COMILLAS
UNIVERSIDAD PONTIFICIA
ICAI

Master in Industrial Engineering (MII)

Assessment of dynamic load-altering attacks on power system small signal stability

Author: Pablo López de Hierro Puértolas

Director: Lukas Sigrist

Master Final Thesis

Madrid

30 of August 2024

Abstract

The development of information and communication technologies (ICT) combined with the implementation of smart grids has significantly enhanced the efficiency and reliability of power grid systems. However, without robust security measures, these technological innovations can introduce new vulnerabilities, making power grids susceptible to a wide range of cyberattacks.

In cyberattacks targeting the generation sector, an attacker may attempt to hack into large power plants to disrupt or take control of generation units. In attacks on the distribution and transmission sectors, the attacker might try to manipulate with energy sensors installed throughout the power grid. In the consumer sector, the focus may be on executing load-altering attacks (LAA) to disrupt normal operation.

The shared goal of these attacks is to compromise power system stability which is defined as the capability of the system to return to normal operation status after a disturbance.

Disturbances can be classified as large disturbances which are related to major events related to generator or transmission line outages whose equations cannot be linearized while small disturbances are related to minor events such as small generation or demand variations and whose equations can be linearized. Therefore, if a system is not stable under small disturbances, it will not be stable under large disturbances either so it is important to first evaluate small disturbance stability also known as small signal stability.

The small signal stability analysis is based on the calculation of the eigenvalues of the state matrix A of the system which is given by formulating the equations of the system in standard linearized form in which the derivatives of the state variables are related to the state variables with through the state matrix A. If eigenvalues have negative real part the system is stable but if at least one eigenvalue have positive real part the system becomes unstable.

Related to demand cyberattacks, LAA attempts to control and modify the demand of a group of remotely controllable and insecure loads in order to damage the grid. Several types of loads are potentially vulnerable to attacks of this type, e.g. remotely controllable loads, loads that automatically respond to price commands or direct load control signals, frequency-dependent loads etc.

LAA disruption attacks can be classified based on type, controller type and scope. In this thesis we focus on closed-loop multi-point dynamic load altering attacks (D-LAA) which are characterized of being demand multi-attacks in which the attacker has real-time monitoring of network conditions and focuses on coordinated attacks on multiple loads.

Previously described attack is modeled in frequency dependent loads (FDL), which are those demands that incorporate a frequency controller that modifies the demanded load as a function of the frequency variation in the system mainly for system stabilization purposes. The goal is to design the frequency controller in order to destabilize the system instead of stabilizing it.

Therefore, this master's final thesis has as its overall objective to analyze small signal stability to multi-point closed-loop FDL D-LAA on the IEEE 39-bus system using small signal stability analysis Matlab toolbox.

To this end, this master's final thesis aims to fullfil the following specific objectives:

- Development of a fundamental model to analyze FDL D-LAA small signal stability
- Implementation of FDL D-LAA into a small signal stability analysis Matlab toolbox, which allow more accurate and complex calculations than the fundamental model
- Evaluation of the impact of existing stabilization means such as Power System Stabilizers on the effectiveness of FDL D-LAA

From the development of the fundamental model to analyze FDL D-LAA small signal stability, a system of n generators was modeled with network simplifications such as DC power flow or simplified dynamic generator models, obtaining the following state matrix A for the subsequent eigenvalue calculation.

$$A^{sys} = \begin{bmatrix} 0 & \Omega_{base} & 0 \\ -\frac{1}{2\cdot\omega_0}\cdot H^{-1}\cdot\left(B^{agg}+B^{agb}\cdot B^{\theta\delta}\right) & -\frac{1}{2\cdot\omega_0}\cdot H^{-1}\cdot D & -\frac{1}{2\cdot\omega_0}\cdot H^{-1}\cdot B^{agb}\cdot B^{\theta\varphi} \\ -\frac{1}{T^f}\cdot B^{\theta\delta} & 0 & \frac{1}{T^f}\cdot\left(B^{\theta\varphi}-I\right) \end{bmatrix} \tag{0.1}$$

In addition, the frequency controller was modeled with the following transfer function where K_j^L is the controller gain and $\Delta\theta_j(s)$ is the bus angle.

$$\Delta p_j^L(s) = K_j^L \cdot \frac{s}{1+s\cdot T^f}\cdot\Delta\theta_j(s) \tag{0.2}$$

To carry out the FDL D-LAA small signal stability was analyzed by means of Matlab toolbox developed for this purpose. The toolbox needed to be updated to extend its capability to analyze the impact of FDL D-LAA and to enable to design of FDL D-LAA.

A destabilizing strategy was subsequently designed based on shifting the eigenvalues of the system towards the plane with positive real part by varying the controller gain having the following main steps:

- Calculation of the system eigenvalues and selection of the weakest eigenvalue
- Selection of nodes on which to perform the attack based on weakest eigenvalue sensitivities analysis
- Implementation of the attack by means of two control destabilization strategies, manual iterative design and coordinated eigenvalue design

Analyses were conducted in two scenarios within the IEEE 39-bus system: Scenario 1, where only some of the system's generators have stabilizers, and Scenario 2, all of the system's generators have stabilizers.

Some of the main results obtained include: In Scenario 1, using the manual iterative method, the system is destabilized at a controller gain value of k = *-10.* Conversely, in Scenario 2, the system becomes unstable at a controller gain value of k = *-80.*

These gain values indicate that the attacker must be able to modify the demand by a factor of 10 and 80 respectively in order to destabilize the system. That is, with a variation in demand of 1%, the attacker must be able to vary the demand by 10% and 80% in each of the corresponding scenarios.

Based on the results obtained, it was clearly observed that:

- The presence of stabilizers in the generators significantly hinders the destabilization of the system, requiring the attacker to manipulate large amounts of demand to induce system instabilities, which is often not feasible
- The weakest eigenvalue is not necessarily the easiest to destabilize, which makes it difficult to determine which nodes in the system are the most effective for a cyberattack

Additionally, several constraints were identified that must be met to enable a successful cyberattack:

- The attacker must have prior knowledge of which system loads are most vulnerable to causing system instability
- The attacker must have a foundational understanding of controllers design
- The targeted loads must have sufficient power capacity to be increased or decreased

Resumen

El desarrollo de las tecnologías de la información y la comunicación (TIC), combinado con la implantación de redes inteligentes, ha mejorado considerablemente la eficiencia y la fiabilidad de los sistemas eléctricos. Sin embargo, sin medidas de seguridad sólidas, estas innovaciones tecnológicas pueden introducir nuevas vulnerabilidades, haciendo que las redes eléctricas sean susceptibles de sufrir una amplia variedad de ciberataques.

En los ciberataques dirigidos al sector de la generación, un atacante puede intentar manipular grandes centrales eléctricas para interrumpir o tomar el control de las unidades de generación. En los ataques a los sectores de distribución y transmisión, el atacante podría intentar manipular con sensores instalados a lo largo de toda la red. En el sector de los consumidores, el objetivo puede ser ejecutar ataques de alteración de la demanda (LAA).

El objetivo común de estos ataques es comprometer la estabilidad del sistema eléctrico, que se define como la capacidad del sistema de volver a su estado normal de funcionamiento tras una perturbación.

Las perturbaciones se pueden clasificar en grandes perturbaciones, que están relacionadas con grandes eventos como caídas de generadores o líneas de transmisión, cuyas ecuaciones no se pueden linealizar, mientras que las pequeñas perturbaciones están relacionadas con eventos menores, como pequeñas variaciones de la generación o la demanda, y cuyas ecuaciones se pueden linealizar. Por lo tanto, si un sistema no es estable ante pequeñas perturbaciones, tampoco lo será ante grandes perturbaciones, por lo que es importante evaluar primero la estabilidad ante pequeñas perturbaciones, también conocida como estabilidad de pequeña señal.

El análisis de estabilidad pequeña señal se basa en el cálculo de los autovalores de la matriz de estado A del sistema, que se obtiene formulando las ecuaciones del sistema en forma linealizada estándar en la que las derivadas de las variables de estado se relacionan con las variables de estado a través de la matriz de estado A. Si todos los autovalores tienen parte real negativa, el sistema es estable, sin embargo, si al menos un autovalor tiene parte real positiva el sistema es inestable.

En relación con los ciberataques de la demanda, los LAA intenta controlar y modificar la demanda de un grupo de cargas controlables e inseguras con el fin de generar interrupciones en el servicio. Varios tipos de cargas son potencialmente vulnerables a ataques de este tipo, por ejemplo, cargas controlables a distancia, cargas que responden automáticamente a comandas de precios, cargas dependientes de la frecuencia, etc.

Los ataques de alteración de la demanda pueden clasificarse en función del tipo, el control y el alcance. En este trabajo nos centramos en los ataques dinámicos de alteracíín de la demanda (D-LAA) multipunto y en lazo cerrado que se caracterizan por ser ataques múltiples por demanda en los que el atacante dispone de monitorización en tiempo real de las condiciones de la red y se centra en ataques coordinados a múltiples cargas.

Este tipo de ataque se modelan en cargas dependientes de la frecuencia (FDL), que son aquellas que incorporan un controlador de frecuencia que modifica la carga demandada en función de la variación de frecuencia principalmente con fines de estabilización del sistema. El objetivo es diseñar el controlador de frecuencia para desestabilizar el sistema en lugar de estabilizarlo.

Por lo tanto, este trabajo de fin de máster tiene como objetivo general analizar la estabilidad de pequeña señal ante D-LAA en lazo cerrado y multipunto sobre FDL en el sistema IEEE 39-buses utilizando una toolbox de Matlab especializada en el análisis de estabilidad de pequeña señal.

Para ello, es necesario cumplir con los siguientes objetivos específicos:

- Desarrollar un modelo fundamental para analizar estabilidad de pequeña señal ante D-LAA en FDL
- Implementar D-LAA en FDL en una toolbox de Matlab especializada en el análisis de estabilidad de pequeña señal ya que ofrece mayor precision y potencia de calculo que el modelo fundamental
- Evaluar el impacto de la presencia de estabilizadores en los generadores la red en la efectividad de los D-LAA en FDL

A partir del desarrollo del modelo fundamental para analizar la estabilidad de pequeña señal ante D-LAA en FDL, se modeló un sistema de n generadores con simplificaciones de red como el uso del flujo de cargas DC o el modelo dinámico simplificado de generador, obteniendo la siguiente matriz de estado A para el posterior cálculo de autovalores.

$$A^{sys} = \begin{bmatrix} 0 & \Omega_{base} & 0 \\ -\frac{1}{2\cdot\omega_0}\cdot H^{-1}\cdot\left(B^{agg}+B^{agb}\cdot B^{\theta\delta}\right) & -\frac{1}{2\cdot\omega_0}\cdot H^{-1}\cdot D & -\frac{1}{2\cdot\omega_0}\cdot H^{-1}\cdot B^{agb}\cdot B^{\theta\varphi} \\ -\frac{1}{T^f}\cdot B^{\theta\delta} & 0 & \frac{1}{T^f}\cdot\left(B^{\theta\varphi}-I\right) \end{bmatrix} \tag{0.3}$$

Además, el control de frecuencia se modeló con la siguiente función de transferencia donde K_j^L representa la ganancia del control y $\Delta\theta_j(s)$ el ángulo del nudo.

$$\Delta p_j^L(s) = K_j^L \cdot \frac{s}{1+s\cdot T^f}\cdot\Delta\theta_j(s) \tag{0.4}$$

Para llevar a cabo D-LAA en FDL se analizó la estabilidad de pequeña señal mediante la toolbox de Matlab especializada. Para ellos fue necesario primero actualizar la herramienta para ampliar su capacidad de analizar el impacto de D-LAA en FDL y actualizarla para permitir el diseño del control de FDL.

Se diseñó posteriormente una estrategia de desestabilización basada en el desplazamiento de los autovalores del sistema hacia el plano con parte real positiva variando la ganancia del control teniendo los siguientes pasos:

- Cálculo de los autovalores del sistema y selección del autovalor más débil
- Selección de los nudos de demanda sobre los que realizar el ataque a partir de un análisis de las sensibilidades del autovalor más débil
- Implementación del ataque basado en dos estrategias de desestabilización del control, diseño iterativo manual y diseño coordinado de autovalores

Los análisis se llevaron a cabo en dos configuraciones distintas dentro del sistema IEEE de 39 buses: el Escenario 1, con estabilizadores solamente en algunos de los generadores del sistema; y el Escenario 2, con estabilizadores en todos los generadores del sistema.

Algunos de los resultados más destacados indican que, en el Escenario 1, utilizando el método iterativo manual, el sistema se desestabiliza con un valor de ganancia del controlador de k = *-10.* Por otro lado, en el Escenario 2, también mediante el método iterativo manual, se observa que el sistema se vuelve inestable con un valor de ganancia del controlador de k = *-80.*

Estos valores de ganancia indican que el atacante debe ser capaz de modificar la demanda en un factor de 10 y 80 respectivamente para desestabilizar el sistema. Es decir, con una variación de la demanda del 1%, el atacante debe ser capaz de variar la demanda un 10% y un 80% en cada uno de los escenarios correspondientes.

A partir de los resultados obtenidos en los distintos análisis, se pudo apreciar claramente que:

- La presencia de estabilizadores en los generadores dificulta considerablemente la desestabilización del sistema, ya que obliga al atacante a manipular grandes cantidades de demanda para inducir inestabilidades en el sistema, lo que a menudo no es factible
- El autovalor más débil no es necesariamente el más fácil de desestabilizar, lo que dificulta determinar qué demanda del sistema son los más eficaces para un ciberataque.

Además, se identificaron varias limitaciones que deben cumplirse para que un ciberataque tenga éxito:

- El atacante debe tener conocimiento previo de qué cargas del sistema son más vulnerables a causar inestabilidad en el sistema
- El atacante debe tener conocimientos básicos de diseño de controles
- Las cargas a atacar deben tener suficiente reserva de potencia a subir o a bajar

Contents

List of Figures

1 Introduction

1.1 Problem statement

The development of information and communication technologies (ICT) combined with the implementation of smart grids has significantly enhanced the efficiency and reliability of power grid systems. However, without robust security measures, these technological innovations can introduce new vulnerabilities, making power grids susceptible to a wide range of cyberattacks.

In cyberattacks targeting the generation sector, an attacker may attempt to hack into large power plants to disrupt or take control of generation units. In attacks on the distribution and transmission sectors, the attacker might try to tamper with energy sensors installed throughout the power grid. In the consumer sector, the focus may be on executing load-altering attacks (LAA) to disrupt normal operation. Across all these scenarios, the common goal is typically to inject false data into the wide-area control system to induce network instability.

Related to demand cyberattacks, LAA attempts to control and modify the demand of a group of remotely controllable and insecure loads in order to damage the grid. Several types of loads are potentially vulnerable to attacks of this type, e.g. remotely controllable loads, loads that automatically respond to price commands or direct load control signals, frequency-dependent loads etc.

One possible way of LAA cyberattacks is the manipulation of demand via Internet of Things also known as MaDIoT. IoT devices typically possess lower security levels, and when compromised on a large scale, they can be exploited to diminish the overall security margins of the power system. The ultimate goal of these attacks is to manipulate power demand in a way that overloads or under-utilises the power system, thus causing service interruptions. The possible results of these disruptions can range from localised blackouts to major power outages affecting entire regions or even entire countries.

