ISTANBUL TECHNICAL UNIVERSITY ★ GRADUATE SCHOOL

UNKNOWN INPUT OBSERVER BASED CYBER ATTACK DETECTION IN LOAD FREQUENCY CONTROL SYSTEMS

M.Sc. THESIS

Arslan Mete BAYBARS

Department of Electrical Engineering

Electrical Engineering Programme

JUNE 2025

ISTANBUL TECHNICAL UNIVERSITY ★ GRADUATE SCHOOL

UNKNOWN INPUT OBSERVER BASED CYBER ATTACK DETECTION IN LOAD FREQUENCY CONTROL SYSTEMS

M.Sc. THESIS

Arslan Mete BAYBARS
(504221001)

Department of Electrical Engineering

Electrical Engineering Programme

Thesis Advisor: Prof. Dr. V. M. İstemihan GENÇ

JUNE 2025

ISTANBUL TEKNİK ÜNİVERSİTESİ ★ LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

YÜK FREKANS KONTROL SİSTEMLERİNDE BİLİNMEYEN GİRİŞ GÖZLEMCİSİ TEMELLİ SİBER SALDIRI TESPİTİ

YÜKSEK LİSANS TEZİ

Arslan Mete BAYBARS
(504221001)

Elektrik Mühendisliği Anabilim Dalı

Elektrik Mühendisliği Programı

Tez Danışmanı: Prof. Dr. V. M. İstemihan GENÇ

HAZİRAN 2025

Arslan Mete BAYBARS, a M.Sc student of İTU Graduate School student ID 504221001, successfully defended the thesis entitled "UNKOWN INPUT OBSERVER BASED CYBER ATTACK DETECTION IN LOAD FREQUENCY CONTROL SYSTEMS", which he prepared after fulfilling the requirements specified in the associated legislations, before the jury whose signatures are below.

Thesis Advisor :	**Prof. Dr. V. M. İstemihan GENÇ** İstanbul Technical University	.....
Jury Members :	**Prof. Dr. Emine AYAZ** Istanbul Technical University	.....
	Asst. Prof. Dr. Oben DAĞ Arel University	.....

Date of Submission : 30 May 2025
Date of Defense : 23 June 2025

To my mother,

FOREWORD

I would like to express my deepest gratitude to my advisor, Prof. Dr. V. M. İstemihan GENÇ, for his invaluable guidance, support, and expertise throughout the planning, execution, and completion of this thesis. His encouragement and insightful feedback were instrumental in shaping the direction of this work.

I also extend my sincere thanks to Prof. Dr. Fikret ÇALIŞKAN, whose theoretical insights and thoughtful suggestions significantly contributed to my understanding of the subject matter. His support during the development of the theoretical framework of this study has been greatly appreciated.

I am thankful to all my colleagues and friends at the university who supported me throughout this journey with their help and encouragement.

Finally, I owe my deepest gratitude to my beloved family, whose unwavering moral and financial support has been a constant source of strength in every step of my academic life.

June 2025

Arslan Mete BAYBARS
(Electrical Electronics Engineer)

TABLE OF CONTENTS

Page

ABBREVIATIONS

ACE	**:** Area Control Error
DOS	**:** Dedicated Observer Scheme
FDI	**:** Fault Detection and Isolation
FDIA	**:** False Data Injection Attack
GOS	**:** Generalized Observer Scheme
GUIO	**:** Global Unknown Input Observer
IoT	**:** Internet of Things
LFC	**:** Load Frequency Control
PI	**:** Proportional Integral
SCADA	**:** Supervisory Control and Data Acquisition
UIO	**:** Unknown Input Observer

SYMBOLS

A, B, C, E	**:** State space matrices
d, x, u, y	**:** State space vectors
F, H, K, T	**:** Observer matrices
r, z	**:** Observer vectors
D	**:** Damping coefficient
e	**:** Estimation error
f, f_0	**:** Frequency, Nominal system frequency
H	**:** Inertia constant
K_I	**:** Integral gain
P	**:** Active power
P_0	**:** Initial active power
P_c	**:** Control input power
P_d	**:** Load demand (disturbance)
P_e	**:** Electrical power
P_g	**:** Generated power
P_m	**:** Mechanical power
P_{tie}	**:** Tie-line power flow
R	**:** Speed regulation coefficient
t	**:** Time
T	**:** Torque
T_e	**:** Electromagnetic torque
T_{gv}	**:** Governor time constant
T_m	**:** Mechanical torque
T_t	**:** Turbine time constant
T_{12}	**:** Synchronizing coefficient between Area 1 and 2
β	**:** Frequency bias factor
ω	**:** Angular velocity
ω_r	**:** Angular velocity of rotor
δ	**:** Rotor angle
Δ	**:** Deviation from nominal value

LIST OF TABLES

Page

LIST OF FIGURES

Page

UNKNOWN INNPUT OBSERVER BASED CYBER ATTACK DETECTION IN LOAD FREQUENCY CONTROL SYSTEMS

SUMMARY

The global energy demand continues to rise with accelerating industrialization, urbanization, and improving living standards. In response, modern power systems have experienced a significant transformation with the widespread adoption of smart grid technologies, which enable real-time monitoring, bidirectional communication, and decentralized control. While these advancements including the integration of renewable energy sources, distributed generation units, and advanced control infrastructures enhance the flexibility and efficiency of the grid, they also increase its complexity and vulnerability. In particular, critical control mechanisms such as load frequency control have become more sensitive to cyber threats. Among these threats, false data injection attacks, which manipulate sensor measurements to mislead state estimations, pose a serious risk to system stability and reliability.

This thesis addresses the cyber-security challenges in modern power systems by employing observer-based strategies, specifically unknown input observers, to detect false data injection attacks in load frequency control systems. Two primary observer schemes are investigated: the dedicated observer scheme and the generalized observer scheme.

Unknown input observers effectively detect anomalies caused by malicious sensor manipulations while remaining robust against external disturbances. The study involves simulating these observer structures within a two-area load frequency control system using MATLAB/Simulink, applying various false data injection attack scenarios to evaluate their detection performance.

Simulation results demonstrate that the global unknown input observer structure effectively detects cyber threats, producing minimal residual signals during normal operation but significantly higher residuals during false data injection incidents. The generalized observer scheme approach further enhances detection capability by isolating the specific sensor affected by the attack. Observers using generalized observer scheme remain unaffected when their respective sensors are targeted, clearly highlighting the compromised sensor.

In contrast, the dedicated observer scheme failed to build applicable observer models for the given system due to fundamental limitations in observability. Since each observer in the dedicated observer scheme framework relies only on a single sensor’s measurement, the amount of information available for state estimation becomes significantly restricted. As a result, the observability conditions required for the successful design of unknown input observers could not be satisfied particularly for critical states such as frequency deviations. This inadequacy prevented the formulation of proper observer structures, rendering the dedicated observer scheme approach ineffective for this specific multi-area load frequency control application.

Overall, integrating global unknown input observer and generalized observer scheme structures provides an efficient and robust detection framework for identifying and localizing singular cyber attacks in power systems. Future research aims to extend this framework to detect simultaneous multiple sensor attacks, validate scalability of the method in larger systems and it will contribute to increasing continuity, stability and reliability in modern energy systems.

YÜK FREKANS KONTROL SİSTEMLERİNDE GÖZLEMCİ TABANLI SİBER SALDIRI TEPİTİ

ÖZET

Küresel enerji talebindeki artış, endüstriyel gelişim, şehirleşme, nüfus artışı ve yaşam standartlarındaki istikrarlı artış gibi birçok faktörün etkisiyle her yıl düzenli bir biçimde devam etmektedir. Özellikle gelişmekte olan ekonomilerin enerji tüketimindeki hızlı yükselişi, küresel enerji ihtiyacını önemli ölçüde artırmaktadır. Enerji talebindeki bu artış, enerji üretim ve dağıtım sistemlerinin kapasite, güvenilirlik, verimlilik ve esneklik açısından daha da geliştirilmesini zorunlu hale getirmiştir. Elektrikli araçların dünya genelinde hızla yaygınlaşması, endüstrilerin artan dijitalleşmesi ve otomasyon süreçleri, bilgi teknolojilerindeki hızlı ilerlemeler ve genişleyen elektrifikasyon süreçleri enerji sistemlerinin karmaşık ve hassas bir yapıya dönüşmesine neden olmuştur. Bu yeni ve karmaşık sistemler, klasik enerji altyapılarının güvenlik açıklarını daha belirgin hale getirerek, siber saldırılara karşı daha duyarlı hale gelmesine sebep olmaktadır.

Geleneksel merkezi güç sistemlerinin yerini yenilenebilir enerji kaynakları, dağıtık üretim birimleri, mikro şebekeler ve enerji depolama sistemlerinin entegre edildiği akıllı şebekeler almaya başlamıştır. Akıllı şebeke konsepti, enerji sistemlerinin performansını, güvenilirliğini ve esnekliğini artırmak üzere tasarlanmıştır; ancak çoklu sensör ve gelişmiş haberleşme kanallarının kullanılması, sistemlerin siber saldırılara maruz kalma olasılığını artırmaktadır. Siber saldırılar enerji sistemlerinin işleyişini ciddi şekilde etkileyebilir, enerji arzını kesintiye uğratabilir ve büyük ekonomik kayıplara neden olabilir. Bu nedenle enerji sistemlerinin güvenliğini sağlamak ve sürdürmek için yenilikçi, etkin ve dayanıklı tespit mekanizmalarının geliştirilmesi hayati önem taşımaktadır.

