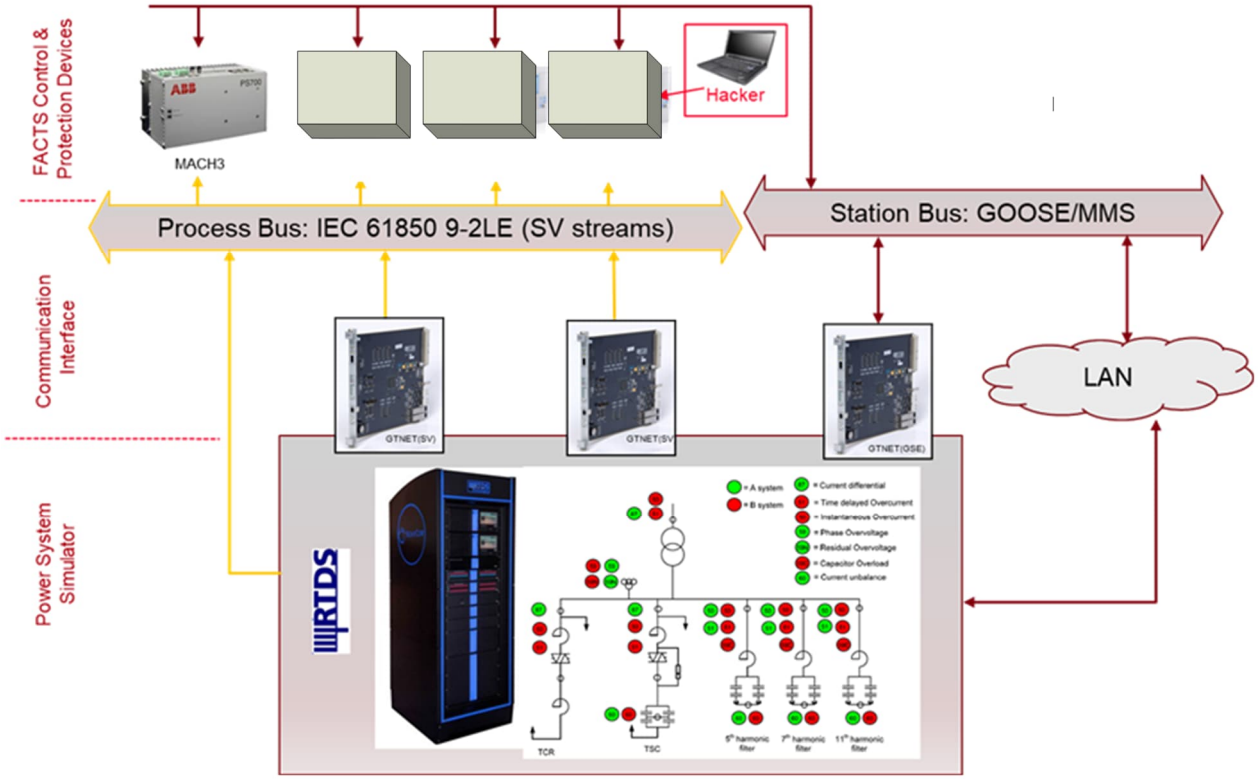


Figure 14 RTDS model with FACTS substation components

4.3.1.1. Power System Simulator:

A Real Time Digital Simulator (RTDS) is used for power system simulation, a representative FACTS substation power system model is shown in Figure 15 below. The power system model has enough detailed simulated FACTS substation components i.e., power transformer, TCR, TSC and filter banks. Analog measurements (e.g., voltages, currents, power factors, active and reactive powers) and digital status values (circuit breaker status) from the RTDS simulator are transmitted to the FACTS controller, protection IEDs through IEC 61850 based GOOSE and SV streams via a process bus and station bus respectively. The simulator together with the power system model provide basis for testing environment and the configuration can be programable to generate multiple test case scenarios to validate functional unit testing.

While modeling the system in RSCAD (the GUI software for RTDS), the dual time-step strategy has been adopted. The transformer, power electronic components, and the AC filter banks are modeled inside small time-step (3 µs) subnetworks. Whereas the AC source along with AC breakers are modeled in large time-step (50us). With this dual-time step technique, two different parts of the simulation runs with two different time-steps (3 us and 50 us). This arrangement makes sure the simulated system has enough detail needed for various test case scenarios.

4.3.1.2. FACTS controller and Protective devices:

The same class of IEDs employed for the protection of the FACTS equipment will be used in the demonstrator. Various types of protective IEDs (e.g., ABB RED670 and RET670 for implementing differential, overcurrent, and overvoltage protection) will be implemented to simulate the consequence of cyberattacks to FACTS substation. This configuration also can be applied to multi-vendor relay configuration (i.e., protective IEDs from different vendors). In this case, IEDs and RTDS are all configured to communicate the analog SV values and GOOSE messages with FACTS controller. The cybersecurity mitigation functions will be realized in the controller.

4.3.1.3. FACTS & IEDs communication interface:

The FACTS controller consists of multiple applications, and it is assumed to have capabilities to handle multiple communication protocols, e.g., IEC 61850 based GOOSE and SV. All power system analog and digital measurements will be sent to IEDs and then IEDs will send all information to the controller via GOOSE. Once the controller receives required information from IEDs and field devices, it calculates the implemented cybersecurity mitigation algorithms and then makes decisions, e.g., to block controls, send alarms or allow controls.

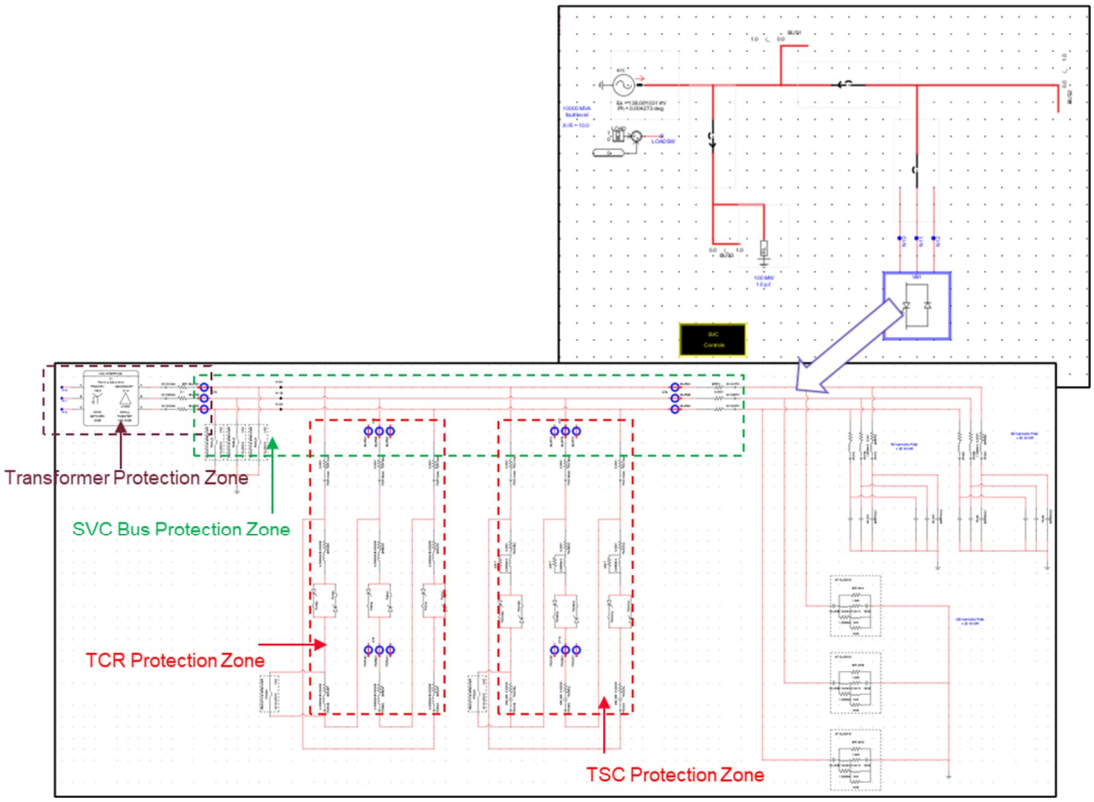


Figure 15 FACTS substation components and transformer protection zone

4.3.1.4. HW and SW components.

4.3.1.5. HW components

The test bed introduced in Figure 14 shows all necessary pieces of hardware that would make up the demonstrator for *CODEX* functionality. Below, Table 4 provides the list of planned hardware for the *CODEX* test bed

Table 4: CODEX Hardware Components

Equipment	**Description**
RTDS Simulator with communication capabilities	Real time digital simulator.
Development Computer	Host Computer for RTDS Simulator
ABB Relion protection relays - 1x RET670 - 2x RED670	IEC 61850 compatible protection relays to realize FACTS protection functions

ABB AFS675 switch	Ethernet switch with Gigabit up links for Process bus Communication
Netgear - ProSAFE (JFS524)	24- Port Ethernet Switch for Station bus communication
Hitachi Energy MACH3 Devices (PS700, PS935, PS74x)	Hardware for realizing FACTS control system

4.3.1.6. SW components

To configure the testbed for different use cases multiple software applications are required. Below, Table 5 provides the list of software components used in realizing *CODEX* test bed.

Table 5 : List of Software components for realizing CODEX testbed

Software	**Description**
RSCAD	• GUI for real-time modeling tool used creating SVC Station model with Individual components • Establish and configure communication with HIL devices by simulating Merging Units with IEC61850-9-2 SV streams, and GOOSE messages with status of simulated devices
PCM 600	• Configuration tool for realization and implementation of protection functions in multi-functional IEDs (ABB Relion relays) • Defining IEC61850 communication at the individual IED level • Generate ICD (IED capability description) files that contains description of the functions and IEC61850 objects that an IED needs for SV and GOOSE communication
IET600	• System Configuration Tool (SCT) to build SCD (Substation Configuration Description) file that contains the engineering design for IEC61850 communication inside the FACTS station.
ITT600 SA Explorer	• Integrated testing tool for diagnosis and troubleshooting of IEC 61850 compliant substation automation systems and applications. The tool essentially used to validate communication configuration among the devices.
HiDraw	• Development and debugging tool for configuring MACH3 control devices

4.3.2. Realization of SVC station protection

Realization of SVC protection system and tripping scheme with device specific protection elements is done according to std. IEEE SC-WG19. The protection is implemented will cover each device in the SVC station i.e., Transformer, SVC MV Busbar, TCR, TSC and filter banks shown in Figure 16.

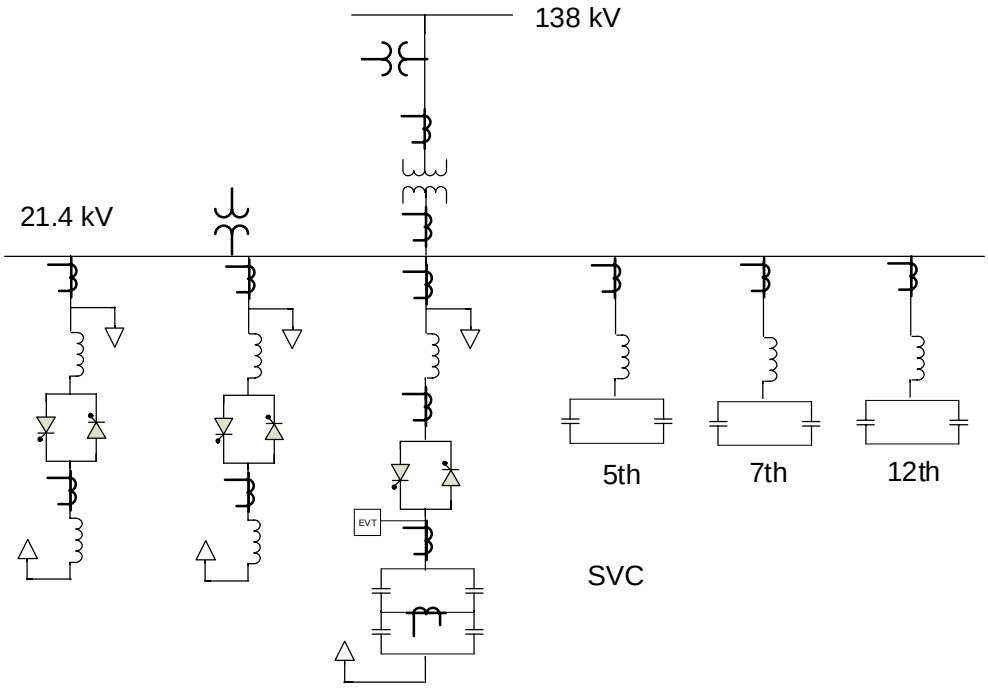


Figure 16 SVC single line diagram showing typical configuration consists of all the devices

As part of HIL implementation the protection functions will be realized using three ABB Relion series IEDs i.e., one RET670 and two RED670 relays. Each of these IEDs has capability to realize multiple protection functions and together should cover protection of all the equipment in SVC station. Below Table 6 provides functional allocation of protection elements to these IEDs according to std. IEEE SC-WG19. The IEDs are then configured in PCM600 configuration tool according to the functional allocation available in the configuration library. Figure 17 show IED configurations and mapping of protection functions from the PCM600 library as needed for the implementation.

Table 6 Functional allocation of protection elements

IED	**Protected Object(s)**	**Function**	**Number of Analog IOs**
RET670	Transformer	87T,	6 (2 x3I)
	SVC - MV Bus	59/59N	6 (2x 3V)
	Filter – 7^{th}	50, 60	3I, 6 (2x 3V)
RED670	TSC	87, 60	6 (2x 3I), 6 (2x 3V)
	Filter – 5^{th}	50	3I
RED670	SVC - MV Bus	87L	12 (4x 3I)
	TCR	87	6 (2 x3I)
	Filter – 5th	60	6 (2x 3V)

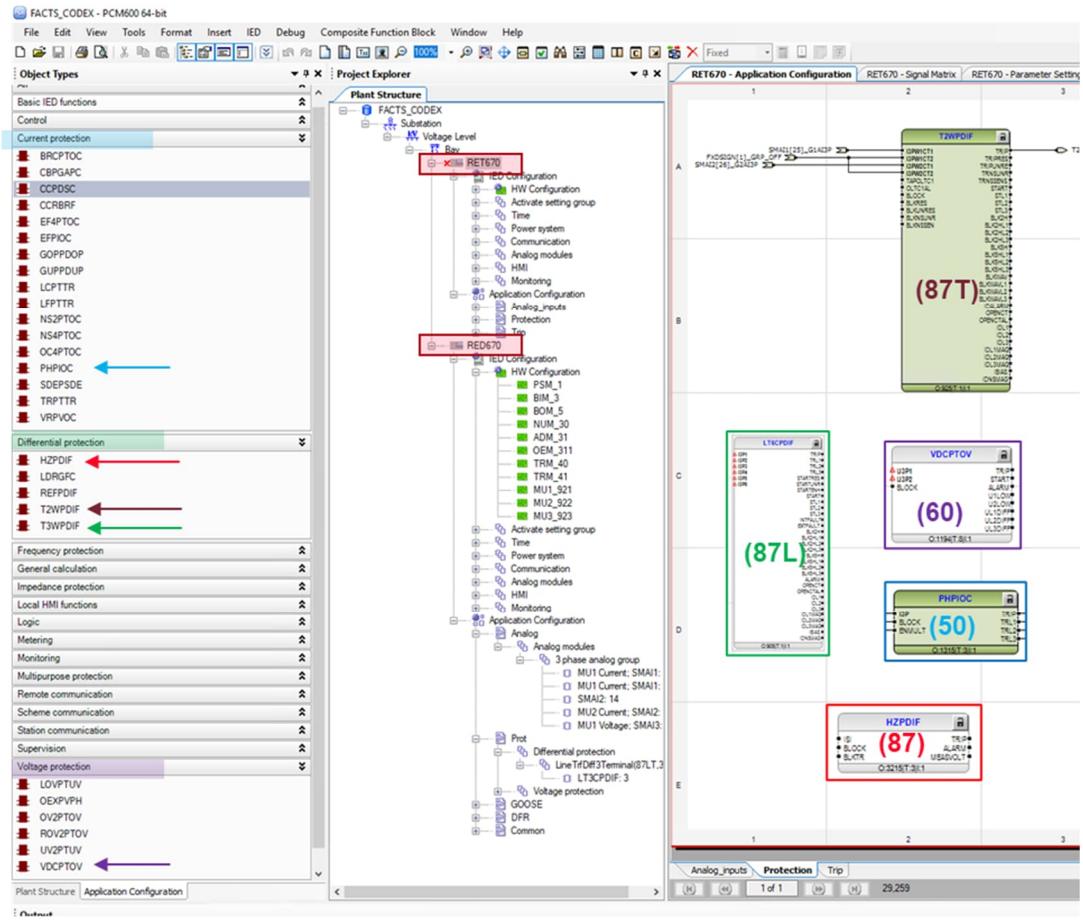


Figure 17: Mapping of protection functions in PCM600 configuration tool

4.4. Results

4.5. Testing Results and Performance Analysis

Testing of the *CODEX* functionality is done for various scenarios and are listed in Table 7. The similar scenario tests are done for three different SVC operating states. The operating states are corresponding to (1). Minimum reactive power export/injection from SVC (i.e., Vset = 1.01pu, QVar ~= +1MVar), (2). Rated reactive power export/injection from SVC (i.e., Vset = 1.04pu, QVar ~= +4MVar), (3). Rated reactive power import/absorption (i.e., Vset = 0.975pu, QVar ~= -2.25MVar)

Table 7: *CODEX* testing results and performance

Scenario	**Description**	**Detection Confirmation**	**Test Result**
Transformer Protection Zone			
Cyberattack	87T - Trip Signal Compromised	Block Trip Signal	Pass þ
Cyberattack	DoS attack - block 87T during system fault	Trip & Alert with CODEX function	Pass þ
Normal fault with CODEX Enabled	In-the -zone Fault --> Ph-Ph	Accept Trip Signal	Pass þ

Normal fault with CODEX Enabled	In-the -zone Fault --> 3Ph-G	Accept Trip Signal	Pass þ
Normal fault with CODEX Enabled	In-the -zone Fault --> Ph -G	Accept Trip Signal	Pass þ
Normal fault with CODEX Enabled	In-the -zone Fault --> Ph -Ph -G	Accept Trip Signal	Pass þ
Normal fault with CODEX Enabled	out-of-the-zone Fault --> Ph-Ph (HV side of the transformer)	No Trip Signal	Pass þ
Normal fault with CODEX Enabled	out-of-the-zone Fault --> 3Ph-G (HV side of the transformer)	No Trip Signal	Fail ý
Normal fault with CODEX Enabled	out-of-the-zone Fault --> Ph-G (HV side of the transformer)	No Trip Signal	Pass þ
SVC Busbar Protection Zone			
Cyberattack	87B - Trip Signal Compro-mised	Block Trip Signal	Pass þ
Cyberattack	DoS attack - block 87B during system fault	Trip & Alert with CODEX function	Pass þ
Normal fault with CODEX Enabled	In-the -zone Fault --> Ph-Ph	Accept Trip Signal	Pass þ
Normal fault with CODEX Enabled	In-the -zone Fault --> 3Ph-G	Accept Trip Signal	Pass þ
Normal fault with CODEX Enabled	In-the -zone Fault --> Ph -G	Accept Trip Signal	Pass þ
Normal fault with CODEX Enabled	In-the -zone Fault --> Ph -Ph-G	Accept Trip Signal	Pass þ
Normal fault with CODEX Enabled	out-of-the-zone Fault --> Ph-Ph	No Trip Signal	Pass þ
Normal fault with CODEX Enabled	out-of-the-zone Fault --> 3Ph-G	No Trip Signal	Pass þ
Normal fault with CODEX Enabled	out-of-the-zone Fault --> Ph-G	No Trip Signal	Pass þ
TCR Protection Zone			
Cyberattack	87TCR - Trip Signal Compro-mised	Block Trip Signal	Pass þ
Cyberattack	DoS attack - block 87TCR during system fault	Trip & Alert with CODEX function	Pass þ
Cyberattack	87TCR – Trip signal for SVC bus fault	Trip & Alert with CODEX function	Pass þ

Normal fault with CODEX Enabled	Fault in the Zone --> Ph -G	Accept Trip Signal	Pass þ
Normal fault with CODEX Enabled	out-of-the-zone Fault --> Ph-G	No Trip Signal	Pass þ
TSC Protection Zone			
Cyberattack	87TSC - Trip Signal Compro-mised	Block Trip Signal	Pass þ
Cyberattack	DoS attack - block 87TSC during system fault	Trip & Alert with CODEX function	Pass þ
Cyberattack	87B – Trip signal for TCR dif-ferential fault	Trip & Alert with CODEX function	Pass þ
Normal fault with CODEX Enabled	Fault in the Zone --> Ph -G	Accept Trip Signal	Pass þ
Normal fault with CODEX Enabled	out-of-the-zone Fault --> Ph-G	No Trip Signal	Pass þ

NOTE: The test Scenario is considered as ‘Pass þ‘, if the simulation results in an expected behavior as listed under the column ‘Detection Confirmation’

The *CODEX* algorithm is performing well under various system events. So, far there is one false positive has been identified for all SVC operating states.

The *CODEX* figures of merits based on the tests that are listed in Table 7 were classified and presented below in Table 8 and Figure 18 : 1) dependability in terms of detection percent is 100%, 2) misclassification in terms of false positives is 5%, 3) misclassification in terms of false negatives is 0%, and security in terms of not de-tecting a cyberattack during a physical event is 95%.

Table 8 Performance of *CODEX* classified for different test scenarios

Classification of Test Scenario	**Figure of Merit**
False Positive	5%
Dependability (Use Cases with Cyberattack)	100%
Security (Use Cases without Cyberattack)	95%
False Negative	0%

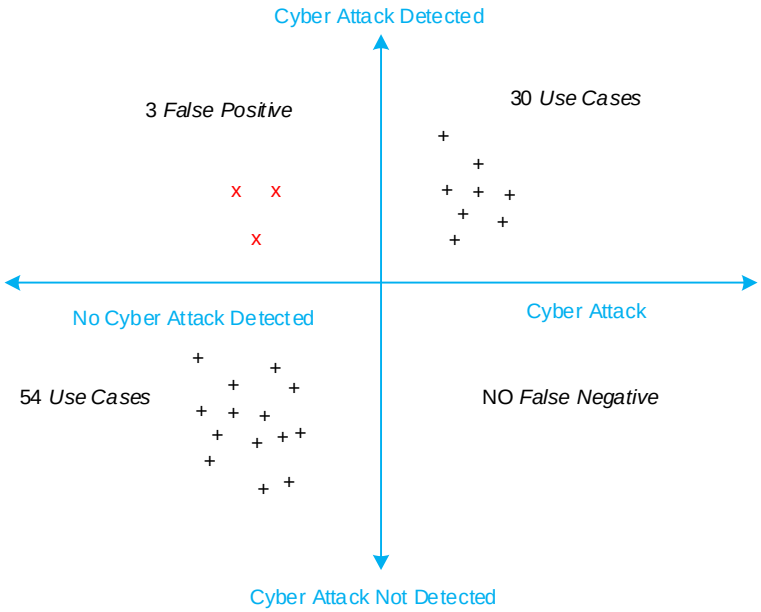


Figure 18: Performance of *CODEX* classified for different test conditions

4.6. Conclusions

Based on the tests performed on RTDS/RSCAD real-time simulation platform, the *CODEX* algorithm response is high in dependability (100%) and secured (95%) without compromising the traditional protection functionality, in terms of operation and speed for real-time applications.

4.7. Future Work

The CODEX algorithm assumes that the sampled values are secured according to the IEC62351 extension of IEC 61850. This extension secures against main in the middle attacks form on injection into the process bus. A cyberattacker can also deploy a malware on the merging unit to corrupt the sampled values, such as through manipulation of scaling factors. This vulnerability could be addressed by other security features beyond CODEX, including but not limited to securing supply chains. However, one possible future work within CODEX could be to perform a consistency check of sampled values by applying Kirchhoff's circuit laws to identify which measurement is potentially malicious.

5. CAPX

5.1. Problem Description

Incorporating series capacitors in suitable power lines can improve both power system steady-state performance and dynamic characteristics. The maximum active power transferable over a certain power line is inversely proportional to the series inductive reactance of the line. Thus, by compensating the series inductive reactance to a certain degree, typically between 25 and 70%, using series capacitors, an electrically shorter line is realized, and higher active power transfer and improved system dynamic performance can be achieved. The benefits of applying series compensation in transmission systems include enhanced system stability, desirable load division among parallel lines, improved voltage regulation and reactive power balance. As shown in Figure 19, the series-capacitor compensation equipment comprises series-capacitor banks (SCB), located in the line terminals or in the middle of the line, overvoltage protection circuit for the capacitor bank and bypass breaker.

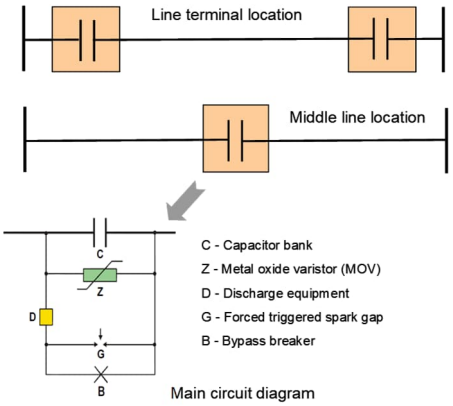


Figure 19 Series capacitor bank locations and main circuit diagram

Figure 20 illustrates the structure of a series capacitor station and control commands for switching the bypass breakers. The series capacitors normally are inserted in the line under high line power transfer conditions and bypassed under low line loading conditions, and the bypass breakers is controlled by the system operator through the Supervisory Control and Data Acquisition/Energy Management System (SCADA/EMS). Under emergency conditions, the bypass breakers may be directly controlled by Line Protection System (LPS) or system Remedial Action Schemes (RAS). Transmission lines with high degree of series compensation have increased transient recovery voltage (TRV) levels which may exceed the circuit breaker capability leading to failure of the equipment and possibly further damage to the system. Fast bypassing the SCB before circuit breaker opening can effectively reduce the TRV levels. In practices, the LPS will send simultaneously a line trip signal to line circuit breaker and a bypass signal to the SCB controller whenever it detects a line fault. Given that the speed of fast bypass breaker (FBB) is much faster than that of line circuit breaker (e.g., ~5 milliseconds vs. 20~30 milliseconds), the SCB can be bypassed well in advance of the line circuit breaker opening. Fast bypass or fast insertion commands may also come from RAS to mitigate risk of instability caused by major generation or transmission contingencies.

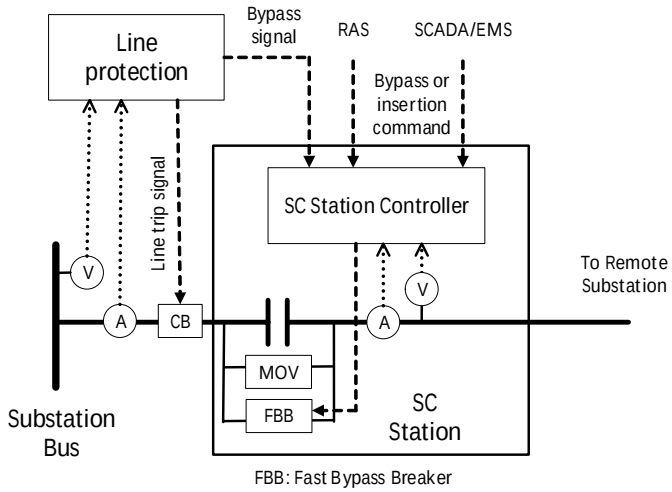


Figure 20 Structure of series capacitor station and bypass breaker control commands

Security against malicious direct control of series capacitors is deemed critical. The attacker may gain access to the communication channels and initiate unauthorized or altered control commands to manipulate SCB positions. Potential failure scenarios may include: 1) the attacker may issue malicious control commands to manipulate SCB positions under normal system conditions, 2) the attacker may block or compromise the control commands from LPS or RAS under emergency system conditions, 3) the attack may generate successive bypassing and insertion commands to the SCBs, etc. Unauthorized or altered control commands may cause overloading issues of power lines, voltage violations, inter-area oscillations, reduced stability margin against contingencies, and risk of system instability.

5.2. Requirements

The security functions of SCB station controller have been developed with consideration of the following performance requirements:

- Fast and reliable detection of line faults within the primary protection zone and system disturbances indicative of the concerned contingencies.
- High dependability for detecting malicious commands and high security for not detecting a cyberattack during a physical event.
- Inclusion of security functions in the SCB controller must not affect or compromise SCB controller performance.

5.3. Solution

A protective layer is added in the controller of SCB station for detecting malicious SCB control commands as shown in Figure 21. The controller of SCB station receives remote control commands (SCADA/EMS or LPS or RAS) and monitors system conditions through real time local measurements. Present system operating condition data such as line currents and terminal voltages are collected and processed to derive system conditions such as line loading levels, incremental line flow changes, grid frequency deviations, line faults, etc. Direct control command from SCADA/EMS or LPS or RAS is assessed by the protective layer first before the attempted switching action is executed. If significant physical state inconsistency is identified, the control command will be blocked, and alarm is issued.

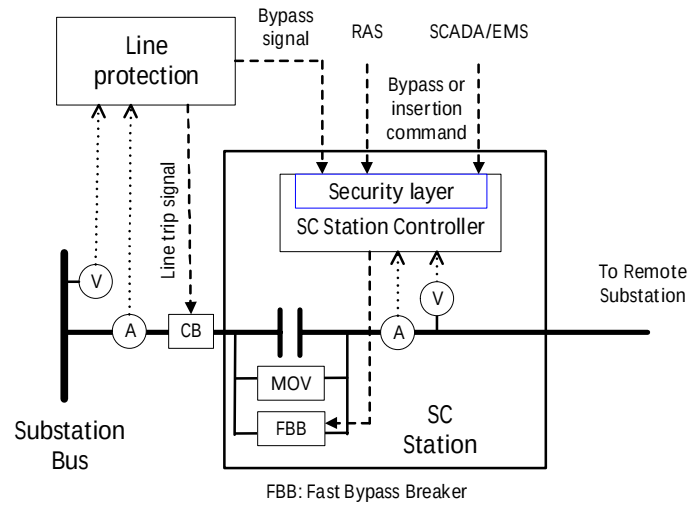


Figure 21. Security layer stored within the controller of a SCB station

The protective layer has two main security functions: Line Fault Detection (LFD) function and System Disturbance Detection (SDD). The LFD function is intended to secure fast SCB bypassing which is triggered by LPS under line fault conditions. Fast bypass command will be executed only if the line fault is confirmed by LFD prior to or within a few milliseconds of the receipt of the bypass signal. The SDD function is intended to secure fast SCB bypass or insertion triggered by RAS in response to critical generation or transmission outages. Fast bypass or insertion command will be executed only if the indicative system disturbance is confirmed by SDD prior to or within a few hundred milliseconds of the receipt of the RAS signal.