This master thesis aims to implement and analyze system's small signal stability under dynamic load altering attacks (D-LAAs), which are characterized by being multi-attacks per load, with focus on converting loads to destabilizing frequency-dependent loads (FDL).

Power system stability refers to the grid's ability to return to normal operating conditions after a disturbance. The term "normal" is emphasized because the post-perturbation state must be one where key variables (angles, voltages, and frequency) remain within acceptable ranges defined by system operators. Additionally, the system's topology should remain intact, meaning that protection devices and control actions triggered by the disturbance should not lead to significant system losses or grid separation into islands, which are protective mechanisms to prevent total blackouts.

Disturbances can be classified classified as "large" or "small." Large disturbances, or transient stability issues, involve significant events like short circuits or major transmission line outages. Small disturbances involve minor perturbations that can be analyzed through linearization of system model equations.

Power system stability is categorized based on key system variables: generator rotor angles, bus voltage magnitudes, and system frequency, as shown in the accompanying figure. The stability classifications are defined and characterized as follows:

- **Angle Stability.** Rotor angle stability refers to the ability of synchronous machines in the grid to remain in synchronism after disturbances.
- **Voltage Stability.** Voltage stability is the ability of the power system to maintain steady voltages at all buses following a disturbance.
- **Frequency Stability.** Frequency stability involves the recovery of system frequency after significant imbalances between generation and load due to disturbances.

1.2 State of the art

Nowadays, studies related to cyber-attack protection systems and the possible consequences of cyber-attacks are crucial to understand the possible risks and mitigation actions in the face of an accelerated technological development driven by IoT and the artificial intelligence boom.

Several projects related to the need for reliable and secure electricity systems have been developed, such as the development of security systems to protect power grids against cyber-attacks, the study of the security attributes of power grid systems current cyber-security problem or the impact of cyber-attacks on electricity grid generation.

Firstly, the concept of an internet-based load-altering attack was defined, identifying direct and indirect loads that could potentially be compromised [8]. The MaDIoT attack was introduced as an attack that disrupts the normal operation of the power grid by altering power demand using IoT devices to which the attacker has access [11]. They studied these attacks on the Polish grid model, managing to cause local outages and large blackouts in the grid. However, studies suggest the possibility that the Polish grid model under analysis was not N-1 secure, which would lead to an overestimation of the impact of the attacks [3].

The previously mentioned studies show that causing a wide area blackout in a large North American regional system using evenly distributed MaDIoT attacks is extremely difficult. Even if the grid is in a vulnerable state before the attack, such attacks would only cause partial blackouts due to the partial disconnection of loads and generators. The system would quickly recover its stability after this [3].

Researchers examined MaDIoT attacks on the IEEE 39-Bus system by assuming that the attacker has advanced knowledge of the system, allowing them to carry out more sophisticated attacks targeting the most vulnerable nodes in the power system. Results show that these attacks have success rates between 67% and 91% in causing widespread blackouts. However, the likelihood of an attacker with the required system knowledge and resources is estimated to be low.[10]

To date, the LAA literature has mainly focused on static load disruption attacks (S-LAA), where the attack focuses mainly on the volume of vulnerable loads being altered in a single attack per load. In contrast, this project is concerned with D-LAA, which is characterized by being multi-attacks per load rather than a single attack [9] [6] [5].

Related to D-LAA, we can find a paper which proposes protection schemes after D-LAA based on stability results obtained with a different method from the one that will be used in this project for the small signal stability analysis [1].

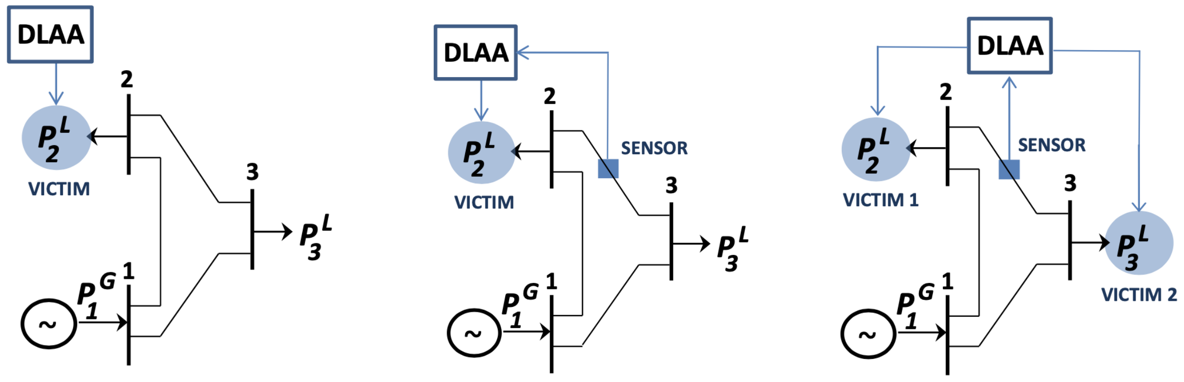
1.2.1 D-LAA classification

A Dynamic Load Altering Attack can operate in two different ways: open-loop or closed-loop.

In an open-loop D-LAA, the attacker manipulates unsecured loads without real-time monitoring of grid conditions or the attack's impact on the grid. This approach relies on historical data collected before the attack to determine a pre-programmed trajectory for the compromised loads [4].

In contrast, a closed-loop D-LAA involves continuous monitoring of grid conditions such as price, voltage magnitude or frequency among others depending on the typology of the load. The attacker uses sensors into the existing power system monitoring infrastructure to adjust the load trajectory based on real-time grid conditions. This method allows for precise control over the load changes at the victim load buses [4].

D-LAAs can also be categorized by scope: single-point or multi-point. Single-point D-LAAs target vulnerable loads at one victim load bus, while multi-point D-LAAs involve coordinated attacks on multiple load buses [7]. Figures (1a) and (1b) illustrate examples of single-point and multi-point closed-loop D-LAAs, respectively.



(a) (b) (c)

Figure 1: Classification of dynamic load altering attacks: a) open-loop D- LAA, b) single-point closed-loop D-LAA, c) multi-point closed-loop D-LAA

Finally, D-LAAs can be classified based on the type of controller used to manipulate load consumption at the victim buses. Open-loop attacks may use feed-forward controllers, while closed-loop attacks typically use feedback controllers. In closed-loop D-LAAs, attackers might employ controllers such as P, PI, or PID, or more complex feedback control mechanisms [1].

To execute a successful D-LAA, the attacker must compromise a sufficient amount of vulnerable loads, being more effective with a higher amount of unsecured and flexible loads to manipulate.

1.2.2 Closed-loop FDL D-LAA

Frequency-dependent loads are essential in modern power systems, enhancing grid stability, efficiency, and reliability by adjusting power consumption based on frequency changes having the possibility of reducing consumption when the frequency drops and increasing it when the frequency rises helping balance supply and demand.

However, through the internet of things, there is potential for cyber manipulation of frequency controllers to achieve the opposite effect, aiming to destabilize the system in response to frequency changes [1]. Therefore, attacks on FDL can be classified as D-LAA since frequency is a parameter that is continuously measured by the frequency controller, leading to continuous multi-attacks.

As discussed in [12], the impact of this type of attack can potentially force generators offline, causing major system disruptions. These disturbances can trigger cascading effects across the interconnected system, with small localized perturbations potentially causing disruptive impacts in distant areas [2].

To carry out a closed-loop FDL D-LAA, a cyber attacker may typically follow these three main steps:

- **Frequency Monitoring.** Measuring the power grid frequency is generally simple and can be done at any power outlet using an inexpensive commercial sensor. Such sensing mechanisms are already embedded in FDLs that help regulate power usage for frequency regulation.

- **Load Calculation.** Calculate the amount of vulnerable load that can be compromised at the victim bus(es) based on information about how much load is currently being consumed and how much load can potentially be manipulated.

- **Destabilizing Controller Design.** Adjust the victim load frequency controller to generate system instability based on the monitored frequency and the calculated load alteration capability.

1.3 Objectives and methodological approach

This master's final thesis has as its overall objective to analyze small signal stability to multi-point closed-loop FDL D-LAA on the IEEE 39-bus system using small signal stability analysis Matlab toolbox.

To this end, this master's final thesis aims at the following specific objectives:

- Development of a fundamental model to analyze FDL D-LAA small signal stability

- Implementation of FDL D-LAA into a small signal stability analysis Matlab toolbox, which allow more accurate and complex calculations than the fundamental model

- Evaluation of the impact of existing stabilization means such as Power System Stabilizers on the effectiveness of FDL D-LAA

In order to achieve the overall and specific objectives, the small signal disturbance is analyzed by means of Matlab toolbox developed for this purpose. The toolbox needs to be updated to extend its capability to analyze the impact of FDL D-LAA. Further, the toolbox needs to be updated to enable to design of FDL D-LAA.

1.4 Thesis structure

The thesis is organized into seven main sections to facilitate a clear and methodical understanding.

- **Section 1** provides a general introduction to the thesis, setting the context and objectives of the study
- **Section 2** describes the fundamentals of small signal stability, providing an essential theoretical foundation for the analyses
- **Section 3** introduces the FDL D-LAA model
- **Section 4** presents a methodology for designing effective FDL D-LAA systems, outlining the steps and considerations involved
- **Section 5** presents the analysis results, detailing the outcomes of implementing the FDL D-LAA in the IEEE 39-bus system.
- **Section 6** discusses how the work aligns with the Sustainable Development Goals (SDGs), highlighting the contributions and relevance of the study to broader sustainability objectives
- **Section 7** illustrates the conclusions drawn from the research, summarizing key findings and suggesting directions for future work

2 Small signal stability analysis

This section details the study of small signal stability. First, simplified small signal stability analysis for simple systems is described and then the study methodology is generalized for any system.

2.1 Simplified small signal stability analysis

In order to carry out explanation, we consider the classical eigenvalue of a single machine connected to an infinite bus. In this case, small signal stability analysis consists of determining whether the generator's equilibrium point comes back to the original stable equilibrium point, or reaches a new stable equilibrium point after a small-disturbance in the mechanical power supplied by the turbine. This study assumes that the initial equilibrium point is stable and that after the perturbation.

In the case of small disturbances, the nonlinear differential equations that describe the generator dynamic behavior can be linearized around the operating point to study the generator response as follows, based on a Taylor-series expansion:

$$\frac{d\Delta\delta}{dt} = \Delta\omega \tag{2.1}$$

$$\begin{aligned} \frac{d\Delta\omega}{dt} &= \frac{\omega_0}{2H}\left(\Delta P_m - \frac{E'V_\infty}{X_e}\cos\delta_0\Delta\delta - \frac{D}{\omega_0}\Delta\omega\right) \\ &= \frac{\omega_0}{2H}\left(\Delta P_m - K\Delta\delta - \frac{D}{\omega_0}\Delta\omega\right) \end{aligned} \tag{2.2}$$

Observe in eq. (2.2) that, apart from the mechanical torque (represented by ΔP_m), there is a synchronizing torque (proportional to the rotor angle, that is, $K\Delta\delta$) and a damping torque (proportional to the rotor speed deviation, that is, $\frac{D}{\omega_0}\Delta\omega$) applied to the generator's rotor. The constant K is typically referred to as the synchronizing torque coefficient.

Equations eq. (2.1) and eq. (2.2) can be also written in matrix form as

$$\begin{bmatrix} \Delta\dot{\delta} \\ \Delta\dot{\omega} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -\frac{K\omega_0}{2H} & -\frac{D}{2H} \end{bmatrix} \begin{bmatrix} \Delta\delta \\ \Delta\omega \end{bmatrix} + \begin{bmatrix} 0 \\ \frac{\omega_0}{2H} \end{bmatrix} \Delta P_m \tag{2.3}$$

which in "standard" linear system compact form are

$$\Delta\dot{x} = A\Delta x + b\Delta u \tag{2.4}$$

where A is the state matrix and b is the input vector.

The small-signal stability of a generator connected to an infinite bus can be analyzed by applying the Laplace transform to the set of linear differential equations. Assuming zero initial conditions, the result is:

$$\Delta x(s) = (sI - A)^{-1} b \Delta u(s) \tag{2.5}$$

$$\frac{\Delta x(s)}{\Delta u(s)} = \frac{b}{sI - A} \tag{2.6}$$

The small-signal stability of the generator can be therefore determined by calculating the roots of the characteristic equation:

$$\det(sI - A) = 0 \tag{2.7}$$

which results in

$$\det \begin{bmatrix} s & -1 \\ \frac{K\omega_0}{2H} & s + \frac{D}{2H} \end{bmatrix} = s^2 + \frac{D}{H}s + \frac{K\omega_0}{2H} = 0 \tag{2.8}$$

If damping D is positive, the oscillations are damped while if is negative, the oscillations are undamped.

This simple example of one generator can be extended to several generators. Equation (2.9) shows the state-space equations for n generators represented by their classical model[1].

$$\begin{bmatrix} \Delta\dot{\delta} \\ \Delta\dot{\omega} \end{bmatrix} = \underbrace{\begin{bmatrix} 0 & \Omega_{base} \\ -\frac{1}{2\cdot\omega_0} \cdot H^{-1} \cdot K^s & -\frac{1}{2\cdot\omega_0} \cdot H^{-1} \cdot D \end{bmatrix}}_{=A^{sys}} \cdot \begin{bmatrix} \Delta\delta \\ \Delta\omega \end{bmatrix} + \begin{bmatrix} 0 \\ \frac{1}{2\cdot\omega_0} \cdot H^{-1} \end{bmatrix} \cdot \Delta P^m \tag{2.9}$$

[1] For more information about state-space representation for n classical model generators see A

Small signal stability is determined by the eigenvalues of the system matrix, A^{sys}. If all eigenvalues have negative real part, the system is asymptotically stable. In other words, if Δp^m is disturbed, generator speeds start oscillating but these oscillations are damped out over time. The damping is mainly affected by the equivalent damping matrix, D, and the distribution of the inertia, whereas the oscillation frequency is affected by the synchronizing power matrix, K^s, and the distribution of the inertia.