Bu çalışmada, enerji sistemlerinin temel kontrol mekanizmalarından biri olan yük frekans kontrolü sistemlerinin siber saldırılara karşı güvenliğini artırmak amacıyla, yanlış veri enjeksiyonu saldırılarının tespiti üzerine odaklanılmıştır. Bu amaçla, daha önce sistemlerde arıza tespit ve izolasyonunda yaygın olarak kullanılan bilinmeyen giriş gözlemcisi temelli yöntemler detaylı biçimde incelenmiştir. Bu kapsamda, bilinmeyen giriş gözlemcisi temeline dayanan iki farklı gözlemci şeması ele alınmıştır: ayrılmış gözlemci şeması ve genelleştirilmiş gözlemci şeması.

Ayrılmış gözlemci şeması herbir parametreyi kendi çıktısı üzerinden gözlemleyen bilinmeyen giriş gözlemcilerinden oluşurken, genelleştirilmiş gözlemci şeması gözlemlenen parametreyi dışarda bırakarak diğer tüm parametrelerin çıktılarını gözlemleyip diğer parametreler üzerinnden çıkarım yapılmasını sağlar. Ayrılmış gözlemci şemasının daha basit bir yapısı varken, genelleştirilmiş gözlemci şeması daha karmaşık bir yapıya sahiptir.

Bilinmeyen giriş gözlemcileri, sistem davranışlarını sürekli izleyerek sensör ve aktüatörlerden gelen olağan dışı verileri ayrıştırma ve dış bozucu etkileri elimine

ederek doğru sistem durum tahmini yapma yeteneğine sahiptir. Bu gözlemcilerin temel avantajlarından biri, model tabanlı bir yaklaşımı benimseyerek sensörleri hedef alan siber saldırılara karşı yüksek hassasiyet göstermeleri ve dış bozucu girişlere karşı dayanıklılık sağlamalarıdır. Bu gürbüzlük özelliği, özellikle bozucu etkilerin sık ve sürekli olduğu sistemlerdeki olağan dışı durumları tespit etmek adına son derece elzem bir gerekliliktir.

Yapılan literatür incelemesinde, Chen ve Patton'un geliştirdiği bilinmeyen giriş gözlemcisi temelli hata tespit ve izolasyon yöntemlerinin genellikle tekil sensör ya da aktüatör hatalarını başarılı biçimde tespit ettiği; ancak birden fazla sensörün eş zamanlı olarak arızalanması durumunda performanslarının düştüğü görülmüştür. Liu ve arkadaşları tarafından yapılan çalışmalarda ise yanlış veri enjeksiyonu saldırılarının klasik kötü veri tespit yöntemlerini atlatabildiği ve enerji sistemlerinin kontrol kararlarını ciddi şekilde manipüle edebildiği ortaya konmuştur.

Bu araştırmada, iki alanlı bir yük frekans kontrol sistemi üzerinde bilinmeyen giriş gözlemcisi temelli ayrılmış gözlemci ve genelleştirilmiş gözlemci şemaları MATLAB/Simulink ortamında detaylı simülasyonlarla analiz edilmiştir. Öncelikle gözlemci şemalarının dış kaynaklı bozulmalara ne denli dayanıklı oldukları yani gürbüzlük özelliğine sahip olup olmadıkları test edilmiştir. Sonrasında farklı siber saldırı senaryolarının uygulandığı simülasyon çalışmaları sonucunda bu gözlemci şemalarının yanlış veri enjeksiyonu saldırılarını ne derece etkin biçimde tespit edebildiği incelenmiştir.

Simülasyon sonuçları, global bilinmeyen giriş gözlemcisi yapısının gürbüz olduğunu ve yanlış veri enjeksiyonu saldırıları durumlarında tespit konusunda yüksek başarı sergilediğini ortaya koymuştur. Normal operasyon koşullarında hata sinyalleri teorik olarak sıfıra yakın seviyelerdeyken, saldırı koşullarında hata sinyallerinde belirgin yükselmeler gözlemlenmiştir. Bu da global bilinmeyen giriş gözlemcisinin, enerji sistemlerinde anormal durumları etkin ve güvenilir biçimde tespit ettiğini doğrulamaktadır.

Ayrılmış gözlemci şeması yaklaşımı belirli gözlenebilirlik koşullarını sağlayamadığı için bu simülasyon çalışmasında başarısız sonuçlar vermiştir. Her gözlemcinin tek sensörle kısıtlı veri alması gözlemci oluşturma şartlarının sağlanamamasına neden olmuştur. Gözlemci oluşma şartlarını sağlayan parametrelerin gözlemcileri de gürbüzlük özelliği gösterememiştir. Bu nedenle ayrılmış gözlemci şemasının bu sistem için uygun bir siber güvenlik yaklaşımı olmadığı sonucuna varılmıştır.

Genelleştirilmiş gözlemci şeması ise her gözlemcinin belirli bir sensör haricindeki tüm sensör verilerini kullanarak sistem durumunu takip etmesini sağlar. Böylece, saldırıya uğrayan sensör kolaylıkla tespit edilebilir hale gelmektedir. Saldırıya uğramayan sensörleri takip eden gözlemciler hata sinyallerinde olağandışı durumlar sergilerken, saldırıya uğrayan sensörle ilişkili gözlemci normal davranış göstererek saldırının yerini açıkça belirtir. Fakat yapısı itibariyle genelleştirilmiş gözlemci şemasının aynı anda birden fazla sensöre saldırı olduğunda bunun yerini tespit etmesi pek olası değildir. Genelleştirilmiş gözlemci şeması yöntemiyle çoklu sensor saldırıları saptanabilir fakat yeri tespit edilemediği için izole edilemez.

Global bilinmeyen giriş gözlemcisi ve genelleştirilmiş gözlemci şemalarının birlikte kullanımı ile tekil yanlış veri enjeksiyonu saldırılarının varlığı güvenilir şekilde tespit edilmekte ve saldırıya maruz kalan sensör net biçimde lokalize edilebilmektedir. Çoklu sensor saldırılarında ise sisteme saldırı olduğu saptanabilir fakat lokalize edilemez. Arıza durumunda arızalı sensörün yerinin saptanması bir kolaylık sağlasa

da siber saldırı hususunda bu durum çok büyük bir değişiklik yaratmaz. Sistemde çoklu sensör saldırısı varsa sensörlerin yalıtımından ziyade öncelik siber güvenliği sağlayıp, kötü niyetli kullanıcıların sisteme erişimini kesmektir. Sonuç olarak bu çalışma, enerji sistemlerinde siber tehditlere karşı gözlemci temelli yöntemlerin büyük bir koruma potansiyeline sahip olduğunu göstermiştir.

Gelecek çalışmalarda, çoklu sensör saldırılarını eş zamanlı olarak tespit ve lokalize edcek, yanlış veri enjeksiyonu saldırılarının yapılarını ve genliklerini belirleyerek gerçek zamanlı düzeltme stratejileri geliştirecek mekanizmaların oluşturulması planlanmaktadır. Ayrıca, yöntemin daha karmaşık enerji sistemlerine uygulanarak ölçeklenebilirliği ve gürbüzlüğü değerlendirilecek, modern enerji sistemlerinde süreklilik, kararlılık ve güvenilirlik artırılmasına katkı sağlanacaktır.

1. INTRODUCTION

Every year, the global energy demand continues to increase, primarily due to industrial growth, urban expansion, and improvements in living standards. The growing adoption of electric vehicles, digitalization in industries, advancements in information technologies, and ongoing electrification processes have significantly raised energy dependence. Consequently, energy generation, transmission, and distribution systems have become more complex and sensitive. This development highlights the necessity to evaluate power systems not only based on technical performance but also considering their integration with information technologies.

In recent years, the development of smart grids, smart home systems, IoT-based devices, and smart meters has led to the development of distributed structures that interact directly with users. While these systems have the potential to enhance grid flexibility, efficiency, and consumer engagement, they also create new cyber-security vulnerabilities. Today, power systems must be protected not only against physical faults but also against cyber attacks potentially executed by malicious people or external threat actors. In particular, digital components such as sensors, control signals, and communication lines have become targets for attackers, making cyber-security a critical necessity in power systems.

In parallel with these advancements, the increasing digitalization of power systems has significantly expanded the cyber attack surface. As sensor networks, communication protocols, and control units become more deeply integrated into grid operations, attackers are now able to exploit system vulnerabilities without needing physical access. Manipulating measurement data, tampering with control signals, or targeting communication infrastructure can lead to severe operational disruptions. Among these threats, false data injection attacks (FDIAs) pose a particularly insidious risk, as they can bypass conventional detection mechanisms by injecting carefully crafted false information into system inputs or measurements potentially misleading state estimation and compromising the reliability of grid control.

Sensor faults in power systems have long been addressed using observer-based methods, with unknown input observers (UIOs) standing out as an effective tool for detecting such anomalies. Since FDIAs also manipulate sensor outputs, it is reasonable to consider whether these same observer structures could be adapted for cyber-security purposes. Building on this idea, the present study investigates the potential of UIO-based approaches for detecting FDIAs in load-frequency control systems (LFC). To explore this, several observer schemes are implemented and compared in terms of their ability to detect and localize cyber attacks targeting measurement signals.

1.1 Purpose of Thesis

The primary objective of this thesis is to develop an effective and practically applicable observer-based strategy for providing cyber-security by detecting FDIAs in power systems with LFC. In this study, two different observer structures based on UIOs namely the dedicated observer scheme (DOS) and the generalized observer scheme (GOS) are examined.

The primary objective of this thesis is to develop an effective detection mechanism against FDIAs in load frequency control systems by using observer-based structures such as the DOS and the GOS. These observer schemes are designed using UIO theory to monitor system behavior, isolate inconsistencies caused by malicious data manipulation, and provide reliable indicators of cyber attacks. The proposed approach focuses on constructing a model-based detection framework that is not only sensitive to cyberattacks targeting sensor data but also robust to external disturbances. By implementing these schemes within realistic simulation environments, the thesis aims to contribute a resilient and practical solution for enhancing the cyber-security of control loops in modern power systems.