5.4. Results

The security functions of CAPX for detection of malicious control commands by attackers have been verified through comprehensive case simulations in real-time dynamic simulation environment (RSCAD/RTDS) . The test system setup is shown in Figure 22 which is based on a reduced WECC (micro-WECC) model. The

interties between the two regions include a ±500kV HVDC link and two series-compensated 500kV ac lines. The compensation degree is 60% and the series capacitor banks are located at line terminals with equal ratings.

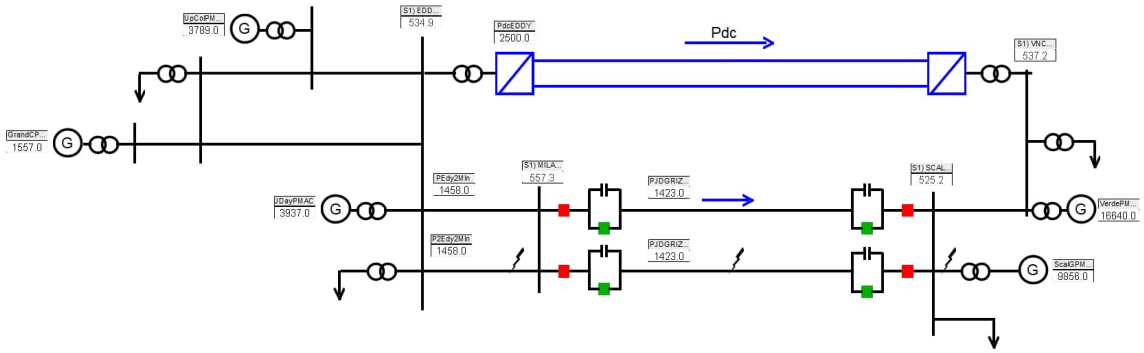
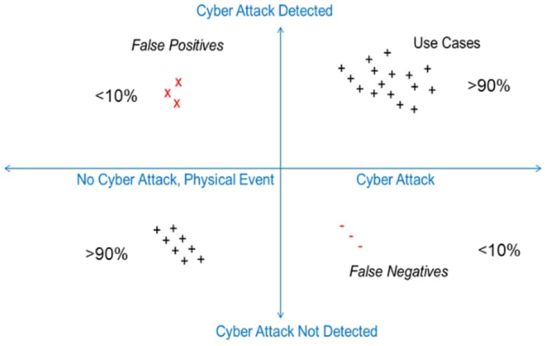


Figure 22. Test system setup in RTDS for security function verification

Figure 23 shows the performance of the security functions for the total of 136 tested cases. Test results show that both the LFD and the SDD functions have high dependability (>90%) for detecting a cyberattack and high security (>90%) for not detecting a cyberattack during a physical event. The identified misclassification of the LFD functions is in the cases with external faults in forward direction. Mitigation is possible by increasing the LFD settings to cover 50~70% of the line length instead of the entire line. Reduced fault detection zone is not an issue because the transient recovery voltages of line circuit breakers are not severe for remote fault clearing. The identified misclassification of the SDD functions is in the cases with generation trips downstream the corridor while extreme generation outages involving multiple large generators are extremely low possibility events.



Case Description	LFD		SDD		LFD+SDD	
	#	%	#	%	#	%
Non-attack cases	40		28		68	
False positive	4	10%	1	4%	5	7%
Physical event	36	90%	27	96%	63	93%
Attack cases	40		28		68	
Detected	36	90%	27	96%	63	93%
False negative	4	10%	1	4%	5	7%
LFD: Line Fault Detection function						
SDD: System Disturbance Detection function						

Figure 23 Performance of the security functions of CAPX

5.5. Conclusions

The cyber-secure functions of CAPX have been developed and tested in real-time dynamic simulation environment. The protective layer for detecting malicious SCB control commands is stored within the controller of the SCB station. It makes use of real time local measurements and applies effective detection algorithms and rules to assess system physical state consistency with respect to the received control commands. Test results have shown satisfactory performance of the security functions in terms of speed, reliability, dependability, and security.

5.6. Future Work

For mitigation of denial-of-service attacks, further efforts are needed to investigate the feasibility of activating fast bypass or fast insertion of SCB directly by the security functions under certain emergency conditions.

6. XDSE

6.1. Problem Description

A STATCOM is a fast-acting power electronics device that is capable of regulating the voltage at the point of interconnection by providing or absorbing reactive current. There are multiple use cases of the STATCOM, such as

- To alleviate transmission line congestion and facilitate controlled power flow. The steady-state power flow through the given transmission line can be in-creased by reactive power injection, preferably at the line's mid-point.
- To improve transient stability and small-signal stability by appropriate control.
- To improve voltage stability by providing voltage support at the end of the radial transmission line.
- To enable high renewable energy penetration by providing functionalities, such as voltage and frequency ride-through, power factor control, voltage regulation etc.

Because of the STATCOM’s role of ensuring reliable and efficient operation of the power grid, STATCOM is considered to be a critical asset and it is very important to protect it against the cyberattacks.

6.2. Requirements

A STATCOM (Static Synchronous Compensator) is a power electronic converter that can generate reactive power (both inductive and capacitive) by circulating current among the ac system phases. The output of the power converter is coupled to the ac system using a tie reactance. The reactive power compensation can be provided using the STATCOM by controlling the amplitude of the AC voltages of the STATCOM. Because of the power converter's fast switching ability, the STATCOM offers fast control (small transport delay). The fast control also poses cyber-physical system securities as fast intrusion detection approach is inevitable for preventing tripping or malfunctioning.

6.2.1. STATCOM Control Structure

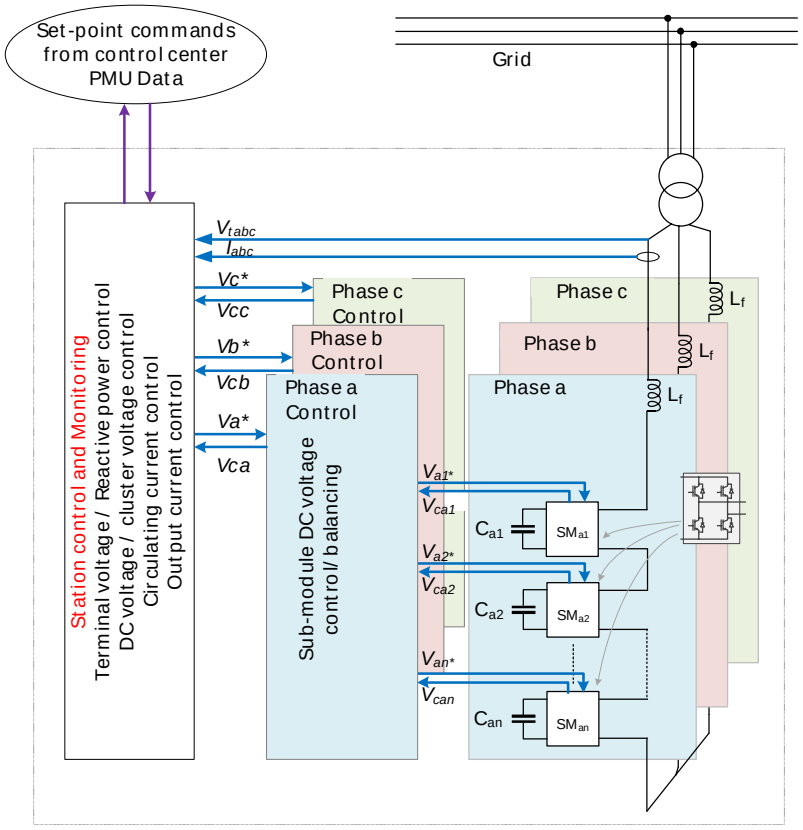


Fig. 1 Power electronic stage and control architecture of the STATCOM, along with the cyber layer.

A typical power electronic stage of Single Star Bridge Cells (SSBC) architecture for the STATCOM, along with the control architecture and cyber layer, is shown in Fig. 1. The standard bridge cells, termed as Sub-Modules (SMs), are connected in cascade to achieve required voltage ratings. The cascade-connected SMs form three clusters for the three-phase systems and are connected in start configuration. Although this study investigates star connected configuration, the findings can also be applied to the delta connected configuration. Since the STATCOM typically has a large number of SMs, controlling all SMs (and semiconductor devices withing SMs) based on the system measurement and SM level measurement using a centralized controller is challenging. Therefore, a distributed control architecture is considered, as shown in Fig. 1. The control architecture consists of:

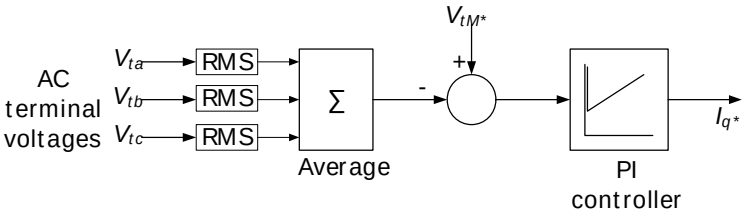


Fig. 2 (a) AC terminal voltage regulator.

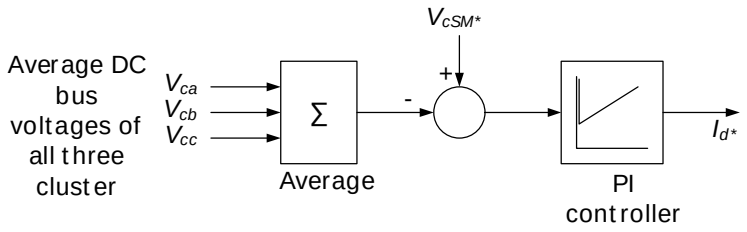


Fig. 2 (b) DC voltage regulator.

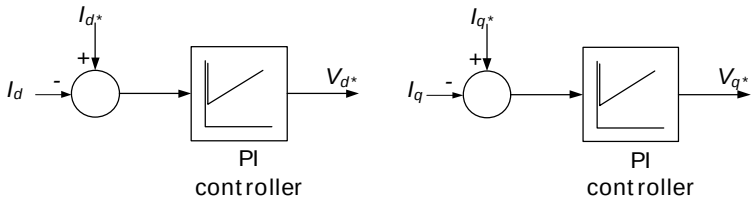


Fig. 2 (c) Current regulator

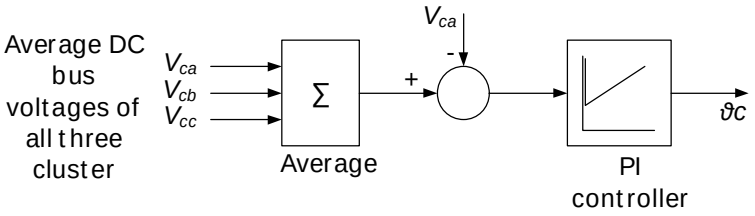


Fig. 2 (d) Cluster balancing / circulating current control

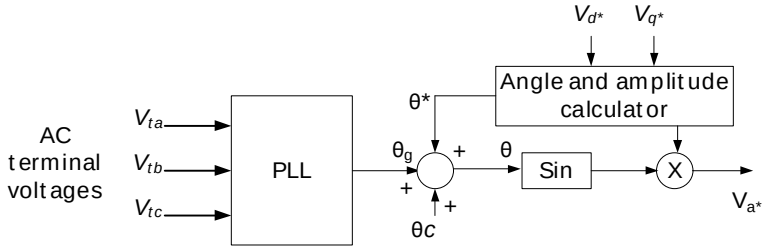


Fig. 2 (e) Phase locked loop and reference voltage generation

1. **Top-level controller** (embedded with the station-level controller), is responsible for executing high-level control functions, such as terminal voltage control, reactive power control, oscillation damping control, average DC voltage control, circulating current control (phase-balancing control), etc.
2. **Cluster-level controller** is responsible for the DC bus voltage balancing control of the SMs within the cluster, phase-shift modulation, and gate-pulse generation, etc.

The top-level controller may receive setpoint commands from the control center through the communication layer. In addition, the terminal voltage (V_{tabc}) and injected current (I_{abc}) is used as feedback for closed-loop control. The terminal voltage information is used for synchronization and terminal voltage control, whereas line current feedback is required for the current regulation. In addition, the average values of all the SM DC bus voltages of three clusters (V_{ca}, V_{cb}, and V_{cc}) are used for the average DC bus control. The top-level controller calculates the average values of the SM ac voltages of all the three clusters, which are communicated to the respective cluster-level controllers. The cluster-level controller generates ac voltage reference setpoints for individual SMs within that cluster by modifying the reference ac voltage command received from the top-level controller based on the individual SM DC voltage balancing control. The individual SM DC balancing control uses SM DC voltage measurements from the SMs within the cluster and generates the ac voltage reference component, which is then added to the reference ac voltage command received from the top-level controller. The modified reference is then passed to the modulator to generate gate pulses for the semiconductor devices. The EtherCAT communication protocol is considered for the communication between the top-level controller and the cluster-level controller. EtherCAT communication is also considered for communicating SM DC bus voltage measurement to the cluster-level controller.

6.2.2. STATCOM Control: Vulnerability Analysis

Vulnerability analysis of the following cyberattacks on the STATCOM is performed, where the following intrusion approaches are considered.

1. **Intrusion into communication link**: The intrusion into the communication link between the control station and STATCOM station, as well as the intrusion into the EtherCAT communication between the top-level controller and the cluster-level controller within the STATCOM station is considered. In addition, the intrusion into the communication link, transmitting the terminal voltage and line current measurement, is also considered.
2. **Attack on the controller** through back door entry using hardware trojans and remote access trojans is considered. Such an attack may lead to the denial of the service and manipulation of the data stored in the register, including controller gain and reference set points.

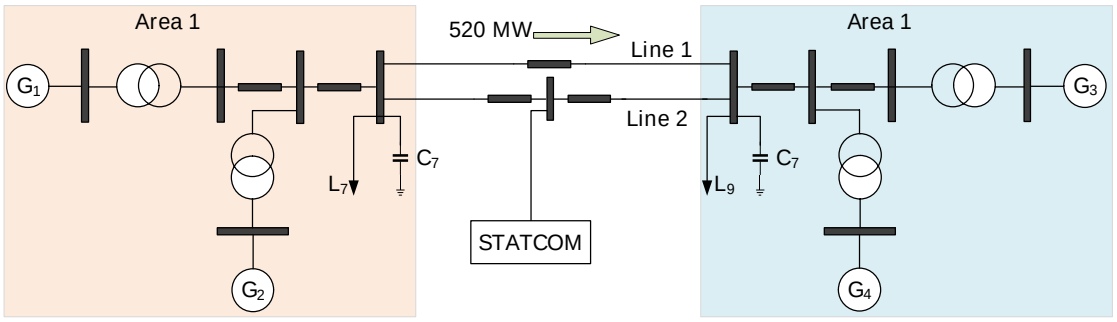


Fig. 3 Basic use case of the STATCOM application to improve the transmittable power between two areas. Kundur's two-area system is considered.

Kundur's two-area system is considered as a basic use case. The two areas are connected through two 220 km lines to facilitate power exchange. The STATCOM is connected to the mid-point of one of the lines to increase transmittable power between the two areas.

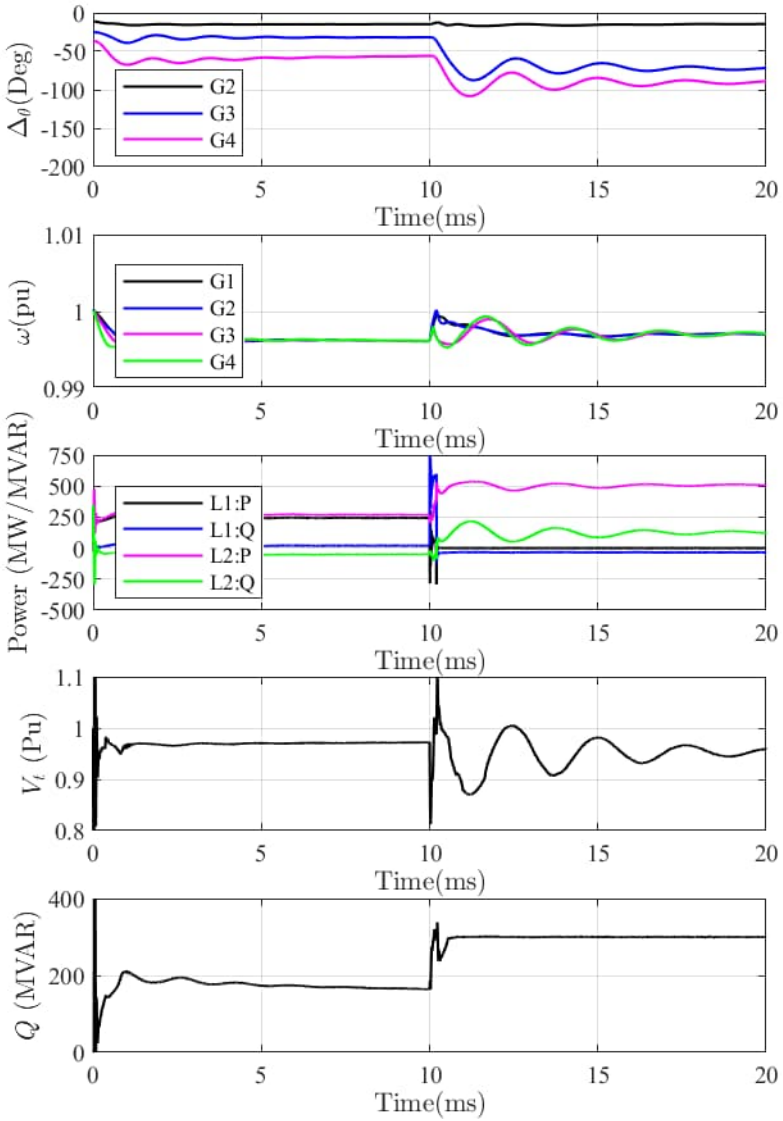


Fig. 4 System performance with the normal operation of the STATCOM. The line 1 experiences fault at 10s and breaker opens at 10.2s. The total power flow of 520MW is handled by line 2 because of the increase in the transmittable power of line 2.

The increase in the transmittable power due to the mid-point voltage compensation using the STATCOM is verified by performing system simulations. The power of 520MW was exported from area 1 to area 2, with both line 1 and line 2 carrying approximately the same amount of power. The STATCOM was regulating the mid-point voltage of line 2. The fault occurs on line 1 at 10s and results on the line isolation by breaker opening at 10.2s. Thanks to the increase in the transmittable power due to the mid-point voltage regulation due to the STATCOM, line 2 carries full 520MW power after opening line 1. The results are shown in Fig. 4, where the simulation is stops when the rotor angle difference between the generators of two areas increases beyond 180°.

6.2.2.1. Attack on Breaker through Authorization Violation:

The insider attack on the breaker through authorization violation is simulated, where the case scenario of the coordinated attack has been evaluated. Following the breaker opening of line 1 due to the permanent fault on line1 at 10s, the STATCOM breaker is attacked at 12s, which results in a breaker opening. The absence of mid-point voltage regulation due to the STATCOM disconnection leads to a large rotor angle difference. As a result,

both the areas fall out of synchronization and creates a significant load-generation imbalance in area 2, which may activate under frequency relay and shutdown generators in area 2.

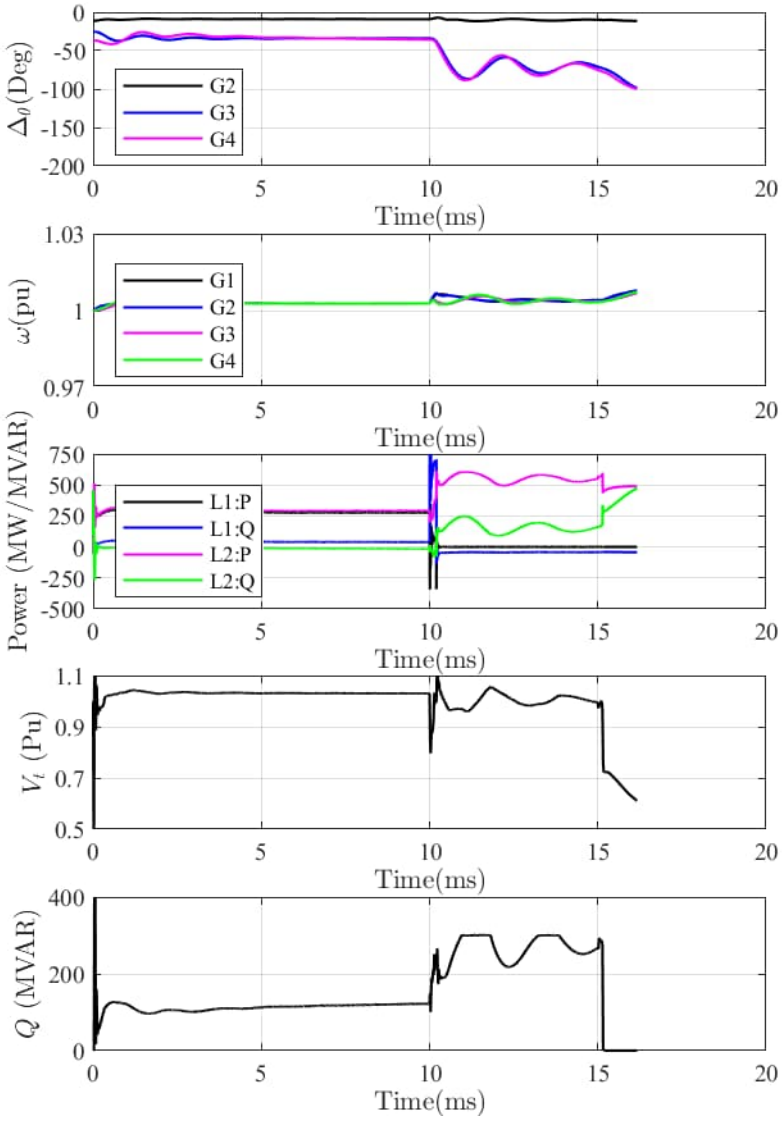


Fig. 5 Attack on the STATCOM breaker through authorization violation is simulated. The system was already stressed due to the loss of line1 at 10s. The breaker is attacked and opened at 15s.

6.2.2.2. False Data Injection:

For the distributed control architecture, considered in this study, EtherCAT protocol is used to communicate data between the top-level controller and all three cluster-level controllers. The top-level control functions, such as ac terminal voltage control, average DC bus voltage, phase balancing control, are implemented in the top-level control, as shown in Fig. 2. The top-level controller requires information about the average DC-link voltages of all three clusters (Vca, Vcb, Vcc), as shown in Fig. 1. The false data injection on these average DC-link voltages of all three clusters has been simulated, where the negative bias was added to average DC-link voltage of cluster a, as shown in Fig. 6.

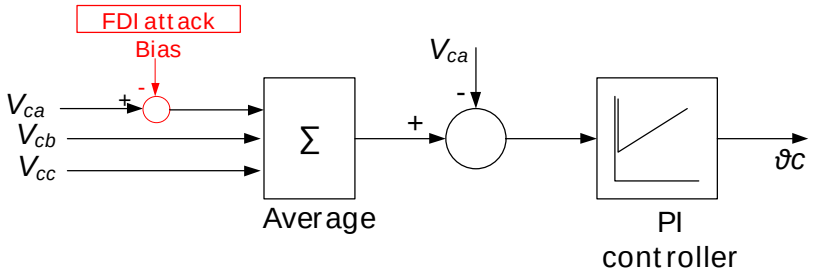


Fig. 6 False data injection attack by intrusion into the communication link between the top-level controller and cluster-level controller of phase a.

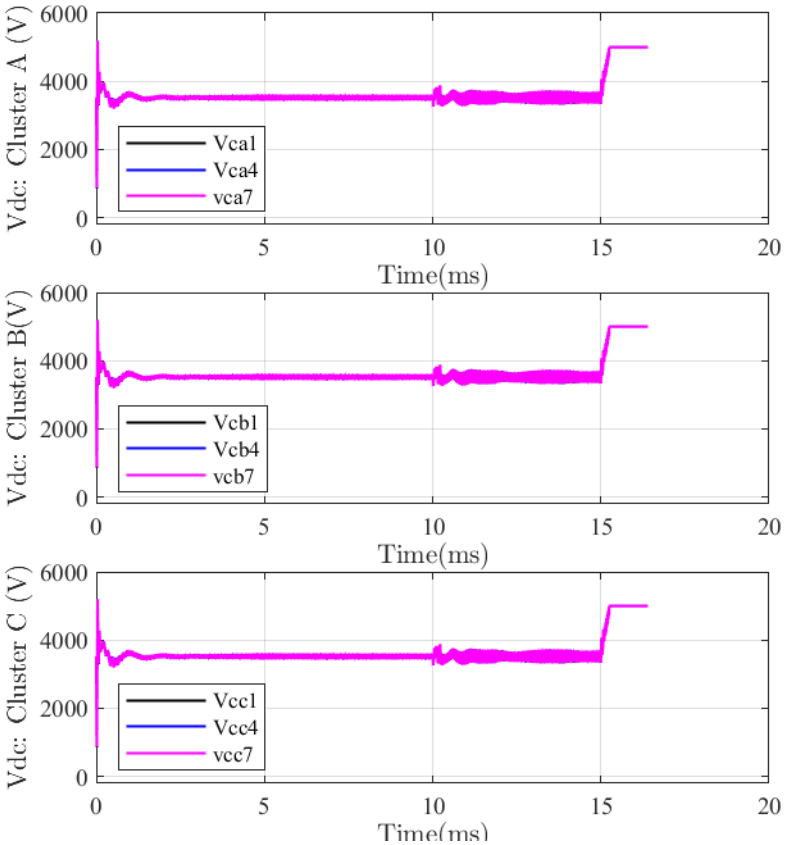


Fig. 7 False data injection attach. The average value of the DC voltages of the phase A submodules has been modified. The attack was initiated at 15s.

The results of the FDI attack on Vca is shown in Fig. 7. Although only the Vca measurement is compromised, its impact is observed in the Vcb and Vcc as well. This is because of the phase-balancing control, which takes appropriate control actions to ensure equal average DC voltages for all the three clusters. Because of the FDI attack, where the bias is subtracted from the Vca, the DC voltage controller will act to increase the DC bus voltage, which triggers the over-voltage protection of SMs, leading to the tripping of the STATCOM. As a result, system level results, shown in Fig. 5, are obtained. The tripping of the STATCOM during the stressed grid operation results in the desynchronization of both the areas and potential activation of the under-frequency and over-frequency relays.

6.2.2.3. Reference Setpoint Manipulation:

The communication link between the control center and STATCOM center can be compromised. Commonly used Supervisory Control and Data Acquisition (SCADA) makes it highly susceptible to malicious intrusions. Moreover, the reliability factor involved with deep integration of the communication layers to achieve

coordination between different FACTS devices also play a vital role in new security concerns. The attack scenario, where the attacker introduces attack element in terms of the reference setpoint for the line 2 midpoint (STATOM terminal) voltage, is simulated. Since the terminal voltage should stay within the specified limit, usually 0.95 pu to 1.05 pu, any attempt by the intruder to set the terminal value out of the specified range can be filtered out. The intruder can change the terminal voltage reference setpoint periodically within the specified voltage range and can introduce oscillations, as shown in Fig. 8.

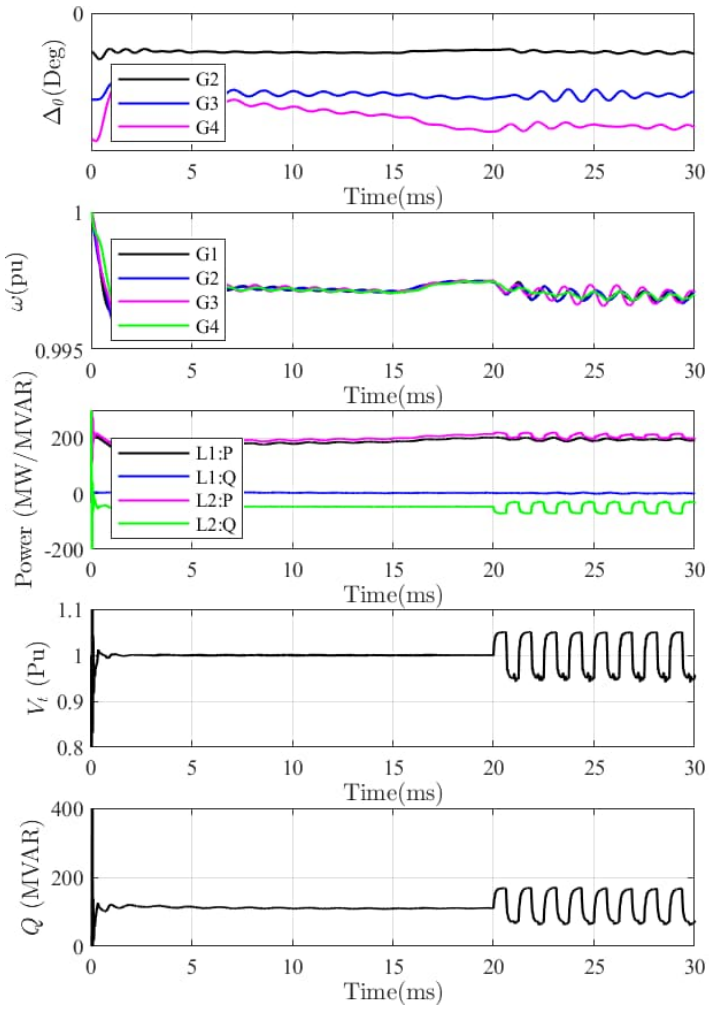


Fig. 8 Oscillations introduced by the attacker by manipulating the terminal voltage setpoint in a periodic manner.

The oscillations in the STATCOM terminal voltage and injected reactive power is clearly observed. This is propagated to both the areas, as oscillations are observed in the rotor angle of all the generators. The generator 4 is equipped with the power system stabilizer. As a result, the oscillations are somewhat damped, especially the rotor angle oscillations of generator 4.

6.3. Solution

The intrusion detection approach is designed to identify attacks on the primary controller of the power electronics controller. The control architecture of the STATCOM is shown in Fig. 9. The digital primary control implements control and protection functionalities. The primary control can receive reference commands from the secondary controller, which is communicated digitally. The measurements required to implement the feedback control are also digitally communicated to the controller.