2.2 Generalization of small signal stability analysis

Let us consider a dynamic system described by a set of non linear differential equations written in explicit form (the derivatives of the state variables depend only on the state variables x):

$$\dot{x} = f(x) \quad x \in \mathbb{R}^{N \times l} \tag{2.10}$$

If the set of non linear differential equations are linearized around an operating point $x = x_0$, it results in:

$$\Delta\dot{x} = \left.\frac{\partial f(x)}{\partial x}\right|_{x=x_0}, \Delta\dot{x} = A\Delta x, \quad A \in \mathbb{R}^{N \times N}, \quad \Delta x = x - x_0 \tag{2.11}$$

The small signal stability analysis of complex eigenvalues is not performed in practice based on computing the roots of the characteristic equation, given the difficulties of calculating the determinant of a matrix that can be of large dimension. Thus, this analysis is typically carried out by determining the analytical solution of the linear system expressed in terms of the exponential of the state matrix A.

$$\Delta x = e^{At}\Delta x(0) \tag{2.12}$$

The exponential of the state matrix A may be computed using the Taylor expansion:

$$e^{At} = I + \frac{A}{1!}t + \frac{A^2}{2!}t^2 + \cdots \tag{2.13}$$

However, this method is not always numerically robust. A physically meaningful alternative is based on the eigenvalues and eigenvectors of the state matrix A. An eigenvalue λ_i of the state matrix A and the associated right v_i and left w_i eigenvectors are defined as:

$$Av_i = v_i\lambda_i \tag{2.14}$$

$$w_i^T A = \lambda_i w_i^T \tag{2.15}$$

The study of eq. (2.14) and eq. (2.15) indicates that the right and left eigenvectors are not uniquely determined (they are computed as the solution of a linear system of N equations and $N+1$ unknowns). An approach to eliminate that degree of freedom is to introduce a normalization such as:

$$w_i^T v_i = 1 \tag{2.16}$$

in case of N distinct eigenvalues, eq. (2.14) and eq. (2.15) and can be written together for all eigenvalues in matrix form as:

$$AV = V\Lambda \quad WA = \Lambda W \quad WV = I \tag{2.17}$$

where Λ, V y W are respectively the matrices of eigenvalues and right and left eigenvectors:

$$\Lambda = \begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_N \end{bmatrix}, \quad V = [v_1 \cdots v_N], \quad W = \begin{bmatrix} w_1^T \\ \vdots \\ w_N^T \end{bmatrix} \tag{2.18}$$

If the exponential of the state matrix e^{At} is expressed in terms of eigenvalues and right and left eigenvectors of the state matrix, it results in:

$$\begin{aligned} e^{At} &= VW + \frac{V\Lambda W}{1!}t + \frac{V\Lambda^2 W}{2!}t^2 + \cdots \\ &= V\left(I + \frac{\Lambda}{1!}t + \frac{\Lambda^2}{2!}t^2 + \cdots\right)W = Ve^{\Lambda t}W \end{aligned} \tag{2.19}$$

The solution of the set of linear differential equations eq. (2.11) can be expressed in terms of the eigenvalues and right and left eigenvectors of the state matrix A as:

$$\Delta x = Ve^{\Lambda t}W\Delta x(0) = \sum_{i=1}^{N} v_i e^{\lambda_i t}[w_i^T \Delta x(0)] \tag{2.20}$$

The study of eq. (2.20) allows to draw the following conclusions:

- The system response is expressed as the combination of the system response for N eigenvalues.
- The eigenvalues of the state matrix determine the system stability. A real negative (positive) eigenvalue indicates an exponentially decreasing (increasing) behaviour. A complex eigenvalue of negative (positive) real part indicates an oscillatory decreasing (increasing) behaviour.
- The components of the right eigenvector v_i indicate the relative activity of each variable in the i-th eigenvalue.
- The components of the left eigenvector w_i weight the initial conditions in the i-th eigenvalue.

2.2.1 Modal controllability and observability factors

Let us consider that in the linear dynamic system written in explicit form eq. (2.11) an input u and an output y have been selected:

$$\begin{aligned}\Delta\dot{x} &= A\Delta x + b\Delta u \\ \Delta y &= c^T\Delta x\end{aligned} \tag{2.21}$$

Let us apply to the previous equations a variable transformation defined by the matrix of right eigenvectors $\Delta x = V\Delta\tilde{x}$:

$$\begin{aligned}\Delta\dot{\tilde{x}} &= \Lambda\Delta\tilde{x} + Wb\Delta u \\ \Delta y &= c^TV\Delta\tilde{x}\end{aligned} \tag{2.22}$$

or:

$$\begin{cases}\Delta\dot{\tilde{x}}_i = \lambda_i\Delta\tilde{x}_i + w_i^Tb\Delta u \\ \Delta y = c^Tv_i\Delta\tilde{x}_i\end{cases} \qquad i = 1,\ldots,N \tag{2.23}$$

The study of eq. (2.23) allows to draw the following conclusions:

- $w_i^T b$ measures the controllability of the eigenvalues associated to the variable $\Delta\tilde{x}_i$ from the input Δu. In other words, it indicates if the eigenvalu λ_i can be controlled from the input Δu.

- cv_i measures the observability of the eigenvalue associated to the variable $\Delta\tilde{x}_i$ from the input Δy. In other words, it indicates if the eigenvalue λ_i can be observed from the variable Δy.

These results can be summarized as follows: the effectiveness of a control action on an eigenvalue requires that both the eigenvalue is observable from the measured variable Δy and the eigenvalue is controllable from the control variable Δu.

2.2.2 Transfer function residues

The transfer function between Δu and Δy is obtained applying the Laplace transform to the equations (3.16) and eliminating the Laplace transform of the state variables $\Delta x(s)$:

$$\frac{\Delta y(s)}{\Delta u(s)} = c^T(sI - A)^{-1}b \tag{2.24}$$

The transfer function eq. (2.24) can also be written as a partial fraction expansion in terms of the poles p_i and the associated residues $R_{\Delta y/\Delta u,i}$:

$$\frac{\Delta y(s)}{\Delta u(s)} = \sum_{i=1}^{N} \frac{R_{\Delta y/\Delta u,i}}{(s - p_i)} \tag{2.25}$$

If equation eq. (2.25) is written in terms of the eigenvalues and eigenvectors of the state matrix, it becomes:

$$\frac{\Delta y(s)}{\Delta u(s)} = c^T V(sI - \Lambda)^{-1}Wb = \sum_{i=1}^{N} \frac{c^T v_i w_i^T b}{(s - \lambda_i)} \tag{2.26}$$

The comparison of eq. (2.25) and eq. (2.26) confirms that the eigenvalues of the state matrix are the poles of the open loop transfer function and that the transfer function residues can be computed as the product of the modal controllability and observability factors.

$$R_{\Delta y/\Delta u,i} = cv_i w_i^T b = v_{\Delta y,i} w_{\Delta u,i} \tag{2.27}$$

2.2.3 Eigenvalue sensitivities in feedback systems written in transfer function form

The state space representation of linear dynamic systems is appropriate for the analysis of large scale systems. In this context, the expressions obtained in the previous sections are very useful. However, the transfer function representation of linear dynamic systems is more useful when the design of control systems is considered.

Let us consider the feedback system of Figure 2. The plant to be controlled is eigenvalueed by the transfer function $H(s)$ and the controller is represented by the transfer function $F(s, q)$.

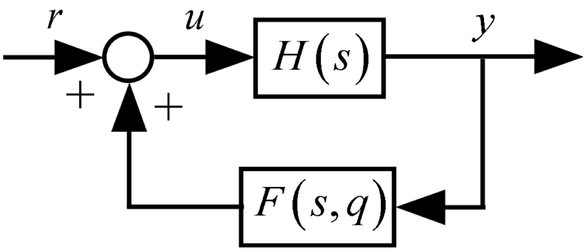


Figure 2: Feedback system in transfer function form

The sensitivity of a pole (eigenvalue) λ_i of the close loop transfer function $\Delta y(s)/\Delta r(s)$ with respect to a parameter q of the controller transfer function $F(s, q)$ is product of the residue of closed loop transfer function $\Delta y(s)/\Delta r(s)$ corresponding to the pole λ_i and the partial derivative of the controller transfer function with respect to the parameter q for $s = \lambda_i$:

$$\frac{\partial \lambda_i}{\partial q} = R_{\Delta y/\Delta r,i} \cdot \left.\frac{\partial F(s,q)}{\partial q}\right|_{s=\lambda_i} \tag{2.28}$$

Therefore, the residue plays a crucial role in the design of controllers, as the variation of an eigenvalue λ_i with respect to a certain controller parameter q for a specific input and output $\Delta y(s)/\Delta r(s)$ is proportional to the residue $R_{\Delta y/\Delta r,i}$ associated with that eigenvalue, input, and output.

3 FDL D-LAA small signal stability model

3.1 Fundamental model

Equation (2.9) can be extended to include frequency-dependent loads. This will show how frequency-dependent loads can affect state matrix and thus the eigenvalues of the system.

A frequency-dependent load at bus j varies its active power consumption according to the bus frequency deviation.

$$\Delta p_j^L = K_j^L \cdot \Delta\dot{\theta}_j \tag{3.1}$$

where K_j^L is the load-frequency damping factor.Since the pure derivative of the bus voltage angle is not causal, the following approximation is used:

$$\Delta\dot{\varphi}_j = \frac{1}{T^f} \cdot (-\Delta\varphi_j + \Delta\theta_j) \tag{3.2a}$$

$$\Delta p_j^L = \frac{K_j^L}{T^f} \cdot (-\Delta\varphi_j + \Delta\theta_j) \tag{3.2b}$$

where $\Delta\varphi_j$ is a new state variable that represents the bus voltage frequency at bus j and T^f is a small filter time constant. Equation (3.2) is the state-space formulation of the following transfer function:

$$\Delta p_j^L(s) = K_j^L \cdot \frac{s}{1 + s \cdot T^f} \cdot \Delta\theta_j(s) \tag{3.3}$$

In matrix form,

$$\Delta\dot{\varphi}^b = \frac{I}{T^f} \cdot (-\Delta\varphi^b + \Delta\theta^b) \tag{3.4a}$$

$$\Delta P^L = \frac{K^L}{T^f} \cdot (-\Delta\varphi^b + \Delta\theta^b) \tag{3.4b}$$

where $K^L = diag([..., K_j^L, ...])$ is diagonal matrix with the load-frequency damping factors on its diagonal.

Considering small perturbations, the bus voltage angle variations can be expressed in terms of the nodal load variations and the internal voltage angle variations (see eq. (A.9)):

$$-\Delta P^{L} = B^{abg} \cdot \Delta\delta + B^{abb} \cdot \Delta\theta^{b} \tag{3.5}$$

Further, if all loads were frequency dependent, merging eq. (3.4b) and eq. (3.5) leads to:

$$\begin{aligned}\Delta\theta^{b} &= \left(\frac{K^{L}}{T^{f}} + B^{abb}\right)^{-1} \cdot \left(\frac{K^{L}}{T^{f}} \cdot \Delta\varphi^{b} - B^{abg} \cdot \Delta\delta\right) \\ &= B^{\theta\varphi} \cdot \Delta\varphi^{b} - B^{\theta\delta} \cdot \Delta\delta\end{aligned} \tag{3.6}$$

$$B^{\theta\delta} = \left(\frac{K^{L}}{T^{f}} \cdot \Delta\varphi^{b} - B^{abg} \cdot \Delta\delta\right) \tag{3.7}$$

Equation (3.4a) becomes then:

$$\Delta P^{L} = \frac{K^{L}}{T^{f}} \cdot \left(B^{\theta\varphi} - I\right) \cdot \Delta\varphi^{b} - \frac{K^{L}}{T^{f}} \cdot B^{\theta\delta} \cdot \Delta\delta \tag{3.8a}$$

$$\Delta\dot{\varphi}^{b} = \frac{1}{T^{f}} \cdot \left(B^{\theta\varphi} - I\right) \cdot \Delta\varphi^{b} - \frac{1}{T^{f}} \cdot B^{\theta\delta} \cdot \Delta\delta \tag{3.8b}$$

By using eq. (3.7), active power generation injection can now be computed in terms of the state variable as follows:

$$\begin{aligned}\Delta P^{Gg} &= B^{agg} \cdot \Delta\delta + B^{agb} \cdot \Delta\theta^{b} \\ &= \left(B^{agg} - B^{agb} \cdot B^{\theta\delta}\right) \cdot \Delta\delta + B^{agb} \cdot B^{\theta\varphi} \cdot \Delta\varphi^{b}\end{aligned} \tag{3.9}$$

Equation (A.12) finally becomes by including the load-frequency dynamics:

$$\begin{bmatrix} \Delta\dot{\delta} \\ \Delta\dot{\omega} \\ \Delta\dot{\varphi} \end{bmatrix} = A^{sys} \cdot \begin{bmatrix} \Delta\delta \\ \Delta\omega \\ \Delta\varphi \end{bmatrix} + \begin{bmatrix} 0 \\ \frac{1}{2\cdot\omega_0} \cdot H^{-1} \\ 0 \end{bmatrix} \cdot \Delta P^{m} \tag{3.10}$$

where

$$A^{sys} = \begin{bmatrix} 0 & \Omega_{base} & 0 \\ -\frac{1}{2\cdot\omega_0}\cdot H^{-1}\cdot\left(B^{agg}+B^{agb}\cdot B^{\theta\delta}\right) & -\frac{1}{2\cdot\omega_0}\cdot H^{-1}\cdot D & -\frac{1}{2\cdot\omega_0}\cdot H^{-1}\cdot B^{agb}\cdot B^{\theta\varphi} \\ -\frac{1}{T^f}\cdot B^{\theta\delta} & 0 & \frac{1}{T^f}\cdot\left(B^{\theta\varphi}-I\right) \end{bmatrix} \tag{3.11}$$

Given the state matrix eq. (3.11), small signal stability can be analyzed using the simplified method by directly calculating the roots of the characteristic equation, as described in the example in Section 2.1, or by applying the generalized methodology outlined in Section 2.2.

3.2 Detailed model

Although the fundamental model allows us to simplify the analysis of small signal stability for FDL D-LAA, this model employs simplifications both in terms of calculations and representation of network elements, which does not clearly reflect reality.

So, to analyze FDL D-LAA small signal stability with greater accuracy, frequency-dependent load model was implemented in a Matlab small signal stability toolbox. In this tool, the various network elements are represented in more detail, and employs more accurate calculation methods, such as AC-PF instead of DC-PF, or the generalized methodology for small signal stability calculation described in Section 2.2. Elemental network elements are modeled as follows:

- Generator units are modeled taking into account the rotor equations, the turbine governor, the excitation system, and the stabilizing units
- Loads can be modeled as constant admittances, constant current, or constant power
- The network is represented by its admittance matrix expanded into its real and imaginary parts

FDLs were modeled in Matlab toolbox using the following dynamic controller system which corresponds with previously described eq. (3.3):

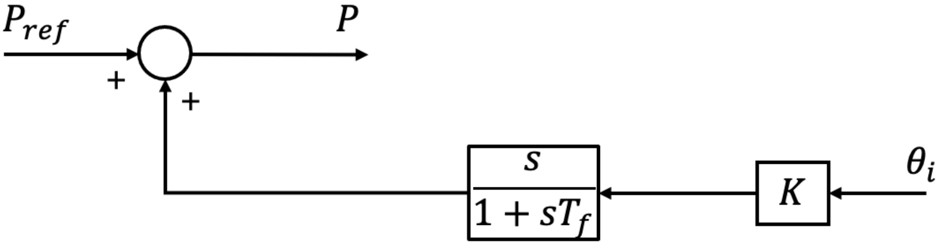


Figure 3: FDL controller

4 FDL D-LAA destabilizing methodology

Small signal stability analysis for FDL D-LAA were carried out using the Matlab toolbox previously described in Section 3 with the aim of determining how easy or difficult it was to destabilize the IEEE 39-bus system [2].

The methodology used is as follows:

- First, eigenvalues of the system are calculated, and the weakest eigenvalue selected
- Secondly, the demand buses on which to carry out the cyberattacks are selected. For the weakest eigenvalue, sensitivity analysis was conducted for a transfer function with frequency as the input and power as the output. This analysis aimed to identify the demand buses with the highest residues related to this eigenvalue and transfer function, as attacks on these nodes would have a greater impact on the eigenvalue and consequently to system stability
- Finally, the attack was carried out on the three demand buses with the highest residues by designing a destabilizing FDL controllers with the aim of destabilizing the system. Two different destabilizing controller designs were implemented: manual iterative design and coordinated eigenvalue sensitivity design

4.1 Manual iterative design

This destabilizing controller design consists of iteratively modifying the value of the selected FDL controller gain K shifting eigenvalues to the half-plane with positive real part until one of the system's eigenvalues, usually the one that was initially the weakest, begins to have positive real part, thereby destabilizing the system.