1.2 Literature Review

The increasing complexity and digitalization of modern energy systems driven by the integration of renewable sources, decentralized generation units, and intelligent control infrastructures have made it necessary to develop robust detection and isolation methods that are resilient not only to physical faults but also to systemic and cyber threats. In this context, UIOs represent a widely used model-based approach,

particularly in systems where external disturbances are dominant, to distinguish the effects of faults [1,2]. UIOs are specifically designed to be insensitive to external disturbances, while remaining sensitive to system deviations caused by faults.

Chen and Patton [1] laid the theoretical groundwork for UIO-based fault detection structures, particularly for the detection and isolation of single sensor or actuator faults. Their approach utilizes directional residual analysis, where residual signals are decoupled from unknown inputs, enabling accurate fault detection and isolation (FDI). However, as highlighted in their study, when multiple faults occur simultaneously, especially within the sensor layer, the observer design assumptions may become invalid. As a result, residual signals can lose their directional uniqueness, which in turn reduces isolation accuracy. In such cases, GOS composed of multiple individual UIOs, each assigned to monitor a specific sensor may fail to fully resolve overlapping residual responses, especially when fault effects interfere with each other.

One of the key studies that directly implements this approach in the context of LFC was conducted by Fikret Çalışkan and İstemihan Genç [3]. In their work, a UIO-based scheme using the GOS structure was developed, where both sensor and actuator faults were individually modeled and applied to the LFC loop. The study demonstrated that, with a proper selection of observer and system parameters, single faults could be detected and isolated with high precision. While the simultaneous failure of multiple sensors presents limitations for the GOS, such scenarios are considered relatively rare in real-world applications. Therefore, the GOS remains a practical and effective solution for implementing FDI strategies, especially under typical operating conditions.

In more recent literature, researchers have expanded the application of observer-based techniques beyond traditional fault diagnosis, toward the detection of cyber-attacks targeting sensor and actuator data. Liu, Ning, and Reiter [4] introduced the concept of FDIAs in state estimation processes, demonstrating that such attacks can bypass traditional bad data detection mechanisms and compromise the integrity of control decisions in power systems. While traditional bad data is often caused by random errors, sensor failures, or communication issues, FDIAs are deliberate and planned attacks. Unlike unintentional bad data, FDIAs are more dangerous and harder to detect because they are carefully crafted by attackers to covertly manipulate system metrics.

This work marked a turning point, highlighting the vulnerability of cyber-physical infrastructures to stealthy manipulation of measurements.

Building upon this, Teixeira et al. [5] conducted a comprehensive cyber-security analysis for state estimators in SCADA-based control environments, characterizing how different attack strategies can affect system observability and proposing structural conditions under which attack detection is possible. These studies collectively laid the foundation for integrating control-theoretic security analysis into power system protection strategies.

To address these threats from a model-based perspective, Pasqualetti, Dörfler, and Bullo [6] proposed a mathematical framework for attack detection and identification in cyber-physical systems. Their work introduced observability-based metrics to quantify the detectability of cyber intrusions and illustrated how UIO-like observer structures could be used to systematically identify tampered states. Similarly, Giraldo et al. [8] provided a broad survey of physics based intrusion detection systems, outlining the advantages of using structural, observer based models for identifying cyber threats in critical infrastructure. These contributions demonstrate that UIOs originally developed for physical fault detection, can also be effectively extended to cyber threat scenarios, including stealthy and coordinated data manipulation attacks.

This thesis builds upon the aforementioned studies by developing observer based detection framework for identifying undesired external interventions in load frequency control systems. The proposed approach focuses on constructing a model-based detection mechanism that uses residual signals generated by these observers to reliably detect malicious data manipulation. Particular emphasis is placed on ensuring that the detection framework maintains high sensitivity to attack attempts while remaining robust against external disturbances and system uncertainties. Through this methodology, the thesis contributes a practical and resilient solution for enhancing the cyber security of modern power system control loops.

1.3 Hypothesis

The hypothesis of this thesis is on the based following:

"*Observer schemes based on UIOs can effectively detect cyberattacks in the form of false data injection targeting sensors in load frequency control systems. These types*

of attacks actually similar to dynamic behavior of physical sensor faults. However, unlike unintentional faults, FDIAs can be deliberately structured in various signal forms and different magnitudes. It is therefore hypothesized that UIO based observer schemes, due to their ability to decouple unexpected disturbances and isolate residuals associated with anomalies, can serve as a robust and accurate model-based detection method for identifying FDIAs, even under realistic noise and disturbance conditions."

This hypothesis is proposed based on the fault diagnosis method based on UIOs presented in Chen and Patton's book [1], and inspired by the successful application of this method to a load frequency control system by Çalışkan and Genç [3].

2. LOAD FREQUENCY CONTROL

2.1 Generators

In electric power systems, energy is generated from a variety of sources. Although electrical energy generation is increasing with renewable energy sources such as solar and wind in recent years, the most of our energy demand is still provided by conventional methods.

In power systems, electrical energy (excluding that derived from photovoltaic solar sources) is generated by electrical generators. In conventional thermal power plants, which utilize fossil fuels such as coal, oil, and natural gas, synchronous generators are the industry standard due to their ability to provide both active and reactive power, as well as their stability characteristics within large interconnected grids [8].

Although there has been research [9] on the integration of asynchronous (induction) generators in hydropower systems, synchronous machines remain the dominant choice due to their grid-synchronization capability and efficiency under steady-state operation [10].

In the case of wind energy**,** asynchronous (induction) generators (especially doubly-fed induction generators) are widely used because of their feasibilities and ease of grid connection. However, synchronous generators, including permanent magnet synchronous generators are increasingly preferred in offshore and high-capacity wind farms due to their higher efficiency and better fault-ride-through performance [11].

Similarly, in geothermal power plants, which are also classified as renewable energy sources, synchronous generators are typically employed owing to their compatibility with the steam turbine technologies commonly used in such systems and their ability to maintain voltage and frequency stability in isolated or weak grids [12].

2.2 Active Power and Frequency

In an electric power system, consumption and generation must always be coordinated and balanced. For a high-quality, reliable, and stable power grid, generation units must

respond instantly to load variations and adjust their power output in accordance with the demand.

An increase in load, regardless of its type, increases the current drawn from the grid. The increase in current drawn from generators leads to higher losses due to the impedance of both the transmission lines and the generators themselves. This causes a drop in both the operating voltage and the operating frequency. However, since an increase in active power demand has very little effect on the terminal voltage [13], reactive power variation is directly related to voltage control.

In electric power generation, active power is generated by converting mechanical energy into electrical energy through a rotating generator. All generators are driven by a prime mover or mechanical drive system, such as a turbine or engine, which supplies the required mechanical torque. When active power is drawn from the generator, the mechanical load on the prime mover increases, as more torque is needed to maintain the generator's rotational speed.

If the mechanical input power is not increased proportionally in response to a rise in active power demand, the generator will begin to decelerate. This reduction in rotational speed results in a drop in system frequency. Therefore, variations in active power are directly linked to frequency control in power systems.

For this reason, changes in active and reactive power are addressed separately in electric power systems [14], and their control parameters and mechanisms are distinct. Active power is regulated through frequency control by adjusting the mechanical input of turbines, whereas reactive power is managed within the scope of voltage control via generator excitation systems or compensation equipment. Since these two control processes operate on different time scales and through separate control loops, they must be analyzed independently to ensure overall system stability.

There is a linear relationship between the power, torque, and speed of a rotating machine, whether it is electrical or mechanical. If the power stays the same, an increase in the torque applied by the load causes the speed of the rotating machine to decrease.

This relationship is defined by the following equation:

$$P = \omega T \tag{2.1}$$

In dynamic system analysis, power, torque, and rotor speed can be expressed as the sum of their nominal (initial) values and small deviations from those values.

$$P = P_0 + \Delta P$$
$$T = T_0 + \Delta T \quad (2.2)$$
$$\omega_r = \omega_0 + \Delta\omega_r$$

Here, P_0, T_0 and ω_0 represent the nominal values of power, torque, and rotor speed, respectively, while ΔP, ΔT, and $\Delta\omega_r$ denote small deviations.

A mismatch between the mechanical power input (P_m) and the electrical power output (P_e) leads to a deviation in system frequency. This imbalance occurs, for instance, when the load increases and the mechanical input remains momentarily constant, causing the generator to slow down.

There is a proportional relationship between the system frequency and the angular velocity of the generator rotor, which depends on the number of poles and the factor 2π. Since the analysis is carried out in per unit (p.u.) terms, the deviation in rotor speed is considered numerically equal to the deviation in system frequency. This allows frequency and speed to be used interchangeably in LFC system analysis.

The relationship between power imbalance and frequency dynamics can be expressed as:

$$\frac{df(t)}{dt} = \frac{1}{2H}(P_m(t) - P_e(t)) \quad (2.3)$$

Electrical loads are not entirely independent of frequency. For example, the power consumed by lighting or heating systems typically remains constant regardless of frequency changes. However, the power of rotating machine loads is directly affected by frequency. As the system frequency decreases, the speed and torque of these machines are also reduced, causing a drop in their power demand. This behavior provides a natural damping effect in the system. To reflect this in the model, a damping coefficient D is included, which accounts for the frequency-dependent portion of the load.

And when we add this damping coefficient, the formula becomes:

$$\frac{df(t)}{dt} = \frac{1}{2H}\left(P_m(t) - P_e(t) - Df(t)\right) \quad (2.4)$$

2.3 Single-Area Load Frequency Control System

In electrical power system, to keep operating frequency stable, generated and consumed power must always be balanced. Any change in load causes deviation in frequency. Accordingly, the generation side must be countinously and instantly adjusted to consumption. To fix the deviation in frequency, LFC systems are used. A single-area LFC system aims to automatically adjust the mechanical power in response to frequency deviations and restore the system to its nominal operating point.