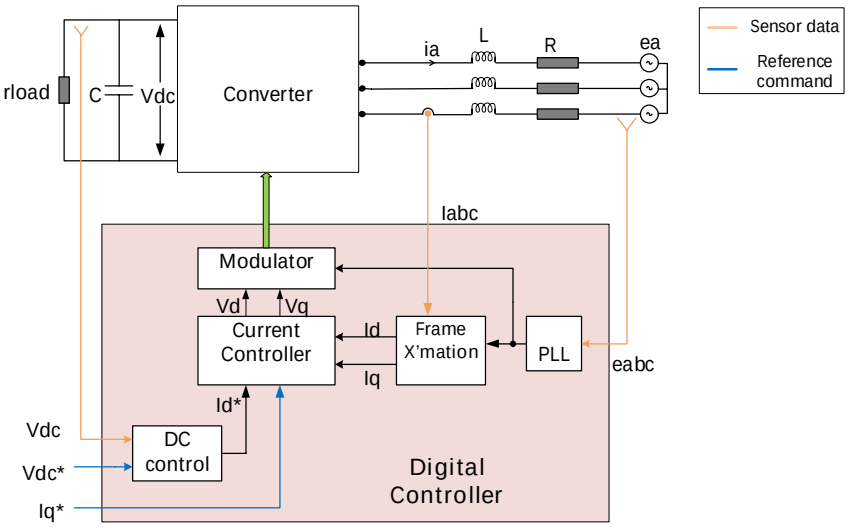


Fig. 9 Hardware and primary control architecture of the STATCOM based on two-level voltage source converter.

The digital controller and data exchange between the sensors and controller are the vulnerabilities at the primary control level, which attacker can exploit. The attacker can manipulate **1) sensor data, 2) controller parameters by gaining backdoor entry through the Remote Access Trojan (RAT).** Moreover, the sensor data can be manipulated by gaining access to the digital signal processor of the sensor that converters analog sensor measurement to digital and communicate it to the converter controller. Tight control over the supply-chain of the digital controller can potentially avoid unauthorized access to the digital controller. However, in the modern-day semiconductor manufacturing, where the multiple vendors contribute to the single chip design and manufacturing, possibility of planting RAT still exists. Therefore, the defense mechanism is still required for such low probability attacks, especially for the valuable grid assets such as STATCOM.

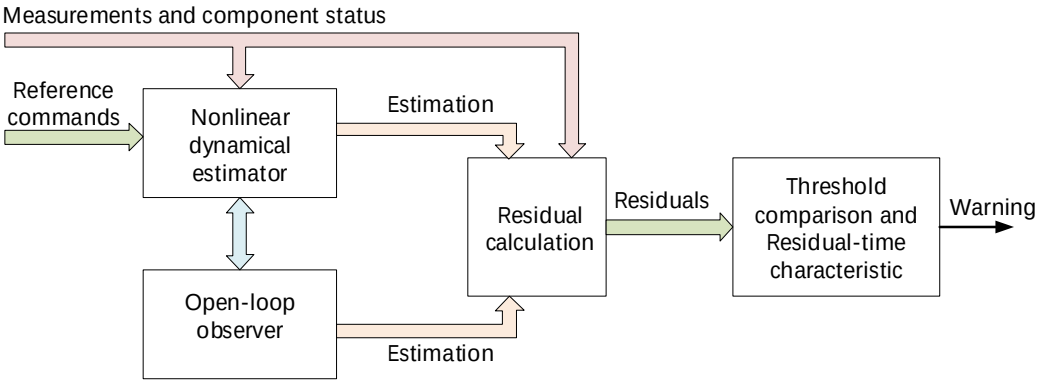


Fig. 10 Proposed defense mechanism against the attack on the primary controller.

The defense mechanism against such attack has been designed and the basic concept is shown in Fig. 10. Power electronics system is a time-varying non-linear system. To estimate the states, an averaged non-linear model is derived, which is a very important component of the dynamical estimator. The dynamical estimator is complemented by an open-loop observer. The major issue with the open-loop observers is unknown initial conditions, which has been resolved by updating the initial condition using the estimated states from the synchronized dynamical estimator. The estimated states and the measurements are then used for the residual calculation. If the residual value exceeds the threshold, a warning flag has been using the residual-time characteristics.

6.4. Results

6.4.1. Test Bed Description

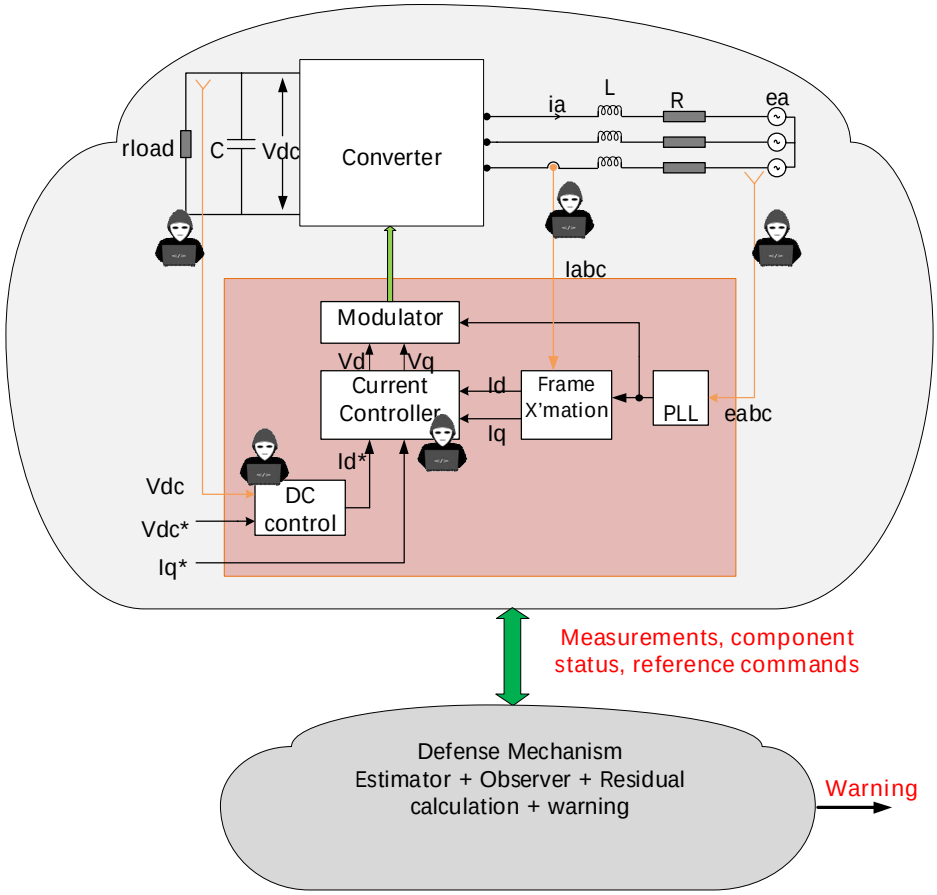


Fig. 11 Implemented test bed in the MATLAB Simulink environment.

The test bed is implemented in the MATLAB Simulink environment, where the full switching model of the STATCOM, along with its control has been implemented. The defense mechanism that includes non-linear dynamical estimator, observer, residual calculation, and intrusion detection is also implemented in the MATLAB. A provision for manipulating sensor data as well controller gain has been made.

6.4.2. Results

The following attack scenarios are simulated to evaluate the efficacy of the designed defense mechanism. The manipulation range is selected such that the manipulated data still stays withing the operating region of the converter. Data manipulation that leads to the measurement outside the operating region of the converter can be easily detected through a simple status check, which will be explored in the future studies.

Table 9 Description of the attack scenarios and disturbances considered to evaluate the performance of the proposed defense mechanism.

Attack scenario / Disturbance	Type	Manipulation range (pu)

DC voltage sensor data manipulation	Scaling attack (Gain manipulation)	0.6 – 1.2 (0.05 pu steps)
	Bias	-0.4 to 0.2 (0.05 pu steps)
AC current sensor data manipulation	Scaling attack	0.6 – 1.4 (0.05 pu steps)
	Delay attack: Phase manipulation	2.5° - 20° (2.5° steps)
AC voltage sensor data manipulation	Scaling attack	0.6 – 1.4 (0.05 pu steps)
	Delay attack: Phase manipulation	2.5° - 20° (2.5° steps)
External disturbance	3L fault at PCC: % dip in the PCC voltage	10% - 90% (10% steps)

6.4.3. Performance Validation

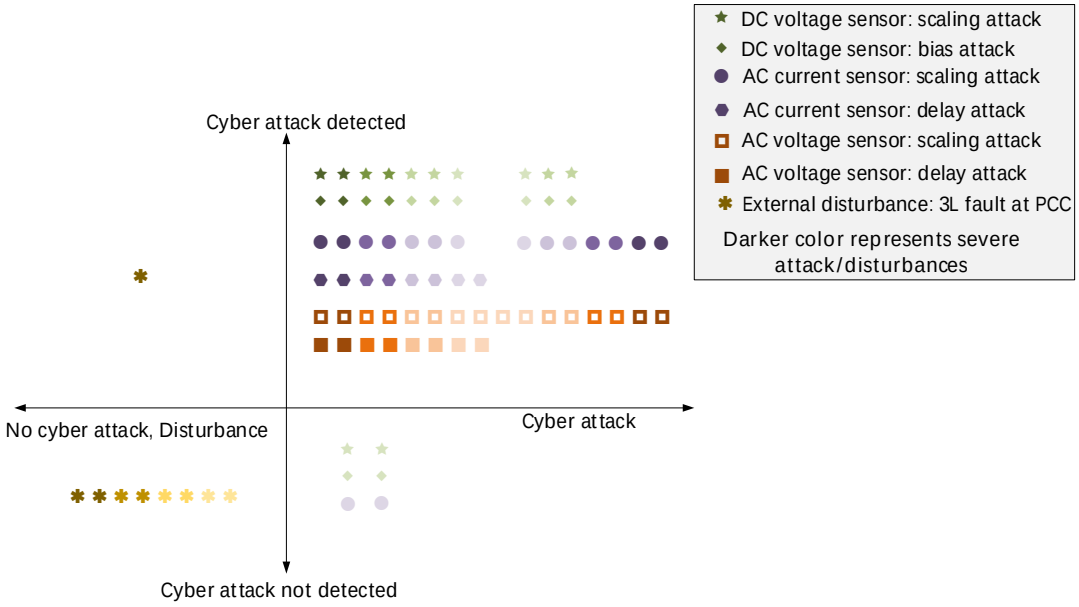


Fig. 12 Performance of the proposed defense mechanism.

The performance of the proposed defense mechanism is evaluated for different attack scenarios and external disturbance tabulated in Table 9 and the results are shown in Fig. 12. The use cases are color coded and darker colors are used to represent severity of the attack/disturbance. The figure of merits of the designed defense mechanism is also given in Table 10. The defense mechanism accurately detects AC voltage sensor attack (both the scaling and delay attack) in the considered range. On the other hand, it fails to detect mild (±5%) scaling and bias attack on the DC voltage sensor. This is because 5% data manipulation has insignificant impact on the system states, leading to a very small residual. With increased severity, the attacks on the DC voltage and AC current sensors are detected, leading to highly dependable defense mechanism. The security in terms of not detecting a cyberattack during an external disturbance (3L fault at PCC) is also evaluated by varying the fault impedance and therefore the dip in the voltage. The defense mechanism gives false positive in only one case, where the dip in the PCC voltage was 90%. In all other case, it securely detects the disturbance and do not raise false warning flag.

Table 10 Figure of merits of the defense mechanism. dependability in terms of detection percent and security in terms of not detecting a cyberattack during a physical event are presented.

Attack type / Disturbance	Dependability (%)	False negative (%)	Security (%)	False positive (%)
DC voltage sensor: scaling attack	83.3%	16.7%	NA	NA
DC voltage sensor: bias attack	83.3%	16.7%	NA	NA
AC current sensor: scaling attack	83.3%	16.7%	NA	NA
AC current sensor: Delay attack	100%	-	NA	NA
AC voltage sensor: scaling attack	100%	-	NA	NA
AC voltage sensor: Delay attack	100%	-	NA	NA
External disturbance: 3L fault at PCC	NA	NA	88.8%	11.2%

6.5. Conclusions

The defense mechanism against the cyber-attack on the primary controller of the STATCOM has been designed. The performance of the defense mechanism has evaluated by measuring dependability (ability to detect cyberattack) under different kind of sensor attacks, including scaling attack, bias attack, and delay attack. These attack scenarios on the DC voltage, AC current, and AC voltage sensors have been simulated and the dependability is measured. The defense mechanism detects attacks on the AC voltage sensors. Attacks on the DC voltage and AC current sensors have also been detected, except least severe attack in all the considered cased. The performance in case of the external disturbance is also evaluated by applying voltage dip at the PCC and the ability to separate disturbance from the cyber-attack has been measured in terms of the security. Total nine cases of voltage dip have been simulated. The defense mechanism does not raise warning when the voltage dip is between 10-80%. However, it raises false warning flag in the case of voltage dip of 90%.

6.6. Future Work

The work so far focuses on the defense mechanism against the cyber-attack on the primary controller using dynamic state estimator. In order to prevent the tripping due to the over-current in the event of attack, fast detection and mitigation is required. The proposed defense algorithm is executed (state progression is evaluated at 10 uS) at significantly smaller time steps. Therefore, faster processing is required. Implementation of the proposed algorithm requires significant development work due to the smaller time step requirements. Alternatively, the proposed algorithm can be implemented on the commercially available real-time power electronics simulator system, such as Typhoon HIL.

The model developed for the dynamic state estimator is valid for the STATCOM with balanced three-phase operation. In case of the unbalanced operation, the model must be modified to consider unbalance operation. This can be incorporated by including dynamical model in a rotating reference frame, rotating in the reverse direction at the fundamental frequency.

7. Additional Information

7.1. Listing of related documents

Ref #	Document Kind, Title	Document No
[1]	Wikstrom K, Gajic Z, Poulsen B., “The design of a modern protection system for a Static Var Compensator”, Cigre Study Committee B5 Colloquium, October 2009	

8. Addendum

Text

9. Revisions

Rev.	Chapters	Description	Date / Unit / Name

9.1. Reviews

Rev.	Chapters	Description	Date / Unit / Name

APPENDIX B: UNIVERSITY OF ILLINOIS AT URBANA CHAMPAIGN FINAL REPORT

Cyber Physical Security of Wide-area-controlled Static Var Compensator System

Executive Summary....2
Introduction....2
Implementations of FACTS control by WAMS/WACS....4
Threat Models....5
Development of Cyber Threat Detection and Mitigation Approach....7
Matrix Pencil Method....9
Oscillation Amplitude Monitoring (OAM)....9
Key Achievements....9
Papers....9
Reports....10
Threat Model....10
Red Team and Red Team Response....10
References:....10

Executive Summary

This report summarizes the results of a project performed by the University of Illinois at Urbana-Champaign (UIUC) supporting Hitachi Energy (formerly Hitachi-ABB power systems). The project examined cyber and cyber-physical threats and mitigations in Flexible Alternating Current Transmission Systems (FACTS) integrated and controlled by Wide Area Measurement/Wide Area Control Systems (WAM/WACS). Such an ecosystem can benefit from advantages enabled by the ability of FACTS to enhance resiliency and robustness of transmission system. For this system to inter-operate, there must be communication over networks, currently using the IEEE C37.118 protocol. The objective of this project has been to examine this wide area communication as a potential cyber attack surface.

It is possible to implement communication network control host defenses in such an integrated system. These defenses potentially detect and block attacks against C37.118 as well as violations of communication and protocol whitelists. UIUC developed physics-informed defense that examined system behavior in response to a disturbance and in the presence of an adversary with capability to corrupt the modulation signal from the WAM/WACS to the FACTS. A successful attack of this type can result in destabilizing system conditions. Our physics-based defense is based on extensive system analysis and simulation to rapidly identify when the modulation fails to achieve the expected result (for example, successfully damping an inter-area oscillation).

UIUC met project deliverables in the form of quarterly progress reports, milestone reports, and a Red Team report. The procedure for the RT evaluation was for the development team to submit the threat model and assumptions to the Red Team for critique as far as realism and completeness of coverage. The Red Team prepared a report with their findings. The development team prepared a response to these findings as an appendix to the Red Team report. The development team also proposed and executed an attack suite in which a simulated attacker can set parameters for the various attacks considered. The development team ran a number of attacks sampling the space of attack parameters. We were able to verify that all significant attacks were detected and mitigated. The attacks that evaded detection were all of acceptably low impact in terms of system stability.

UIUC published two conference papers based on this work, and one of these won the Best Student Paper award in the conference.

Introduction

FACTS devices in power systems are increasingly deployed to enhance resiliency and operational robustness. Present FACTS implementations have limited remote configurability and interoperability features, often requiring on-site presence for reconfiguration. We may envision future FACTS with the ability to support communication (measurement and control commands) as well as collaborative operation in support of use cases such as distributed operation for stability control. This evolution potentially exposes a cyberattack surface.

The objectives of this project are to examine cybersecurity considerations of Flexible AC Transmission Systems (FACTS) and their interaction with Wide Area Measurement Systems (WAMS)/Wide Area Control Systems (WACS). One important use case to consider is that of inter-area oscillations, which are a concern for weakly connected systems, and can lead to loss of stability.

A weakly connected transmission system is one that is composed of regions each with significant generation capacity, with relatively few lines connecting the regions. Based on modeling, it is often possible to determine analytically what oscillatory modes will be present (oscillations between which points and at what oscillatory frequency). FACTS are a class of devices that can react to damp such inter-area oscillations. At design time, FACTS devices can be deployed and configured to detect and respond to modes that are expected to be present in a system.

FACTS can damp oscillations based on local control, which has a limited spatial view, or control from WACS, which is increasingly adopted in transmission systems, and will likely be more prevalent in future systems. In the latter case, a correctly functioning WACS will send control signals to FACTS it controls so as to dampen an oscillation. Recent investigations in the literature examine how transient oscillatory behaviors in power systems can be effectively mitigated via the WAMS/WACS detecting the oscillations and sending modulation reference signals to FACTS devices that are distributed in the WACS's footprint. These signals are communicated over wide area networks, using the IEEE C37.118 standard (the standard for phasor measurement unit, or PMU, communication).

APPLICATIONS OF FACTS DEVICES

FACTS devices have been increasingly adopted in power transmission systems to address bottlenecks and limitations in the bulk transfer of power. These bottlenecks and limitations often arise due to one or more of the following limits:

1. Steady-state stability limits
2. Transient stability limits
3. Power system oscillation limits
4. Inadvertent flows
5. Short circuit current limits
6. Thermal limits

While there have been traditional solutions to tackle some aspects of these problems, FACTS devices have been increasingly implemented to mitigate these limits, especially in cases where dynamic control is needed at time scales that cannot be provided by traditional solutions, or where FACTS devices have cost and performance advantages over conventional solutions.

FACTS devices can be broadly categorized into series devices and shunt devices.

Shunt devices are primarily nodal devices that provide voltage regulation capability by modulating the reactive power injections into the power system network. The nature of the voltage regulation that these devices can provide may be in the steady state regime (such as support for sustained undervoltage conditions) or dynamic regime (addressing voltage sags or swells). The following are examples of shunt FACTS devices:

1. Static VAR compensator (SVC)
2. Static Synchronous Compensator (STATCOMs)

Series devices are primarily line devices that provide active power flow regulation capability by modulating the line currents of transmission lines. They therefore see use in alleviating power flow problems by counteracting dynamic machine swings, controlling loop flows, and minimizing voltage variations across lines. Based on how these devices achieve this objective, they can be further subdivided primarily into two classes: devices that emulate a series connected controlled-voltage source, and devices that modulate line current by varying their impedance. The following are examples of series connected controlled-voltage source type devices:

1. Static synchronous series compensator (SSSC)
2. Unified Power Flow Controller (UPFC)

The devices listed below are examples of series connected variable impedance type devices:

1. Thyristor switched series capacitor (TCSC)
2. Gate controlled series capacitor (GCSC)
3. Thyristor controlled reactor in parallel with fixed capacitor (TCSC)

Implementations of FACTS control by WAMS/WACS

While the specifics of FACTS devices vary, they share certain central characteristics in terms of how their core control functionality is implemented. These devices receive some form of reference signal that defines the modulation of their network characteristics. These may include voltage signals for nodal shunt-type devices, or the target impedance for branch series-type devices. These reference signals can be internally generated based on *a priori* determined values chosen based on long term operating forecasts, or dynamically computed, based on system measurements obtained in real time. These measurements - and the corresponding signal computation - may be locally obtained, or may be received from more distant controllers over some type of communication channels. These distant sources may be centralized or distributed.

The addition of a cyber-physical layer in the form of a communication layer can enable faster data transfer to, from, as well as between FACTS devices in a network. Such a communication layer, implemented upon a WAMS/WACS allows data to be collected over a wide geographical area, and correspondingly larger system footprint. WAMS measurements typically come from Phasor Measurement Units (PMUs) distributed at key points in the system, communicating through Phasor Data Concentrators (PDCs) to some WACS (which may be either centralized or distributed). These controllers implement coordinated control actions to improve system resiliency in the event of system instability events or other contingencies. A major value proposition of such control is that it enables a system to take corrective control action in the event of a disturbance at speeds that cannot be matched by human operators. Of the various types of FACTS devices, the most common one currently deployed across the world is perhaps the Static VAR Compensator [1]. SVC are often deployed to address short- to medium-term stability issues as they can improve an existing system's performance margin without the need for capital-intensive upgrades.

One major application of the SVC is for addressing inter-area power oscillations in large and weakly connected power systems. Inter-area power oscillations in extant power networks have been extensively studied, such as the Western Electricity Coordinating Council (WECC) system in Western North America[2][3].

Strategically implemented SVCs in such systems, controlled by a WAMS/WACS, have the potential to dampen problematic oscillatory phenomena observed during system operation. The Norwegian system is an example of such an implementation [4]

he addition of the cyber-physical communication layer, however, also creates pathways for cyber-attacks that may take advantage of these interface interaction channels to hinder or alter the normal functioning of these schemes, ultimately adversely affecting the reliability or stability of the power system. Possible attack surfaces for an attacker in such WAMS/WACS-assisted SVC control schemes may involve data integrity attack on the modulation signal transmitted to the SVC, a timing attack that falsifies the time stamp of the measurements obtained from the PDCs, a Denial-of-Service (DoS) attack on the modulation signal being transmitted to the SVC, among a variety of other possibilities, including a combination thereof.

The modeling of the threats, based on a conceptual implementation of WACS control of SVCs in a simple system, is presented in the following section.

Threat Models

To better describe how a cyber attacker may compromise a system, we present a conceptual layout of a SVC controlled by WACS systems, shown in Figure 1.

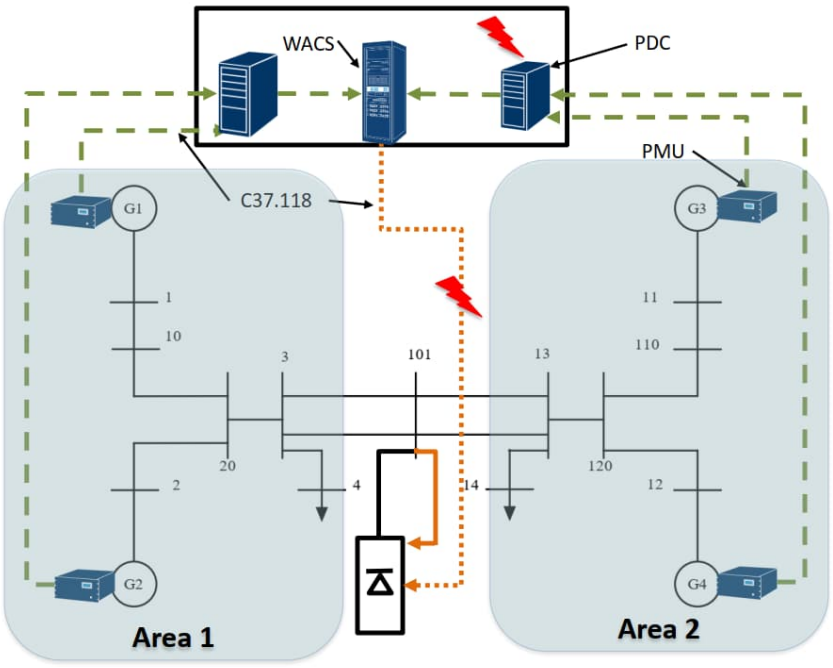


Figure 1 - A conceptual WAMS/WACS layer on the classical 2-area system [5]. An SVC is connected at the inter-area node for inter-area power oscillation damping (POD).

The power network in Figure 1 is the classical two area system. It is a simple system with two distinct areas connected by an inter-tie line. The WAMS/WACS system is overlaid on the physical power system. The WAMS transmits system measurements, obtained from PMUs located throughout the network, via PDCs to the WACS. Using these transmitted measurements, the WACS computes a modulation signal which it then transmits to the SVC. The SVC also collects local measurements from its local bus.

At the SVC device level, the conceptual architecture of the FACTS controller is shown in Figure 2, and is based on [4], [6]. As shown, the SVC can perform its power oscillation damping (POD) functionality using either local measurements or the WACS-generated modulation signal.

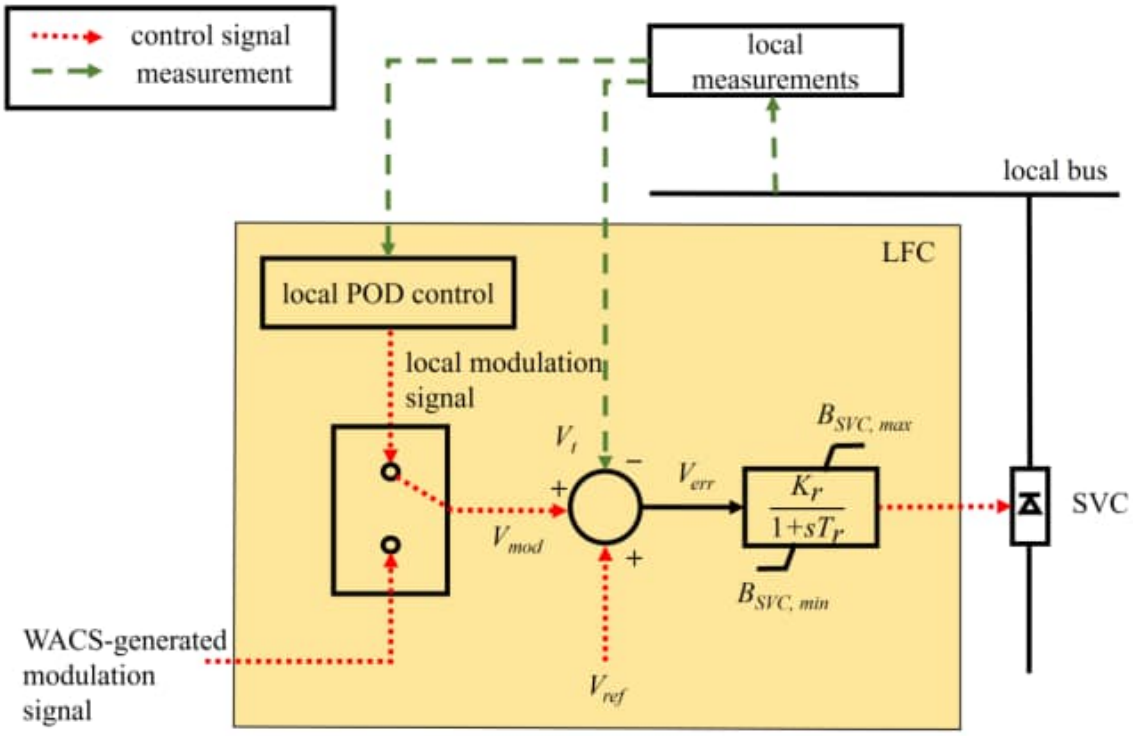


Figure 2 - The local FACTS controller (LFC) architecture adopted for this study. The controller possesses an inner voltage control loop, and an outer POD control loop. The POD functionality may be locally derived, or from the WACS.

Within this system, we now present some generalized threat models for cybersecurity surfaces that are exposed due to the existence of the communications layer. The mathematical models of the threats are also presented herein.

Timing attacks: Timing attacks are types of attacks that falsify the time synchronization stamps of measurement signals, so that a false association is created between the content of the packet and its time stamp. This may be achieved by compromising the synchronization process of one or more PDCs, which collect and temporally align system measurements.

Control data integrity attacks: The integrity of the modulation signal is crucial for the right corrective action to take place in a system. Control data integrity attacks work by corrupting the data in the modulation signal.

Replay attacks: In these types of attacks are realized in two stages. In the first step, attackers gain access to the communication channels that transmit signals and record a portion of a valid signal. In the second stage, the recorded signal is replayed at a later, more opportune moment so as to cause an improper response. Replay attacks may be directed at the WACS-generated control signal, or the measurements in the WAMS.

Denial-of-Service (DoS) attack: This is a type of attack where the communication to the SVC is jammed by flooding the network with spurious packets. This will result in the loss of critical information exchange and thus can affect the SVC's control response by attenuating it.

Development of Cyber Threat Detection and Mitigation Approach

As noted, the WAM/WACS/FACTS ecosystem communicate over the C37.118 protocol used for Synchrophasor communications. It is possible to implement network intrusion/prevention measures relevant to the C37.118 network, which would examine the protocol messages to ensure syntactic correctness as well as adherence to expected communication patterns (whitelisted communication). The defenses implemented by the University of Illinois complement this by introducing a physics-aware defense as we describe below.

The majority of the simulation and analysis work done by the University of Illinois addresses the threat of inducing instability in inter-area oscillations by affecting the mitigative performance of SVCs when performing power oscillation damping (POD). Under correct operation, if a power oscillation arises between weakly connected regions of a transmission system, the WACS can use measurements from the WAMS to compute and transmit a modulation signal to the SVC in its region of control to perform POD We make the following assumptions about the system, and about the cyber attacker's abilities:

1. Individual FACTS devices can effectively dampen oscillations in the power system.
2. The power system is stable when subject to small perturbations under normal WACS control.
3. Only the WAMS/WACS system is subject to attack. All local measurements at the SVC are trusted.

To a reasonable extent, the assumptions made above can be justified.

The first assumption stems from the current practice in power system operations wherein FACTS devices are installed as a short- to medium-term solution. The installation of individual FACTS devices in a power system is done based on preliminary planning studies to dampen troublesome oscillatory modes observed during system operations. Subsequent on-site tuning of the installed FACTS devices on an individual basis is often carried out to ensure each device's damping

characteristics to its locally observed oscillations are ``reasonably good''. The second assumption stems from the typical approach used to design WACS controllers in literature for small-signal instability mitigation. Deployment of a WACS in a power system is usually based on extensive preliminary engineering studies. These studies specify the system level controller designs.

We work with the central premise that a cyber attacker's primary objective is to cause an instability in the system. Based on this central premise, and the assumptions above, we create our stability monitoring (SM) approach to cyber threat detection and mitigation.

A correctly functioning WACS system will result in all observed oscillations at the SVC device to be damped, and a sufficient deviation from this damped behavior may be grounds for the SVC to consider the signal from the WACS to be incorrect or corrupt, in which case the SVC falls back to using its locally modulation capability. Mitigation consists of falling back to local control.

From an implementational standpoint, the local power oscillation at the SVC is monitored in close to real time, and an indication of growing oscillations is used as the trigger to switch the SVC from WACS control mode to local mode. An implementation of this approach is shown in Figure 3.