It is important to consider the sign of the controller gain to shift eigenvalues in the right direction and help destabilize the system. For the demand to contribute to destabilizing the system, it should be reduced when the frequency rises to increase excess generation and increased when the frequency drops to worsen the generation deficit. These actions

[2] For more information about the IEEE 39-bus system see Appendix B

amplify the disparity between generation and demand, leading to greater instability in the system's frequency. Therefore, the sign of the FDL controller gain k must be negative.

4.2 Coordinated eigenvalue sensitivity design

The coordinated eigenvalue sensitivity approach to design a destabilizing controller to destabilize an eigenvalue comprises two steps, the design of the phase compensation network of the controller and the computation of the controller gain.

- The phase compensation network of the controller need to be designed so that the phase of the eigenvalue sensitivity becomes 0 degrees at the eigenvalue natural frequency
- The controller gain needs to be determined such that the eigenvalue moves to the desired position, which in this case is to the point where the eigenvalue begins to have a positive real part

The following Figure 4 shows a geometric interpretation of the eigenvalue sensitivity approach to design a destabilizing controller.

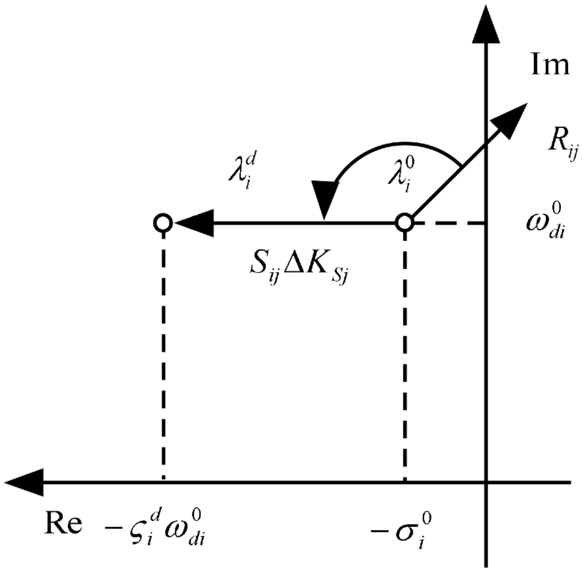


Figure 4: geometric interpretation of the eigenvalue sensitivity approach

Assuming the filtering ratio α_j and the number of stages N_{sj} of the phase compensation networks of the j-th controller, the design of the phase compensation network consists of determining the time constant T_{sj} of the transfer function

$$\left(\frac{1+sT_{sj}}{1+sT_{sj}/\alpha_j}\right)^{N_{sj}} \tag{4.1}$$

so that the phase of the eigenvalue sensitivities with respect to the j-th controller becomes as close as possible to 0 degrees. In other words:

$$\max_{T_{sj}} G(T_{sj}) = \max_{T_{sj}} \sum_{i=1}^{N_E} \beta_{ij} \cos\left(\arg\left[S_i(T_{sj})\right]\right) \tag{4.2}$$

where N_E is the total number of eigenvalues and:

$$\beta_{ij} = \frac{|R_j|}{\sum_{k=1}^{N_E} |R_{kj}|} \tag{4.3}$$

The filtering ratio of the controllers is determined from the average phase of the sensitivities corresponding to the nodes of interest and assuming the number of stages of the phase compensation networks. It should be noted that φ_j is the average phase of the eigenvalue sensitivities:

$$\varphi_j = \arg\left(\sum_{i=1}^{N_k} S_i(T_{sj}=0)\right) \tag{4.4}$$

Once the phase of the sensitivities is close to 0, the gains of the controllers are determined to move the eigenvalues to the desired position. The gains of the controllers are determined by solving a linear programming problem. The objective function is to minimize the control action. The control action is expressed as the sum of the gains weighted by the sensitivities:

$$\min \sum_{j=1}^{N_C} \gamma_j \Delta K_{sj} \tag{4.5}$$

where N_C is the total number of controllers being designed and:

$$\Delta K_{sj} = K_{sj} - K_{sj}^0 \tag{4.6}$$

$$\gamma_j = \sum_{i=1}^{N_E} \left|\frac{\partial \lambda_i}{\partial K_{sj}}\right| \tag{4.7}$$

The constraints are the maximum values of the real part of the eigenvalues and the lower and upper bounds of the gains:

$$\sum_{j=1}^{N_C} \mathrm{Re}\left(\frac{\partial \lambda_i}{\partial K_{sj}}\right) \Delta K_{sj} \geq \mathrm{Re}\left(\lambda_i^d - \lambda_i^0\right), \quad i = 1, \ldots, N_E \tag{4.8}$$

$$K_{sj}^{\min} \leq K_{sj}^0 + \Delta K_{sj} \leq K_{sj}^{\max}, \quad j = 1, \ldots, N_C \tag{4.9}$$

λ_i^0 and λ_i^d are respectively the original and the desired eigenvalues. Assuming that the phase of the eigenvalue sensitivity is 0 degrees, the imaginary part of the desired eigenvalue remains constant and the real part is defined by the desired eigenvalue.

The estimated eigenvalue λ_i^c after incorporating the destabilizing controllers can also be determined using the first order eigenvalue sensitivity:

$$\lambda_i^c = \lambda_i^0 + \Delta\lambda_i = \lambda_i^0 + \sum_{j=1}^{N_C} \frac{\partial \lambda_i}{\partial K_{sj}} \Delta K_{sj} = \lambda_i + \sum_{j=1}^{N_C} S_i(T_{sj}) \cdot K_{sj} \tag{4.10}$$

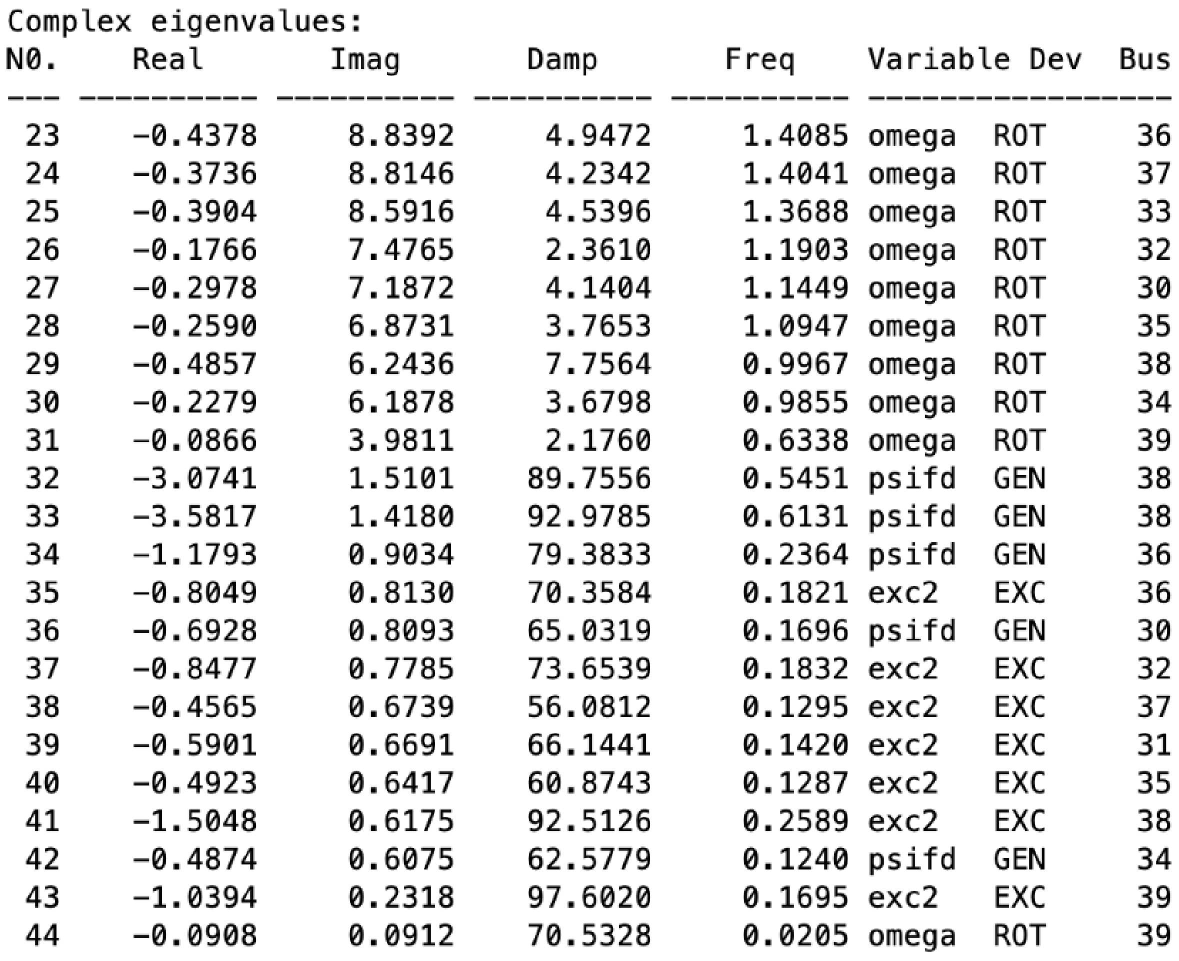
5 Results analysis

Small signal stability analysis for FDL D-LAA were conducted using the detailed model described in Section 3 and following the destabilizing methodology outlined in Section 4. Two different scenarios were considered:

- Scenario 1: Stabilizers on some of the IEEE 39-bus system generators
- Scenario 2: Stabilizers on all of the IEEE 39-bus system generators

5.1 Scenario 1 results analysis

First, system eigenvalues illustrated in the Figure 5 were calculated.



```
Complex eigenvalues:
N0.    Real       Imag       Damp       Freq      Variable Dev  Bus
--- ---------- ---------- ---------- ---------- ----------------
 23    -0.4378     8.8392     4.9472     1.4085 omega   ROT     36
 24    -0.3736     8.8146     4.2342     1.4041 omega   ROT     37
 25    -0.3904     8.5916     4.5396     1.3688 omega   ROT     33
 26    -0.1766     7.4765     2.3610     1.1903 omega   ROT     32
 27    -0.2978     7.1872     4.1404     1.1449 omega   ROT     30
 28    -0.2590     6.8731     3.7653     1.0947 omega   ROT     35
 29    -0.4857     6.2436     7.7564     0.9967 omega   ROT     38
 30    -0.2279     6.1878     3.6798     0.9855 omega   ROT     34
 31    -0.0866     3.9811     2.1760     0.6338 omega   ROT     39
 32    -3.0741     1.5101    89.7556     0.5451 psifd   GEN     38
 33    -3.5817     1.4180    92.9785     0.6131 psifd   GEN     38
 34    -1.1793     0.9034    79.3833     0.2364 psifd   GEN     36
 35    -0.8049     0.8130    70.3584     0.1821 exc2    EXC     36
 36    -0.6928     0.8093    65.0319     0.1696 psifd   GEN     30
 37    -0.8477     0.7785    73.6539     0.1832 exc2    EXC     32
 38    -0.4565     0.6739    56.0812     0.1295 exc2    EXC     37
 39    -0.5901     0.6691    66.1441     0.1420 exc2    EXC     31
 40    -0.4923     0.6417    60.8743     0.1287 exc2    EXC     35
 41    -1.5048     0.6175    92.5126     0.2589 exc2    EXC     38
 42    -0.4874     0.6075    62.5779     0.1240 psifd   GEN     34
 43    -1.0394     0.2318    97.6020     0.1695 exc2    EXC     39
 44    -0.0908     0.0912    70.5328     0.0205 omega   ROT     39
```

Figure 5: Scenario 1 eigenvalues

It can be observed that the weakest eigenvalue is associated with the generator rotor speed of bus 39, as it has the real part closest to positive values (-0.0866) and the lowest damping ratio (2.176).

Sensitivity analysis was then performed on the previously identified eigenvalue. The residues associated with the weakest eigenvalue for each node of the system, with a frequency input and power output transfer function, are shown in the following Figure 6.

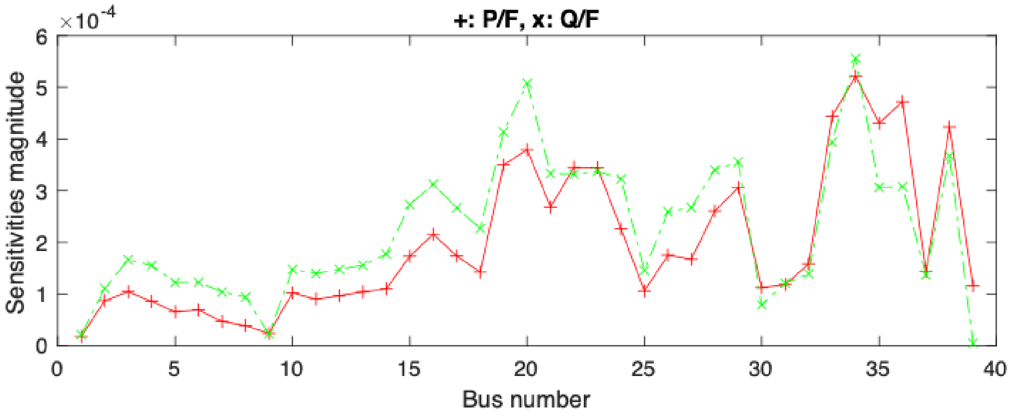
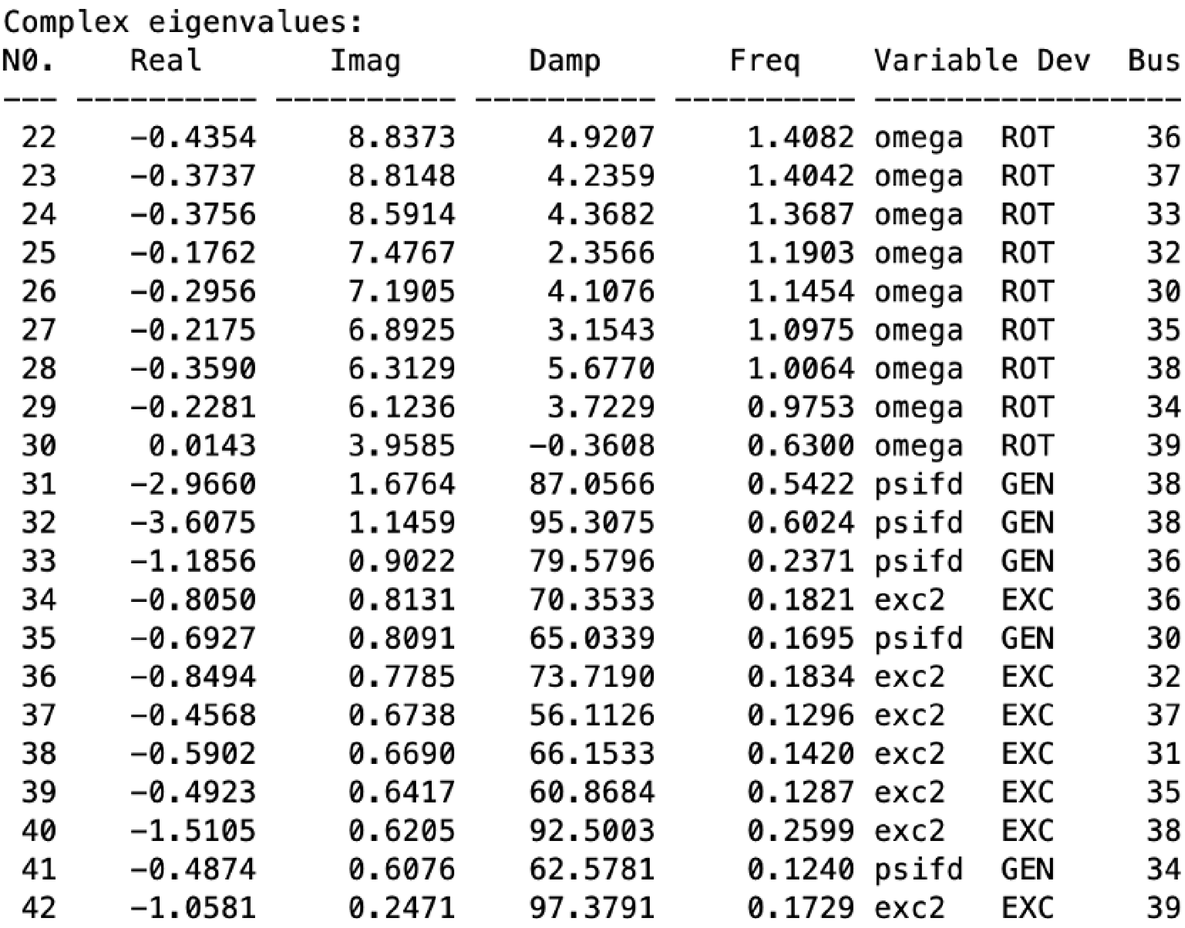


Figure 6: Scenario 1 weakest eigenvalue residues

The demand nodes where the attack would have the greatest impact were selected, being buses 20, 23 and 29 due to their higher resiudes.