This control structure is designed as a closed-loop feedback system. The frequency deviation is used as a feedback signal and passed through various control blocks, which affect the mechanical power input. The adjusted mechanical power is then applied to the power system, which affects the frequency. In this way, the frequency deviation is gradually suppressed.

As shown in Figure 2.1, the output value i.e., the frequency deviation passes through a proportional gain of 1/R, which converts this deviation into a power signal. This signal is then compared with the reference load value and sent to the input of the governor block. The governor block generates the mechanical power command that is delivered to the turbine. The following turbine block converts this power signal into actual mechanical power. Finally, the mechanical power, together with the load disturbance, is applied to the load-frequency block, which represents the effect of mechanical power changes on system frequency.

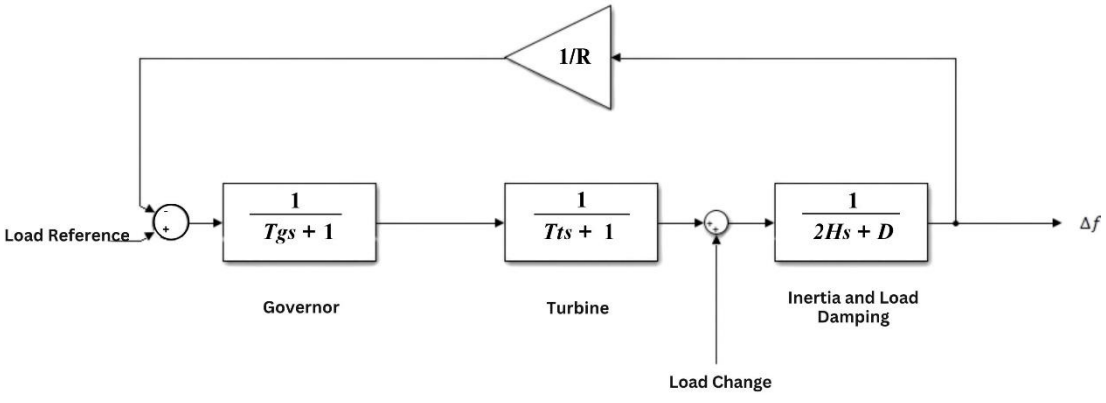

Figure 2.1 : Primary load frequency control block diagram.

When a sudden load increase occurs, the electrical power demand P_e rises while the mechanical input P_m initially remains unchanged. As a result, system frequency drops.

This frequency deviation is fed back to the governor, which adjusts its output accordingly. The turbine responds by increasing the mechanical input to the generator, and the frequency gradually returns to its nominal value.

The control block diagram is shown in Figure 2.1 represents the primary load frequency control mechanism. While primary control is effective to reduce frequency deviations following load disturbances, it inherently results in a steady-state error due to its proportional nature. To eliminate this residual error and to boost the overall stability of the power system, the implementation of a secondary control layer is essential. This secondary control is typically realized through a Proportional-Integral (PI) controller, which restores the frequency to its nominal value by continuously adjusting the load reference.

There may be multiple generation units (generators) within a single control area. Each generator is equipped with a primary load frequency control system, while some units also include a secondary control mechanism [14]. Although secondary control operates more slowly compared to primary control, it is essential in every area as it eliminates the steady-state error. Through the units equipped with secondary control, the power outputs of the other generators in the area are also adjusted to appropriate levels.

2.4 Two-Area Load Frequency Control System

In large scale electric power systems, the whole grid is usually divided into multiple control areas. Each area contains its own generating plant and the loads it supplies, and these areas are connected to each other via tie-lines, allowing power exchange. The main purpose of a two-area LFC system is not only to regulate the local frequency of each area, but also to keep the power flow through the tie-line at the planned level.

Each area operates its own frequency control loop and responds to local load changes. However, due to the interconnected nature of the systems, a load change in one area can also affect the frequency and power balance of the other area. Therefore, two-area LFC systems are designed to provide power balance between areas along with local frequency control.

A typical two-area model includes:

- Two separate generation-control loops, each with its own governor, turbine, and system dynamics,

- A tie-line model that represents the power flow between the areas,
- A secondary controller in each area that adjusts the reference power based on frequency deviation and tie-line error (Area Control Error – ACE).

This structure ensures that each area can correct its own frequency deviation while also restoring the tie-line power to its scheduled value, thus maintaining both local and system-wide balance.

The two-area LFC system is illustrated in Figure 2.2.

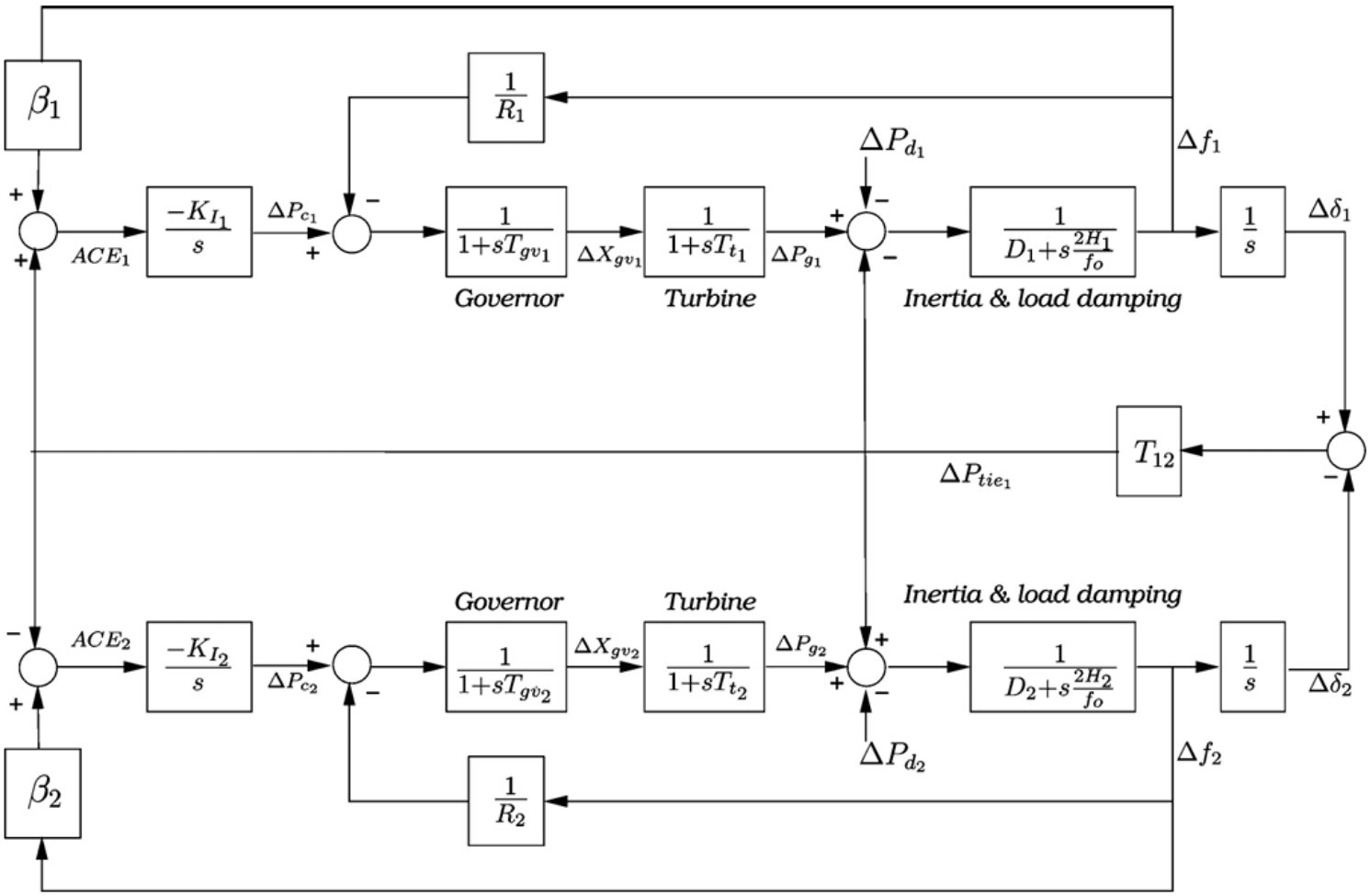

Figure 2.2 : Two-Area LFC system block diagram [3].

3. UNKNOWN INPUT OBSERVER AND OBSERVER SCHEMES

The observer concept was first introduced by Luenberger in the 1960s as a linear state observer [15]. Since then, many observer designs have been developed for systems with known and unknown inputs, and in particular, architectures called “unknown input observer (UIO)” have taken their place in the literature [15].

An UIO is a tool that estimates the state of a dynamic system by observing its inputs and outputs. Observers predict how the system should behave by monitoring unmeasurable state variables. Owing to these features observers are an ideal method for detecting fault or unexpected interventions.

The structural arrangements used when placing observers in a control system are called observer schemes. The observer scheme refers to the general framework that determines how signals will be generated, which quantities will be monitored by which observers, and how these structures are related to each other.

UIOs can be structured under different observer schemes. The two most commonly used schemes are known as the GOS and the DOS. While the GOS structure evaluates all sensor data except for the sensor under consideration through a single observer structure, a separate observer is configured for each sensor in the DOS structure.