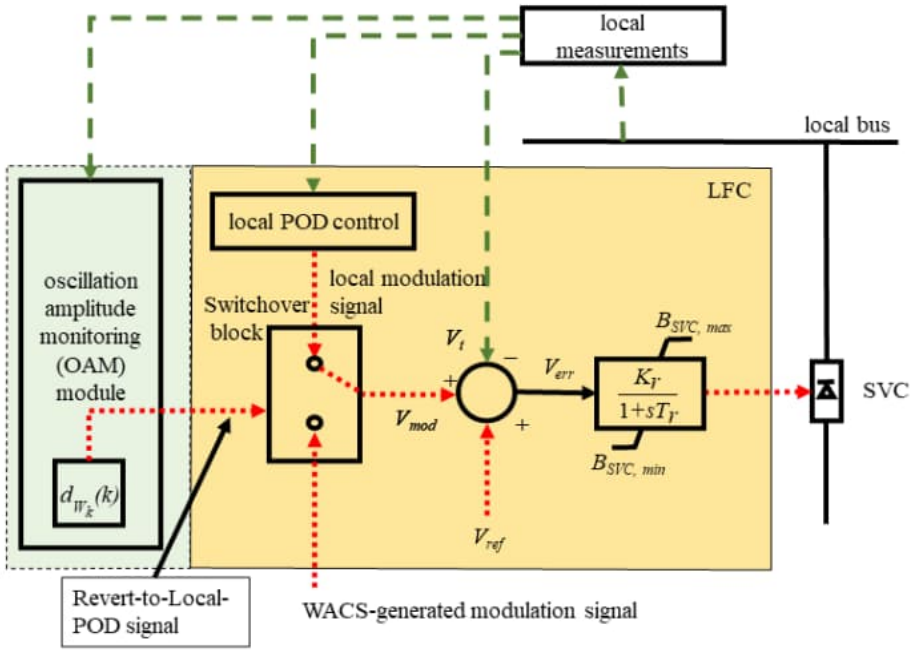


Figure 3 - The implementation of the SM approach to detection and mitigation is accomplished by adding an additional module (in green) to the LFC controller from Figure 2.

We tested two different algorithms to assess stability, and a short description of both are provided below.

Matrix Pencil Method

The Matrix Pencil Method (MPM) [7] for modal analysis is an algorithm that approximate an observed signal into a linear combination of sinusoidal signals. The approximation involves performing singular value decomposition of the data, structured into Hankel matrices. to obtain From this calculation, we are able to reliably identify all modes in the observed oscillation. If any of the observed oscillation modes exceeds a threshold, we conclude that the WACS signal is incorrect, possibly corrupted by a cyberattack. The technical details are in a paper submitted to the 2021 14th IEEE Powertech [8].

Oscillation Amplitude Monitoring (OAM)

During our simulations and extensive testing of the MPM, we observed issues with using the MPM to monitor system oscillation modes in real time over a sliding window. In particular, the reconstruction was found to be unreliable when the data window was small (had few data points). To get over this challenge, we developed a simpler algorithm to monitor decaying oscillation, which we refer to as Oscillation Amplitude Monitoring (OAM), OAM uses the maximum and minimum values of an observed signal as a first-order approximation for the signal amplitude. This approximation is monitored for decreasing amplitude. If the amplitude is found to increase, it is a sign that the observed oscillation is growing. The OAM has the advantage that it can also be used in situations where the power flow shows non-smooth behavior, is much less resource intensive to implement, and can provide tighter bounds on the acceptable threshold. The full details are in a paper submitted to IEEE SmartGridComm, 2021 [9].

Key Achievements

Papers

1. A.Chattopadhyay, A.Valdes, P. W. Sauer, R. Nuqui, "A Cyber threat Mitigation Approach For Wide Area Control of SVCs using Stability Monitoring", 14th IEEE PowerTech, 2021 (Recipient of the Basil Papadias Award for the Best Student Paper).

Abstract: We propose a stability monitoring (SM) approach for the mitigation of cyber threats directed at the wide area control (WAC) system used for coordinated control of Flexible AC Transmission Systems (FACTS) used for power oscillation damping (POD) of active power flow on inter-area tie lines. The approach involves monitoring the modes of the active power oscillation on an inter-area tie line using the Matrix Pencil (MP) method. We use the stability characteristics of the observed modes as a proxy for the presence of destabilizing cyber threats. We monitor the system modes to determine whether any destabilizing modes appear after the WAC system engages to control the POD. If the WAC signal exacerbates the POD performance, the FACTS falls back to POD using local measurements. The proposed approach does not require an expansive system-wide view of the network. We simulate replay, control integrity, and timing attacks for a test system and present results that demonstrate the performance of the SM approach for mitigation.

2. A.Chattopadhyay, A.Valdes, P. W. Sauer, R. Nuqui, "A Localized Cyber Threat Mitigation Approach For Wide Area Control of FACTS", IEEE SmartGridComm, 2021

Abstract: We propose a localized oscillation amplitude monitoring (OAM) method for the mitigation of cyber threats directed at the wide area control (WAC) system used to coordinate control of Flexible AC Transmission Systems (FACTS) for power oscillation damping (POD) of active power flow on inter-area tie lines. The method involves monitoring the inter-area tie line active power oscillation amplitude over a sliding window. We use system instability – inferred from oscillation amplitudes growing instead of damping – as evidence of an indication of a malfunction in the WAC of FACTS, possibly indicative of a cyberattack. Monitoring the presence of such a growth allows us to determine whether any destabilizing behaviors appear after the WAC system engages to control the POD. If the WAC signal increases the oscillation amplitude over time, thereby diminishing the POD performance, the FACTS falls back to POD using local measurements. The proposed method does not require an expansive system-wide view of the network. We simulate replay, control integrity, and timing attacks for a test system and present results that demonstrate the performance of the OAM method for mitigation.

Reports

Threat Model

The university prepared and submitted a threat model document as a project deliverable. In order to make the present report self-contained, key material from the threat model document has been incorporated here.

Red Team and Red Team Response

The Red Team evaluation was done by the University of Illinois under a separate contract from the main project. The red team evaluated our system model, threat assumptions, and results. They responded with findings to be clarified and addressed. The project team compiled a response to the initial red team document. The final red team document includes this project team response as an appendix.

References:

[1] X.-P. Zhang, C. Rehtanz, and B. Pal, Flexible AC Transmission Systems: Modelling and Control. Springer, 2012

[2] "Modes of inter-area power oscillations in western interconnection," Western Electricity Coordinating Council, Tech. Rep., 2013.

[3] B. J. Pierre, *et. al*, "Design of the pacific DC intertie wide area damping controller," *IEEE Transactions on Power Systems*, vol. 34, no. 5, pp. 3594–3604, September 2019.

[4] K. Uhlen et. al, *"Wide-area power oscillation damper implementation and testing in the Norwegian transmission network," in* Proceedings of the 2012 IEEE Power and Energy Society General Meeting, *San Diego, CA, July 2012, pp. 1–7*

[5] P. Kundur, Power System Stability and Control. McGraw-Hill, 1994

[6] E. V. Larsen and J. H. Chow, “SVC control design concepts for system dynamics performance,” *IEEE Special Symposium on Applications of Static VAR Systems for System Dynamic Performance*, 1987.

[7] Y. Hua and T. Sarkar, “Matrix pencil method for estimating parameters of exponentially damped/undamped sinusoids in noise,” *IEEE Transactions on Acoustics, Speech, and Signal Processing*, vol. 38, no. 5, pp. 814–824, May 1990.

[8] A. Chattopadhyay, A. Valdes, P. W. Sauer, & R. Nuqui, “A Cyber Threat Mitigation Approach for Wide Area Control of SVCs using Stability Monitoring” 2021 IEEE Madrid PowerTech

[9] A. Chattopadhyay, A. Valdes, P. W. Sauer and R. Nuqui, "A Localized Cyber Threat Mitigation Approach For Wide Area Control of FACTS," 2021 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), 2021, pp. 264-269.

APPENDIX C: IOWA STATE UNIVERSITY FINAL REPORT

Anomaly Detection and Mitigation System for FACTS-based Wide-Area Control System (WACS)

Project Title: Cyber Resilient Flexible AC Transmission System (Lead: ABB)

Iowa State University, January 2022

Participants: Burhan Hyder, Vivek Kumar Singh, Kush Khanna, Manimaran Govindarasu (PI)

Table of Contents

1. Executive Summary 3
2. Products 3
3. Problem Description 3
4. Concept Development 4
4.1 FACTS-based WAVCS: Architecture & Design 4
4.2 Design of FLC 4
4.3 Proposed Anomaly Detection and Mitigation System: Methodology and Architecture 6
4.3.1 Offline Process 6
4.3.2 Real-Time Implementation Process 9
5. HIL Testbed-based Real-Time Evaluation 10
5.1 HIL Testbed Architecture and Implementation 10
5.2 Testing and Performance Evaluation 11
5.2.1 FL-WAVCS Model Simulation for Dataset Generation 11
5.2.2 Performance evaluation of the MLADS (Offline Process) 11
5.2.3 Real-Time Performance Evaluation 13
6. Red Team Testing 15
6.1 Red Team Attack Scenarios 15
6.2 Performance Evaluation for Red Team Test Scenarios 16
7. Conclusion 17
8. References ..... **Error! Bookmark not defined.**

1. Executive Summary

With the increasing deployment of Flexible AC Transmission System (FACTS) devices in wide-area voltage control systems (WAVCS) for achieving improved voltage stability of bulk power systems, the possibility for cyber-attacks on these systems is also increasing. Successful stealthy cyber-attacks that are difficult to detect by traditional informational technology (IT)-based cybersecurity solutions or threshold-based bad data detectors can lead to a voltage collapse in power grid. This report presents: (1) Testbed-based WAVCS implementation with attacks; (2) Real-time implementation and evaluation of machine learning (ML) algorithm for detecting and mitigating stealthy cyber-attacks on FACTS-based WAVCS on a hardware-in-the-loop (HIL) testbed; and (3) Testing and evaluation of the proposed anomaly detection and mitigation (ADM) system based on attack scenarios and responses suggested by the Red-Team. First, it outlines FACTS-based WAVCS and the implementation of the ML-based Anomaly Detection and Mitigation System. Then, it discusses the performance of the ADM system, evaluated within ISU's cyber-physical HIL testbed, using attack scenarios suggested by the red team. The attacks were injected in real-time over the wide-area network (WAN) within the testbed. The results show accurate and effective performance of ADM system in detecting and mitigating anomalies/attacks while keeping the grid stable and within the System Operating Limits (SOL), defined by the North America Electric Reliability Corporation (NERC).

2. Products

1. V.K. Singh, "Attack Resilient Algorithms and Testbed Federation for Wide-Area Protection and Control in Smart Grid," Ph.D. Thesis, Iowa State University, Fall 2020.
2. V.K. Singh, M. Govindarasu, and R. Nuqui, "Impact analysis of data integrity attacks on facts-based wide-area voltage control system," IEEE PES ISGT, 2021.
3. B. Hyder, V.K. Singh, M. Govindarasu, and R. Nuqui, "Machine Learning-based Cyber-Physical Anomaly Detection in Wide Area Voltage Control Systems," IEEE PES ISGT, 2022 [accepted].
4. B. Hyder, V.K. Singh, M. Govindarasu, and R. Nuqui, "Anomaly Detection and Mitigation in FACTS-based Wide-Area Voltage Control Systems using Machine Learning," IEEE PESGM, 2022 [submitted].

3. Problem Description

With the ever-increasing demand of electric loads, reliable operation of the power grid faces new challenges everyday especially given the uncertain and extreme weather conditions and a shift from conventional power sources to the distributed energy resources (DERs). Voltage security is one of the most crucial areas of concern when it comes to reliable operation of the grid. The North American Electric Reliability Corporation (NERC) recommends the application of wide-area monitoring systems using the synchrophasor technology necessary to identify and prevent major voltage collapses [1]. This implies that wide-area voltage control systems (WAVCS), one of the critical applications within Wide-Area Control System (WACS), are now a priority for power utilities to control, protect, and ensure reliable operations of the bulk power system [2].

The North American Transmission Forum (NATF) recommends use of FACTS devices, such as Static VAR Compensator (SVC) and Static Synchronous Compensator (STATCOM) for improving voltage stability [3]. Since the WAVCS relies on the wide-area network (WAN) for monitoring and control, it is susceptible to cyber-attacks that exploit the vulnerabilities in the system [4], [5]. Successful cyber-attacks

on these systems can be catastrophic and can lead to voltage collapse of the grid. It has, thus, become imperative to design, develop, and deploy defense-in-depth measures that can fend off stealthy cyber-attacks when the traditional IT cybersecurity systems fail to do so.

4. Concept Development

4.1 FACTS-based WAVCS: Architecture & Design

In this section, we discuss a high-level system architecture, as shown in **Figure 4-1**, of the fuzzy logic-based wide-area voltage control system (FL-WAVCS). It consists of a fuzzy logic controller (FLC) that receives phasor measurements from different sensitive buses and sends an optimal voltage setpoint (Vref) every 0.2 seconds to the deployed static VAR compensator (SVC) device of rating 300 MVAR to inject or absorb reactive power as required to improve the voltage profile during disturbances. This architecture is implemented on the modified Kundur's four-machine two-area system, which consists of four generators, and an additional PQ load (60 MW, 30 Mvar) is connected to the bus 10 to create a voltage stress in the selected system. **Figure 4-1** also illustrates attack surfaces on measurement and control signals, as highlighted by lightning bolt symbols, that can be exploited to inject severe disturbances in the grid network.

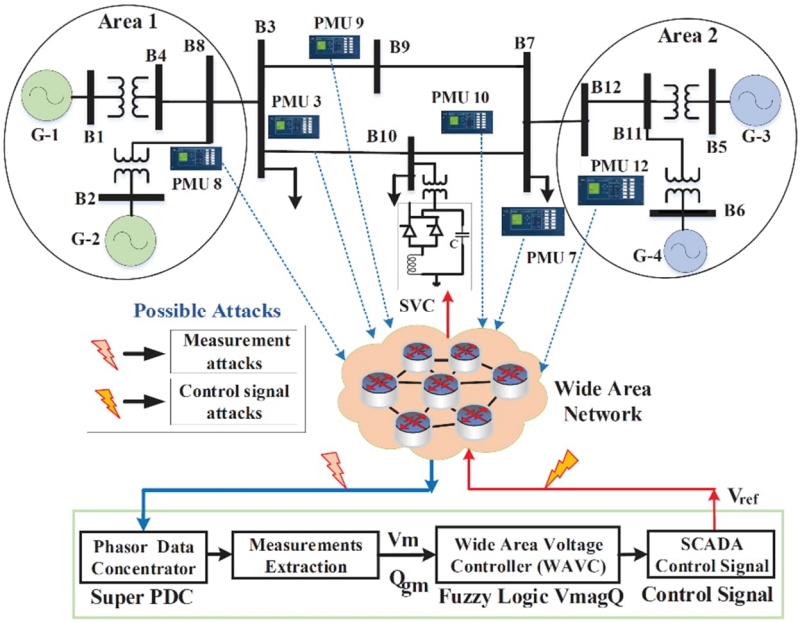


Figure 4-1: High-level system architecture of WAVCS with its attack surfaces

4.2 Design of FLC

We have developed a control center-based FLC, as discussed by the Bonneville Power Administration (BPA) [6], [7]. The design of this controller is discussed in several steps here.

Step 1 (Voltage stability analysis): For developing this controller, we have initially computed sensitive voltage nodes using the static voltage stability analysis [8] based on the Jacobian matrix, J, as shown in (1). ΔP and ΔQ represent the incremental changes in active and reactive powers. ΔΘ and ΔV are incremental changes in bus voltage angle and magnitudes. Assuming change in real power is zero, Q-V analysis can be performed using (2) and (3).

$$J = \begin{bmatrix} J_{P\Theta} & J_{PV} \\ J_{Q\Theta} & J_{QV} \end{bmatrix} = \begin{bmatrix} \Delta P \\ \Delta Q \end{bmatrix} \cdot \begin{bmatrix} \Delta\Theta \\ \Delta V_{PQ} \end{bmatrix}^{-1} \quad (1)$$

$$\Delta Q = \left[J_{QV} - J_{Q\Theta} \cdot J_{P\Theta}^{-1} \cdot J_{PV} \right] \cdot \Delta V_{PQ} \quad (2)$$

$$\Delta Q = J_R \cdot \Delta V_{PQ} \quad (3)$$

$$\Delta V = J_R^{-1} \cdot \Delta V_{PQ} \qquad (4)$$

For the given Kundur system, the computed reduced Jacobian matrix, J^{-1} , is a square matrix; and hence singular value approach can be applied for the static voltage stability analysis. **Figure 4-2** illustrates the computed magnitude of the output singular vector for all buses for a maximum singular value of 0.135. Bus 10 represents the most sensitive node with a computed magnitude of 0.65734 and SVC is deployed on this bus to improve the transient voltage stability during disturbances.

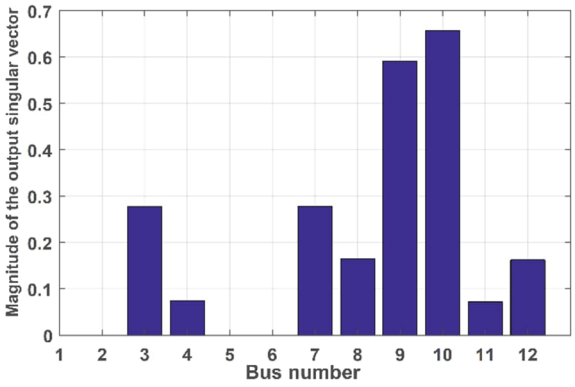


Figure 4-2: Output singular vector plot for the static voltage stability analysis

Step 2 (Apply VmagQ algorithm): We have applied the rules-based VmagQ algorithm [7] to calculate *Vref* to the local SVC (FACTS) device. **Figure 4-3** illustrates the VmagQ algorithm-based control scheme for FL-WAVCS. This algorithm utilizes voltage magnitude measurements (Vb9, Vb3, Vb7, and Vb10) of top four sensitive buses — bus 9, bus 3, bus 7, and bus 10, based on their rankings on the magnitude of the output singular vector. Also, reactive powers (Qb8 and Qb12) of area 1 and area 2 using bus 8 and bus 12 are considered for input features as they provide the accumulative power injection for these four sensitive buses. The overall scheme is categorized into four major stages:

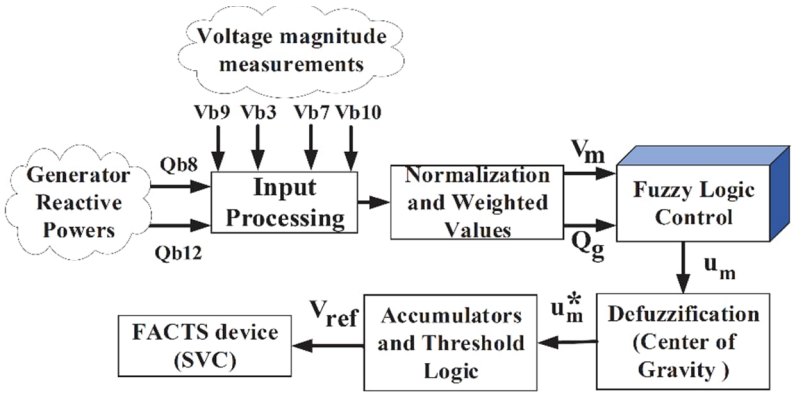


Figure 4-3: VMagQ algorithm-based FLC scheme of FL-WAVCS

Stage 1: Performs an input processing to validate input phasor signals and later compute V_m and Q_g as normalized and weighted values as input features for FLC. In this case, different weights for selected buses are assigned based on their magnitudes of output singular vector. We have performed offline analysis to compute weights of 0.58 to bus 8 and 0.42 to bus 12 for reactive power measurements based on the reactive power injection during physical disturbances.

Stage 2: Applies a set of fuzzy rules, as defined in [6], and provides an output u_m using membership functions. For example, if Q_g is positive large and V_m is low, then u_m is positive large so that SVC can inject more reactive power to improve voltage profile. We have considered triangular membership functions, where isosceles triangle membership functions are applied for small and medium values and end functions are considered for large values while the output is residing between 1 to -1. Further, we have considered min-max logic during fuzzy inference where maximum value is selected when multiple rule conflicts the output variable.

Stage 3: The computed u_m is forwarded for defuzzification that produces a crisp output value u_m^* with domain ±1 using the center of sums method [6].

Stage 4: Finally, *Vref* is computed by re-scaling the output domain ±1 to 0-1 range. Further manual tuning and testing is required to avoid frequent changes in output value, computing threshold logic for output updates, and analyze voltage profile for different *Vref.*

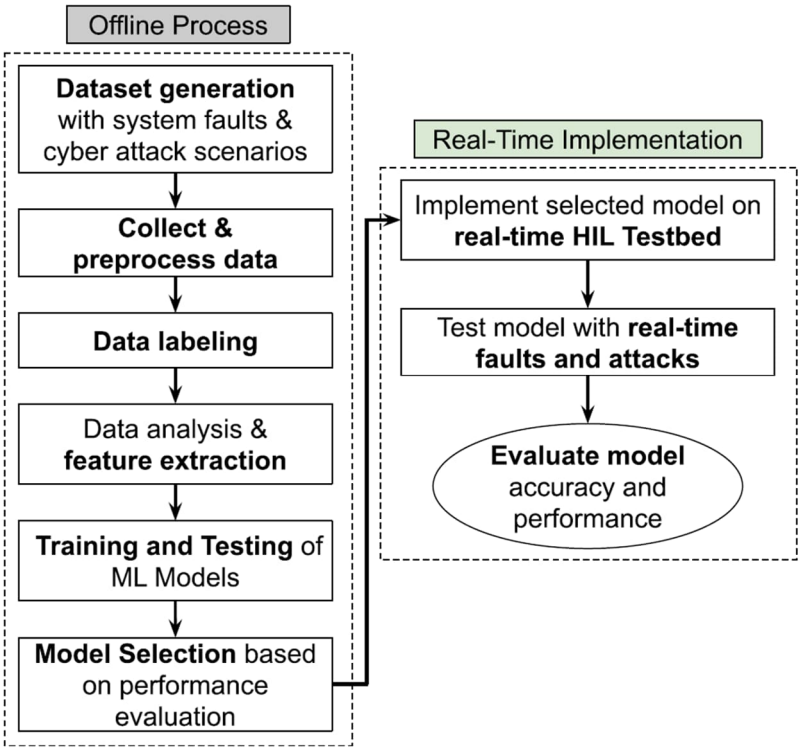


Figure 4-4: Proposed Anomaly Detection and Mitigation System Methodology

4.3 Proposed Anomaly Detection and Mitigation System: Methodology and Architecture

Figure 4-4 shows the methodology adopted for the development and evaluation of the proposed Anomaly Detection and Mitigation (ADM) system. The methodology involves two broad steps, *offline process* and *real-time implementation process.*

4.3.1 Offline Process

Machine Learning algorithms are being extensively used for detection of anomalies in Cyber-Physical Systems (CPS). By making predictions, decisions, and classifications based on data, ML algorithms enable us to build models for applications that otherwise are challenging to design. We propose a ML-based Anomaly Detection System (MLADS) for accurate classification and detection of a broad range of anomalies that can exist in the WAVCS due to stealthy cyber-attack injections. The essential components for building the MLADS include dataset generation, feature extraction from the generated dataset, and the ML algorithms for classification or regression. A flowchart depicting the MLADS algorithm is shown in **Figure 4-5**.

Dataset Generation: Prior to creation of ML-based models, ensuring availability of sufficient data is vital for the design and optimal performance of any anomaly detector. To have enough data for highly accurate performance of the MLADS, we consider a combination of system faults and stealthy cyber-attack vectors for the dataset generation. Stealthy cyber-attacks are carried out on both measurement signals coming into the FLC from PMUs and control signals being forwarded by the FLC to the SVC over the wide-area network, as shown in **Figure 4-1**. Two types of data-integrity attacks are considered:

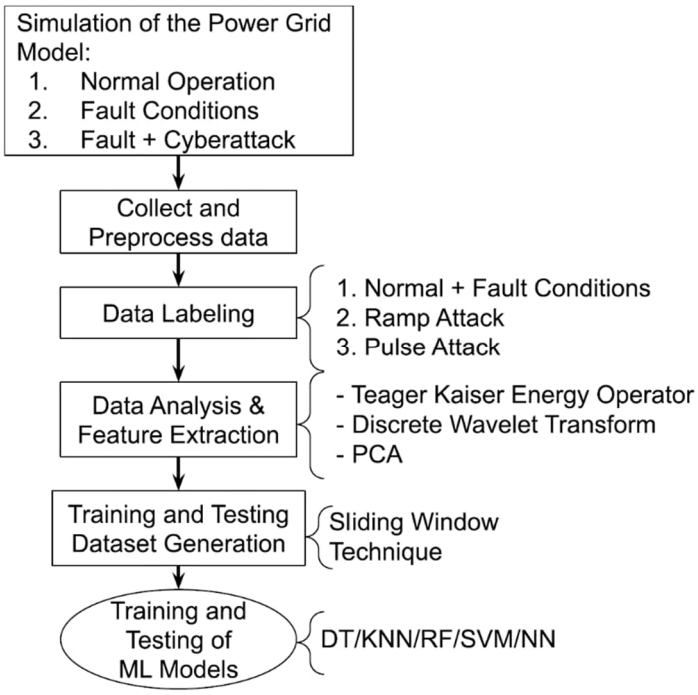


Figure 4-5: Flowchart depicting Offline Process

a. **Ramp Attack**: Ramp attack on the measurement or control signals involves either continuous increase or decrease of the amplitude of the signal being attacked by addition or subtraction of attack vector parameters, respectively, to the target signal. Ramp attack involves adding a time-changing ramp signal with a ramp signal parameter, λ_{ramp} to the input signal, $P_i(t)$, shown in (5).

$$P_{ramp}(t) = P_i(t) + \lambda_{ramp} \times t \qquad (5)$$

b. **Pulse Attack:** Pulse attack on the measurement or control signals involves a usually high frequency (as compared to system frequency) pulse signal multiplication to the target signal, rapidly manipulating its magnitude. Pulse attack vector periodically changes an input control signal, $P_i(t)$, by adding the pulse attack parameter, λ_{pulse}, for a small-time interval, (t1) and retaining the $P_i(t)$, for a remaining interval, (T- t1), for the given time period, (T), as shown in (6).

$$P_{pulse} = \begin{cases} P_i(1 + \lambda_{pulse})(t = t_1) \\ P_i(t = T - t_1) \end{cases} \qquad (6)$$

Appropriate adjustment of the parameters of the attack vectors enables cyber attackers to bypass the conventional bad-data detectors. To generate a wide variety of data integrity attacks on the measurement and control signals, we use the combination of a wide range of parameters of the ramp and pulse signal attacks in addition to simulating system faults in the two-area Kundur system. Since MLADS uses supervised ML algorithms for detection of anomalies, the next stage after the collection of data from attack and fault simulations is labeling of the data. The labeling stage involves assignment of tags to each data point in the generated dataset for the corresponding event in the power system.

Feature Extraction: Appropriate feature extraction and selection from the raw dataset is an effective way of increasing efficiency and accuracy of trained ML-models. For accurately distinguishing cyber-attacks from system faults and normal operation, it becomes necessary to extract physics- and entropy-based features apart from using the raw data. MLADS uses two such feature vectors extracted for each data point in the generated dataset to improve the accuracy of anomaly detection:

a. **Discrete Wavelet Transform (DWT)**: This feature allows for accurate and fast decomposition of the given signals in the frequency domain both for short-period frequency components (transients) and for long-period frequency components (fundamental and harmonics). Such a decomposition is very efficient in differentiation between short- and long-term faults and normal operation. The DWT is defined by the approximation wavelet coefficients C_j^a (low-frequency component) and the detail wavelet coefficients C_j^d (high-frequency component) at each wavelet decomposition level j. The energies of the approximation coefficitents g_j^a and the detail coefficients g_j^d at the jth decompostion level are shown below.

$$g_j^a = \sum |C_j^a|^2$$
$$g_j^d = \sum |C_j^d|^2$$

b. **Teager Kaiser Energy Operator (TKEO)**: This feature represents instantaneous energy of the signal at any point of time and, thus, allowing for an accurate segregation of normal operation, fault, and attack scenarios where the instantaneous energy can differ significantly. For a discrete time-signal x_n, where n is the time-step, the Teager Kasier operator is shown below.

$$\Psi[x_n] = x_n^2 + x_{n-1} \times x_{n+1}$$

Post feature extraction, *Principal Component Analysis (PCA)* is carried out on the feature dataset. PCA helps in dimensionality reduction of the feature dataset by giving higher weightage to the highly uncorrelated features present in the data which explain majority of the variance (e.g., >95% variance) in the output, thus, reducing the computational burden of the algorithm being used.

ML Algorithms: Once the dataset is generated with extracted features and PCA, training and testing datasets are extracted from this dataset for training and testing different ML algorithms, respectively. The proposed MLADS uses supervised ML algorithms for classification and detection of anomalies in the FL-WAVCS. Using the training dataset, multiple algorithms including *Support Vector Machine (SVM), K-Nearest Neighbor (KNN), Decision Tree (DT), Neural Network (NN),* and *Random Forest (RF)* algorithms are trained. The performance of these algorithms is compared using the test dataset. For creating training and testing datasets, we use the sliding window technique to aggregate multiple data points from the originally generated time-series dataset which allows for improved performance of these algorithms. The sliding window technique aggregates multiple data points together based on the selected window size and uses a first-in first-out method to include the latest data point in the window while removing the oldest data point.

4.3.2 Real-Time Implementation Process

The *real-time implementation* process involves: (1) Implementation of trained KNN model in the HIL Testbed; (2) Simulation of system faults and injection of real-time stealthy cyber-attacks through the communication network; and (3) Evaluating the performance of the ADM system using attack detection time and accuracy as well as monitoring power system stability after mitigation of cyber-attacks.

We use the Voltage Profile Index (VPI) of the power grid given by (7) as a metric to monitor the voltage stability of the grid and to evaluate the performance of the ADM system.

$$VPI = \frac{1}{n}\sum\sqrt{\frac{1}{T}\sum_{i=1}^{T}(|V_{i,ref}| - |V_i|)^2}$$

where T is the simulation time-step, V_i is the voltage magnitude at bus i, and $V_{i,ref}$ is 1 pu for all the buses. The bus voltages taken into consideration for calculating the VPI are V_{B3}, V_{B7}, V_{B8}, V_{B9}, V_{B10}, and V_{B12} (n = 6) shown in **Figure 4-1:** High-level system architecture of WAVCS with its attack surfaces.