First, manual iterative design of destabilizing FDL controller was implemented in these three nodes. After iterating the control gain value K for each of the selected FDLs, from a value of K = *-10*, the system became unstable. The recalculated eigenvalues of the system for this gain value are shown below in Figure 7.



```
Complex eigenvalues:
N0.    Real       Imag       Damp       Freq      Variable Dev  Bus
--- ---------- ---------- ---------- ---------- ----------------
 22    -0.4354     8.8373     4.9207     1.4082 omega  ROT     36
 23    -0.3737     8.8148     4.2359     1.4042 omega  ROT     37
 24    -0.3756     8.5914     4.3682     1.3687 omega  ROT     33
 25    -0.1762     7.4767     2.3566     1.1903 omega  ROT     32
 26    -0.2956     7.1905     4.1076     1.1454 omega  ROT     30
 27    -0.2175     6.8925     3.1543     1.0975 omega  ROT     35
 28    -0.3590     6.3129     5.6770     1.0064 omega  ROT     38
 29    -0.2281     6.1236     3.7229     0.9753 omega  ROT     34
 30     0.0143     3.9585    -0.3608     0.6300 omega  ROT     39
 31    -2.9660     1.6764    87.0566     0.5422 psifd  GEN     38
 32    -3.6075     1.1459    95.3075     0.6024 psifd  GEN     38
 33    -1.1856     0.9022    79.5796     0.2371 psifd  GEN     36
 34    -0.8050     0.8131    70.3533     0.1821 exc2   EXC     36
 35    -0.6927     0.8091    65.0339     0.1695 psifd  GEN     30
 36    -0.8494     0.7785    73.7190     0.1834 exc2   EXC     32
 37    -0.4568     0.6738    56.1126     0.1296 exc2   EXC     37
 38    -0.5902     0.6690    66.1533     0.1420 exc2   EXC     31
 39    -0.4923     0.6417    60.8684     0.1287 exc2   EXC     35
 40    -1.5105     0.6205    92.5003     0.2599 exc2   EXC     38
 41    -0.4874     0.6076    62.5781     0.1240 psifd  GEN     34
 42    -1.0581     0.2471    97.3791     0.1729 exc2   EXC     39
```

Figure 7: Scenario 1 eigenvalues with FDLs at buses 20, 23, and 29, with a gain value of K = -10

It can be observed that the eigenvalue associated with the generator rotor speed of bus 39 now has a positive real part (0.0143) and consequently a negative damping ratio (-0.3608), destabilizing the system.

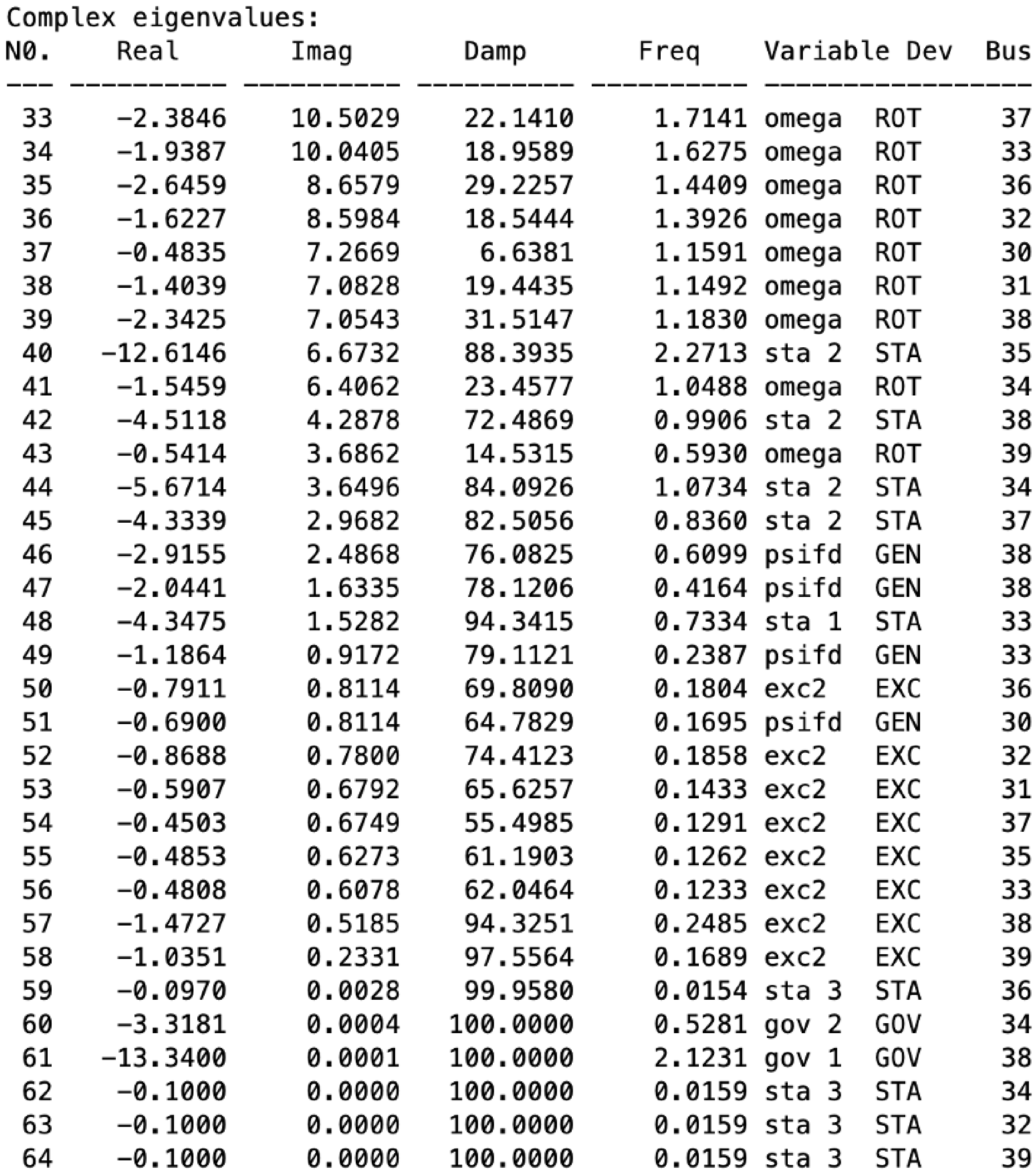
This result indicates that the demand should be changed by a factor of 10 times the frequency in pu in each of the three demand nodes to destabilize the system. For example, if there is a 1% deviation in frequency, demand must be modulated by 10% to destabilize the system.

Secondly, coordinated eigenvalue sensitivity design of FDL destabilizing controller was implemented in the previous three demand nodes, resulting in a value of $k = -6$ for each of the nodes to destabilize the selected eigenvalue and consequently the system, accompanied by a phase compensation of 91°.

This result indicates that if a phase compensation of 91º is added to the controller, the demand should be changed by a factor of 6 times the frequency in pu in each of the three demand nodes to destabilize the system. For example, if there is a 1% deviation in frequency, demand must be modulated by 6% to destabilize the system.

5.2 Scenario 2 results analysis

First, system eigenvalues illustrated in the Figure 8 were calculated.



```
Complex eigenvalues:
NO.     Real       Imag       Damp       Freq     Variable Dev  Bus
--- ---------- ---------- ---------- ---------- ----------------
 33    -2.3846    10.5029    22.1410     1.7141 omega  ROT      37
 34    -1.9387    10.0405    18.9589     1.6275 omega  ROT      33
 35    -2.6459     8.6579    29.2257     1.4409 omega  ROT      36
 36    -1.6227     8.5984    18.5444     1.3926 omega  ROT      32
 37    -0.4835     7.2669     6.6381     1.1591 omega  ROT      30
 38    -1.4039     7.0828    19.4435     1.1492 omega  ROT      31
 39    -2.3425     7.0543    31.5147     1.1830 omega  ROT      38
 40   -12.6146     6.6732    88.3935     2.2713 sta 2  STA      35
 41    -1.5459     6.4062    23.4577     1.0488 omega  ROT      34
 42    -4.5118     4.2878    72.4869     0.9906 sta 2  STA      38
 43    -0.5414     3.6862    14.5315     0.5930 omega  ROT      39
 44    -5.6714     3.6496    84.0926     1.0734 sta 2  STA      34
 45    -4.3339     2.9682    82.5056     0.8360 sta 2  STA      37
 46    -2.9155     2.4868    76.0825     0.6099 psifd  GEN      38
 47    -2.0441     1.6335    78.1206     0.4164 psifd  GEN      38
 48    -4.3475     1.5282    94.3415     0.7334 sta 1  STA      33
 49    -1.1864     0.9172    79.1121     0.2387 psifd  GEN      33
 50    -0.7911     0.8114    69.8090     0.1804 exc2   EXC      36
 51    -0.6900     0.8114    64.7829     0.1695 psifd  GEN      30
 52    -0.8688     0.7800    74.4123     0.1858 exc2   EXC      32
 53    -0.5907     0.6792    65.6257     0.1433 exc2   EXC      31
 54    -0.4503     0.6749    55.4985     0.1291 exc2   EXC      37
 55    -0.4853     0.6273    61.1903     0.1262 exc2   EXC      35
 56    -0.4808     0.6078    62.0464     0.1233 exc2   EXC      33
 57    -1.4727     0.5185    94.3251     0.2485 exc2   EXC      38
 58    -1.0351     0.2331    97.5564     0.1689 exc2   EXC      39
 59    -0.0970     0.0028    99.9580     0.0154 sta 3  STA      36
 60    -3.3181     0.0004   100.0000     0.5281 gov 2  GOV      34
 61   -13.3400     0.0001   100.0000     2.1231 gov 1  GOV      38
 62    -0.1000     0.0000   100.0000     0.0159 sta 3  STA      34
 63    -0.1000     0.0000   100.0000     0.0159 sta 3  STA      32
 64    -0.1000     0.0000   100.0000     0.0159 sta 3  STA      39
```

Figure 8: Scenario 2 eigenvalues

It can be observed that the weakest eigenvalue is now associated with the generator rotor speed of bus 30, as it has the real part closest to positive values (-0.4835) and the lowest damping ratio (6.6381).

Sensitivity analysis was then performed on the previously identified eigenvalue. The residues associated with the weakest eigenvalue for each node of the system, with a frequency input and power output transfer function, are shown in the following Figure 9.

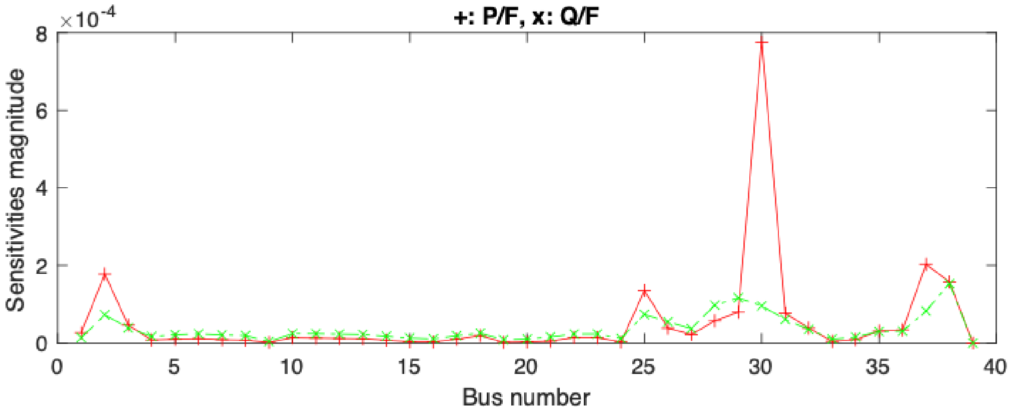
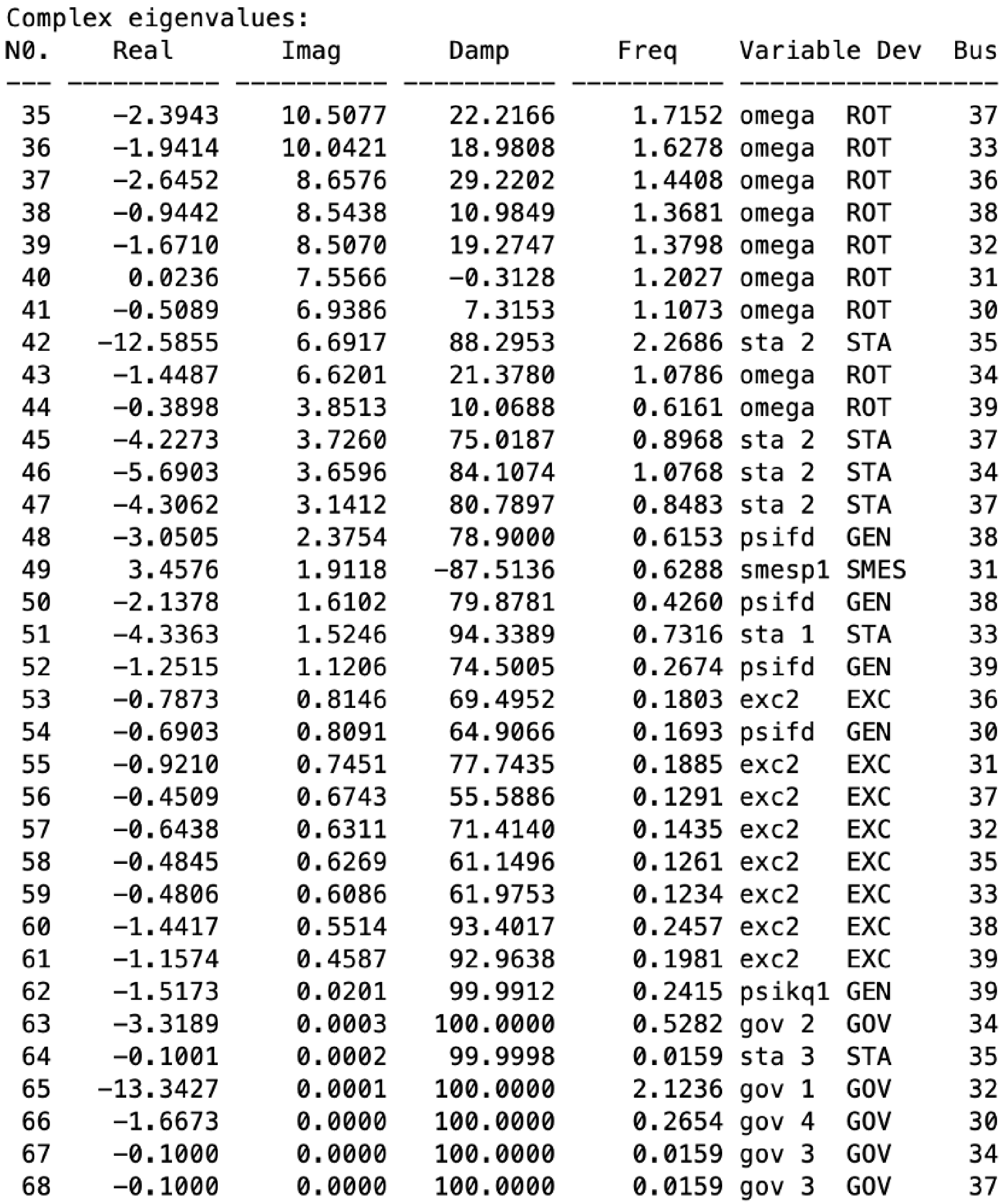