3.1 Unknown Input Observer

An unknown input observer is a type of observer that can make accurate state estimations despite the presence of external influences (e.g., disturbance inputs, modeling errors) that are not included in the system model or cannot be measured. Mathematically, if the state estimation error (e) of an observer converges to zero over time, even if the system contains unknown inputs, then that observer is defined as a UIO. In other words, UIO is an observer structure that can asymptotically eliminate the observation error even in the presence of uncertain inputs. Considered as a general extension of the classical Luenberger state observer, UIO is designed to be insensitive to certain disturbances [1]. In this way, the UIO observer makes the residual signal generated from the difference between the predicted outputs and the actual outputs

sensitive only to faults, while eliminating the effect of uncertain inputs on the residual. As a result, UIO enables the separation of unknown input effects in order to avoid generating false alarms in model-based fault detection [15].

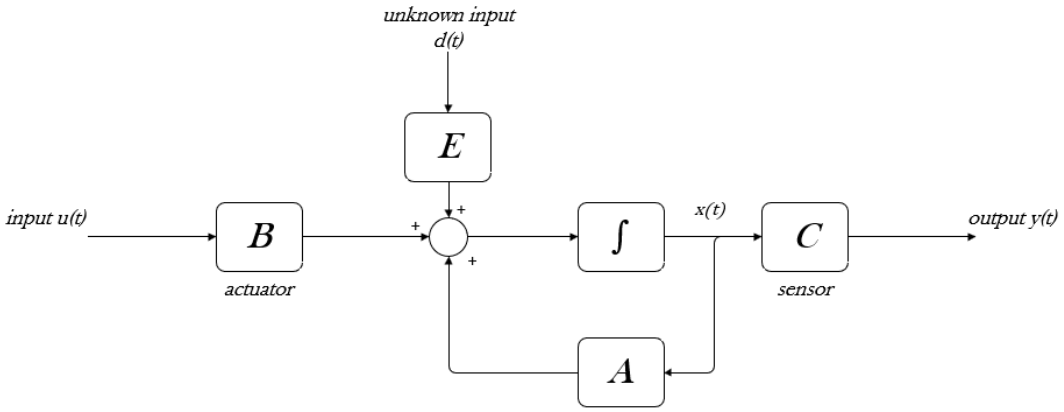

Figure 3.1 : System model with unknown input.

The block diagram of a linear dynamic system subject to a disturbance input is shown in Figure 3.1. The state-space representation of this system is modeled as follows:

$$\dot{x}(t) = Ax(t) + Bu(t) + Ed(t) \tag{3.1}$$
$$y(t) = Cx(t)$$

Where:

- $x(t) \in \mathbb{R}^n$ is the state vector.
- $u(t) \in \mathbb{R}^r$ is the known control input.
- $d(t) \in \mathbb{R}^r$ represents the unknown (disturbance) input.
- $y(t) \in \mathbb{R}^m$ is the measured output.

The system matrices are defined as follows:

- $A \in \mathbb{R}^{n\times n}$: The system matrix that describes the internal dynamics and state transitions of the system.
- $B \in \mathbb{R}^{n\times r}$: The input matrix that determines the influence of the known input *u(t)* on the state vector.
- $C \in \mathbb{R}^{m\times n}$: The output matrix that maps the state vector *x(t)* to the measurable output *y(t)*.

- $E \in \mathbb{R}^{n \times r}$: The disturbance matrix that characterizes how the unknown input *d(t)* affects the system states.

According to the block diagram shown in Figure 3.2, the mathematical model of the UIO is defined as follows:

$$\dot{z}(t) = Fz(t) + TBu(t) + Ky(t) \tag{3.2}$$
$$\hat{x}(t) = z(t) + Hy(t)$$

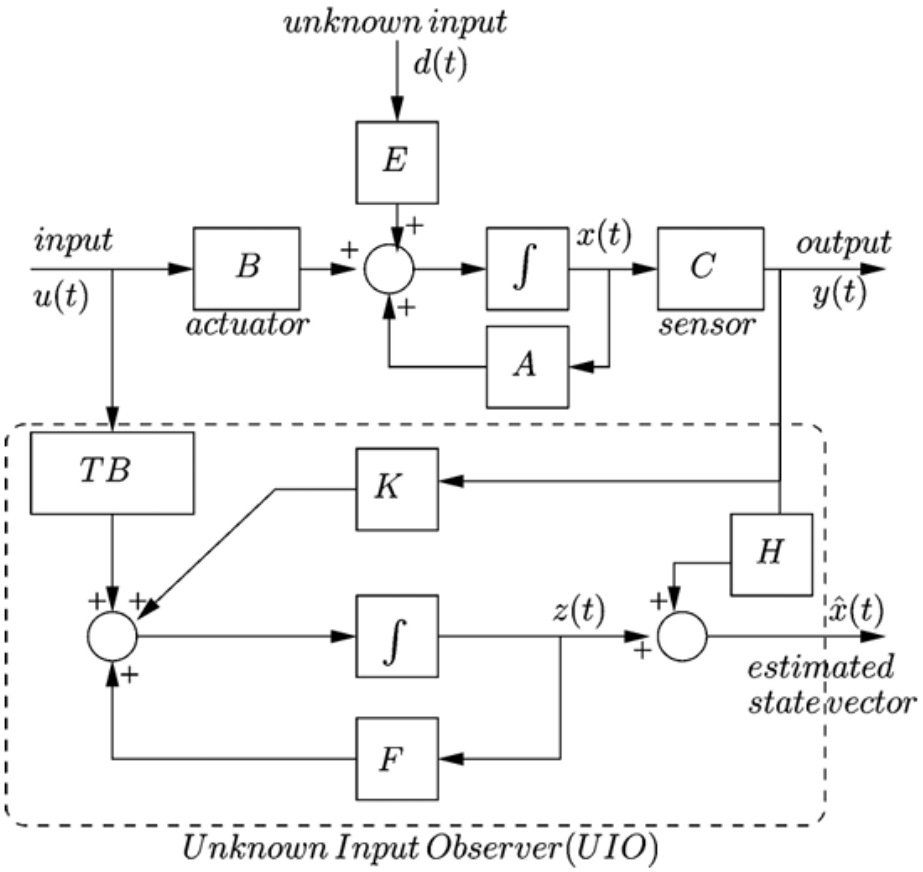

Figure 3.2 : UIO-based state estimation structure for a dynamic system [1].

In this observer structure, *z(t)* represents the internal state vector of the observer, while *x̂(t)* denotes the estimated state vector of the original system. The matrices *F, T, K* and *H* are determined through the observer design process. To ensure that the estimation is not affected by the unknown input *d(t)*, the following conditions must be satisfied to eliminate the effect of the disturbance:

$$H = E[(CE)^T(CE)]^{-1}(CE)^T \tag{3.3}$$
$$K_1 = (A - F - HCA)C^{-1} \tag{3.4}$$

$$K_2 = FH \tag{3.5}$$

$$K = K_1 + K_2 \tag{3.6}$$

$$T = I - HC \tag{3.7}$$

If the conditions illustrated in Figure 3.3 are satisfied, a UIO exists and can be properly designed. Moreover, the state estimation error of the UIO is given by:

$$\dot{e} = Fe \tag{3.8}$$

The residual signal is defined and computed as:

$$r(t) = y(t) - C\hat{x}(t) = (I - HC)y(t) - Cz(t) \tag{3.9}$$

In order to design a UIO, the observer gain matrices K, K_1 and K_2 used in eq. (3.4), (3.5) and (3.6) such that all eigenvalues of the resulting matrix are stable. Specifically, K_1 is choosen so that F is Hurwitz. The necessary and sufficient conditions for the existence of such a UIO are given as follows:

1) rank(CE) = rank (E);
2) (C, A_1) is a detectable pair where

$$A_1 = A - HCA \tag{3.10}$$

As seen above, K_1 is a free design parameter of the UIO model. Once K_1 is defined, other parameters can be calculated respect to it. Since the observer design problem is inherently multivariable, so that the matrix K_1 makes the matrix F is Hurwitz.

According to the UIO design procedure shown in Figure 3.4, if the pair (C, A_1) is not observable, a transformation matrix P is constructed to perform the observable canonical decomposition such that:

$$PA_1P^{-1} = \begin{bmatrix} A_{11} & 0 \\ A_{12} & A_{22} \end{bmatrix}, \quad CP^{-1} = [C^* \ 0] \tag{3.11}$$

Here, the submatrix A_{22} contains the unobservable dynamics, and its eigenvalues represent the unobservable modes.