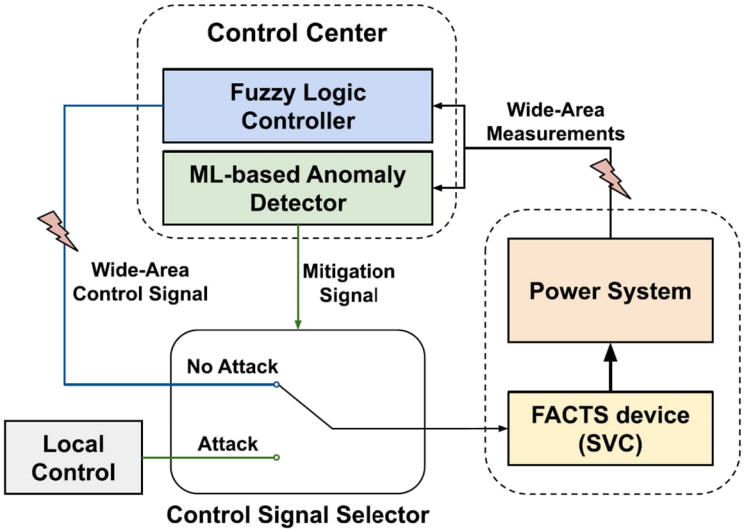


Figure 4-6: Overview of Anomaly Detection and Mitigation Implementation Methodology

The methodology used for mitigating the cyber-attacks is depicted in **Figure *4-6***. The FACTS device (SVC)-controlled power system sends wide-area measurements to the FLC and the ADM system situated in the control center. The FLC calculates a control signal based on the input measurements and sends an appropriate control signal (V_{ref}) to the SVC. The ADM system constantly monitors the power system for anomalies using the input measurements. In case the ADM system detects an anomaly, it sends a mitigation signal to the *Control Signal Selector* which switches the control signal of the SVC from *wide-area control* to *local control*. The *Local Control* provides a constant V_{ref} to the SVC affecting the optimal operation of the power system. When the cyber-attack is stopped, the ADM system resets the mitigation signal and subsequently, the input control signal to the SVC is switched back to the wide-area control signal sent by the FLC to allow for wide-area voltage control of the power system for optimal operation of the grid.

5. HIL Testbed-based Real-Time Evaluation

5.1 HIL Testbed Architecture and Implementation

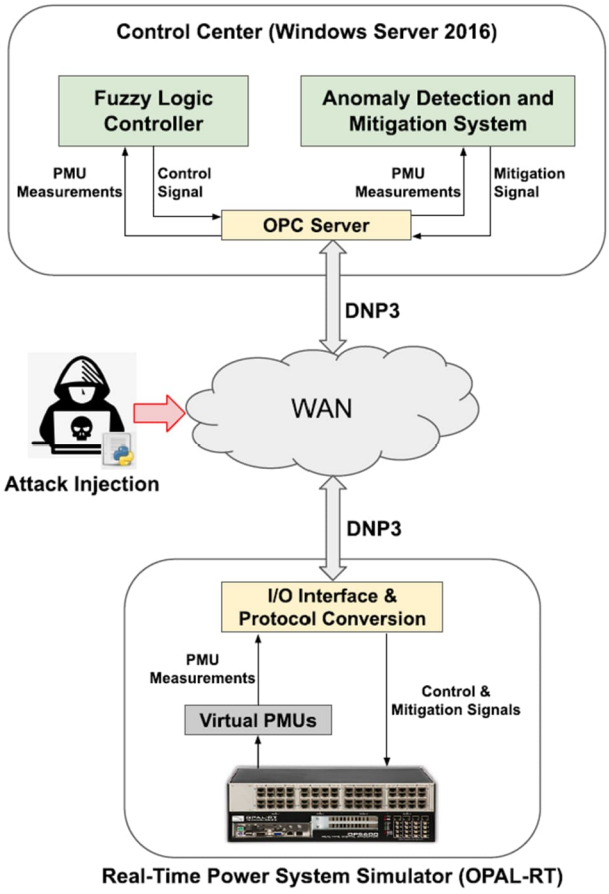


Figure 5-1: HIL Testbed-based architecture for Anomaly Detection and Mitigation

Figure 5-1 shows the overall architecture for implementation of the ADM system in the HIL testbed present at the Iowa State University. The SVC-based two-area Kundur power system is implemented in the real-time power system simulator, OPAL-RT, using the eMEGASIM solver. The PMU measurements from the virtual PMUs within OPAL-RT are converted to DNP3 communication protocol and sent over the wide-area network (WAN) to the OPC server in the control center. The control center is emulated using a Windows 2016 Server machine with the FLC and the ADM system implemented in real-time MATLAB environment. The FLC and the ADM system receive wide-area measurement signals from the OPC server. The FLC sends the control signal to the SVC in OPAL-RT over the WAN through the OPC Server. Pulse and ramp attack signals are injected by the attacker (emulated on a Windows 2016 Server) through the WAN. After injection of attacks, the ADM system detects and classifies the attacks and sends an appropriate mitigation signal back to the power grid (as depicted in **Figure 5-1**) through the OPC server over the WAN. The control signal and the mitigation signal are also sent using DNP3 communication protocol to the OPAL-RT.

5.2 Testing and Performance Evaluation

5.2.1 FL-WAVCS Model Simulation for Dataset Generation

The two-area four-machine Kundur power system is implemented on OPAL-RT, a real-time digital simulator, using its ARTEMiS library which allows faster simulations at time-steps of the order of a few microseconds which is necessary for simulating the FACTS device (SVC) model. The simulation (refer to **Figure 4-1**) includes a 3-Phase-to-Phase fault on one of the inter-tie buses (B9) and ramp and pulse attacks with varying parameters on the measurement signals from the PMUs and control signal sent to the SVC from the FLC.

Table 1: Attack Vector Injection Parameters

Attack Vector	**Parameters**
Pulse Attack (Measurement & Control)	Duty Cycle (%) = [30, 50, 80] Period = [0.5, 1, 1.5, 2] Amplitude = 1 Start Time (seconds) = [4, 10]
Ramp Attack (Measurement & Control)	Slope = [1, 2, 3, 4, 5] Start Time (seconds) = [4, 10]
Fault Type	**Fault Duration**
L-L-L (A-B-C) at B9	Start Time (seconds) = 8 End Time (seconds) = 8.2

Various parameters for the attack vector injection are depicted in **Table *1***. The dataset generated consists of 4 bus voltage magnitude signals (Vb9, Vb3, Vb7, and Vb10), 2 reactive power flow measurements (Qb8 and Qb12), 2*6 (12) coefficients of TKEO, and 2*6 (12) coefficients of DWT. The complete feature dataset thus consists of 30 features. For dimensionality reduction, we conduct PCA on the feature dataset which retained 16 features (explaining 99\% variance) that are used for generating the training and testing datasets. The complete dataset contains 3.35 million data points. The training and testing datasets have 70% and 30% of the data points from the complete dataset, respectively, which are split randomly. The training and testing are performed in a MATLAB environment (Classification Learner App) on a Windows Server 2016 with Intel(R) Xeon(R) Gold 5120 CPU @ 2.20GHz, 4 Cores and 32 GB RAM.

5.2.2 Performance evaluation of the MLADS (Offline Process)

Table 2: Performance Comparison of various ML Algorithms

Algorithm	**Overall Accuracy**	**TPR-1**	**TPR-2**	**TPR-3**	**Training Time (sec)**	**Prediction Time (obs/sec)**
Fine KNN	99.99%	100.0%	99.96%	100.0%	44.58	~330000
Fine Gaussian	94.1%	99.9%	90.3%	85.9%	19112	~350
Fine DT	91.3%	99.7%	84.3%	82.1%	23.42	~530000
NN	90.9%	100.0%	78.4%	83.7%	4775.1	~880000
RF	87.7%	99.1%	48%	90.9%	247.58	~100000

Table *2* shows the performance comparison of the four ML algorithms in terms of overall accuracy, true positive rates (TPR) for each class, training time, and prediction time. The overall accuracy is the overall percentage of observations that are correctly classified for all classes, the TPR is the proportion of correctly classified observations per true class, the training time is time taken for the algorithm to train using the training dataset, and the prediction time is the time taken by the trained algorithm to classify test data. We have defined three classes or labels for the dataset used: (i) **Label-1** defines Normal Operation and/or System Fault; (ii) **Label-2** defines Pulse Attack on either the measurement or the control signals; and (iii) **Label-3** defines Ramp Attack on the measurement or control signals. Evidently, the fine KNN algorithm outperforms the other algorithms that have been tested, namely, Support Vector Machine (Fine Gaussian SVM), Decision Tree (Fine DT), 3-layered Neural Network (NN), and Random Forest (RF). We have also shown detailed results for the Fine KNN algorithm.

Table 3: Confusion Matrix for Fine KNN

True↓/Predicted→	**Label-1**	**Label-2**	**Label-3**
Label-1	503415	0	0
Label-2	0	179979	74
Label-3	0	10	324118

Table 4: TPR and FNR for Fine KNN for all Three Classes

	Label-1	**Label-2**	**Label-3**
TPR	503415	0	0
FNR	0	179979	74

Table *3* shows the Confusion Matrix for Fine KNN with the total number of correctly and incorrectly classified observations from the test dataset with an overall accuracy of 99.99%. **Table *4*** shows the TPR and the False Negative Rate (FNR) for Fine KNN for each class. A 10% TPR for Label-1 in case of Fine KNN shows that the algorithm has no false negatives in terms of classifying and detecting anomalies (i.e., 100% detection accuracy). The negligible inaccuracy (~0.04%) in classification for this algorithm exists only within the correct classification of the type of attack within the dataset (**Label-2** and **Label-3**), highlighting the highly accurate attack detection performance of Fine KNN.

Figure 5-2 shows the receiver operating characteristic (ROC) curve for Fine KNN with the area under the curve (AUC) approximately equal to 1 which again depicts the highly accurate performance of the algorithm.

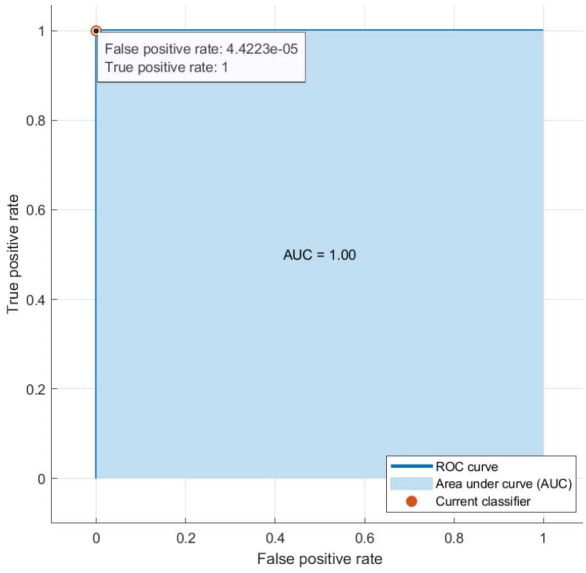


Figure 5-2: ROC curve for Fine KNN

5.2.3 Real-Time Performance Evaluation

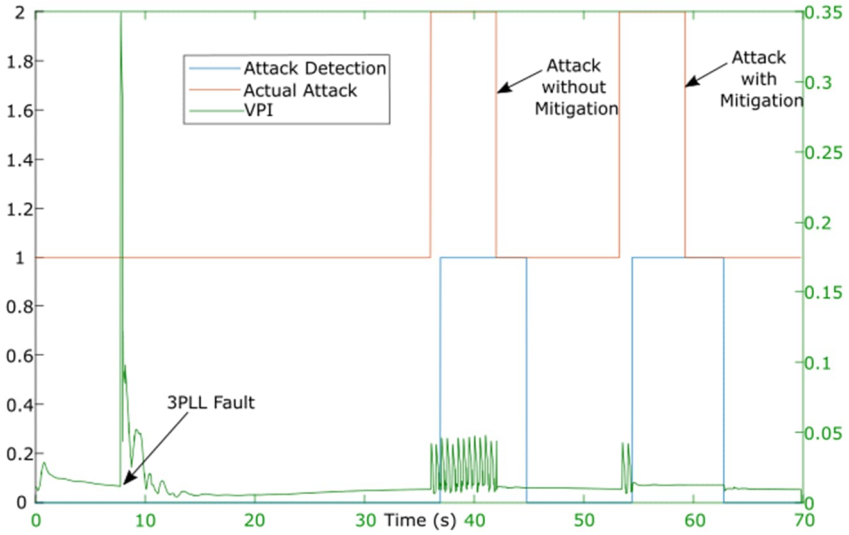


Figure 5-4: VPI and Attack Detection by ADM Algorithm for Pulse Attack on Control Signal

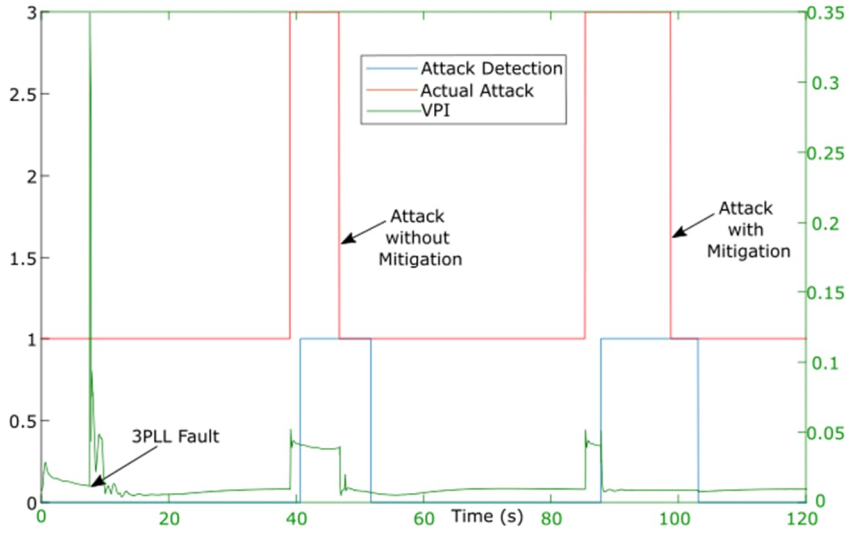


Figure 5-3: VPI and Attack Detection by ADM Algorithm for Ramp Attack on Control Signal

Figure 5-3 and **Figure 5-4** show the VPI of the system under fault conditions (3-phase line-to-line (3PLL) fault) and for pulse and ramp attacks on the control signal. The plots also show the time of actual attack injections and time of detection (with and without mitigation) of attack by the ADM system. These results also show the action of the control signal of the FLC which is able to damp the transient oscillations within a few seconds (up to 5 seconds) after the fault is injected and cleared. The red plots show the attack injection by the attacker and the blue plots show the attack detection (with and without mitigation) by the ADM system. During the attack (left y-axis value is 2 for pulse attack and 3 for ramp attack), when the mitigation is turned off, the impact of the attack on the VPI of the system can be seen for the entire duration of the attack even though the attack is detected by the ADM system (left y-axis

value is 1 for attack detected and 0 for no attack detected). On the other hand, when the mitigation is turned on, the impact of the attack is briefly seen on the system VPI due to the short delay in detection (referred to as detection time). Post the detection of the attack, the mitigation signal immediately mitigates the attack impact and stabilizes the system voltage using *local control* instead of *wide-area control*. The mitigation signal resets the system to *wide-area control* as soon as the ADM system detects the removal of attack, further improving the voltage profile.

Table 5: Attack Parameters for plotted results

Attack Vector	**Parameters**
Pulse Attack	Duty Cycle (%) = 50 Period = 0.5 Amplitude = 1
Ramp Attack	Slope = 1
Fault Type	**Fault Duration**
L-L-L (A-B-C) at B9	Start Time (seconds) = 8 End Time (seconds) = 8.2

The attack parameters for the plots in **Figure 5-3** and **Figure 5-4** are shown in **Table *5***. The results for the real-time performance of the ADM system for all the attack parameters mentioned in **Table *1*** are summarized in **Table *6***, averaged for each attack type. The results show that the power system operating limits are well within the System Operation Limits (SOL) set by NERC for bulk power systems which are summarized in **Table *7***.

Table 6: Real-time performance of the ADM system for various attacks

Attack Type	**Average Detection Time (s)**	**Average VPI during Attack** (% deviation from 1 pu)
Pulse Attack (Control) [24 scenarios]	1.17	1.39%
Ramp Attack (Control) [10 scenarios]	2.5	1.51%
Pulse Attack (Measurement) [24 scenarios]	1.55	1.14%
Ramp Attack (Measurement) [10 scenarios]	1.02	1.18%

Table 7: NERC SOL for Bulk Power Systems

System Voltage Limits (% Deviation from 1 pu)	**System State**
± 5%	Normal State (24 hours)
± 8%	Emergency State (≤ 4 Hours)
± 10%	15-minute Emergency State (≤ 15 minutes)

6. Red Team Testing

The red team attack scenarios include data integrity attacks (data manipulation) on the measurement and control signals as well as network attacks that impact the delivery of data packets to either the control center (OPAL-RT) or the power grid (Fuzzy logic Controller & ADM system). The network attacks were carried out in conjunction with a pulse attack on the control signal to evaluate the impacts of the network attacks.

6.1 Red Team Attack Scenarios

Attack Scenario 1 (Denial of Service Attack):
The Denial of Service (DoS) attack involves dropping some packets that are exchanged between the power grid and the Control Center. The parameters for the DoS attack carried out for the red teaming are given in **Table *8***.

Table 8: DoS Attack Parameters

Data Loss Time	**Data Packets Lost (@10ms data rate)**
5 s	500 packets (every 5 seconds)

Attack Scenario 2 (Time Delay Attack):
The time delay attack involves an increased delay in the delivery of measurement and control packets to either the control center or the power grid. The parameters for the time delay attack carried out for the red teaming are given in **Table *9***.

Table 9: Time Delay Attack Parameters

Time Delay	**Data Packet Delivery Delay (@10ms data rate)**
5 s	100 packets per second

Attack Scenario 3 (Data Integrity Attack):
This involves the manipulation of the measurement or control signal using a special ramp attack injection. The ramp attack starts with a small slope and then switches to a higher slope value after a certain time. The parameters for this attack are given in **Table *10***.

Table 10: Special Ramp Attack Parameters

Signal Attacked	Initial Slope	Final Slope
Control Signal	0.1 (for 2 seconds)	10 (after 2 seconds of attack injection)

6.2 Performance Evaluation for Red Team Test Scenarios

For detecting network attacks, additional logic was added to the ADM System to identify packet loss or packet delay. **Figure *6-1*** shows the attack injection, detection, and system VPI for attack scenarios 1 and 2 with coordinated network and pulse attack on the control signal. The attacks are detected by the ADM System within 1 second of network attack injection and the SVC is switched to local control mode during the attack. This mitigates the impacts of the pulse attack injected while the network attacks are present, and the system operates within the NERC System Operating Limits. The SVC is switched back to wide-area control when the network attacks are removed from the system.

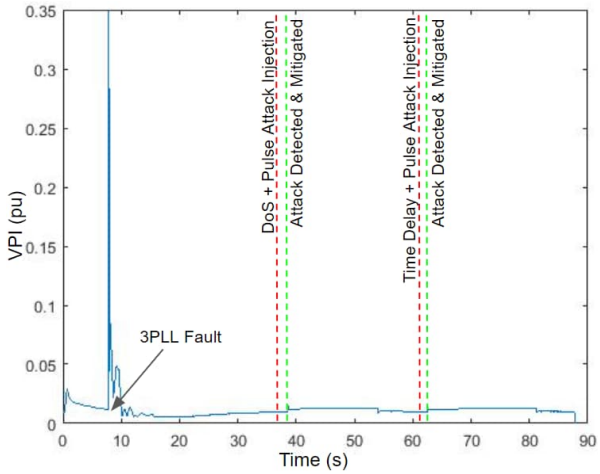


Figure 6-1: Attack Injection, Detection, and System VPI for Attack Scenarios 1 & 2

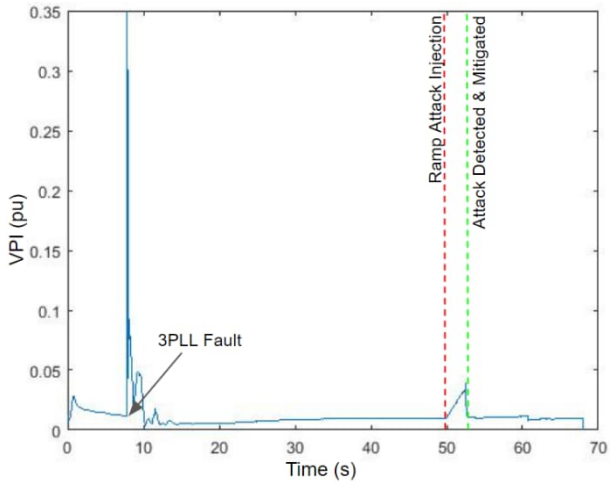


Figure 6-2: Attack Injection, Detection, and System VPI for Attack Scenario 3

Figure 6-2 shows the system performance for Attack Scenario 3 with attack injection and detection. The ADM system detects the attack within 4 seconds of attack injection, mitigating the impacts of the special ramp attack on the control signal and the system operates within the limits. The performance of the system for the red team testing for the attack scenarios is summarized in **Table *11***.

Table 11: Performance Evaluation for Red Team Testing Scenarios

Attack Scenario	**Detection Delay Time**	**Average VPI during Attack** (% deviation from 1 pu)
Attack Scenario 1	1.27 seconds	1.25%
Attack Scenario 2	0.83 seconds	1.26%
Attack Scenario 3	2.48 seconds	1.37%

7. Conclusion

This report shows the development and HIL testbed-based implementation, and red team evaluation of the ML-based anomaly detection and mitigation system for the wide-area voltage control system cybersecurity using local FACTS device in real-time. The experimental results show an efficient performance of the proposed algorithm in presence of stealthy cyber-attacks and system faults by keeping the system stable and within the system operating limits defined by NERC.

8. References

[1] M. Patel, S. Aivaliotis and E. Ellen, "NERC Real-Time Application of Synchrophasors for Improving Reliability," 2010.

[2] M. Perron, E. Ghahremani, A. Heniche, I. Kamwa, C. Lafond, M. Racine, H. Akremi, P. Cadieux, S. Lebeau and S. Landry, "Wide-area voltage control system of flexible AC transmission system devices to prevent voltage collapse," *IET Generation, Transmission & Distribution,* 2017.

[3] NATF, "Transient Voltage Criteria Reference Document," 2016.

[4] NIAC, "Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure," 2017. [Online]. Available: https://www.cisa.gov/.

[5] NIST, "Guidelines for Smart Grid Cybersecurity," 2014.

[6] R. Wilson and C. Taylor, "Using dynamic simulations to design the wide-area stability and voltage control system (WACS)," in *IEEE PES Power Systems Conference and Exposition*, 2004.

[7] C. Taylor, D. Erickson, K. Martin, R. Wilson and V. V. Subramanian, "WACS-Wide-Area Stability and Voltage Control System: R&D and Online Demonstration," in *Proceedings of the IEEE*, 2005.

[8] S. Sridhar and M. Govindarasu, "Model-Based Attack Detection and Mitigation for Automatic Generation Control," *IEEE Transactions on Smart Grid,* 2014.

APPENDIX D: UNIVERSITY OF IDAHO FINAL REPORT

Cyberattack Mitigation on Wind Penetrated Systems Using FACTS Control

University of Idaho

Brian K. Johnson, Dakota Roberson

Christine Page, Andrew Miles, Kendall Bean, Rômulo Bainy

Executive Summary

The initial goal of this work was to develop a scheme to detect power system oscillations triggered by attacks on generator exciters or power system stabilizers, locate the source of the oscillations and use a damping control scheme implemented in a shunt connected flexible ac transmission systems (FACTS) device. The team also included subsynchronous control interactions between type-3 wind turbines and series compensated transmission lines.

The team performed a threat analysis looking at vulnerabilities in synchronous generator controls that could lead to triggering forced oscillations. In addition, the threat analysis also explored approaches an attacker could use to create subsynchronous oscillations in systems with high penetration of wind generation.

In order to test the control scheme the IEEE 12-bus dynamic test system was modified to include a large wind farm installed near a long transmission line. Series capacitor compensation was added to the transmission line.

The damping control scheme was designed and subsequently implemented using a static VAR compensator, and then tested using a real time digital simulator. Phasor measurement units are used as the sensors for the developed frequency deviation regulator. The damping controller was tested in the modified IEEE 12-bus system. Phasor Attack scenarios were created based on the threat analysis document, and the damping controller was tested against these scenarios.

1. Products

a. Publications: None, works in progress
b. Patent Filings: None
c. Other Products:
    i. Panel Sessions Organized
        1. Enhancing Grid Resilience with HVDC and FACTS at IEEE Transmission and Distribution Conference and Exposition, New Orleans, April 2022.
        2. Enhancing Grid Resilience with HVDC and FACTS at IEEE Power and Energy Society General Meeting, Denver, July 2022.

2. Collaborations Fostered

a. Contributing to IEEE Power and Energy Society Power Systems Relaying and Control Committee Working Group on: "Investigate the Effects of SSO Due to IBR on Rotating Machinery"
b. Contribute to formation of IEEE Power and Energy Society Power Systems Relaying and Control Committee Task Force on: "Distributed Cyber Physical Assessment for Grid Resilience"

3. Technical Accomplishment

a. Introduction

The goal of this work was to develop a scheme to detect power system oscillations triggered by attacks on generator exciters or power system stabilizers, locate the source of the oscillations and use a damping control scheme implemented in a shunt connected flexible ac transmission systems (FACTS) device. The team also add a large scale wind farm to the study connected to the power grid via series compensated lines to explore the ability of the damping controller to respond to subsynchronous control interactions between type-3 wind turbines and series compensated transmission lines.

The team performed a threat analysis looking at vulnerabilities in synchronous generator controls that could lead to triggering forced oscillations. In addition, the threat analysis also explored approaches an attacker could use to create subsynchronous oscillations in systems with high penetration of wind generation. In order to test the control scheme the IEEE 12-bus dynamic test system [1] was modified to include a large wind farm installed near a long transmission line. Series capacitor compensation was added to the transmission line.

The damping control scheme was designed and subsequently implemented using a static VAR compensator, and then tested using a real time digital simulator. Phasor measurement units are used as the sensors for the developed frequency deviation regulator. The damping controller was tested in the modified IEEE 12-bus system.

b. Summary of Threat Analysis

The threat analysis performed by the project team showed that attacks on excitation controls for generators could trigger oscillations on a power system. These scenarios looked at cases where either the exciter or the measurement system were accessible through communication network. The attacks of

most interest are those targeting the voltage measurements or voltage references used for the exciter. Since the exciter control primarily impacts reactive power output of a machine, a damping controller based reactive compensator scheme such as a SVC should be able to damp oscillations, even the effects of driven oscillations.

A secondary threat vector looked at attacks on power system stabilizers. It is known that poorly turned power system stabilizers have been observed to create oscillations with neighboring generators. This can be exploited an attacker who either modifies the exciter gains or modifies the measurements received by the exciter. Since the power system stabilizer control primarily impacts reactive power output of a machine, a damping controller based reactive compensator scheme such as a SVC should be able to damp oscillations, even the effects of driven oscillations

A third threat examined in this project was an attack on a machine governor, either the measurements or the set point. Since the control primarily impacts the real power output of a machine, a damping controller based reactive compensator scheme such as a SVC is unlikely to be able to damp driven oscillations, we will be shown in the results.

The threat analysis also identified scenarios where attacks on wind farms or on components in the nearby power system can create oscillations. Attack vectors include attacks on the measurements or references used in the converter controls, attacks that cause circuit breakers to trip transmission lines or transformers, attacks that trip shunt reactors, or attacks that bypass series capacitors. Such attacks can trigger weak grid subsynchronous oscillations in type-3 or type-4 wind turbines. In cases with series compensated lines, a system configuration due to breaker action could create a subsynchronous control interaction that can lead to tripping large wind farms or in the worst case damage to the wind turbines themselves.

c. Research Objectives

The primary goal of this study is to illustrate the efficacy of the use of Static VAR Compensators (SVCs) to modulate reactive power for frequency control for a sample test system which includes a wind park consisting of type 3 wind turbines. Such turbines utilize doubly-fed induction generators (DFIGs) and have been shown to be susceptible to subsynchronous control interactions (SSCI) under various loading conditions [2]. A Phasor Measurement Unit (PMU) is used as the sensor for the developed frequency deviation regulator. SVCs were chosen as the actuator and PMUs as the sensor in the tested control scheme due to their high controllability and increasingly wide-spread adoption in systems with high-penetration of renewable resources. It allows the asset owners to take full advantage of the range of operability of these devices and helps offset costs for wind farm protection.

It has been observed that even under nominal operation, wind turbines generally produce some electrical oscillations in the power systems they are a part of [3], and have observable oscillatory modes [4]. SVCs have the ability to rapidly modulate reactive power and are particularly helpful for compensating high voltage, high impedance lines (i.e., long distances, underwater cabling, etc.). Wind farms tend to be located in remote locations and increasingly offshore [5-7], creating substantial motivation for using SVCs in conjunction with wind power. By controlling the SVCs in a manner which provides support for frequency stability, the costs for implementing proper protective relays for wind farms can be reduced, as well.

PMUs are also seeing more common usage with the increased digitization and remote operation of many substations, and the deployment of 5G cellular communication, the technology surrounding PMUs looks to be advancing rapidly [8]. They have a significantly higher reporting rate than traditional SCADA sensors, usually 30 or 60 Hz, which provides the ability to modulate reactive power at a higher rate (i.e., increased control bandwidth). This enables a controller to reduce the impact of higher frequency oscillations, including harmonics of lower frequency oscillations, though it can introduce more sensor noise into the controller if the controller is improperly designed. As digital sensors are often a predominant bandwidth-limiting feature of a given control system, the importance of a high reporting rate cannot be overstated. Additionally, a PMU can be used as part of many regulating processes simultaneously, which again lowers the potential cost for protective equipment on a grid if it can be used in multiple roles.

d. Modeling

i. Cybersecurity Demonstration System Model in RTDS and EMTP-RV

The IEEE12-Bus system test system [1] shown in Fig. 1 was developed by the IEEE Power and Energy Society working group on Dynamic Performance and Modeling of HVDC Systems and Power Electronics for Transmission Systems. The system was developed as a platform for the study of system dynamics and control for power systems with high penetration of power electronic coupled generation, FACTS devices and HVDC transmission [1]. The test system shown has two 345 kV buses interconnected by a long transmission line, six 230 kV buses with an associated transmission system and four 22 kV buses for generation and load buses. The transmission system consists of 230 kV transmission lines except for one 345 kV linking buses 7 and 8. The generation and loads are separated by long transmission lines such that the system dynamic response has three areas, with boundaries indicated by three green lines in Fig. 1. Bus 9 represents an interconnection point to a stiffer power system and can be treated as an infinite bus in simulation studies.