Figure 9: Scenario 2 weakest eigenvalue residues

The demand nodes where the attack would have the greatest effect were selected, being buses 28, 29 and 31 due to their higher resiudes.

First, manual iterative design of destabilizing FDL controller was implemented in these three nodes. After iterating the control gain value K for each of the selected FDLs, from a value of K = *-80*, the system became unstable. The recalculated eigenvalues for this gain value of the system are shown below in Figure 10.



```
Complex eigenvalues:
N0.     Real       Imag       Damp       Freq    Variable Dev   Bus
--- ---------- ---------- ---------- ---------- ----------------
 35    -2.3943    10.5077    22.2166     1.7152 omega  ROT      37
 36    -1.9414    10.0421    18.9808     1.6278 omega  ROT      33
 37    -2.6452     8.6576    29.2202     1.4408 omega  ROT      36
 38    -0.9442     8.5438    10.9849     1.3681 omega  ROT      38
 39    -1.6710     8.5070    19.2747     1.3798 omega  ROT      32
 40     0.0236     7.5566    -0.3128     1.2027 omega  ROT      31
 41    -0.5089     6.9386     7.3153     1.1073 omega  ROT      30
 42   -12.5855     6.6917    88.2953     2.2686 sta 2  STA      35
 43    -1.4487     6.6201    21.3780     1.0786 omega  ROT      34
 44    -0.3898     3.8513    10.0688     0.6161 omega  ROT      39
 45    -4.2273     3.7260    75.0187     0.8968 sta 2  STA      37
 46    -5.6903     3.6596    84.1074     1.0768 sta 2  STA      34
 47    -4.3062     3.1412    80.7897     0.8483 sta 2  STA      37
 48    -3.0505     2.3754    78.9000     0.6153 psifd  GEN      38
 49     3.4576     1.9118   -87.5136     0.6288 smesp1 SMES     31
 50    -2.1378     1.6102    79.8781     0.4260 psifd  GEN      38
 51    -4.3363     1.5246    94.3389     0.7316 sta 1  STA      33
 52    -1.2515     1.1206    74.5005     0.2674 psifd  GEN      39
 53    -0.7873     0.8146    69.4952     0.1803 exc2   EXC      36
 54    -0.6903     0.8091    64.9066     0.1693 psifd  GEN      30
 55    -0.9210     0.7451    77.7435     0.1885 exc2   EXC      31
 56    -0.4509     0.6743    55.5886     0.1291 exc2   EXC      37
 57    -0.6438     0.6311    71.4140     0.1435 exc2   EXC      32
 58    -0.4845     0.6269    61.1496     0.1261 exc2   EXC      35
 59    -0.4806     0.6086    61.9753     0.1234 exc2   EXC      33
 60    -1.4417     0.5514    93.4017     0.2457 exc2   EXC      38
 61    -1.1574     0.4587    92.9638     0.1981 exc2   EXC      39
 62    -1.5173     0.0201    99.9912     0.2415 psikq1 GEN      39
 63    -3.3189     0.0003   100.0000     0.5282 gov 2  GOV      34
 64    -0.1001     0.0002    99.9998     0.0159 sta 3  STA      35
 65   -13.3427     0.0001   100.0000     2.1236 gov 1  GOV      32
 66    -1.6673     0.0000   100.0000     0.2654 gov 4  GOV      30
 67    -0.1000     0.0000   100.0000     0.0159 gov 3  GOV      34
 68    -0.1000     0.0000   100.0000     0.0159 gov 3  GOV      37
```

Figure 10: Scenario 2 eigenvalues with FDLs at buses 28, 29, and 31, with a gain value of K = -80

It can be observed that the eigenvalue that destabilizes the system had changed. The eigenvalue associated with the generator rotor speed of bus 31 now has a positive real part (0.0236) and consequently a negative damping ratio (-0.3128), destabilizing the system.

This result indicates that the demand should be changed by a factor of 80 times the frequency in pu in each of the three demand nodes to destabilize the system. For example, if there is a 1% deviation in frequency, demand must be modulated by 80% to destabilize the system.

It can be seen that the PSS makes it much more difficult to destabilize the system compared to scenario 1. The difficulty is due to the fact that a larger amount of demand has to be modified, which indicates that MaDIoT must infiltrate much more demand.

Secondly, coordinated eigenvalue sensitivity design of FDL destabilizing controller was implemented in the previous three demand nodes, resulting in a value of $k = -10000$ for each of the nodes to destabilize the selected eigenvalue and consequently the system, accompanied by a phase compensation of 105°.

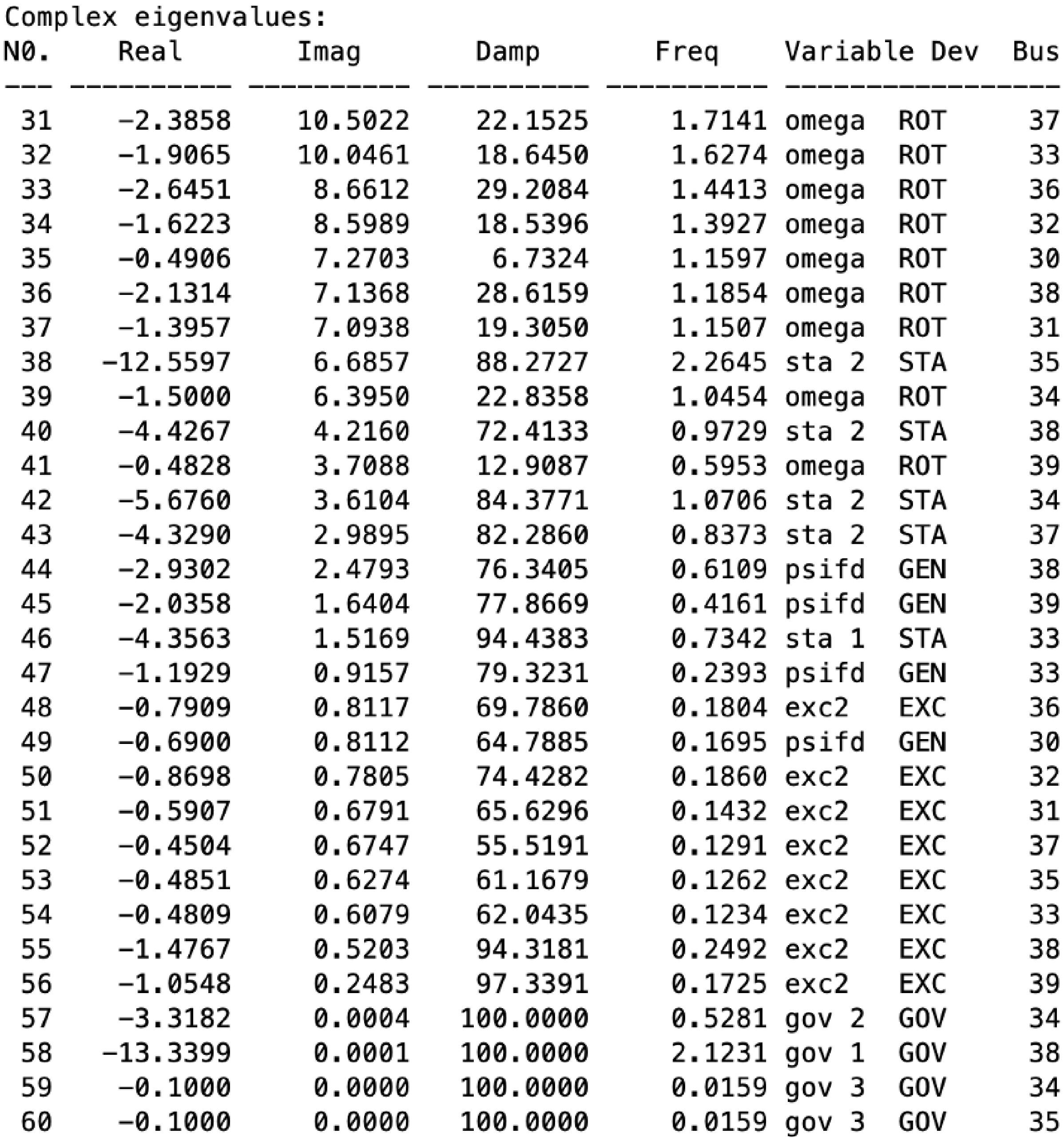
This high result for the control gain k is due to the fact that the coordinated eigenvalue sensitivity design focuses on destabilizing the selected eigenvalue without considering the values of the other eigenvalues in the system. In this case, the eigenvalue that begins to destabilize the system is not the weakest eigenvalue, but the eigenvalue associated to generator rotor speed of bus 31 being this eigenvalue the most sensitive to an attack on the selected nodes. The weakest eigenvalue would start to destabilize at much higher values of k, by which the system would already be destabilized.

5.3 Sensitivity analysis

After conducting the analyses for both scenarios, sensitivity studies were developed, which involved extrapolating the results obtained in Scenario 1 to Scenario 2.

First, the nodes associated with the weakest eigenvalue in Scenario 1—the generator rotor speed of bus 39 eigenvalue—where the attack would have the greatest impact were selected. Nodes 20, 23, and 29 were targeted in Scenario 2 with a controller gain value of $k = 10$, which successfully destabilized the system in Scenario 1.

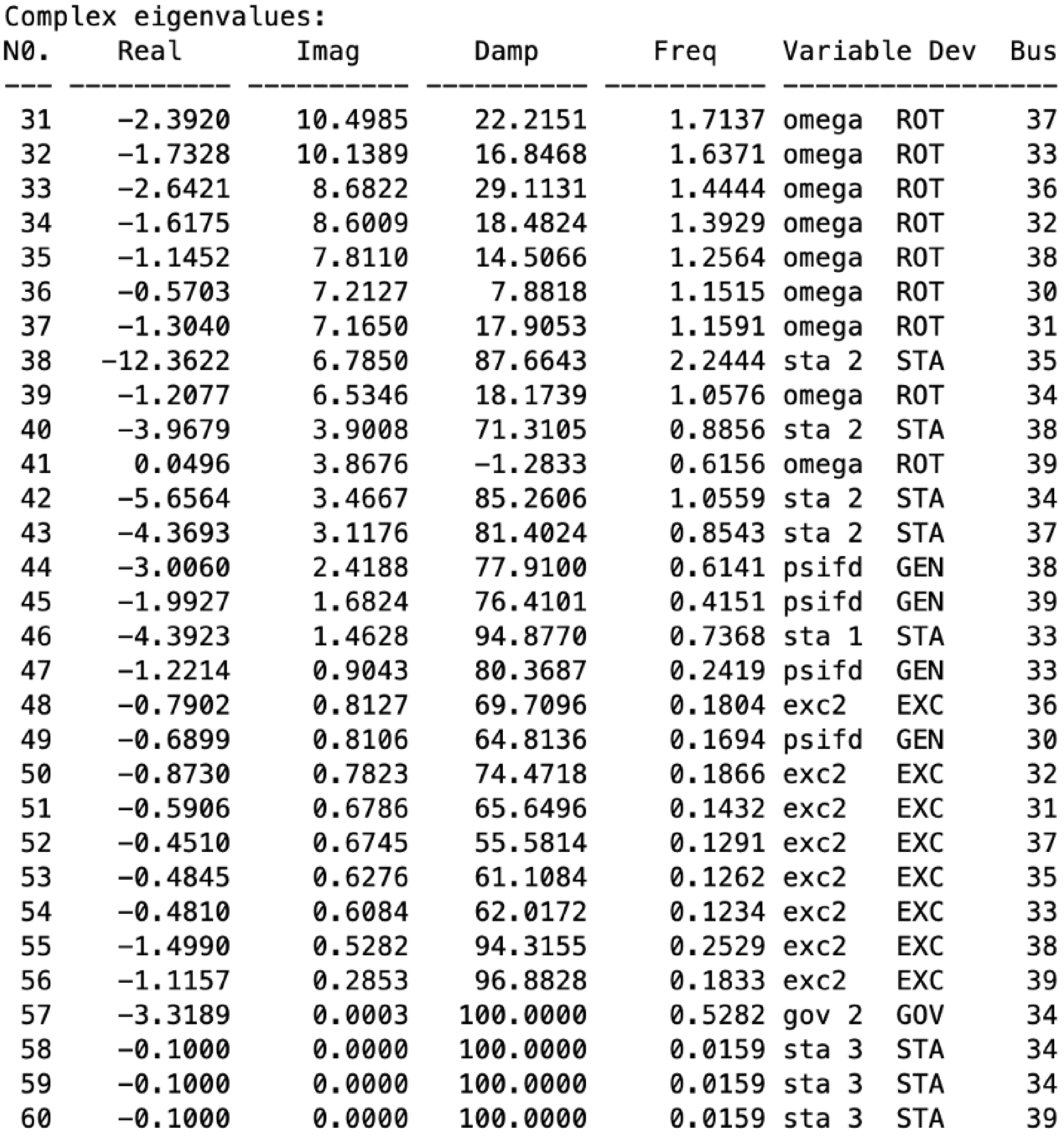
Secondly, the eigenvalues for Scenario 2 were calculated. As shown in the Figure 11, attacking the previously mentioned FDL demand nodes with a control gain value of $k = 10$ does not succeed in destabilizing the system having all eignvalues negative real part.



```
Complex eigenvalues:
N0.    Real       Imag       Damp       Freq     Variable Dev  Bus
--- ---------- ---------- ---------- ---------- ---------------
 31    -2.3858    10.5022    22.1525     1.7141 omega   ROT     37
 32    -1.9065    10.0461    18.6450     1.6274 omega   ROT     33
 33    -2.6451     8.6612    29.2084     1.4413 omega   ROT     36
 34    -1.6223     8.5989    18.5396     1.3927 omega   ROT     32
 35    -0.4906     7.2703     6.7324     1.1597 omega   ROT     30
 36    -2.1314     7.1368    28.6159     1.1854 omega   ROT     38
 37    -1.3957     7.0938    19.3050     1.1507 omega   ROT     31
 38   -12.5597     6.6857    88.2727     2.2645 sta 2   STA     35
 39    -1.5000     6.3950    22.8358     1.0454 omega   ROT     34
 40    -4.4267     4.2160    72.4133     0.9729 sta 2   STA     38
 41    -0.4828     3.7088    12.9087     0.5953 omega   ROT     39
 42    -5.6760     3.6104    84.3771     1.0706 sta 2   STA     34
 43    -4.3290     2.9895    82.2860     0.8373 sta 2   STA     37
 44    -2.9302     2.4793    76.3405     0.6109 psifd   GEN     38
 45    -2.0358     1.6404    77.8669     0.4161 psifd   GEN     39
 46    -4.3563     1.5169    94.4383     0.7342 sta 1   STA     33
 47    -1.1929     0.9157    79.3231     0.2393 psifd   GEN     33
 48    -0.7909     0.8117    69.7860     0.1804 exc2    EXC     36
 49    -0.6900     0.8112    64.7885     0.1695 psifd   GEN     30
 50    -0.8698     0.7805    74.4282     0.1860 exc2    EXC     32
 51    -0.5907     0.6791    65.6296     0.1432 exc2    EXC     31
 52    -0.4504     0.6747    55.5191     0.1291 exc2    EXC     37
 53    -0.4851     0.6274    61.1679     0.1262 exc2    EXC     35
 54    -0.4809     0.6079    62.0435     0.1234 exc2    EXC     33
 55    -1.4767     0.5203    94.3181     0.2492 exc2    EXC     38
 56    -1.0548     0.2483    97.3391     0.1725 exc2    EXC     39
 57    -3.3182     0.0004   100.0000     0.5281 gov 2   GOV     34
 58   -13.3399     0.0001   100.0000     2.1231 gov 1   GOV     38
 59    -0.1000     0.0000   100.0000     0.0159 gov 3   GOV     34
 60    -0.1000     0.0000   100.0000     0.0159 gov 3   GOV     35
```