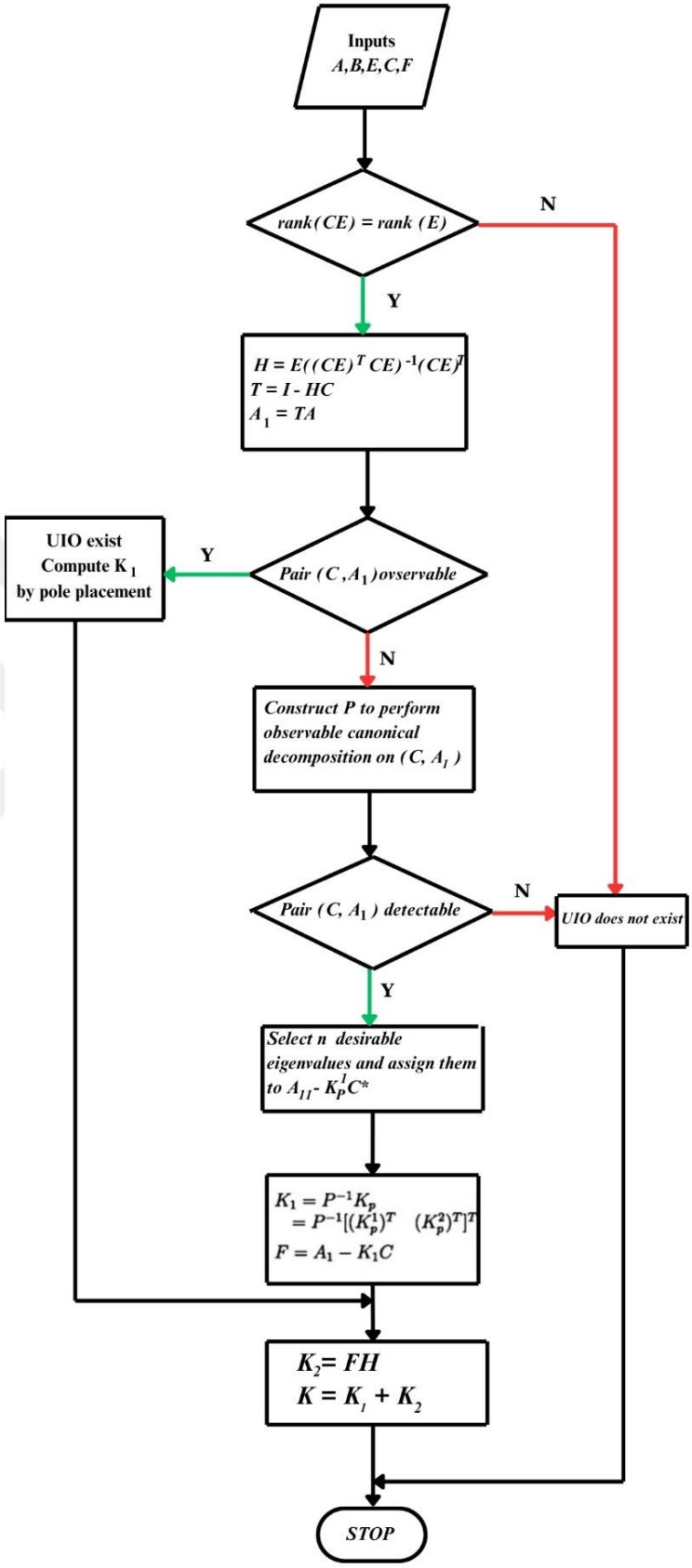

Figure 3.3 : Flowchart of the UIO design [3].

3.2 Observer Schemes

UIO-based approaches are model-based methods developed to detect and isolate various anomalies or unexpected situations that may occur in dynamic systems. In these approaches, multiple observers are usually used together as an observer scheme. Each observer is designed to focus on a different part of the system, so that when unexpected situation occurs, it only affects the residual signal of the observer related to that part. When all of these observers are considered together, different observer schemes are formed.

The most common observer schemes built using observer banks are the DOS and the GOS. In the DOS structure, each observer monitors only the data from its own unit and estimates its own states without considering the rest of the system. On the contrary, in the GOS structure, each observer uses data from all parts of the system except for its own unit, and performs the estimation accordingly.

3.2.1 Dedicated observer scheme

In the DOS each observer is assigned to a specific unit or a specific anomaly. Technically, an observer bank is constructed and each observer within the bank is designed to use only the output of a single sensor [16]. Each observer generates an output estimation for the sensor it is assigned to and by comparing this estimation with the actual sensor measurement, a residual signal is produced. In this way, each observer is sensitive to unexpected situations occurring in its own assigned sensor, while remaining insensitive to issues in other sensors. For instance, in a system with three sensors, the DOS approach would involve designing three separate observers. Since each observer uses data from a different sensor, only faults in that specific sensor will affect its corresponding residual signal. This structure was first proposed by Clark in the 1970s and was shown to be effective for reliably detecting multiple sensor faults [17]. However, the literature points out that ensuring each residual signal is sensitive to only a single anomaly while being completely insensitive to all others can be challenging, specially under model uncertainties and robustness requirements [1]. Chen and Patton emphasize that designing such “perfectly decoupled” residuals may be analytically difficult in practical applications.

3.2.2 Global observer schemes

The GOS was developed to overcome the robustness and design difficulties seen in the DOS [18]. In GOS, each observer in the observer bank uses all control inputs and all sensor measurements, except for one sensor that is intentionally excluded. By doing so, each observer becomes insensitive to a fault in the excluded sensor, but remains sensitive to faults in the others.

For instance, in a system with N sensors, the GOS method typically includes N observers, each constructed by omitting a different sensor from the measurement set. That is, each observer estimates the system states using the measurements from N - 1 sensors, deliberately excluding the data from one distinct sensor [19]. This structure enables a decoupled observation approach based on insensitivity: under normal operation, all observers generate consistent residual signals. However, when an abnormal condition affects one of the sensors, the residuals of the observers using that sensor's data will deviate, while the residual of the observer that excludes the faulty sensor remains unchanged. Therefore, the sensor corresponding to the unchanged residual is identified as the source of the anomaly [19].

This approach was first introduced by Frank in 1987 [20], and has since been widely used in observer-based fault detection systems. Compared to the DOS, the GOS offers more flexibility by ensuring that each residual is only unaffected by one specific fault. This improves robustness and makes the design process more practical [20].

4. METHODOLOGY AND IMPLEMENTATION

This section explains how UIO-based observer schemes originally developed for FDI are adapted and applied to a LFC system in order to evaluate their effectiveness under FDIA. First, the dynamic model of the LFC system is presented. Then, the integration of DOS and GOS into this model is discussed, with a focus on how these structures respond under cyber attack scenarios.

4.1 Mathematical Model of the Load Frequency Control System

In a power system area, the dynamic interactions between generators are often neglected by assuming that they operate coherently. Based on this assumption, the overall dynamic behavior of all generators in a given area can be represented by a single equivalent generation unit, which consists of a generator, a turbine, and a governor. The block diagram of a two-area, decentralized LFC system was presented earlier in Figure 2.2 of Chapter 2. Although this model does not include some practical aspects such as the filtering of the ACE it is still considered sufficient for demonstrating the approach proposed in this study. The dynamic model of the multi-area power system is summarized below.

For a multi-area power system, each area i is represented by an equivalent generation unit. The state variables Δf_i, ΔP_{gi} and ΔX_{gvi} denote the deviations in system frequency, generated power, and governor valve position of area i, respectively. The dynamic behavior of the generator in each area can be modeled as follows:

$$\frac{df(t)}{dt} = \frac{f_0}{2H_i}\left(\Delta P_{g_i}(t) - \Delta P_{d_i}(t) - \Delta P_{tie_i}(t) - D_i \Delta f_i(t)\right) \tag{4.1}$$

where f_0 is the nominal system operating frequency, H_i and D_i are the inertia and damping constants of area i, respectively, and ΔP_d and ΔP_{tiei} represent the deviations in load demand and tie-line power exchange.

$$\frac{d\Delta P_{g_i}(t)}{dt} = -\frac{1}{T_{t_i}}\Delta P_{g_i}(t) + \frac{1}{T_{t_i}}\Delta X_{gv_i}(t) \tag{4.2}$$

$$\frac{d\Delta X_{gv_i}(t)}{dt} = -\frac{1}{T_{gv_i}}\Delta X_{gv_i}(t) - \frac{1}{T_{gv_i}R_i}\Delta f_i(t) + \frac{1}{T_{gv_i}}\Delta P_{c_i}(t) \quad (4.3)$$

Equation (4.2) describes the change in generated power ΔP_{gi}, which is influenced by the valve position ΔX_{gvi} and the turbine time constant T_{ti}. Equation (4.3) defines the governor valve dynamics, depending on the frequency deviation Δf_i , the control input ΔP_{ci} , and the regulation constant R_i. Here, T_{ti} and T_{gvi} represent the time constants of the turbine and governor, respectively.

$$\Delta P_{tie_i}(t) = \sum_{j=1}^{n} T_{ij}\left(\int \Delta f_i(t)dt - \int \Delta f_j(t)dt\right) \quad (4.4)$$

In a power system with n control areas, the deviation in tie-line power for area i is given by equation (15), which considers the integral of frequency differences between area i and all interconnected areas, weighted by the synchronizing coefficient T_{ij}.

$$ACE_i(t) = \Delta P_{tie_i}(t) + \beta_i \Delta f_i(t) \quad (4.5)$$

$$\Delta P_{c_i}(t) = -K_{I_i}\int ACE_i(t)dt \quad (4.6)$$

The Area Control Error (ACE), shown in equation (4.5), is the sum of the tie-line power deviation and the frequency deviation scaled by the frequency bias factor β_i. Finally, equation (4.6) defines the control input ΔP_{ci} as the integral of the *ACE* signal, multiplied by the integral gain K_{Ii}, thus forming a closed-loop control mechanism.