The 12 Bus system can be divided in to three main areas based on the overall system oscillation behavior and swing centers (location where the voltage between two sources is zero when angle between two sources is 180 deg). Area 1 is predominantly a generation area, where generators connected at Bus 9 and Bus 10 in this region are hydroelectric generators rated 800 MVA and 700 MVA respectively and this area is considered as the main generation area with minimum load. Area 3 shown in Figure 1 is the main load center with some generation available. The generator connected at Bus 11 in this region is a 500 MVA hydroelectric generator. Area 2 is the transmission system located between Area 1 and Area 3 with some hydro generation available at Bus12 rated at 500MVA, but this generation is not sufficient to meet the local demand.

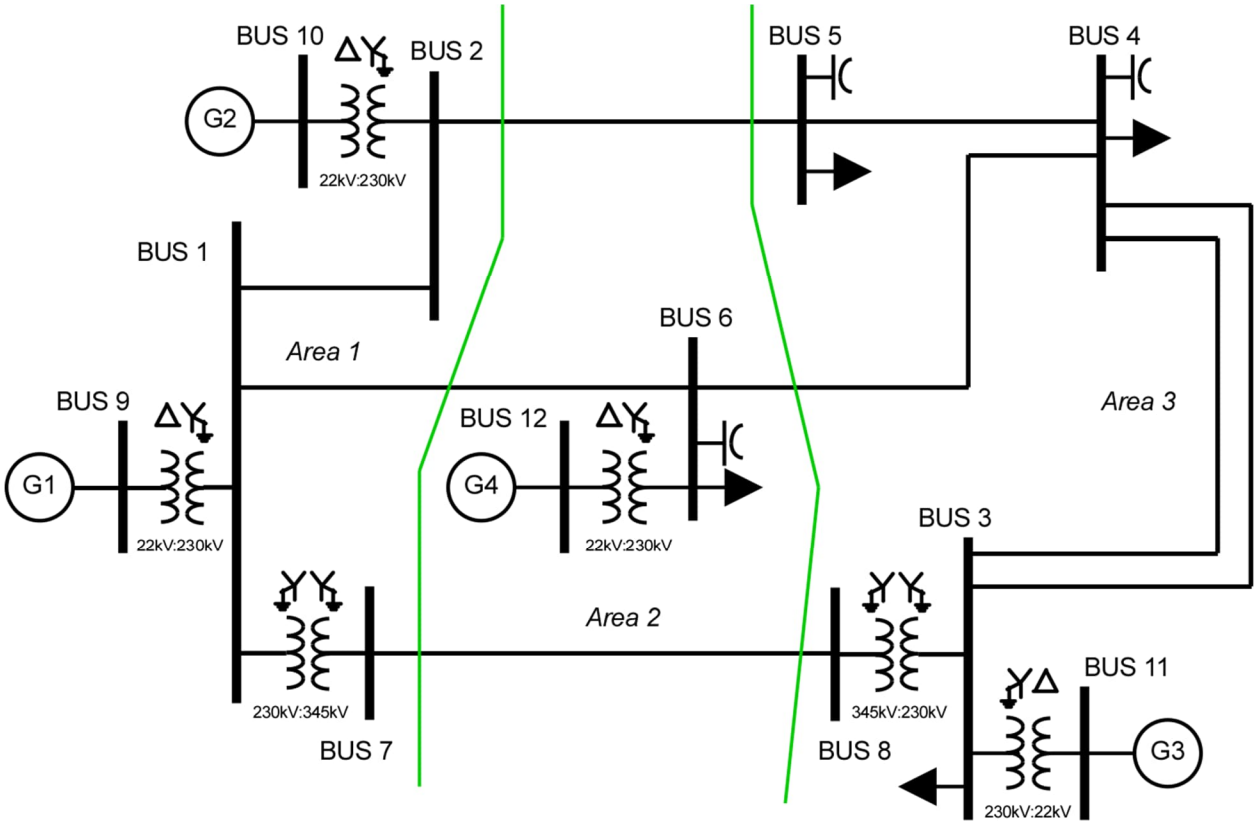


Fig. 1. One Line diagram of IEEE 12-Bus System

The 12-bus system was modified to meet the objectives of this research. The changes included

1) Adding a wind park with type-3 wind turbines to Bus 8.
2) Adding series compensation to the long 345kV transmission line between Bus 7 and Bus 8. The total compensation the can be varied up to 70% of the line inductive reactance. The capacitor banks were added to be able to simulate SSCI.

Table 1 shows the power flow data of the system.

Table 1 Generator, Shunt Capacitor, & Load power flow Data

Bus	Type	Gen (MW)	Shunt (MVar)	Voltage (pu) / Angle (degrees)
1	P-Q	-	-	1.03 ∠ -1.25
2	P-Q	-	90	1.00 ∠ -0.67
3	P-Q	-	40	1.00 ∠ -30
4	P-Q	-	120	0.96 ∠ -60
5	P-Q	-	60	0.94 ∠ -35.5
6	P-Q	-	300	0.98 ∠ -38.8
7	P-Q	-	-	1.03 ∠ -1.25
8	Wind Park	60	-	0.99 ∠ -36.5
9	Slack	-	-	1.04 ∠ 0
10	P-V	500	-	1.02 ∠ -27.8
11	P-V	200	-	1.02 ∠ -65

12	P-V	300	-	1.01 ∠ -77

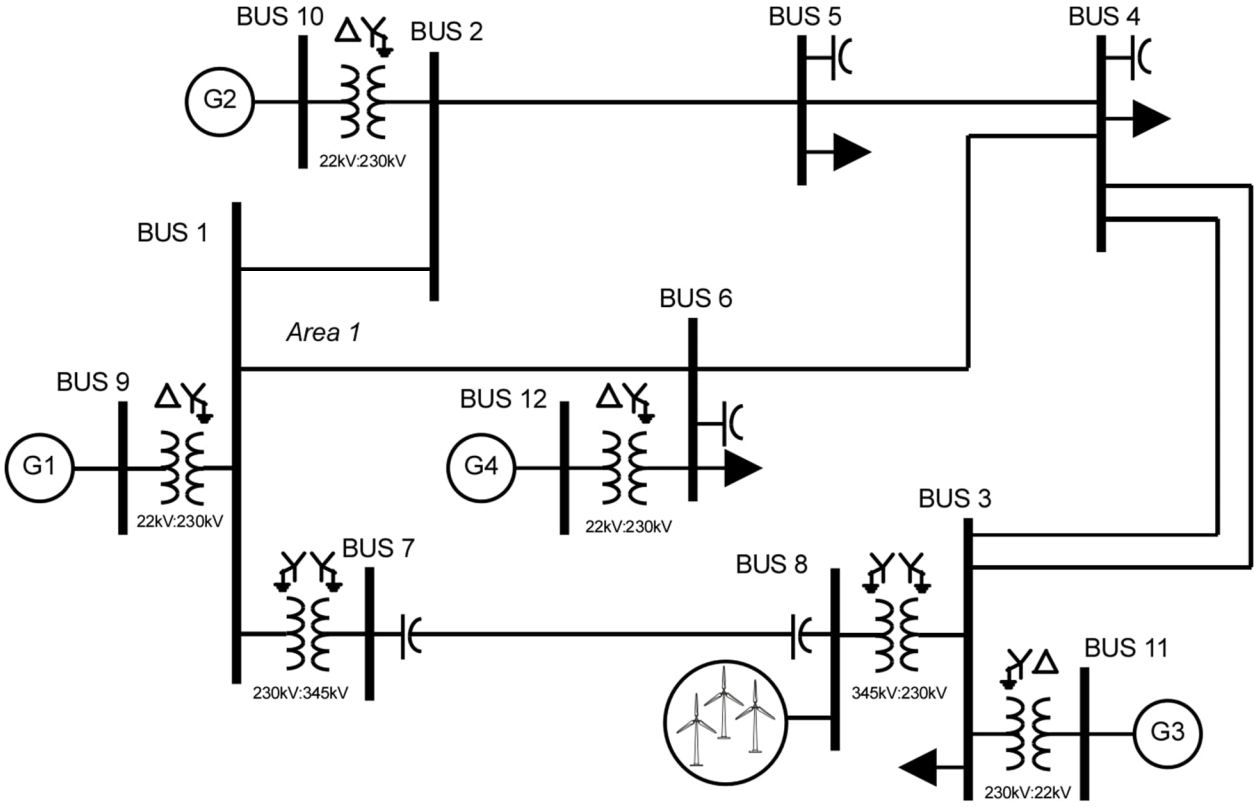


Fig. 2. Single Line Diagram of modified 12-Bus system with wind farm added

ii. Damping Controller Design

The design goal of the developed controller is to damp subsynchronous oscillations in frequency deviation through the use of reactive power modulation of an SVC. A phasor measurement unit (PMU) provides the measured frequency deviation at a sample rate of 30 samples per second (SPS). These devices were chosen since they are readily available in many constrained power systems, and many more will soon be widely adopted with the increase of additional renewable resources. PMUs also deliver measurements at higher fidelity and a higher sample rate than many traditional SCADA-based measurements. It is demonstrated that with minimal control assumptions regarding system configuration, these two devices can significantly increase the security of the power system by damping sustained oscillations, as well as prevent the potential confusion between electromechanical destabilization and single-unit mis-operation. Results of interest include:

- A type 3 wind park using a DFIG configuration can produce significant oscillations under nearby adverse loading conditions.
- SVCs regulating voltage magnitude (i.e., operating solely based on a voltage control signal without concern for frequency deviation) improved wind park resilience to exogenous, rapid load changes, but are unable to meaningfully damp oscillatory frequency deviations induced by the wind park

- The developed controller which provides additional modulation of the SVC reactive power based on frequency regulation greatly improved the frequency response of the 12-bus system, reducing the impact of an oscillating DFIG-based wind park.

iii. Small Validation Case Simulation Setup

The experimental platform is RSCAD FX by RTDS Technologies. It is a real time digital simulator, which allows for most variables in the system to be changed dynamically as the system is running, as well as for real time monitoring of signals. The software connects to hardware racks which run the simulation in real time. The simulation has a default time step of 50 microseconds, which presents no issues for the present experiments. An overview of the system is shown Figure 1.

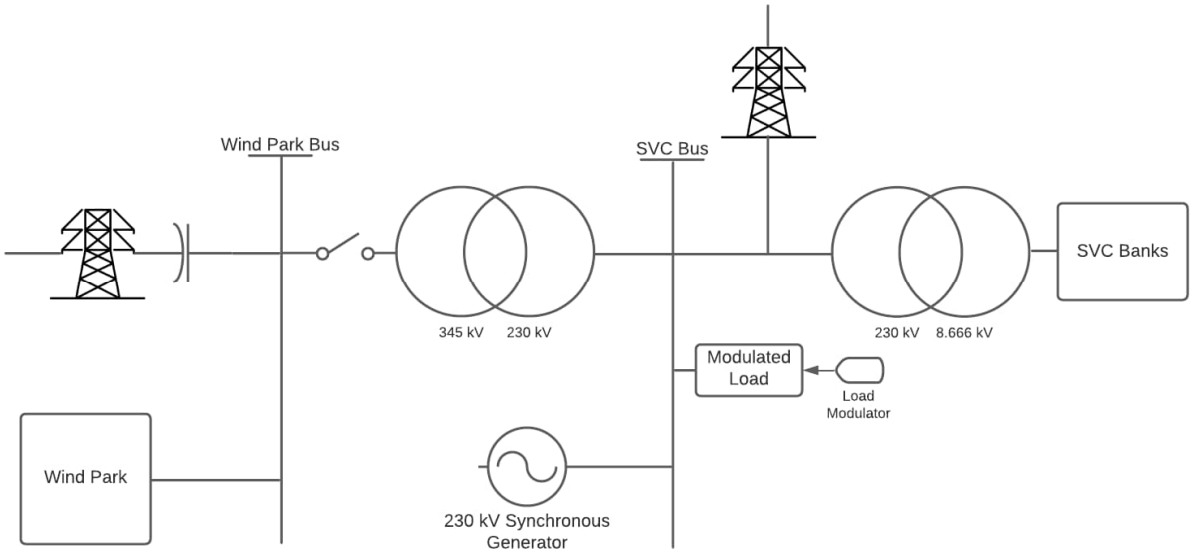


Figure 1 Overview of small system representing part of the 12-bus system serving as the test bed

The controller is set up using a PMU to read the frequency of the bus the SVC is connected to in the system. This bus is separated from the type 3 wind park by a single transformer, and the SVCs are separated from the same bus by another transformer. The frequency of the bus is used as the error signal to generate a reference that is then fed through a filter into the SVCs' voltage controller. This then alters the firing angle calculations done by the SVCs' controller to cause the firing angle to increase or decrease based on frequency fluctuation in addition to the voltage fluctuation.

The frequency compensator sends its control signals into the SVC right before it linearizes its voltage regulation signal to be fed into its firing angle calculation, alpha, as shown on Figure 2. This prevents the frequency regulation signal from interfering with any voltage control signals, only adding onto it based on additional frequency deviation. The current testing system made use of most of the SVCs' modulation capabilities for voltage regulation before the frequency compensator was added. In order to prevent the SVCs' reactive power modulation capacities from saturating, the SVCs' voltage regulation signals are arbitrarily reduced to 70% of their actual gain, freeing up room in the linearization function for the frequency regulation signal to have an effect. Thus the designed frequency compensator assumes that the SVC to which it is attached is not already operating near its maximum capacity.

To design the compensator for the SVC frequency control loop, preliminary online system identification was performed via non-parametric broadband power spectral density estimation using Welch Periodograms. Summarized briefly, a dynamic load component is modulated following an independent, identically distributed white Gaussian time series. This approach is chosen since it excites the power system at all measurable frequencies without altering the Fourier Transform of the power signal [9].

Some key assumptions of this method are as follows:

- The system behaves in a linear, time-invariant manner around the operating points of interest
- The signal being measured is stationary or quasi-stationary, which all periodic, deterministic signals are
- The noise being applied is additive

All of these criteria are met in the system within the operating ranges being testing. This boosts the power signal's frequency response magnitude without altering its frequency characteristics, allowing for rapid identification of system oscillatory modes and providing a means for quantifying disturbance rejection – a key performance metric for an automatic reactive power modulation control system such as the one employed here.

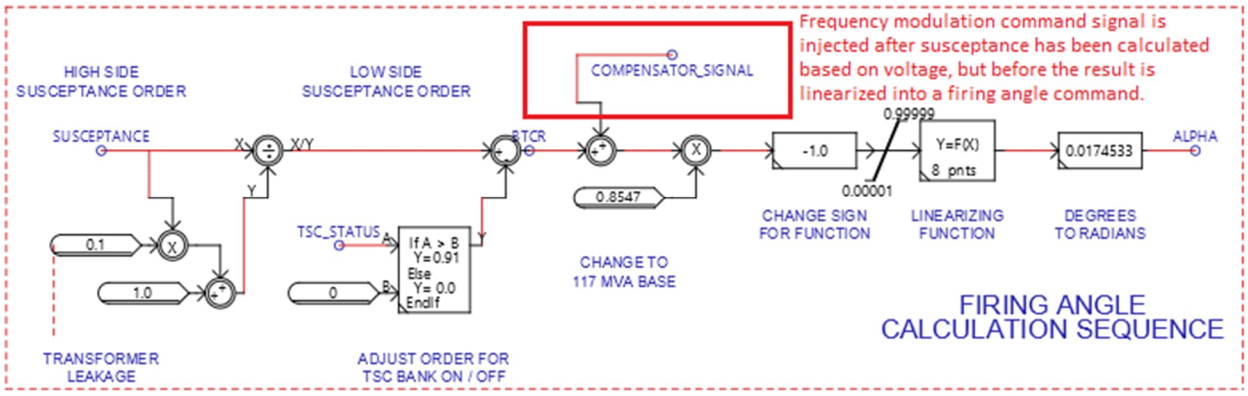


Figure 2 Illustration of where the frequency compensator injects commands into the actuator

Welch Periodograms (making use of the concept of ensemble averaging) of the frequency response of the system are recorded for various levels of disturbance, establishing a baseline and separating the effects of various factors in the system. For each test, the wind parks are operating at 90% capacity; that is, they are operating below rated conditions due to wind speed. This was done in order to test the ability of the frequency compensator to mitigate oscillations in off-nominal conditions.

Periodograms recorded are for the following scenarios:

- *In normal operation using the complete system (i.e. with the wind park) at nominal load with and without the SVCs in their nominal configuration*: The SVCs are then tested with and without the novel frequency compensator. These serve as the control group results.
- *With the system operating with a injected random load power modulation*: In this case the system needs to maintain a roughly .02 Hz deviation from nominal frequency on the SVC bus, also tested with and without the SVC, and with and without the frequency compensator on the SVC.

- *Cases where the load modulation amplitude induces oscillations from the wind parks*. Frequency deviations of roughly 0.2 Hz from nominal on the SVC bus are induced in this case. Cases are recorded both with and without the SVCs, which are tested both with and without the frequency compensator.

The goal of any protective scheme is to provide no interference under nominal conditions and activate both quickly and proportionally when the system experiences disturbances, increasing in regulation power based on the magnitude of the disturbance. In order to induce substantial oscillatory behavior from the wind park, the load modulation magnitude remains variable in the active runtime simulation. This allows data to be gathered from the same simulation at nominal load levels, with load modulation magnitudes where the wind parks can still operate normally, and with load modulation magnitudes that cause them to produce significant oscillations, testing the frequency compensator's ability to meet this criterion as a protection component.

e. Proof of Concept Verification

i. Simulation platform – verification with the small system

For each iteration of system configuration and parameters, six trials of four-minute simulations were run and the frequency response of the simulations were captured and analyzed via Fourier analyses. The graphs were then generated using ensemble averaging of the Fourier Analyses. The magnitude plots generated are graphed on a non-normalized decibel scale, so the plots are interpreted by comparing their relative magnitude responses, as opposed to comparing to a 0 dB response.

At nominal load, any configuration of the system (i.e., with or without the SVCs, which are in turn tested with or without the novel frequency compensator) has no discernible frequency oscillations, proving that it is an adequately designed system for testing. All oscillations for the present tests originate from modulation of the load, whether of small enough magnitude to stay within reasonable bounds of oscillations, or large enough to cause oscillations that would likely cause damage to a physical system. The results are shown on Figure 3.

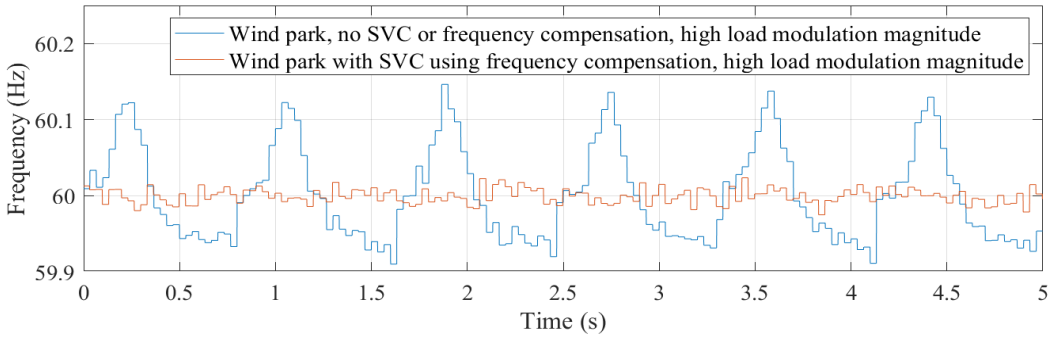


Figure 3 Comparison of the frequency response of the SVC bus when the wind park is and is not capable of compensating for the load modulations

From there, the modulation of the load was set to a small magnitude of variations so as to induce oscillations from the wind park. The largest load modulation the wind park could consistently compensate for on its own was approximately 148% of the baseline of that load, deviating between +/- 12% from 148% in a normal distribution. The frequency signal on the SVC bus oscillated between +/- 0.02 Hz from nominal, approximately. When the SVCs are connected to the system but the novel frequency compensator is

disconnected, the wind parks can consistently compensate for load modulations on the nearby load for approximately 172% of the original load values, deviating by +/- 18% from 172%. The frequency oscillations for this configuration are also approximately +/- 0.15 Hz deviations from nominal.

When the frequency compensator is connected, there is little change. Figure 4 shows the most extreme differences within the scenario of manageable load modulation, with the blue data showing the magnitude response of the frequency of the system containing only the wind park and being modulated at the 148% load setpoint, while the orange data shows the same for the system that includes the SVCs and novel frequency compensator as well.

Figure 4 shows that the frequency compensator does smooth out a small mode in the response, but also slightly increases the low frequency response of the system for all other frequencies in question. Overall, however, there is no significant change to the response of the system, as the observed mode of the wind park operating alone is not very large for this amount of load modulation.

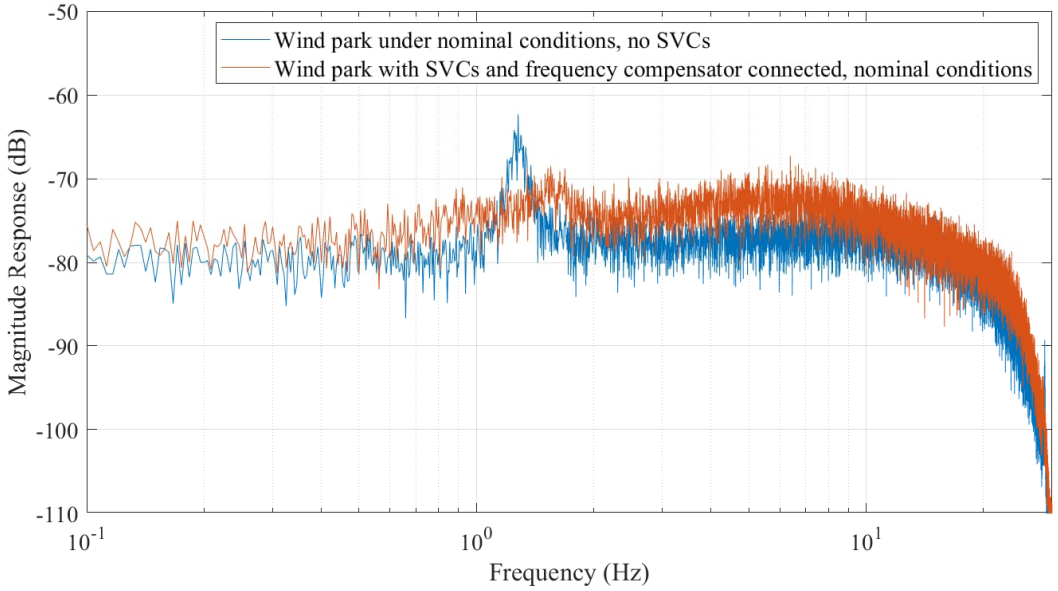


Figure 4 Frequency response of the wind park to nominal operating conditions both alone and with the novel frequency compensator

The wind park on its own is unable to handle much more load modulation than 148% of the baseline for the modulated load. At 154 +/- 13.5% modulation, the wind park is consistently unable to compensate for the increased load, and the frequency of the SVC bus oscillates between approximately +/- 0.15 Hz from nominal. With the SVCs connected, but no frequency compensation on them, the wind park is consistently unable to handle load modulations at 178 +/- 19.5% baseline load, with similar results for frequency oscillations on the SVC bus.

Figure 5 shows the comparison of the frequency magnitude responses of the system at the conditions described. The mode initially seen when the wind park is able to compensate for the load modulation manifests many harmonics once the breaking point of modulation magnitude is reached. Damping the primary mode and its harmonics represents the primary performance criterion for the novel frequency compensator. The responses of the system without the SVCs at the lower modulation magnitudes and

with the SVCs at the higher modulation magnitudes were very similar, with the primary mode and all its harmonics being upshifted by approximately .125 Hz and reduced in magnitude very slightly, as seen in Figure 5.

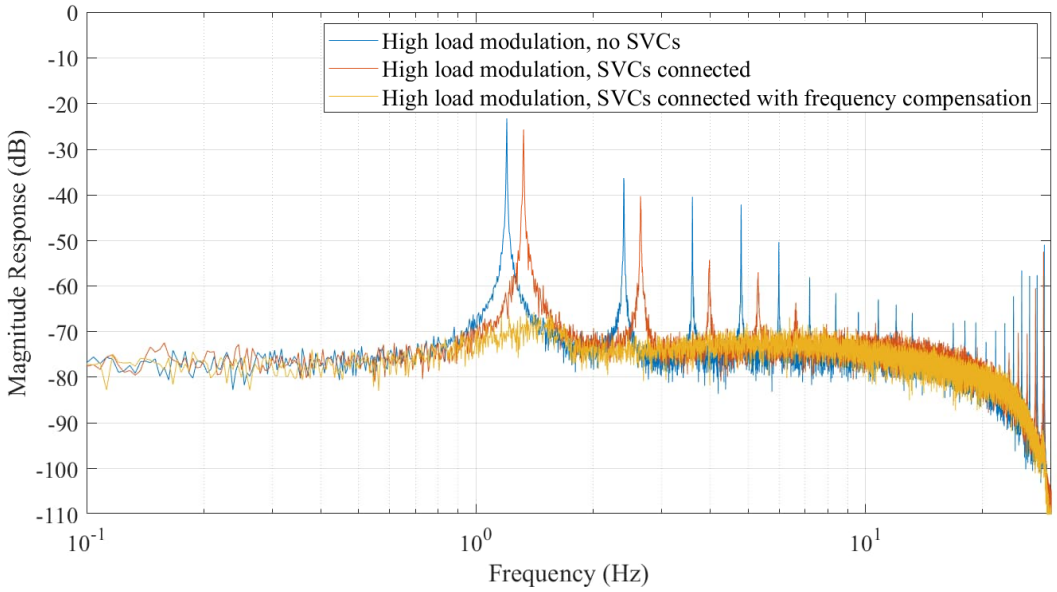


Figure 5 Magnitude response for the wind park to load modulation that it can (blue) and cannot (orange) adequately damp

When the frequency compensator is connected into the system and causes the SVCs to regulate frequency as well as voltage through reactive power modulation, there is a readily observable improvement in the frequency response of the system. There is a reduction of over 40 dB in the response, which translates to the response being less than 1% of the magnitude with the compensator as compared to without it. Additionally, all of the harmonics are damped out completely, and the baseline of the response remains consistent.

c. Generator Component Threat Scenarios

The threat scenarios for generators and relating components for power systems will primarily focus on generator control components such as exciters, power system stabilizers and governors that are coupled with communication abilities. Specially, generation facilities which connected to remote control centers or automatic generation control capabilities.

The cyberattacks that are considered for generation equipment are broken down into two categories: augmentation of measurements, and augmentation of control parameters. Augmentation of measurements would be qualify as the corruption of measurements used for control action for the exciter or governor such as voltage, current, and speed. An augmented control parameter would qualify as the intentional change of control parameters such as the upper and lower boundaries of excitation voltage and speed, or proportional-integral-derivative (PID) feedback control. The scenarios considered describe the effects that cyberattacks could be based upon the categories above.

- Incorrect measurement of excitation field voltage or current
- Incorrect reference for excitation field voltage or current limits
- Incorrect controller feedback loop parameters
- Incorrect measurement of generator speed
- Incorrect measurement of prime mover torque
- Incorrect reference for generator speed limits
- Incorrect controller feedback loop parameters
- Incorrect control command from AGC

i. Excitation system cyberattack

In the first set of cyber-attack vectors, the measured reference signals used by the excitation system were modified by the attacker. The specific vectors targeted were the generator field voltage and current signals. In this, the reference signals were replaced with the designed cyber-attack to create a transient emanating from the generators electrical torque. These tests were conducted on the full 12-bus system, without the wind farm generating power.

In implementing the cyberattack, a 10 second duration repeating vector was created to simulate oscillations on the power system. In each, the reference signal is spoofed and or augmented by the cyber-attack vector. In testing the exciter cyberattacks, spoofing the field current measurement did not result in impactful results, due to the exciter automatically adjusting its voltage, therefore the exciter voltage reference was the most effective. In the case of the following, the reference signal was augmented by a scaling function between 0-200% as shown in (1).

$$Intercepted\ Cyber\ Attack = Cyber\ Attack\ Vector * Original\ Signal \quad (1)$$

The attack vector case to be explored was the generator field voltage measurement read by the exciter. This signal was intercepted and augmented by the time series attack shown in Figure 6. Where the magnitude of the attack was between -15% and +15% of the measured signal.

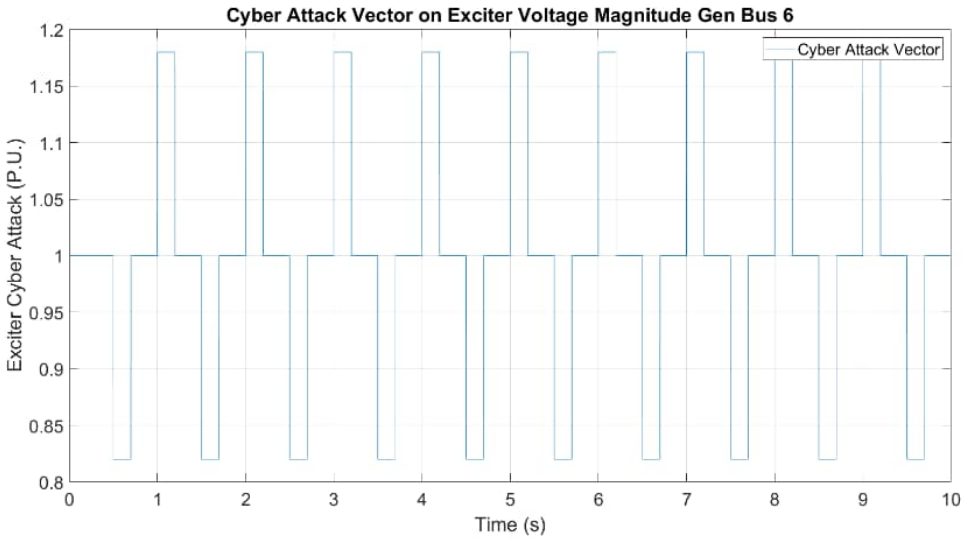


Figure 6 Cyberattack vector conducted on exciter voltage measurement

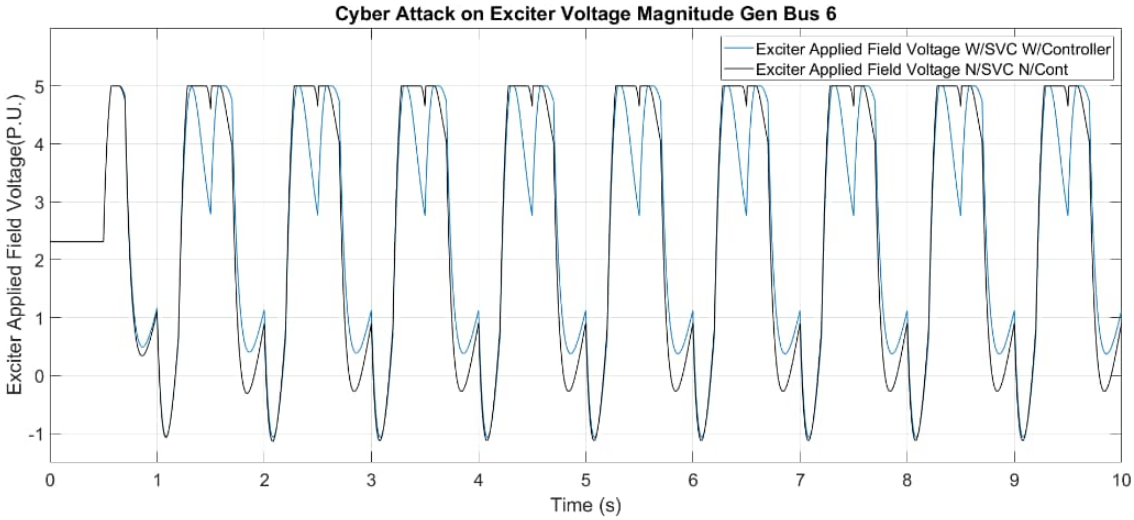


Figure 7 Excitation Voltage Applied to Generator 6

Due to the exciters control system, a response to the cyberattack is expected and is shown in Figure 7. Where the black line denotes the system without the SVC and control system, and the blue is with the SVC and control system active. It can be seen that the waveform is not a square wave, due to the exciter adjusting its voltage with respect to the voltage reference. Below from Figure 8 to Figure 10, the related frequency seen though out the system is plotted. The frequency was recorded at each of the buses to show the system with and without the SVCs.