Figure 11: Scenario 2 eigenvalues with FDLs at buses 20, 23, and 29, with a gain value of K = -10

Thirdly, the gain value K of the FDL controller for demand nodes 20, 23, and 29, at which the Scenario 2 system begins to destabilize, was determined. Manual iterative design of the destabilizing FDL controller was implemented, resulting in a gain value of $k = 70$, from which the system in Scenario 2 becomes unstable, as shown in Figure 12, with the generator rotor speed of node 39 eigenvalue having a positive real part.



```
Complex eigenvalues:
N0.    Real       Imag       Damp       Freq    Variable Dev  Bus
--- ---------- ---------- ---------- ---------- -----------------
 31    -2.3920    10.4985    22.2151     1.7137 omega   ROT     37
 32    -1.7328    10.1389    16.8468     1.6371 omega   ROT     33
 33    -2.6421     8.6822    29.1131     1.4444 omega   ROT     36
 34    -1.6175     8.6009    18.4824     1.3929 omega   ROT     32
 35    -1.1452     7.8110    14.5066     1.2564 omega   ROT     38
 36    -0.5703     7.2127     7.8818     1.1515 omega   ROT     30
 37    -1.3040     7.1650    17.9053     1.1591 omega   ROT     31
 38   -12.3622     6.7850    87.6643     2.2444 sta 2   STA     35
 39    -1.2077     6.5346    18.1739     1.0576 omega   ROT     34
 40    -3.9679     3.9008    71.3105     0.8856 sta 2   STA     38
 41     0.0496     3.8676    -1.2833     0.6156 omega   ROT     39
 42    -5.6564     3.4667    85.2606     1.0559 sta 2   STA     34
 43    -4.3693     3.1176    81.4024     0.8543 sta 2   STA     37
 44    -3.0060     2.4188    77.9100     0.6141 psifd   GEN     38
 45    -1.9927     1.6824    76.4101     0.4151 psifd   GEN     39
 46    -4.3923     1.4628    94.8770     0.7368 sta 1   STA     33
 47    -1.2214     0.9043    80.3687     0.2419 psifd   GEN     33
 48    -0.7902     0.8127    69.7096     0.1804 exc2    EXC     36
 49    -0.6899     0.8106    64.8136     0.1694 psifd   GEN     30
 50    -0.8730     0.7823    74.4718     0.1866 exc2    EXC     32
 51    -0.5906     0.6786    65.6496     0.1432 exc2    EXC     31
 52    -0.4510     0.6745    55.5814     0.1291 exc2    EXC     37
 53    -0.4845     0.6276    61.1084     0.1262 exc2    EXC     35
 54    -0.4810     0.6084    62.0172     0.1234 exc2    EXC     33
 55    -1.4990     0.5282    94.3155     0.2529 exc2    EXC     38
 56    -1.1157     0.2853    96.8828     0.1833 exc2    EXC     39
 57    -3.3189     0.0003   100.0000     0.5282 gov 2   GOV     34
 58    -0.1000     0.0000   100.0000     0.0159 sta 3   STA     34
 59    -0.1000     0.0000   100.0000     0.0159 sta 3   STA     34
 60    -0.1000     0.0000   100.0000     0.0159 sta 3   STA     39
```

Figure 12: Scenario 2 eigenvalues with FDLs at buses 20, 23, and 29, with a gain value of K = -70

These results indicate that the eigenvalue selected to determine which nodes would be most effective for a cyberattack may not necessarily be directly related to the weakest eigenvalue.

In this case, targeting nodes 20, 23, and 29—identified from the sensitivity analysis of the generator rotor speed eigenvalue of node 39—proved to be more effective than attacking nodes 28, 29, and 31, which were identified from the sensitivity analysis of the weakest eigenvalue in Scenario 2, associated with the generator rotor speed of bus 30, requiring FDL controller gain values of 70 and 80 to destabilize the system, respectively.

This ultimately reaffirms the conclusion that the weakest eigenvalue is not necessarily the easiest to destabilize, complicating the task of identifying which nodes in the system are the most effective targets for a cyberattack.

6 Alignment with Sustainable Development Goals (SDGs)

The development and implementation of smart power grids are intrinsically linked to SDG 9 and SDG 11, which emphasize building resilient infrastructure, sustainable cities, promoting inclusive and sustainable industrialization, and fostering innovation.

Smart grids integrate power systems with information and communication technologies (ICT), enhancing reliability and flexibility but also opening the door to cyberattacks.

6.1 SDG 9: Industry, Innovation, and Infrastructure

Power grid infrastructure is a vital component for economic development and job creation. Cyberattacks can severely damage power grid infrastructure, disrupting industries and hindering the ability to innovate. Resilient infrastructure against cyberattacks is critical to maintaining the integrity of these systems and promoting sustainable economic growth.

This project contributes to SDG 9 by providing tools to analyze and understand cyber threats to power grid systems through both a fundamental model and a more precise Matlab implementation. These tools enhance the ability to detect vulnerabilities and improve the resilience of power grid infrastructure.

By advancing cybersecurity in the power grid, the project stimulates innovation in cybersecurity technologies and more efficient energy management systems. This innovation not only protects critical infrastructure but also contributes to the development of advanced technological solutions that can be applied in other industries and sectors, thus fostering resilience and innovation.

6.2 SDG 11: Sustainable Cities and Communities

Urban areas rely heavily on electric power to ensure a high quality of life. Protecting the power grid from cyberattacks is essential for creating safer and more sustainable cities by preventing power supply disruptions that could affect daily life and the operation of essential services.

This project supports SDG 11 by enhancing the capability to study and mitigate the impacts of cyberattacks on smart grids, thereby improving the resilience of urban power infrastructures. The availability of reliable power is critical to the development of both urban and rural communities.

By providing tools for comprehensive analysis and protection against frequency dependent loads dynamic load altering attacks, this research aims to ensure uninterrupted power supply, which promotes the continuous operation of essential services in cities.

Furthermore, studying cyberattacks is essential for the smooth integration of renewable energy sources within smart grids, contributing to sustainable energy management and reducing the environmental impact of urban energy consumption. This holistic approach not only makes cities more resilient but also fosters a cleaner and more sustainable urban environment.

7 Conclusions

It's crucial to understand the significant impact that cyber threats can have on the evolving landscape of smart power grids. The integration of electrical power systems with IoT and smart grids enhances reliability and flexibility, but also opens the door to cyberattacks.

This master's thesis aimed to analyze small signal stability in the IEEE 39-bus system using a Matlab toolbox for small signal stability analysis.

To achieve this, the thesis focused on several specific goals. Firstly, the development of a fundamental model to assess small signal stability of FDL D-LAA. Secondly, the implemetation FDL D-LAA into an advanced Matlab toolbox, enhancing its capability for more accurate and complex calculations compared to the fundamental model. Lastly, the impact evaluation of existing stabilization measures, such as Power System Stabilizers, on the effectiveness of FDL D-LAA.

To meet these objectives, the analysis of small signal disturbances were conducted using the specialized Matlab toolbox after extending its functionality to both analyze and design FDL D-LAA effectively.

Based on the results obtained, it was clearly observed that:

- The presence of stabilizers in the generators significantly hinders the destabilization of the system, requiring the attacker to manipulate large amounts of demand to induce system instabilities, which is often not feasible
- The weakest eigenvalue is not necessarily the easiest to destabilize, which makes it difficult to determine which nodes in the system are the most effective for a cyberattack

Additionally, several constraints were identified that must be met to enable a successful cyberattack:

- The attacker must have prior knowledge of which system loads are most vulnerable to causing system instability

- The attacker must have a foundational understanding of controllers design
- The targeted loads must have sufficient power generation capacity to be increased or decreased

For future work, the small signal stability results presented in this work must be confirmed by non-linear time-domain simulations taking into account the limited amount of load available. This helps understanding to what extent FDL D-LAA could be an actual threat. Further, other type of input signals instead of frequency should be analyzed, to further undestand the impact of the input signal. In general terms and independently of the cyberattack framework, the selection of appropriate eigenvalues a control should act upon without affecting others should be addressed.

References

[1] Sajjad Amini, Fabio Pasqualetti, and Hamed Mohsenian-Rad. "Dynamic Load Altering Attacks Against Power System Stability: Attack Models and Protection Schemes". In: *IEEE Transactions on Smart Grid* 9.4 (2018), pp. 2862–2872. DOI: 10.1109/TSG.2016.2622686.

[2] Sergey V Buldyrev et al. "Catastrophic cascade of failures in interdependent networks". In: *Nature* 464.7291 (2010), pp. 1025–1028. DOI: 10.1038/nature08932.

[3] Bing Huang, Alvaro A. Cardenas, and Ross Baldick. "Not Everything is Dark and Gloomy: Power Grid Protections Against IoT Demand Attacks". In: *28th USENIX Security Symposium (USENIX Security 19)*. Santa Clara, CA: USENIX Association, Aug. 2019, pp. 1115–1132. ISBN: 978-1-939133-06-9. URL: https://www.usenix.org/conference/usenixsecurity19/presentation/huang.

[4] Jian Li et al. "Dynamic load altering attack detection based on adaptive fading Kalman filter in smart grid". In: *IET Generation, Transmission Distribution* 18 (Jan. 2024), n/a–n/a. DOI: 10.1049/gtd2.13057.

[5] Xu Li et al. "Securing smart grid: Cyber attacks, countermeasures, and challenges". In: *Communications Magazine, IEEE* 50 (Aug. 2012), pp. 38–45. DOI: 10.1109/MCOM.2012.6257525.

[6] Angelos K. Marnerides et al. "Power Consumption Profiling Using Energy Time-Frequency Distributions in Smart Grids". In: *IEEE Communications Letters* 19.1 (2015), pp. 46–49. DOI: 10.1109/LCOMM.2014.2371035.

[7] Aradhna Patel and Shubhi Purwar. "Destabilizing smart grid by dynamic load altering attack using PI controller". In: *2017 International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)*. 2017, pp. 354–359. DOI: 10.1109/ICICICT1.2017.8342589.

[8] Amir Rad and A. Leon-Garcia. "Distributed Internet-Based Load Altering Attacks Against Smart Power Grids". In: *IEEE Trans. Smart Grid* 2 (Dec. 2011), pp. 667–674. DOI: 10.1109/TSG.2011.2160297.

[9] Amir Rad and A. Leon-Garcia. “Distributed Internet-Based Load Altering Attacks Against Smart Power Grids”. In: *IEEE Trans. Smart Grid* 2 (Dec. 2011), pp. 667–674. DOI: 10.1109/TSG.2011.2160297.

[10] Tohid Shekari, Alvaro A. Cardenas, and Raheem Beyah. “MaDIoT 2.0: Modern High-Wattage IoT Botnet Attacks and Defenses”. In: *31st USENIX Security Symposium (USENIX Security 22)*. Boston, MA: USENIX Association, Aug. 2022, pp. 3539–3556. ISBN: 978-1-939133-31-1. URL: https://www.usenix.org/conference/usenixsecurity22/presentation/shekari.

[11] Saleh Soltan, Prateek Mittal, and H. Vincent Poor. “BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid”. In: *27th USENIX Security Symposium (USENIX Security 18)*. Baltimore, MD: USENIX Association, Aug. 2018, pp. 15–32. ISBN: 978-1-939133-04-5. URL: https://www.usenix.org/conference/usenixsecurity18/presentation/soltan.

[12] J.C.M. Vieira et al. “Performance of frequency relays for distributed generation protection”. In: *IEEE Transactions on Power Delivery* 21.3 (2006), pp. 1120–1127. DOI: 10.1109/TPWRD.2005.858751.