The state-space model of the two-area LFC system is constructed based on the dynamic equations previously defined. The state vector is given as:

$$x(t) = \left[\int \Delta P_{tie_1}(t)dt \quad x_1 \quad x_2\right]^T \quad (4.7)$$

where each subvector x_i for area i = 1,2 is defined as:

$$x_i(t) = \left[\int \Delta f_i(t)dt \quad \Delta f_i \quad \Delta P_{g_i} \quad \Delta X_{gv_i}\right] \quad (4.8)$$

The control input vector is defined as:

$$u(t) = [\Delta P_{c_1} \quad \Delta P_{c_2}]^T \quad (4.9)$$

The disturbance input vector, which represents the load demand deviations in each area, is given by:

$$d(t) = [\Delta P_{d_1} \quad \Delta P_{d_2}]^T \quad (4.10)$$

The output matrix *C* will be examined in the following section based on observability conditions. The system matrices *A*, *B* and *E* are given as follows:

$$A = \begin{bmatrix} 0 & T_{12} & 0 & 0 & 0 & -T_{12} & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -\frac{f_0 T_{12}}{2H_1} & -\frac{f_0 D_1}{2H_1} & \frac{f_0}{2H_1} & 0 & \frac{f_0 T_{12}}{2H_1} & 0 & 0 & 0 \\ 0 & 0 & 0 & -\frac{1}{T_{t_1}} & \frac{1}{T_{t_1}} & 0 & 0 & 0 & 0 \\ 0 & 0 & -\frac{1}{T_{gv_1} R_1} & 0 & -\frac{1}{T_{gv_1}} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & \frac{f_0 T_{12}}{2H_2} & 0 & 0 & 0 & -\frac{f_0 T_{12}}{2H_2} & -\frac{f_0 D_2}{2H_2} & \frac{f_0}{2H_2} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -\frac{1}{T_{t_2}} & \frac{1}{T_{t_2}} \\ 0 & 0 & 0 & 0 & 0 & 0 & -\frac{1}{T_{gv_2} R_2} & 0 & -\frac{1}{T_{gv_2}} \end{bmatrix}$$

$$B = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ \frac{1}{T_{gv_1}} & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & \frac{1}{T_{gv_2}} \end{bmatrix}, \qquad E = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ -\frac{f_0}{2H_1} & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & -\frac{f_0}{2H_2} \\ 0 & 0 \\ 0 & 0 \end{bmatrix} \tag{4.11}$$

4.2 Applying FDI-Oriented Observer Structures to FDIA Scenarios

Although observer-based fault detection strategies were initially developed for identifying sensor or actuator faults, their structure and logic can be adapted to address cyber threats as well. In particular, UIO schemes originally designed for FDI can be repurposed to detect FDIA, which deliberately manipulate sensor measurements to disrupt the system state estimation.

Figure 4.1 shows a classical FDI mechanism designed to identify sensor faults using a residual-based observer structure. This setup includes a global unknown input observer

(GUIO), which is used to generate residual signals that reflect discrepancies between estimated and actual sensor outputs.

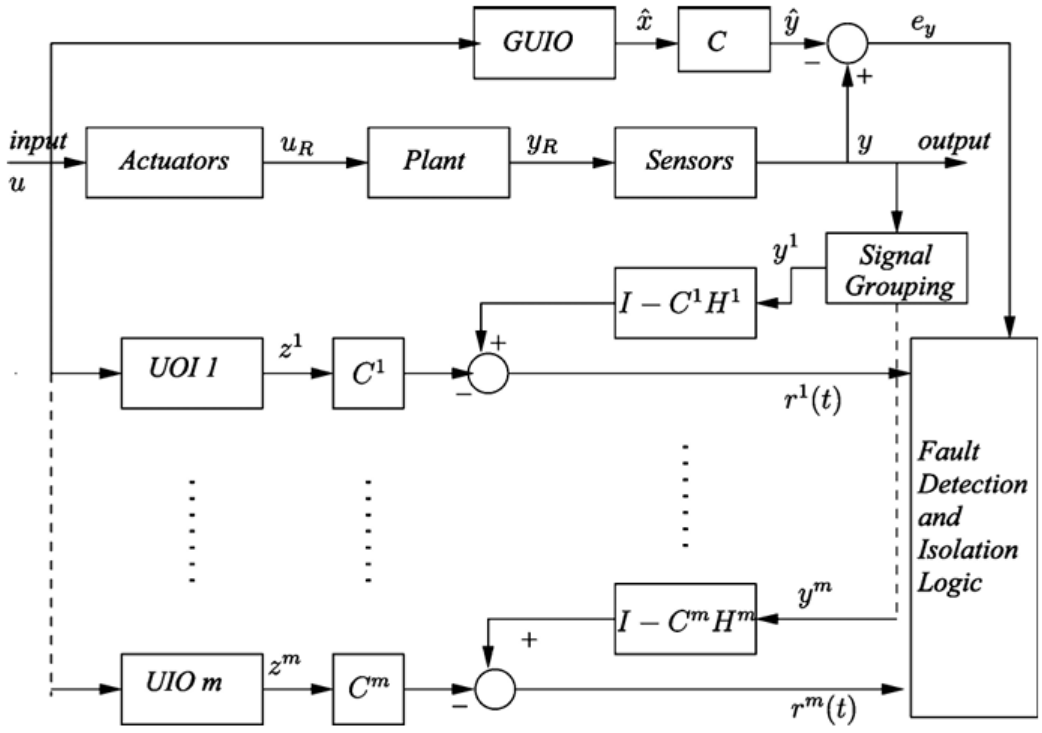

Figure 4.1 : Robust fault detection and isolation structure [3].

In this study, we apply the same structure to FDIA scenarios. Instead of sensor faults, the system is subjected to cyber attacks (f_{fdi}) in the form of additive biases injected into the sensor measurements. The aim is to evaluate whether observer-based residual generation methods originally intended for FDI can also be effective in detecting malicious manipulations introduced by FDIAs.

Assuming that all actuators operate correctly, the system under sensor attack can be modeled as:

$$\dot{x}(t) = Ax(t) + Bu(t) + Ed(t) \tag{4.11}$$
$$y(t) = Cx(t) + f_{fdi}(t)$$

Here, $f_{fdi}(t) \in \mathbb{R}^m$ is an unknown and unmeasurable bias vector that represents the effect of the injected malicious signals targeting the sensors. These additive perturbations alter the actual sensor outputs and are intended to mislead the state estimation process. Based on this structure, the following output expressions can be defined for multi-output and single-output sensor channels, respectively:

$$y^j(t) = C^j x(t) + f_{fdi}^j(t) \tag{4.12}$$

$$y_j(t) = c_j x(t) + f_{fdi,j}(t) \tag{4.13}$$

In the DOS structure, each observer is designed to monitor a single sensor. Therefore, only one output signal is used for each observer. In this case, the output equation is constructed by selecting the corresponding row from the output matrix *C*, denoted as $c_j \in \mathbb{R}^{1\times n}$. Therefore the output is a scalar $y_j(t)$ as directly shown in equation (4.13).

The UIO-based residual generator for the DOS structure is written as:

$$\begin{aligned} z_j(t) &= F_j z_j(t) + T_j B u(t) + K_j y_j(t) \\ r_j(t) &= \big(I - C_j H_j\big) y_j(t) + C_j z_j(t) \quad for \quad j = 1, 2, \dots m. \end{aligned} \tag{4.14}$$

For DOS, the following conditions must be satisfied to design UIOs:

$$\begin{aligned} H_j C_j E &= E \\ T_j &= I - H_j C_j \\ F_j &= T_j A - K_{1,j} C_j \quad must\ be\ Hurwitz \\ K_{2,j} &= F_j H_j \\ K_j &= K_{1,j} + K_{2,j} \end{aligned} \tag{4.15}$$

In contrast, the GOS structure uses all outputs except the one under test. For a system with *m* sensors, each observer monitor *m* – 1 outputs by deleting *j*-th row of the *C* matrix. This modified matrix is denoted as $C^j \in \mathbb{R}^{(m-1)\times n}$, and the corresponding vector $y_j(t)$ as directly shown in (4.12).

The UIO-based residual generator for the GOS structure is written as:

$$\begin{aligned} z^j(t) &= F^j z^j(t) + T^j B u(t) + K^j y^j(t) \\ r^j(t) &= \big(I - C^j H^j\big) y^j(t) + C^j z^j(t) \quad for \quad j = 1, 2, \dots m. \end{aligned} \tag{4.16}$$

For DOS, the following conditions must be satisfied to design UIOs:

$$\begin{aligned} H^j C^j E &= E \\ T^j &= I - H^j C^j \\ F^j &= T^j A - K_1^j C^j \quad must\ be\ Hurwitz \\ K_2^j &= F^j H^j \\ K^j &= K_1^j + K_2^j \end{aligned} \tag{4.17}$$

4.2.1 Selecting of output matrices for observer schemes

In the study [3], the observer-based monitoring focuses on three key state variables: the frequency deviations of the two areas Δf_1 and Δf_2 and the tie-line power deviation ΔP_{tie}. These are the primary outputs intended to be observed by the designed residual generator.

However, according to the findings in [3], performing successful fault detection using the GOS requires more than observing the individual outputs separately. Specifically, it was shown that the inclusion of a linear combination of the frequency deviations $\Delta f_1 + \Delta f_2$ is essential to boost detection performance. As a result, the output vector adopted in this study is defined as:

$$y(t) = [\Delta f_1 \quad \Delta f_2 \quad \Delta P_{tie} \quad \Delta f_1 + \Delta f_2] \tag{4.18}$$

Therefore, based on the findings in [3] and considering the enhanced sensitivity in detecting sensor-related anomalies, the following output matrix C is adopted for the observer schemes:

$$C = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & T_{12} & 0 & 0 & 0 & -T_{12} & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix} \tag{4.19}$$

5. SIMULATION AND RESULTS

In this section, the previously developed GOS and DOS structures are tested on a two-area LFC system. The system parameters used in the simulations are presented in Table 5.1. The simulations are carried out in MATLAB/Simulink. Various FDIA scenarios are applied by injecting additive bias signals into the sensor measurements. The aim is to examine how well each observer can detect these attacks by analyzing the generated residual signals. This also helps evaluate the robustness and reliability of both observer schemes under cyberattack conditions.

Table 5.1 : Parameters of the LFC system

Parameters	Values
f_0	60 Hz
T_{12}	0.545 p.u. MW
$H_1 = H_2$	5 s
$D_1 = D_2$	8.33×10^{-3} p.u. MW / Hz
$T_{t1} = T_{t2}$	0.3 s
$T_{gv1} = T_{gv2}$	0.08 s
$R_1 = R_2$	2.4 Hz / p.u. MW
$K_{I1} = K_{I2}$	1
$\beta_1 = \beta_2$	0.425 p.u. MW / Hz

5.1 Simulation Setup

All simulations were conducted in MATLAB/Simulink software. The system model used is the two-area LFC structure detailed in the previous chapters. Each area is represented by an equivalent generating unit that includes the dynamics of a generator, a turbine, and a governor.