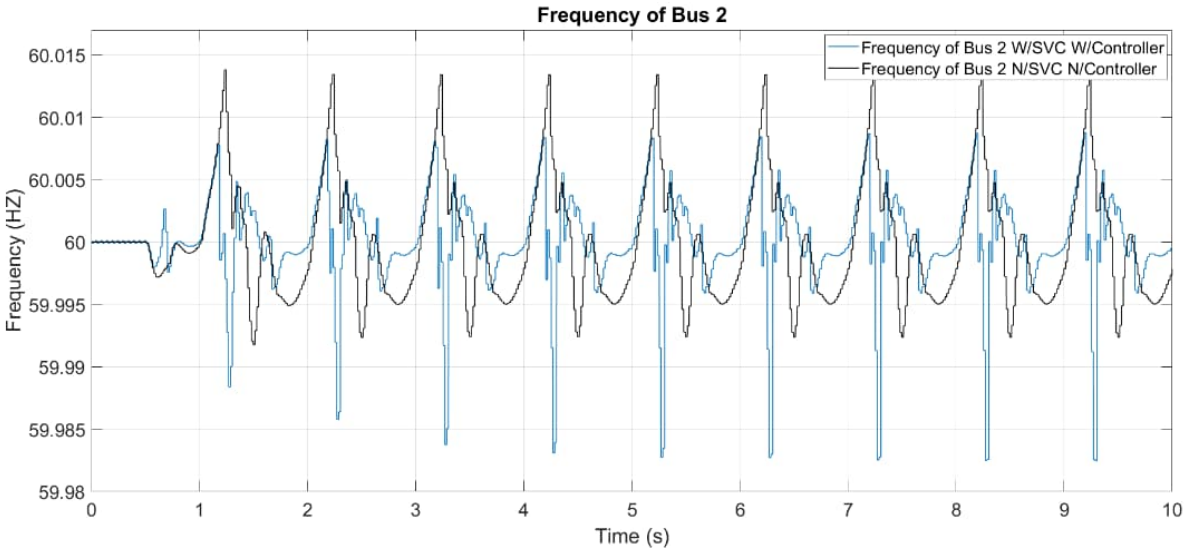


Figure 8 Frequency measured on Bus 2 with and without the SVC

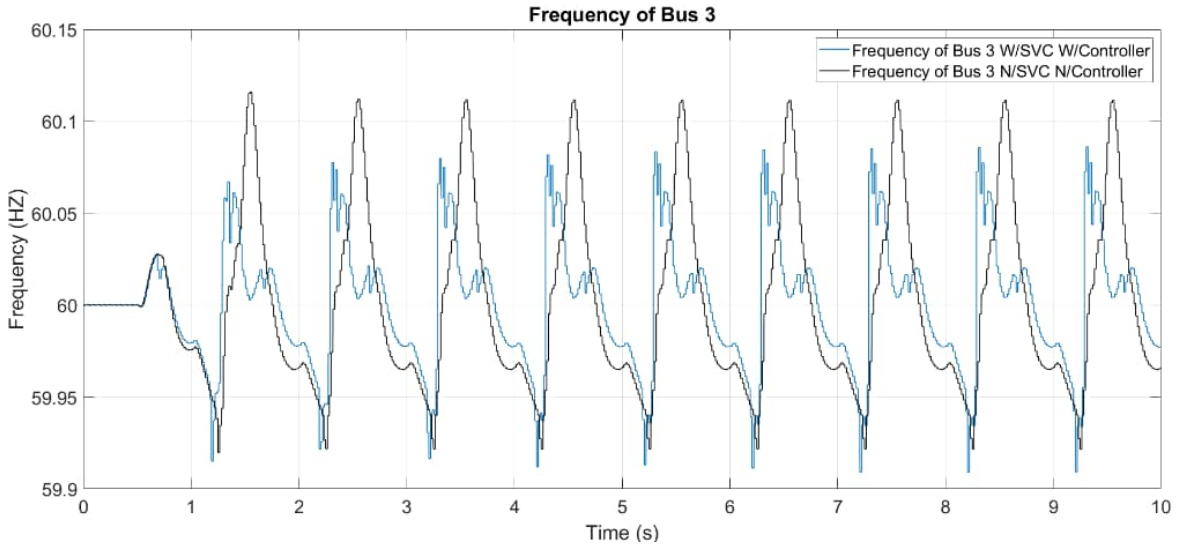


Figure 9 Frequency measured on Bus 3 with and without the SVC

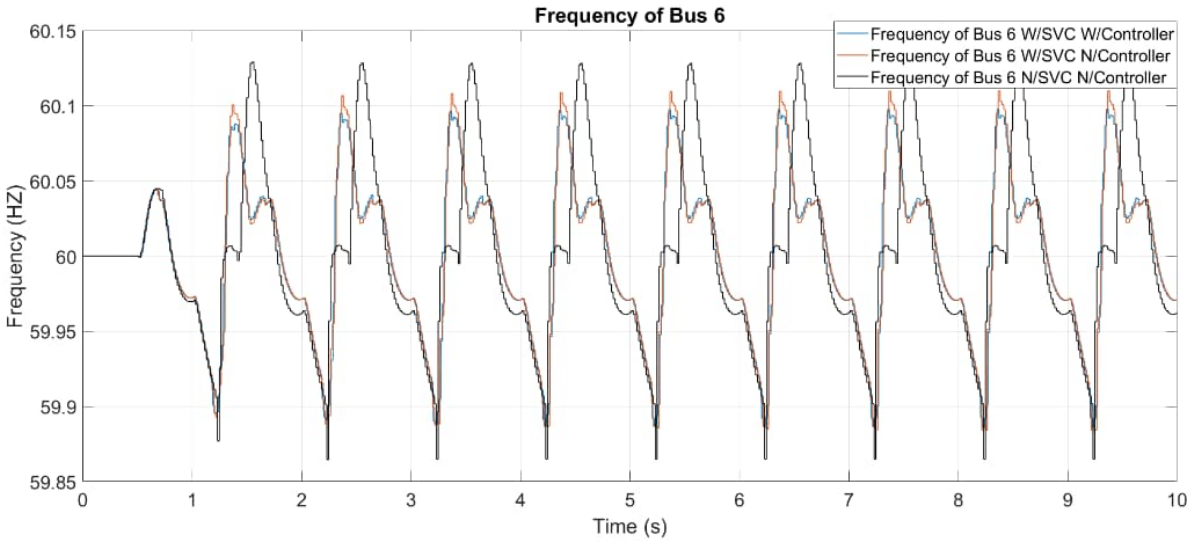


Figure 10 Frequency measured on Bus 6 with and without the SVC

The cyberattack on the excitation system for the generator located at Bus 6 in the system in Figure 1. Figure 10 shows the largest transient in frequency as the power system oscillates due to change in electromechanical torque of the machine. Similarly, Figure 10 also shows three plotted data streams, the original system without the SVCs, the system with SVCs but without the frequency controller, and the SVCs with the frequency controller. As shown, the plot of the SVC with and without the controller are very similar indicating that while the controller is able to damp the oscillations, the amount of damping is limited in this case.

ii. Cyberattack on governor

In the second series of cyberattacks, the governor was targeted and spoofing if its reference signals was also undertaken. The resulting torque signal was intercepted and spoofed, resulting in an augmentation of the torque suppled to the generator, therefore effecting the power supplied by the machine. Similarly

to the excitation spoof, the torque signal was intercepted and augmented by a 10 second cyber-attack signal shown in Figure 11. This Cyber Attack Vector augmented the torque by multiplying the respective values by the sequence shown in Figure 11 much like the excitation attack vector.

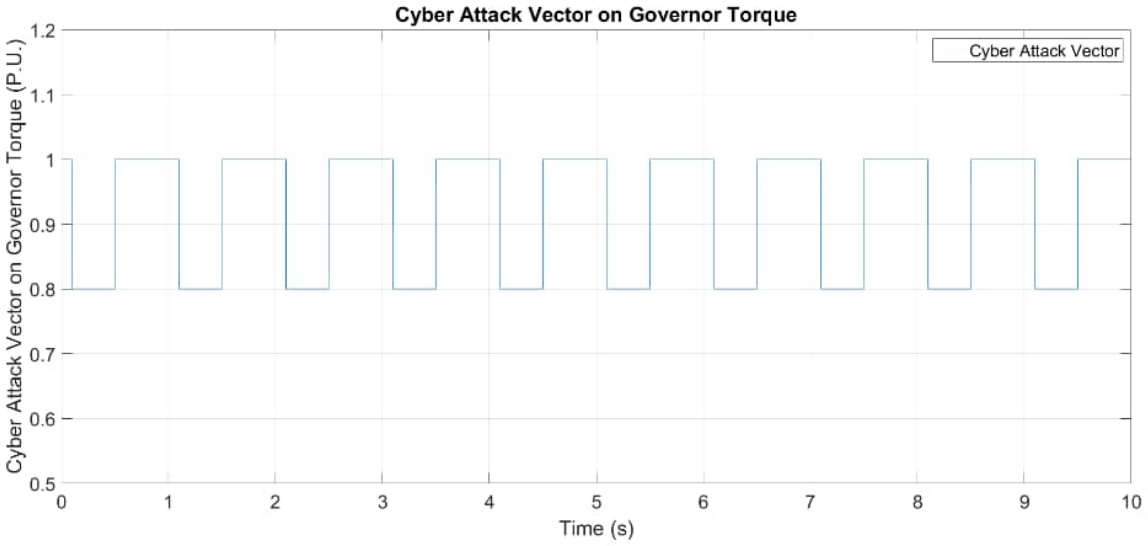


Figure 11 Cyberattack vector targeting governor torque measurement

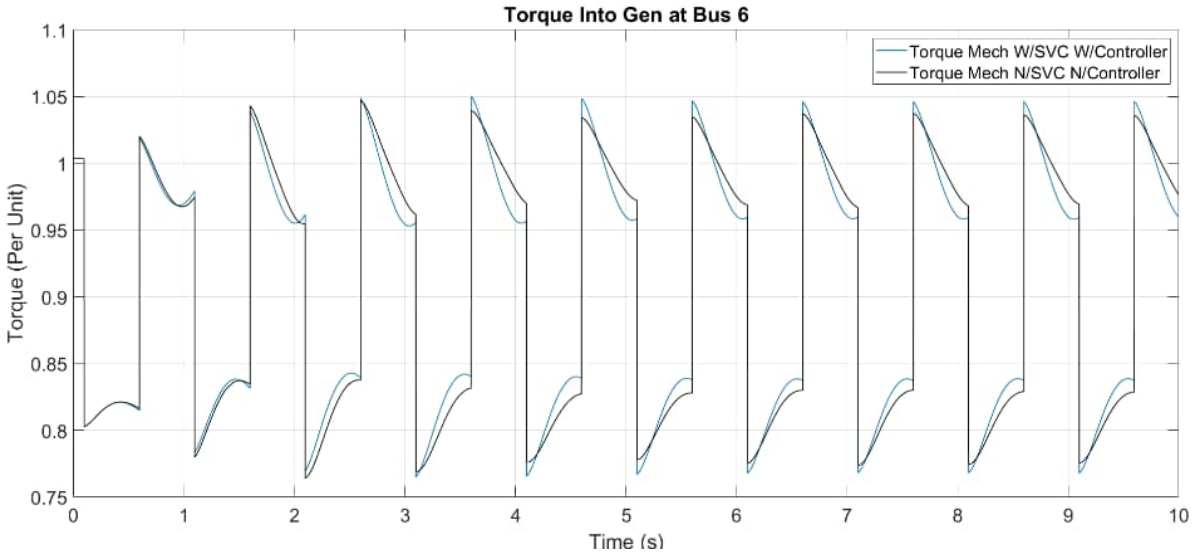


Figure 12 Torque supplied to generator 6

Figure 12 shows the resulting torque supplied to Generator 6 is shown throughout the duration of the cyberattack. Both the original system without the SVC and with the SVC have been included in the plot to show the governors response to the frequency of the machine as it is impacted by the attack.

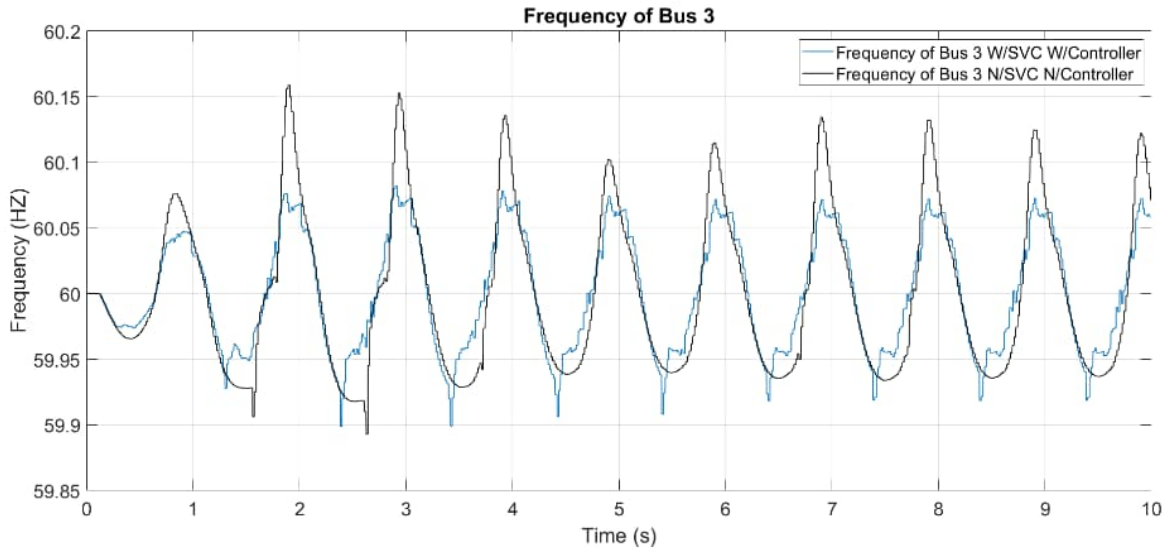


Figure 13 Frequency of Bus 3

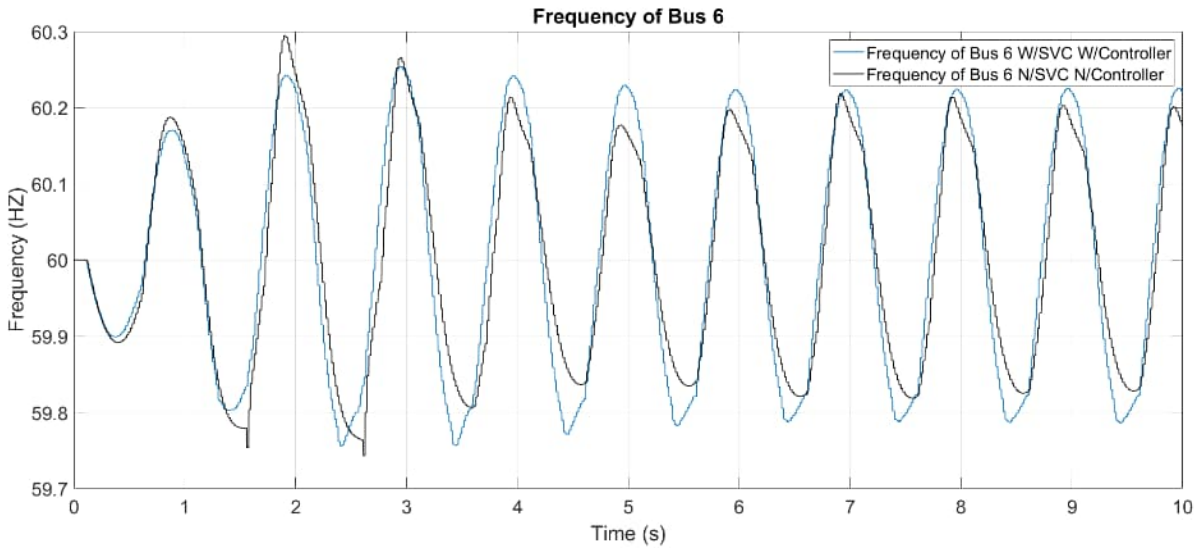


Figure 14 Frequency of Bus 6

Above in Figure 13 and Figure 14 the frequency measured at buses 3 and 6 are shown respectively. Where Bus 6 is the location of the targeted generator, and bus 3 is the location of the SVCs. In the figures, it can be observed that the SVCs have a limited impact on the frequency at the targeted bus, largely due to the limitations of a reactive power compensator in damping driven power oscillations. The damping controllers had the most significant impact if the SVC was near the generator.

d. Wind Turbine and Wind Farm Cybersecurity

When viewing cybersecurity for wind parks, data communications is an extremely important aspect of operation [10]. Whether it's for control purposes or data gathering, the communications network creates a vulnerability. However, vulnerabilities differ depending on the intruder's intentions and how they plan to achieve their intended result [11]. For example, an expert intruder could deliberately target specific measurements at carefully chosen measurement devices to augment the state of the system [12] known

as false data injections (FDI). These FDI attacks can also be used to augment the viewable topology of the system [13-15], creating an issue for topology-based power flow and analysis. Furthering, attacks to intercept [11] and modify to a specific malicious value could be produced to effect control operation or desired behavior known as man-in-the-middle (MITM), or a block of communications as a whole known as the denial of service (DoS) attack [15].

Steps have been taken to evaluate wind industry cybersecurity and resiliency through research regarding cyberattacks on SCADA systems via external networks. Researchers investigated how a malicious actor could gain unauthorized control of a wind plant to cause a cascading outage depending on interconnectivity. This was achieved by exploring access to the wind plant by physical access to the plants local area network (LAN) [16,17]. Additional research was conducted to investigate and exploit fabricated turbine controls [17] through the use of a worm to propagate information throughout the wind plant network topology. These past research projects provide insight into the established vulnerabilities.

i. Attack Vectors Considered

Though convenient, the use of Internet-based platforms to control and monitor physical processes may considerably broaden the wind threat landscape. Such as industrial control systems, are essential in modern wind plants and control centers and may include Internet-facing features. The attack vectors below that we have consider feature different communication applications which are currently involved in power system transmission and generation control. These avenues can be intercepted or augmented in malicious activities such as false data injections (FDI), Man-in-the-middle (MITM), or spoofing.

Attack vectors are broken into three separate areas:

- DNP3
- Human Machine Interface (HMI)
- Control Parameter Augmentation

ii. Subsynchronous Control Oscillations

The subsynchronous phenomena occurs when parts of the power system interact with each other. Figure 15 shows the classification of different subsynchronous oscillations (SSO) according to the devices present on the system: series capacitors, power electronics (i.e., type 3 and 4 wind parks), and gas turbines (or wind turbine shafts) [18]

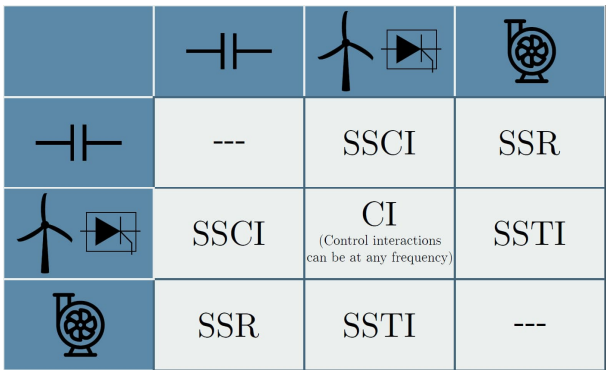


Figure 15 Types of subsynchronous oscillations

Where:

- CI: Control Interactions
  - Interaction between power electronics devices and their control loops
  - Can occur in any frequency range
- SSCI: Subsynchronous Control Interaction
  - Interaction between power electronics devices and series compensated transmission lines
  - Oscillations usually bellow 40 Hz
- SSR: Subsynchronous Resonance
  - Interaction between the torsional masses of a generator and a series compensated transmission line
  - May damage the shaft of a generator due to torque amplification (TA)
- SSTI: Subsynchronous Torsional Interaction
  - Interactions

Wind SSO turned to be a major concern for wind park manufacturers and owners. There are two main types: series capacitor SSO, and weak grid SSO, as shown in Figure 16

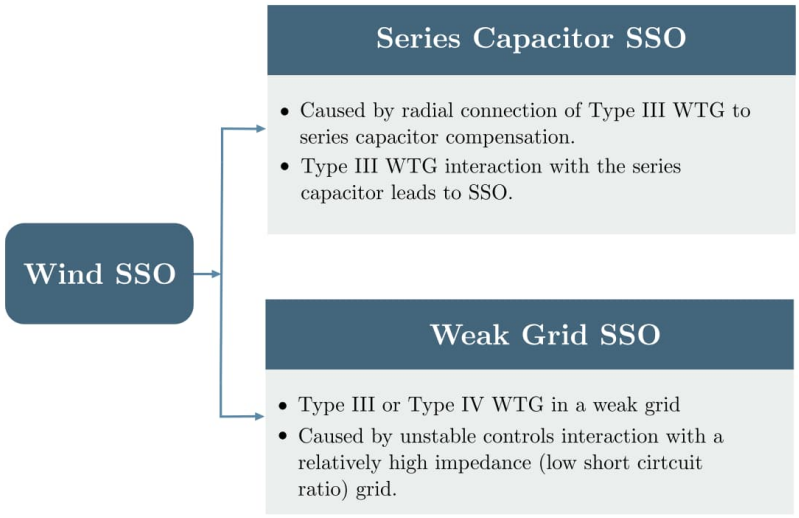


Figure 16 Types of subsynchronous oscillations related to Wind parks

Oscillations interacting with series capacitors is more prominent in type-3 wind turbines. This occurs because at the LC resonance frequency of the series compensated transmission line, the resistance of the complete system is negative, thus triggering SSCI [19]. The slip of the induction machine causes the internal rotor resistance to be negative which makes the overall resistance of the system to be negative.

Weak grid SSO occurs in both type-3 and type-4 wind turbines. These interactions are heavily dependent on control. A common cause is a poorly tuned Phase-Locked Loop (PLL). Another cause is the high impedance of the system causing the controls to become unstable [20].

iii. Real-world Events

Table 2 shows a summary of wind SSO events. Several events were identified in northern China from 2012 to 2016 [18]

Table 2 Historical wind SSO events [18]

Year	Location	Turbine Type	Frequency	Description
2007	Minnesota	3	9-13 Hz	Radial connection to a series compensated line after contingency
2009	Texas	3	20-30 Hz	Radial connection to a series compensated line after contingency. Damage reported on wind turbines (e.g., crowbar) and series capacitors
2011	Texas	4	4 Hz	Weak grid after contingency
2012-2016	Northern, China	3	9-40 Hz	Radial interconnection caused several SSO events. This condition lasted for 4 years.
2014-2015	Xinjian, China	4	26-34 Hz	Weak interconnection (low short-circuit resistance)
2017	Texas	3	20-30 Hz	Radial connection to a series compensated line after contingency
2019	United Kingdom	4 offshore	9 Hz	Weak interconnection. This event resulted on blackout

A total of 4 main events related to type-3 wind parks were registered. Their cause is mainly series capacitor transmission line that ended radially connected to a type-3 wind park. One of the main causes is the negative resistance of the rotor side that contributes negatively close to the LC frequency of the compensated line. The oscillations are usually amplified in the rotor side converter.

Table 2 shows three events involving type-4 wind parks. Investigations concluded that both induction and permanent magnet synchronous machines are susceptible. The main cause for the events involving type-4 wind parks were cases where the power grids that became weak after a contingency occurred, and the control loops, especially the synchronization control were not adequate. Additionally, an inappropriate design of PLL caused the 2014-2015 events in China [20].

iv. Frequency Scan Methodology

All possible contingency conditions (e.g., N-x) can be studied using the frequency scan technique. The analysis is done at the point of interconnection (POI) of the wind park, as shown on Figure 17 [21]. A total of three scans are required:

1. Grid-side scan (R_{grid} and X_{grid})
2. Induction-Based Resource (IBR) side scan (R_{IBR} and X_{IBR})
3. Combined scan (R_{tot} and X_{tot})

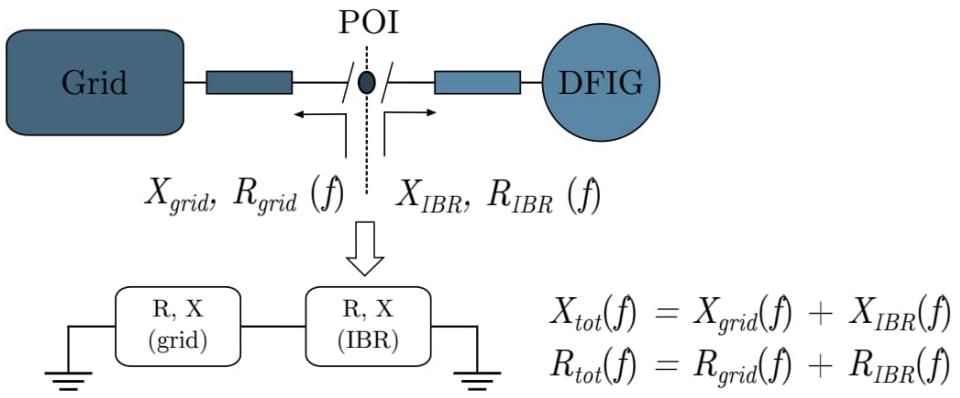


Figure 17 Frequency scan methodology

The curves for R_{tot} and X_{tot} are screened for frequencies where X_{tot} equals to zero. If R_{tot} equals to zero for any of those frequencies, there is high vulnerability to wind SSO. A time-domain verification and extensive transient simulations should be performed to understand the causes of the event.

v. Example of frequency scan for the 12-Bus Modified IEEE System

The 12-bus modified IEEE system is shown on Figure 18. The analysis is performed at the POI [22].

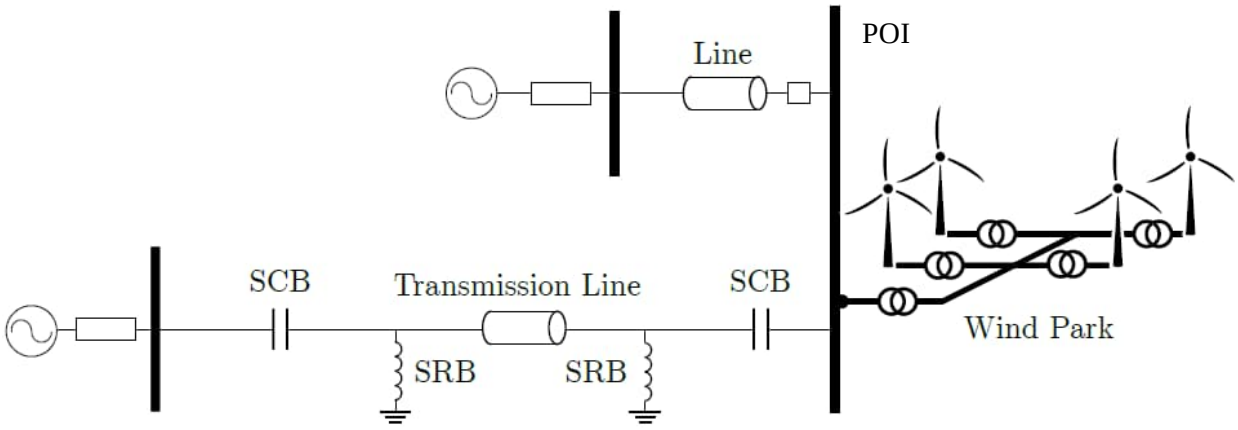


Figure 18 Equivalent version of the 12-bus power system

Step 1: Grid-Side Scan

The values for R_{grid} and X_{grid} are shown on Figure 19 between 5 and 40 Hz. It is noticeable that at the POI, R_{grid} is relatively high which makes the system less susceptible to SSCI.

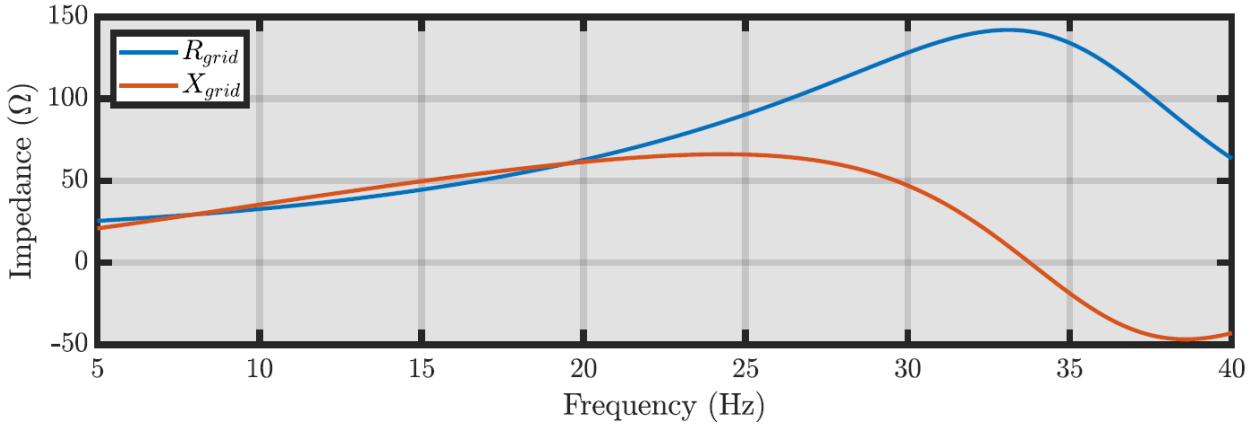


Figure 19 Grid-side scan

Step 2: IBR-Side Scan

The type-3 wind park studied in document presents the frequency response shown on Figure 20.