A State-space representation for n classical model generators

A.1 DC power flow (DC-PF)

The DC-PF assumes that (i) voltage magnitudes are around nominal (1 pu), (ii) branch resistances can be neglected (which is commonly an acceptable assumption in transmission networks), (iii) the angle difference between two adjacent buses is typically small. Equation (A.1a) shows the active power flow of a branch between buses j and k. The active power balance at bus j is shown in (A.1b) according to Kirchhoff's law.

$$p_{jk} = \frac{\theta_j - \theta_k}{x_{jk}} \tag{A.1a}$$

$$p_j = \sum_{k \in \mathcal{B}_j} p_{jk} = p_j^G - p_j^L \tag{A.1b}$$

where p_j and θ_j are the power injection and the voltage angle at bus j and p_{jk} and x_{jk} are the branch flow and the branch reactance of branch from bus j to bus k. The nodal power injection is the difference between the nodal generation, p_j^G, and load, p_j^L. Equation (A.1b) can be generalized for all branches and buses in the system as follows:

$$P^l = X^{-1} \cdot A \cdot \theta^b \tag{A.2a}$$

$$P^b = A^T \cdot P^l = P^G - P^L \tag{A.2b}$$

where $X = diag([..., x_{jk}, ...])$ is a diagonal matrix with the branch reactances on its diagonal, and A is the incidence matrix relating branches and buses in the same order as in X. P^l and P^b are vectors of branch flow and bus injections, and P^G and P^L are vectors of nodal generation and load. From (A.2) one can obtain:

$$P^G - P^L = A^T \cdot X^{-1} \cdot A \cdot \theta^b = B' \cdot \theta^b \tag{A.3}$$

Note that B' is singular (not invertible) given the linear dependency of the A. One way to deal with the singularity is to define a reference bus, where the voltage angle is arbitrarily fixed (e.g., 0 rad/s). The corresponding row and column of this bus are then eliminated for matrix inversion. Further, eq. (A.2b) can be expanded to explicitly represent generator (g) and non-generator buses (ng) in the following way:

$$\begin{bmatrix} P^{Gg} - P^{Lg} \\ -P^{Lng} \end{bmatrix} = B' \cdot \theta^b \tag{A.4}$$

Note that the first buses are generator buses, followed by non-generator buses. Nodal generation at non-generator buses is 0.

A.2 Augmented DC-PF by explicitly representing generators

Matrix B' can be augmented to include the transient reactances of generators. Generators are modelled by a simplified electrical circuit representing an internal voltage, e_g, behind a transient reactance, $x_g k'$, of the generator at bus k as follows:

$$e_g = u_k + j \cdot x'_{gk} \cdot i_{gk} \tag{A.5}$$

In this case, the active power injected by the generator g at bus k can approximated as shown in (A.6) by making use of similar hypotheses as for the DC-PF:

$$p_{gk} = \frac{\delta_g - \theta_k}{x'_{gk}} \tag{A.6}$$

The expression in eq. (A.6) very much resembles the one in eq. (A.1a) and the active power injection can be handled as an active power inflow from the internal voltage of generator g to the bus k. Equation (A.6) can be generalized as follows:

$$P^{lG} = (X')^{-1} \cdot \begin{bmatrix} A^g & A^{ng} \end{bmatrix} \cdot \begin{bmatrix} \delta \\ \theta^b \end{bmatrix} \tag{A.7a}$$

$$P^{Gg} = \begin{bmatrix} (A^g)^T \\ (A^{ng})^T \end{bmatrix} \cdot (X')^{-1} \cdot \begin{bmatrix} A^g & A^{ng} \end{bmatrix} \cdot \begin{bmatrix} \delta \\ \theta^b \end{bmatrix} \tag{A.7b}$$

where $X' = diag([..., x'_{gk}, ...])$ is a diagonal matrix with the transient reactances on its diagonal and $[A^g \; A^{gb}]$ is the incidence matrix of the active power inflows. P^{lG} and P^{Gg} are the vector of active power inflow and the vector of nodal generation, respectively. Note that A^g is a diagonal matrix if the explicit generator representation follows the same order as in eq. (A.4). In that case, the first columns corresponding to the generators in A^{ng} also form a diagonal matrix.

The explicit generator representation can then be included by augmenting B' appropriately. By using eq. (A.4) and eq. (A.7) the augmented DC-PF becomes:

$$\begin{bmatrix} P^{Gg} \\ -P^L \end{bmatrix} = \begin{bmatrix} (A^g)^T \cdot (X')^{-1} \cdot A^g & (A^g)^T \cdot (X')^{-1} \cdot A^{ng} \\ (A^{ng})^T \cdot (X')^{-1} \cdot A^g & B' + (A^{ng})^T \cdot (X')^{-1} \cdot A^{ng} \end{bmatrix} \cdot \begin{bmatrix} \delta \\ \theta^b \end{bmatrix} \tag{A.8}$$

or

$$\begin{bmatrix} P^{Gg} \\ -P^L \end{bmatrix} = \begin{bmatrix} B^{agg} & B^{agb} \\ B^{abg} & B^{abb} \end{bmatrix} \cdot \begin{bmatrix} \delta \\ \theta^b \end{bmatrix} = B^a \cdot \begin{bmatrix} \delta \\ \theta^b \end{bmatrix} \tag{A.9}$$

Further, the matrix B^a in eq. (A.9) is still singular. Again, this can be handled by defining a reference generator (e.g., the first one) and eliminating the corresponding row and column. Note that B^{abb} is non-singular.

A.3 Fundamental dynamic model

The fundamental dynamic model of the power system couples the dynamics of the generators by means of the network. The network is represented by the augmented DC-PF. The dynamics of the generator g at bus k are modelled by means of the classical generator model.

$$\dot{\delta}_g = \Omega_{base} \cdot (\omega_g - \omega_0) \tag{A.10a}$$

$$2 \cdot H_g \cdot \omega_0 \cdot \dot{\omega}_g = p_g^m - p_g^e - D_g \cdot (\omega_g - \omega_0) \tag{A.10b}$$

where H_g and D_g are the inertia constant and the equivalent damping factor (representing damper windings, PSS, etc.) of the generator. Ω_{base} and ω_0 are the base angular speed in rad/s and the nominal angular speed per unit (i.e., 1 pu). p_g^m and p_g^e are the mechanical and electrical power of the generator g at bus k. Note that $p_g^e = p_{gk}$ (see also eq. (A.6)). Equation (A.10) can be expressed in matrix form as follows:

$$\dot{\delta} = \Omega_{base} \cdot (\omega - \omega_0 \cdot I) \tag{A.11a}$$

$$2 \cdot H \cdot \omega_0 \cdot \dot{\omega} = P^m - P^{Gg} - D \cdot (\omega - \omega_0 \cdot I) \tag{A.11b}$$

where H and D are diagonal matrices with the inertia constants and equivalent damping factors on their diagonals. I is the identity matrix. If the perturbations are sufficiently small, eq. (A.11) can be linearized.

$$\Delta\dot{\delta} = \Omega_{base} \cdot \Delta\omega \tag{A.12a}$$

$$2 \cdot H \cdot \omega_0 \cdot \Delta\dot{\omega} = \Delta P^m - \Delta P^{Gg} - D \cdot \Delta\omega \tag{A.12b}$$

Similarly and if the load does not vary (e.g., constant power loads), eq. (A.9) becomes for small variations:

$$\begin{bmatrix} \Delta P^{Gg} \\ 0 \end{bmatrix} = \begin{bmatrix} B^{agg} & B^{agb} \\ B^{abg} & B^{abb} \end{bmatrix} \cdot \begin{bmatrix} \Delta\delta \\ \Delta\theta^b \end{bmatrix} \tag{A.13}$$

From eq. (A.13) it becomes clear that first, under no (or neglectable) load variations, there exists a direct relation between the bus voltage angles, $\Delta\theta$, and the angles of the internal voltages, $\Delta\delta$. Second, generation variations and variations of the angles of the internal voltages are related, too. Finally, bus frequencies (derivative of bus voltage angles) depend on generator speeds (derivative of internal voltage angles)[3].

$$\Delta\theta^b = -(B^{abb})^{-1} \cdot B^{abg} \cdot \Delta\delta \tag{A.14a}$$

$$\Delta P^{Gg} = (B^{agg} - B^{agb} \cdot (B^{abb})^{-1} \cdot B^{abg}) \cdot \Delta\delta = K^s \cdot \Delta\delta \tag{A.14b}$$

$$\Delta\omega^b = -(B^{abb})^{-1} \cdot B^{abg} \cdot \Delta\omega \tag{A.14c}$$

If eq. (A.14b) is substituted in eq. (A.12), then

[3] This relationship has been denoted *frequency divider* in the literature since it highlights that bus frequencies are mainly a result of generator speeds. Indeed, in power systems with synchronous generation, the terminal voltage frequency is due to the rotating field. The frequency divider highlights that bus frequencies are weighted generator speeds, where the weights depend on the electrical distances.

$$\begin{bmatrix} \Delta\dot{\delta} \\ \Delta\dot{\omega} \end{bmatrix} = \underbrace{\begin{bmatrix} 0 & \Omega_{base} \\ -\frac{1}{2\cdot\omega_0} \cdot H^{-1} \cdot K^s & -\frac{1}{2\cdot\omega_0} \cdot H^{-1} \cdot D \end{bmatrix}}_{=A^{sys}} \cdot \begin{bmatrix} \Delta\delta \\ \Delta\omega \end{bmatrix} + \begin{bmatrix} 0 \\ \frac{1}{2\cdot\omega_0} \cdot H^{-1} \end{bmatrix} \cdot \Delta P^m \tag{A.15}$$

which is the matrix form of a n-coupled oscillators. Small signal stability is determined by the eigenvalues of the system matrix, A^{sys}. If all eigenvalues have negative real part, the system is asymptotically stable. In other words, if Δp^m is disturbed, generator speeds start oscillating but these oscillations are damped out over time. The damping is mainly affected by the equivalent damping matrix, D, and the distribution of the inertia, whereas the oscillation frequency is affected by the synchronizing power matrix, K^s, and the distribution of the inertia.

B IEEE 39-bus system

The IEEE 39-bus system, commonly known as the New England Test System, has been widely employed in various studies with different objectives, most of which are related to small signal stability analysis and control. There are multiple versions of the New England Test System, including those with different system technologies, FACTS integration, among other modifications. For this study, we chose to adhere closely to the original data source.

Network elements data are shown on Tables (1), (3), (2) while generators dynamic parameters are provides in Tables (4), (5), (6).

From Bus	To Bus	R (p.u.)	X (p.u.)	B (p.u.)
1	2	0.0035	0.0411	0.6987
1	39	0.001	0.025	0.75
2	3	0.0013	0.0151	0.2572
2	25	0.007	0.0086	0.146
3	4	0.0013	0.0213	0.2214
3	18	0.0011	0.0133	0.2138
4	5	0.0008	0.0128	0.1342
4	14	0.0008	0.0129	0.1382
5	6	0.0002	0.0026	0.0434
5	8	0.0008	0.0112	0.1476
6	7	0.0006	0.0092	0.113
6	11	0.0007	0.0082	0.1389
7	8	0.0004	0.0046	0.078
8	9	0.0023	0.0363	0.3804
9	39	0.001	0.025	1.2
10	11	0.0004	0.0043	0.0729
10	13	0.0004	0.0043	0.0729
13	14	0.0009	0.0101	0.1723
14	15	0.0018	0.0217	0.366
15	16	0.0009	0.0094	0.171
16	17	0.0007	0.0089	0.1342
16	19	0.0016	0.0195	0.304
16	21	0.0008	0.0135	0.2548
16	24	0.0003	0.0059	0.068
17	18	0.0007	0.0082	0.1319
17	27	0.0013	0.0173	0.3216
21	22	0.0008	0.014	0.2565
22	23	0.0006	0.0096	0.1846
23	24	0.0022	0.035	0.361
25	26	0.0032	0.0323	0.513
26	27	0.0014	0.0147	0.2396
26	28	0.0043	0.0474	0.7802
26	29	0.0057	0.0625	1.029
28	29	0.0014	0.0151	0.249

Table 1: Transmission Line Data

From Bus	To Bus	R (p.u.)	X (p.u.)	Tap (p.u.)
6	31	0	0.025	1.007
10	32	0	0.02	1.007
19	33	0.0007	0.0142	1.007
20	34	0.0009	0.018	1.009
22	35	0	0.0143	1.025
23	36	0.0005	0.0272	1
25	37	0.0006	0.0232	1.025
2	30	0	0.0181	1.025
29	38	0.0008	0.0156	1.025

Table 2: Transformer Data

From Bus	To Bus	R (p.u.)	X (p.u.)	Tap (p.u.)
12	11	0.0016	0.0435	1.006
12	13	0.0016	0.0435	1.006
19	20	0.0007	0.0138	1.006

Table 3: Generator Step-Up Transformer Data

Unit No.	T_R	K_A	T_A	T_B	T_C	$V_{setpoint}$	$E_{fd,Max}$	$E_{fd,Min}$
1	0.01	200.0	0.015	10.0	1.0	10.300	5.0	-5.0
2	0.01	200.0	0.015	10.0	1.0	0.9820	5.0	-5.0
3	0.01	200.0	0.015	10.0	1.0	0.9831	5.0	-5.0
4	0.01	200.0	0.015	10.0	1.0	0.9972	5.0	-5.0
5	0.01	200.0	0.015	10.0	1.0	10.123	5.0	-5.0
6	0.01	200.0	0.015	10.0	1.0	10.493	5.0	-5.0
7	0.01	200.0	0.015	10.0	1.0	10.635	5.0	-5.0
8	0.01	200.0	0.015	10.0	1.0	10.278	5.0	-5.0
9	0.01	200.0	0.015	10.0	1.0	10.265	5.0	-5.0
10	0.01	200.0	0.015	10.0	1.0	10.475	5.0	-5.0

Table 4: AVR data for the New England Test System

Unit No.	H	R_a	x'_d	x'_q	x_d	x_q	T'_{do}	T'_{qo}	x_l
1	500	0	0.006	0.008	0.02	0.019	7.0	0.7	0.003
2	30.3	0	0.0697	0.17	0.295	0.282	6.56	1.5	0.035
3	35.8	0	0.0531	0.0876	0.2495	0.237	5.7	1.5	0.0304
4	28.6	0	0.0436	0.166	0.262	0.258	5.69	1.5	0.0295
5	26	0	0.132	0.166	0.67	0.62	5.4	0.44	0.054
6	34.8	0	0.05	0.0814	0.254	0.241	7.3	0.4	0.0224
7	26.4	0	0.049	0.186	0.295	0.292	5.66	1.5	0.0322
8	24.3	0	0.057	0.0911	0.29	0.28	6.7	0.41	0.028
9	34.5	0	0.057	0.0587	0.2106	0.205	4.79	1.96	0.0298
10	42	0	0.031	0.008	0.1	0.069	10.2	0.0	0.0125

Table 5: Generator Data for the New England Test System

Unit No.	**K**	$\mathbf{T_W}$	$\mathbf{T_1}$	$\mathbf{T_2}$	$\mathbf{T_3}$	$\mathbf{T_4}$	$\mathbf{V_{PSS,Max}}$	$\mathbf{V_{PSS,Min}}$
1	$1.0/(120\pi)$	10.0	5.0	0.60	3.0	0.50	0.2	-0.2
2	$0.5/(120\pi)$	10.0	5.0	0.40	1.0	0.10	0.2	-0.2
3	$0.5/(120\pi)$	10.0	3.0	0.20	2.0	0.20	0.2	-0.2
4	$2.0/(120\pi)$	10.0	1.0	0.10	1.0	0.30	0.2	-0.2
5	$1.0/(120\pi)$	10.0	1.5	0.20	1.0	0.10	0.2	-0.2
6	$4.0/(120\pi)$	10.0	0.5	0.10	0.5	0.05	0.2	-0.2
7	$7.5/(120\pi)$	10.0	0.2	0.02	0.5	0.10	0.2	-0.2
8	$2.0/(120\pi)$	10.0	1.0	0.20	1.0	0.10	0.2	-0.2
9	$2.0/(120\pi)$	10.0	1.0	0.50	2.0	0.10	0.2	-0.2
10	$1.0/(120\pi)$	10.0	1.0	0.05	3.0	0.50	0.2	-0.2

Table 6: PSS data for the New England Test System