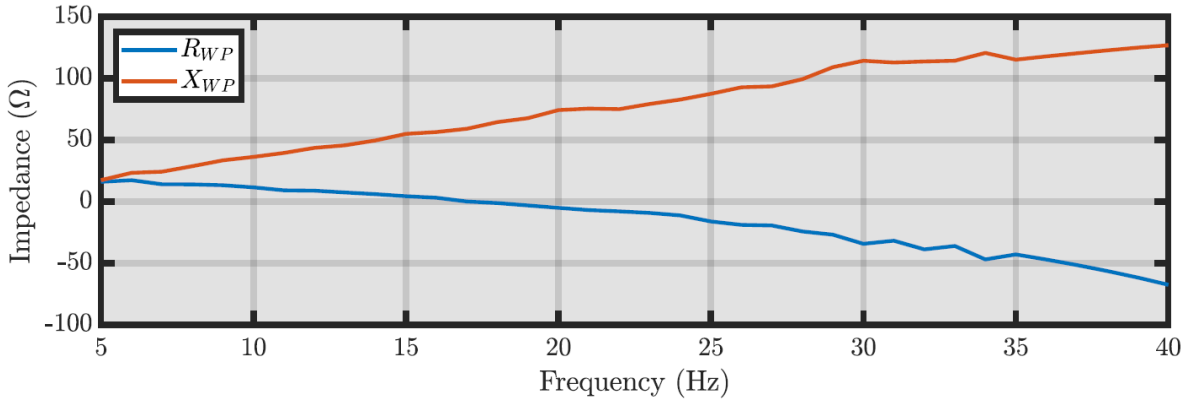


Figure 20 Type-3 wind park

Step 3: Complete scan

The combination of the results from steps 1 and 2 is shown on Figure 21. No crossover is detected, therefore, the system is not susceptible to SSCI for the studied topology

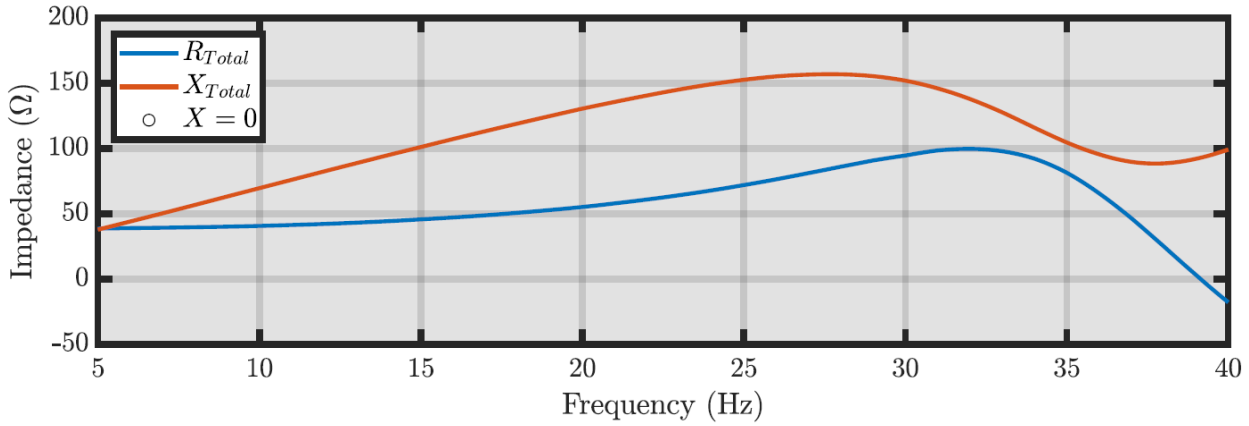


Figure 21 Combined scan: Grid + Wind Park

vi. Impact of change to a radial connection between the wind park and a series compensated line

A possible contingency of this system is if the circuit breaker shown on Figure 18 is opened. Such event results on the system shown on Figure 22. The combined scan is shown on Figure 23 and one crossover (e.g., X_{tot}= 0) occurs at 35Hz. The value of R_{tot} is negative (-27.58 ohms) which means that there is a high susceptible to SSCI.

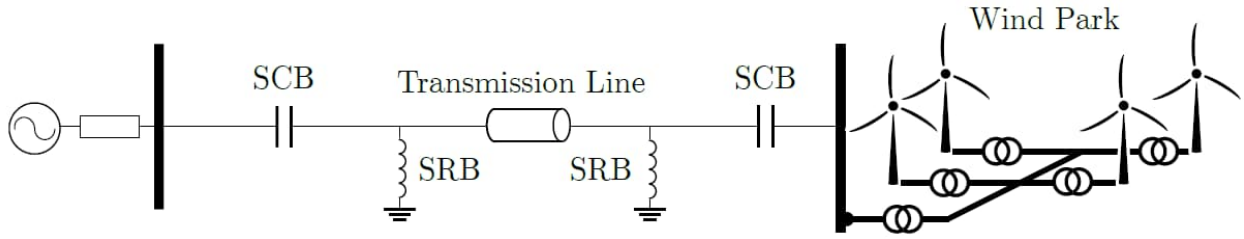


Figure 22 Wind park and series capacitors radially connected

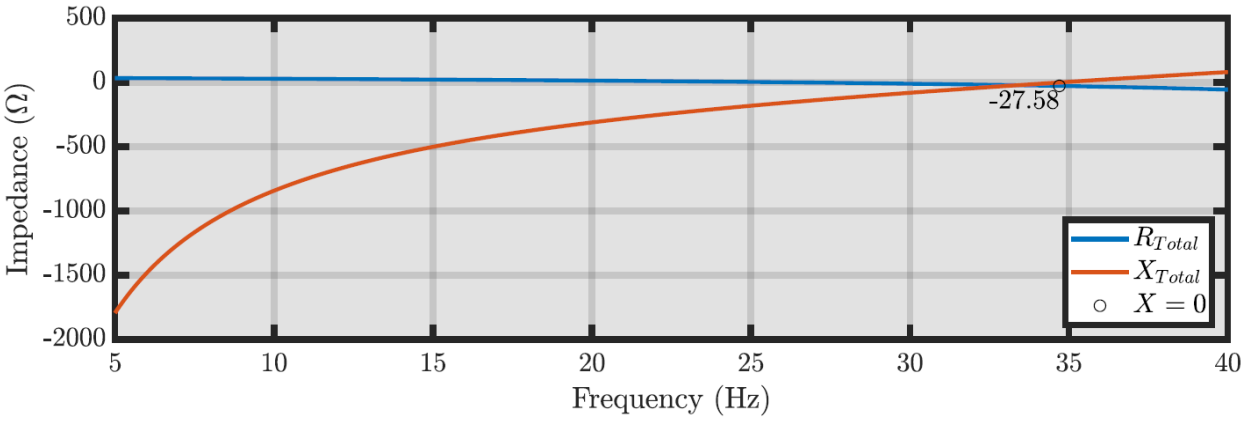


Figure 23 Combined scan: Grid + Wind Park (Park radially connected to the series compensated

A time-domain verification is required if a high susceptibility to SSCI is detected. The 12-bus modified IEEE system is simulated considering a fault occurring at 2 s followed by the CB tripping 100 ms later. Figure 24 shows the SSO starting immediately after the breakers opened. The current reaches a peak of 10 pu which could damage other devices of the system, such as the series capacitors or the wind turbines. The detected frequency is around 35 Hz, as expected from Figure 23.

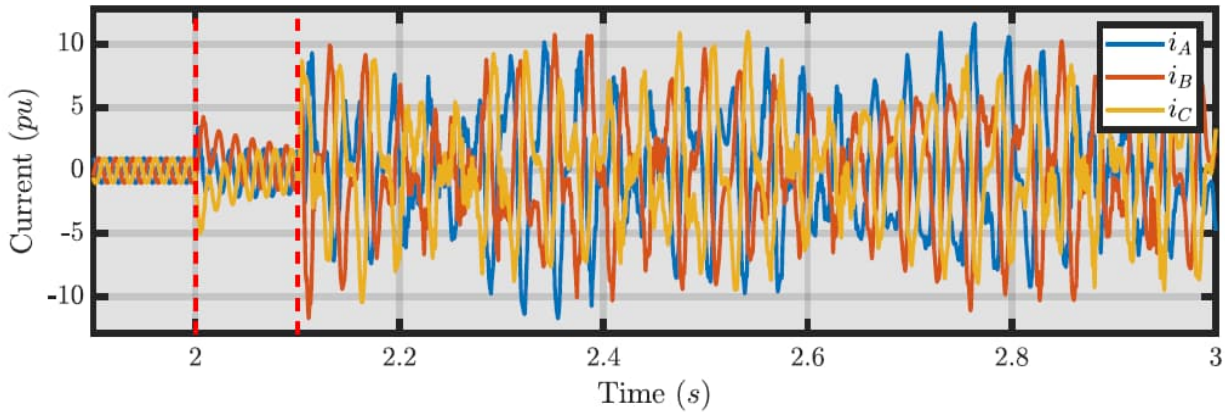


Figure 24 Fault followed by SSCI

vii. Wind farm cyberattack scenario 1: Attack on relay creates radial connection.

In this scenario, the attacker created a topology change in the system by causing the transformer relay in Figure 28 to trip the generator and lockout. As a result in conditions where a Wind Park is radially connected to a series compensated transmission line. Attackers may potentially gain access to a transformer relay if it was connected to the network. Changes on basic settings (e.g., current transformer ratio) can trip the differential element, thus tripping the breakers surrounding the transformer.

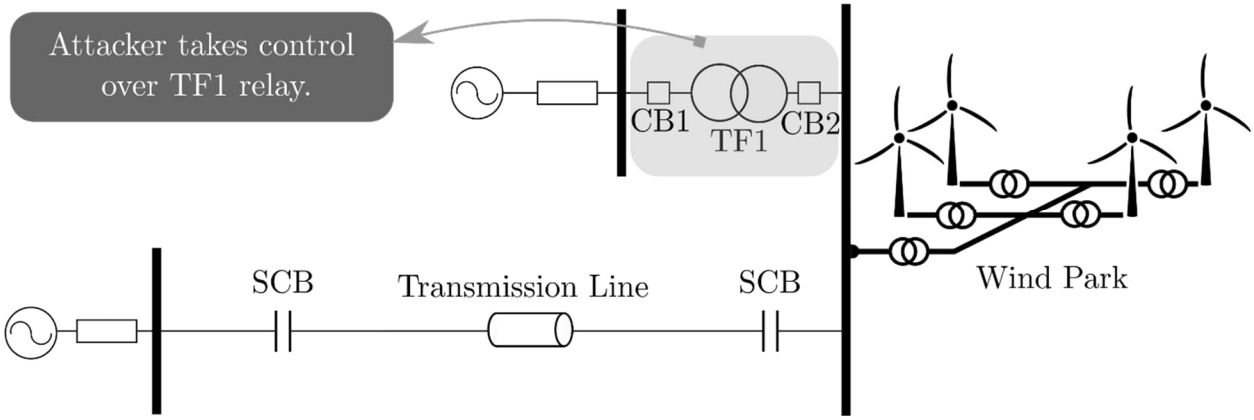


Figure 28 Overview of the scenario 1

The radial connection of the wind farm triggers SSCI and the amplitude of the current from the wind park drastically increases, as shown on Figure 9. The SSCI frequency is shown on 30. The magnitude of the current can damage the series capacitor banks (SCB) and/or the wind turbine (e.g., crowbar). Additionally, the wind park will likely disconnect from the power system leading to an outage or even a blackout.

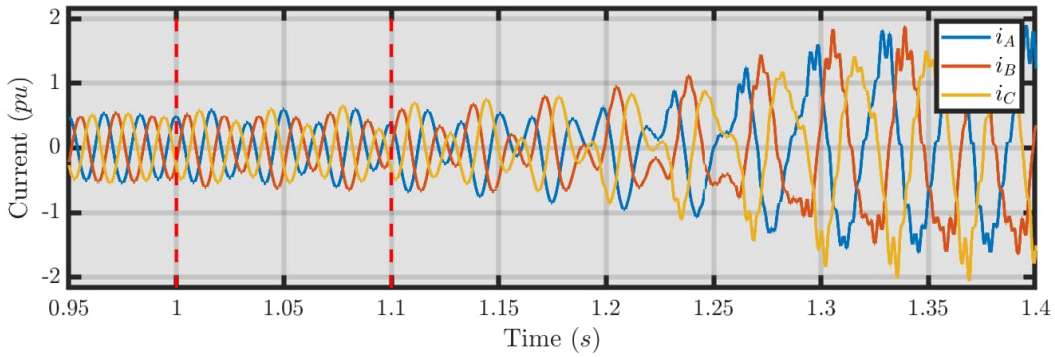


Figure 29 Current injected by the wind park during SSCI triggered by attack

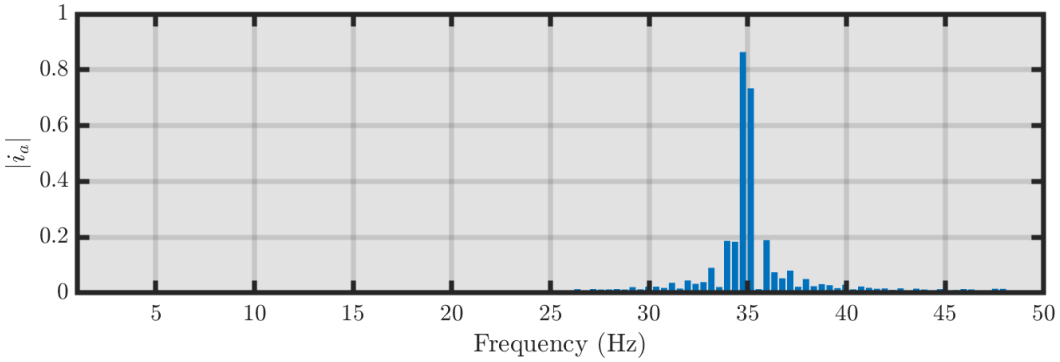


Figure 30 FFT of the current of phase A

viii. Wind farm cyberattack scenario 2: Wind Park Measurement Corruption – Quadrature Current (Rotor side)

In this scenario the control systems of type-3 wind parks are used to control the converter located at the rotor side (RSC) and grid side (GSC). Attackers may potentially gain access to this device through the wind farm vendor asset health monitoring interface. A successful network attack which identifies the location of the RSC parameters could result in augmentation of the quadrature current reference values or the local measurement value.

The attacker modifies the reference value of the quadrature current of the RSC, resulting in a change in excitation to the induction generator will occur causing the voltage at the terminals to increase or decrease. This possible increase or decrease may result in SSCI of the wind park shown in Figure 31.

Figure 32 shows the results of a case where the augmentation occurs at 1 s and lasts for 100 ms. As a result, SSCI starts at 1.2 with main frequency around 35 Hz as shown on Figure 33.

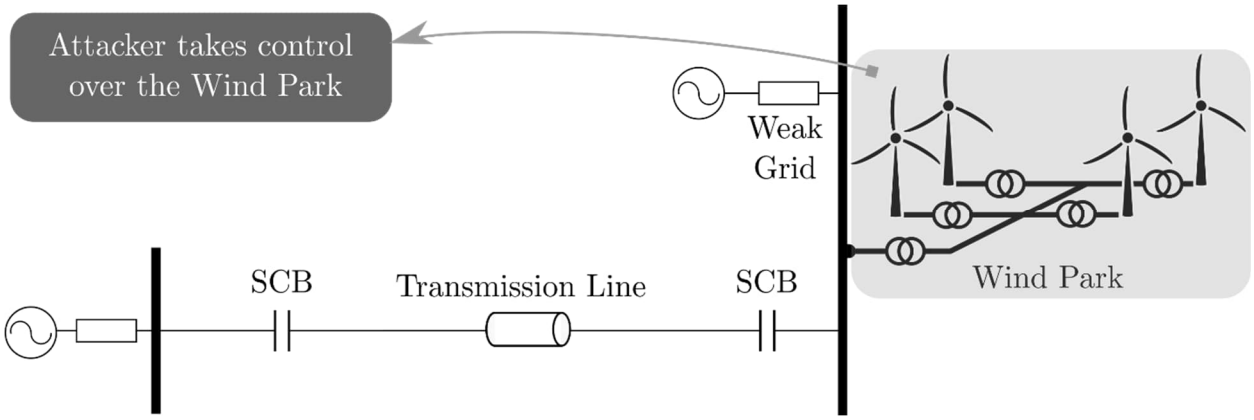


Figure 31 Overview of the scenario 2

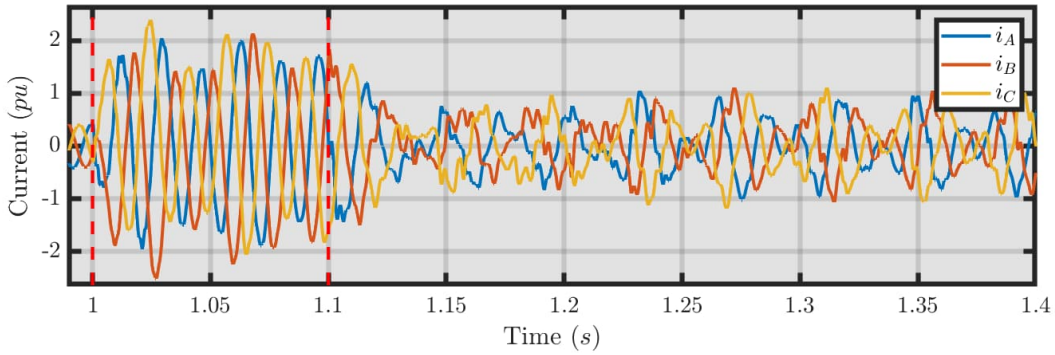


Figure 32 Example of attack at the RSC.

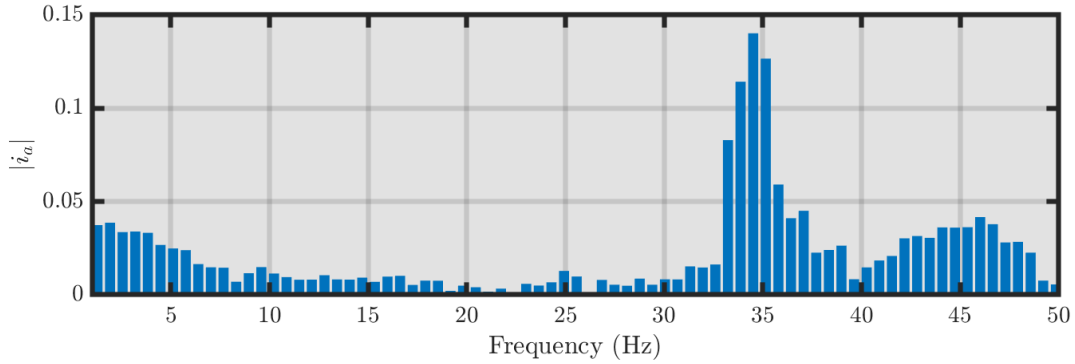


Figure 33 Frequency components present on the current of phase A for scenario 2.

ix. Wind farm cyberattack scenario 3: Bypass of series capacitor bank

Series Capacitor Banks (SCB) are equipped with controls that allow them to be bypassed in event of overcurrent conditions on the transmission line, often due to faults. This bypass is normally triggered when the energy absorbed by the surge arresters connected across the capacitors for overvoltage protection approach their energy limiter. The bypass breaker protects the capacitors and the arrestors. Attackers may potentially gain access to this device and force an unwanted bypass if the controls are connected to the network. Figure 34 provides an overview of this scenario.

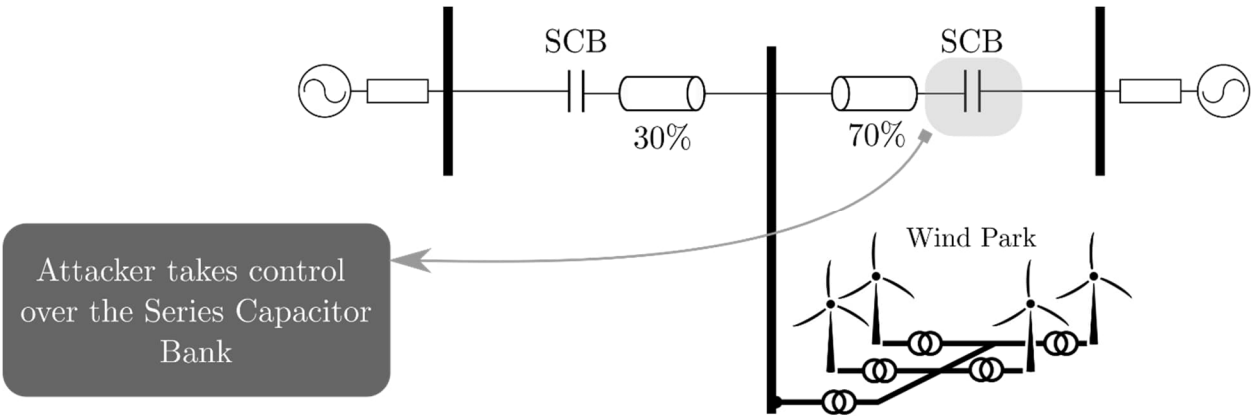


Figure 34 Overview of scenario 3

An attack bypassing the series capacitor creates a weak grid connection for the wind park, which triggers SSCI. Figure 35 shows a scenario where an attack occurs at 1.1s and SSCI slowly starts. The SSCI frequency is shown on Figure 36. The wind park will disconnect from the power system leading to a more severe disturbance for the system if this is a large wind farm.

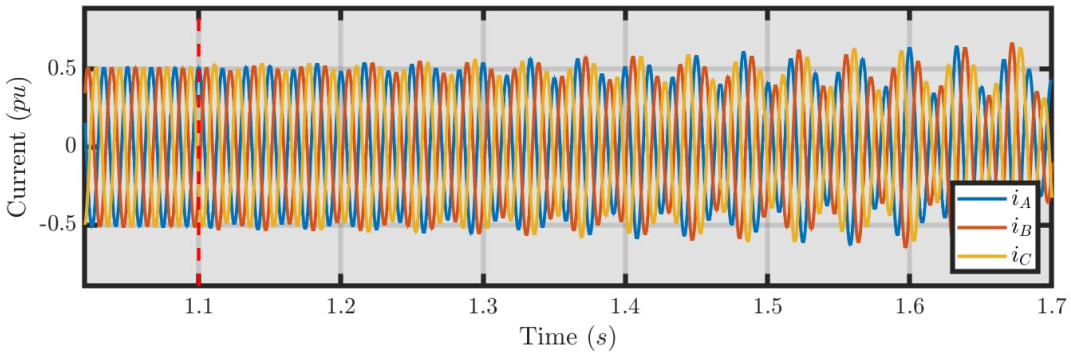


Figure 35 Example of SSCI caused a bypass of a SCB.

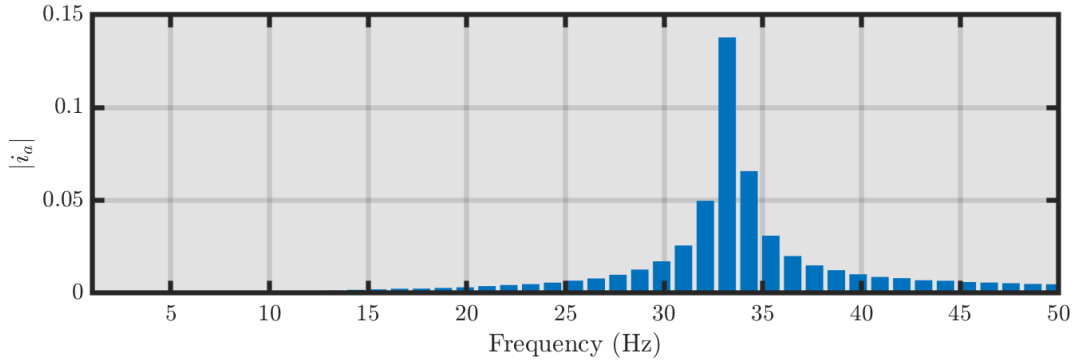


Figure 36 Frequency of the current of phase A.

f. Conclusion

The developed novel frequency compensator has been shown to significantly reduce subsynchronous oscillations in the event of a wind park being unable to handle moderate changes in system load. As the load modulation in the test system is generated by randomly determined values that follow a normal distribution, the cause of the load modulation is irrelevant to the results. These results were achieved components modeling in the RTDS: namely a PMU, an SVC bank, and a custom filter to serve as the compensator, illustrating the ease with which the frequency compensator could be implemented onto a system already containing a PMU and SVC.

The present study is focused on low frequency oscillatory modes of wind farms, and the compensator will be limited in frequencies it can control for by the reporting rate of the sensor, in this case the PMU. The magnitude of modulations the compensator is able to mitigate is likely somewhat dependent on the distance of the load in question from the wind park, and the exact nature of that relationship needs further testing to codify. Additionally, other sources of system instability besides load modulations, such as a cyberattack interfering with the normal operation of one of the system's many synchronous generators, are still being tested so that the compensator may be further refined

The compensator was tested against large load variations, variations in wind farm output (possibly due to a cyberattack0 that cause system oscillations (but not subsynchronous control interactions), and attacks on generator controls. The damping control showed success against the load variations and wind farm variation. The controller showed moderated success against driven voltage oscillations due to attacks against a generator exciter that could be either against the exciter itself or a power system stabilizer. The location of the compensator impacted the results, so further work needs to look at location requirements. The damping control was not as successful against attacks against a governor creating driven oscillations, which verified that a shunt reactive compensator, while effective against event driven oscillations is not as effective against driven real power oscillations.

The team studied scenarios where subsynchronous control interactions can be triggered by cyberattacks. The damping controller has not been tested in these scenarios. That application will be tested in further work as the team prepares papers on this research for publication.

g. References

[1] Shan Jiang, U. D. Annakkage, A. M. Gole, "A Platform for Validation of FACTS Models", *IEEE Transactions on Power Delivery*. Vol. 21, No.1, January 2006.

[2] "Wind Energy Systems Sub-Synchronous Oscillations: Events and Modelling," IEEE Power & Energy Society, July 2020.

[3] Brownlees, S. & Flynn, Damian & Fox, B. & Littler, Tim. (2007). "The Impact of Wind Farm Power Oscillations on the Irish Power System." 195 - 200. 10.1109/PCT.2007.4538316.

[4] L. P. Kunjumuhammed, B. C. Pal, C. Oates and K. J. Dyke, "Electrical Oscillations in Wind Farm Systems: Analysis and Insight Based on Detailed Modeling," in IEEE Transactions on Sustainable Energy, vol. 7, no. 1, pp. 51-62, Jan. 2016, doi: 10.1109/TSTE.2015.2472476.

[5] "Wind explained: Where wind power is harnessed." U.S. Energy Information Administration. https://www.eia.gov/energyexplained/wind/where-wind-power-is-harnessed.php (retrieved 18 Jan 2022)

[6] “Electricity Energy Infrastructure and Resources.” U.S. Energy Information Administration, U.S. Energy Atlas. https://atlas.eia.gov/apps/895faaf79d744f2ab3b72f8bd5778e68/explore (retrieved 18 Jan 2022)

[7] A. Frangoul, “Construction starts at America’s first major offshore wind farm.” CNBC. https://www.cnbc.com/2021/11/19/construction-starts-at-americas-first-major-offshore-wind-farm.html (retrieved 18 Jan 2022)

[8] M. Hojabri et al., “A Comprehensive Survey of Phasor Measurement Unit Applications in Distribution Systems,” MDPI, 29 November 2019. Accessed: 1 Jan 2022. Available: https://www.mdpi.com/1996-1073/12/23/4552/pdf

[9] A. K. Tangirala, “Identification of Non-Parametric Input-Output Models,” in Principles of System Identification: Theory and Practice. 1st ed. Boca Raton: CRC, Taylor & Francis Group, 2015, pp. 542-556. [Online]. Available: https://www.oreilly.com/

[10] U.S Department of Energy Energy Efficiency and R. Energy Wind Energy Technologies Office, “Roadmap for Wind Cybersecurity,” 2020.

[11] A. Sharma, “A combined survey on distribution system state estimation and false data injection in cyber – physical power distribution networks,” no. October 2020, pp. 41–62, 2021, doi: 10.1049/cps2.12000.

[12] K. Pan, A. Teixeira, M. Cvetkovic, and P. Palensky, “Cyber Risk Analysis of Combined Data Attacks Against Power System State Estimation,” IEEE Transactions on Smart Grid, vol. 10, no. 3, pp. 3044–3056, May 2019, doi: 10.1109/TSG.2018.2817387.

[13] F. F. Wu and E. L. Wen-Hsiung, “Detection of topology errors by state estimation,” IEEE Transactions on Power Systems, vol. 4, no. 1, pp. 176–183, 1989, doi: 10.1109/59.32475.

[14] C. N. Lu, J. H. Teng, and B. S. Chang, “Power system network topology error detection,” IEE Proceedings: Generation, Transmission and Distribution, vol. 141, no. 6, pp. 623–629, Nov. 1994, doi: 10.1049/IP-GTD:19941482.

[15] H. Zhang, B. Liu, and H. Wu, “Smart Grid Cyber-Physical Attack and Defense: A Review,” IEEE Access, vol. 9, no. December 2015, pp. 29641–29659, 2021, doi: 10.1109/ACCESS.2021.3058628.

[16] Zabetian-Hosseini, Asal, Ali Mehrizi-Sani, and Chen-Ching Liu. "Cyberattack to Cyber-Physical Model of Wind Farm SCADA." Paper presented at the 44th Annual Conference of the IEEE Industrial Electronics Society, Washington, D.C., October 2018. DOI:10.1109/iecon.2018.8591200.

[17] Staggs, Jason, David Ferlemann, and Sujeet Shenoi. "Wind Farm Security: Attack Surface, Targets, Scenarios and Mitigation." International Journal of Critical Infrastructure Protection 17 (2017): 3-14. DOI:10.1016/j.ijcip.2017.03.001.

[18] Analytic Methods for Power Systems (AMPS) Committee Transient Analysis and Simulations Subcommittee (TASS) Wind SSO Task Force. “Wind Energy Systems Sub- Synchronous Oscillations: Events and Modeling”, 2020.

[19] L. Fan, R. Kavasseri, Z. L. Miao, and C. Zhu, "Modeling of dfig-based wind farms for SSR analysis," IEEE Transactions on Power Delivery, vol. 25, no. 4, pp. 2073–2082, 2010.

[20] H. Liu, X. Xie, J. He, T. Xu, Z. Yu, C. Wang, and C. Zhang, "Subsynchronous interaction between direct-drive pmsg based wind farms and weak ac networks," IEEE Transactions on Power Systems, vol. PP, no. 99, pp. 1–1, 2017.

[21] B. Agrawal and R. Farmer, "Use of frequency scanning techniques for subsynchronous resonance analysis," IEEE Transactions on Power Apparatus and Systems, no. 2, pp. 341–349, 1979.

[22] Sathu, Maadhavi. Design, "Modeling and Analysis of a New Power Swing Protection Scheme for Wind Integrated Systems", 2020.