The detection mechanism implemented in the simulation follows the same structure shown in Figure 4.1. The UIOs used in this structure are also designed based on the model presented in Figure 3.2. Both the GOS and the DOS were integrated into the system using the matrices defined in Chapter 4.

The main goal of the simulation is to examine the behavior of these observer schemes under FDIA scenarios targeting sensor measurements. At certain time intervals, intentional biases were added to specific sensor outputs, and the resulting residual signals were analyzed for each case.

This allowed us to evaluate which observer scheme is more accurate and reliable when it comes to detecting FDIA-type cyber attacks.

5.2 FDIA Scenarios and Simulation Results

In this section, various cyber-attack scenarios are introduced in which the system is subjected to FDIAs targeting specific sensor measurements. These scenarios are designed to assess the detection capabilities of the observer-based schemes developed in the previous sections. The same UIO-based detection mechanism illustrated in Figure 4.1 has been implemented here, with observer structures corresponding to the model presented in Figure 3.2. Furthermore, the system matrices defined in Section 4 have been utilized without any additional modifications. For each scenario, the residual signals produced by both the GOS and the DOS are analyzed to evaluate their effectiveness in identifying and isolating the attacks.

In this part, we test how robust the observer schemes are when there is only an external disturbance and no FDIA applied. For that, we define the disturbance input *d(t)* and apply it to the system. In this case, ΔP_{d1} is kept at zero, and a unit step signal with an amplitude of 0.1 is applied to ΔP_{d2} at the $t = 2$ moment. We then observe how the residual signals behave in both the GOS and DOS structures. If an observer is truly robust, its residuals should not react too much to this kind of disturbance and should stay close to zero. That way, we can be sure it does not produce false alarms when there is no attack. This scenario gives us a baseline before moving on to the actual FDIA tests.

Figure 5.1 shows the norms of the residuals produced by the GUIO under the disturbance input described above. Although there seems to be a small amount of noise, the amplitude of this fluctuation is in the order of 10^{-32}, which is extremely close to zero. This clearly supports the result stated in equation (3.8), where the estimation error is expected to converge to zero. Therefore, we can conclude that the GUIO is robust against this type of disturbance.

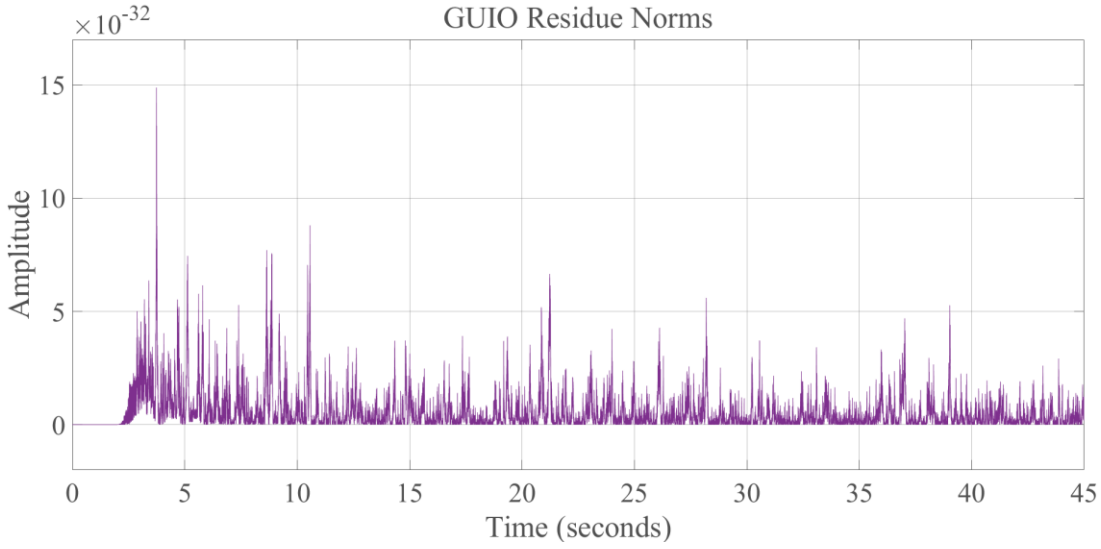

Figure 5.1 : Residual norms of GUIO under single step disturbance.

As illustrated in Figure 5.2, the residual norms obtained from the observers within the GOS structure remain in the order of 10^{-32} to 10^{-33}, closely aligning with those produced by the GUIO under identical disturbance conditions. These results confirm that the GOS configuration preserves its robustness characteristics and maintains insensitivity to such disturbances.

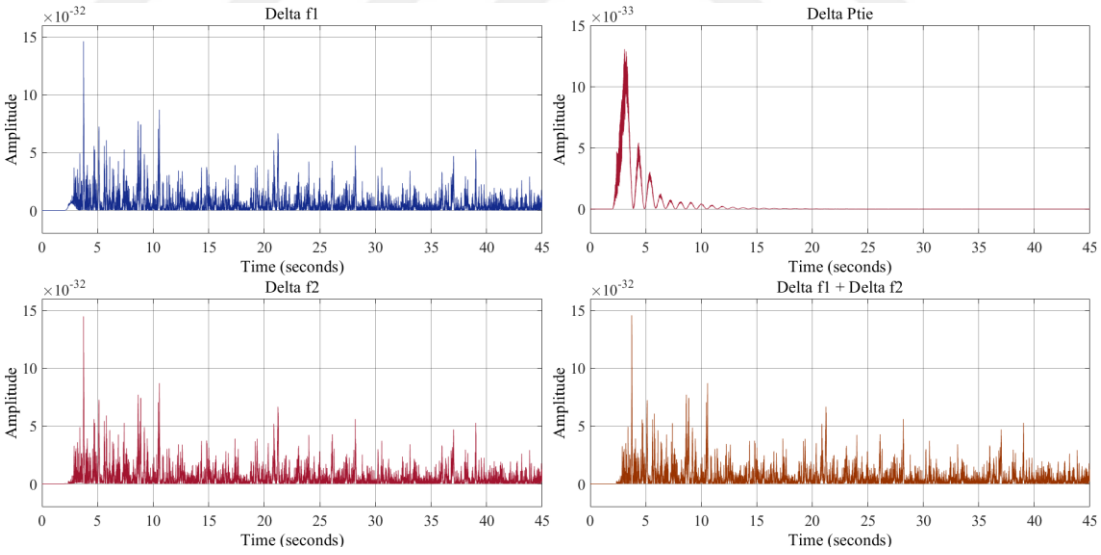

Figure 5.2 : Residual norms of observers in the GOS structure under single step disturbance.

Figure 5.3 shows the norms of the residuals produced by the observers in the DOS structure. Since the DOS design focuses on a single parameter per observer, only one residual is actually generated. Although taking its norm is not strictly necessary, it is done here for comparison purposes. In the results, we observe that the observers

monitoring the sensors for Δf_1 and Δf_2 produce no output. However, the observer assigned to the ΔP_{tie} sensor shows a disturbance response around the order of 10^{-5}, indicating a problem in terms of robustness. Interestingly, the observer monitoring the fourth sensor which represents the linear combination of Δf_1 and $\Delta f2$ shows consistent behavior, and its residuals align well with those seen in the GUIO and GOS structures.

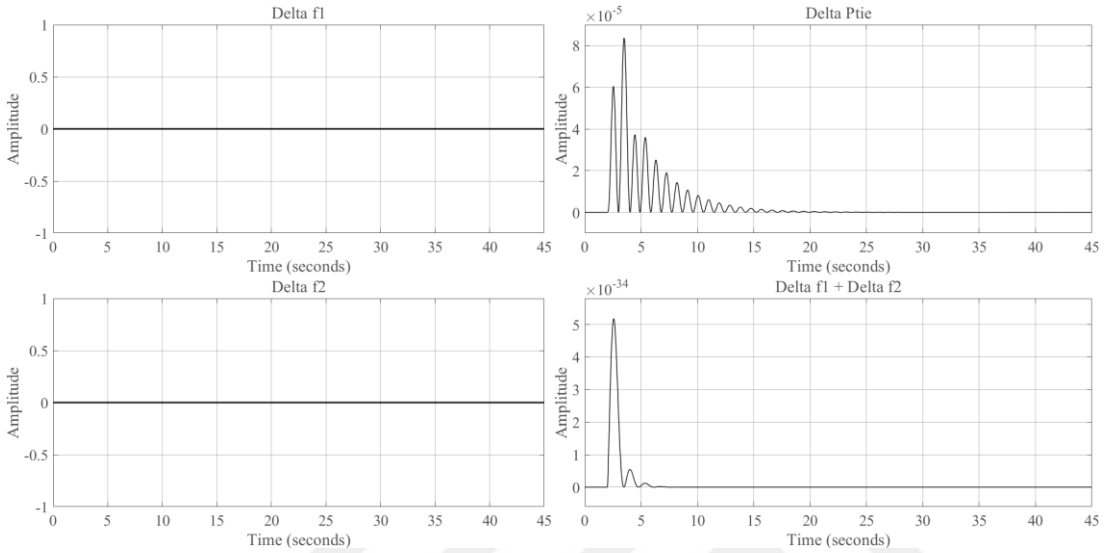

Figure 5.3 : Residual norms of observers in the DOS structure under single step disturbance.

To further evaluate the robustness of the observer schemes, the disturbance function *d(t)* is modified to introduce a more complex input scenario. While a unit step disturbance with an amplitude of 0.1 is still applied to ΔP_{d2} at the t = 2 moment, the ΔP_{d1} signal is now defined as a sinusoidal function with an amplitude of 0.5 and a period of 30 seconds, specifically given by $\Delta P_{d1}(t) = 0.5\sin(2\pi 2t)$ at the t = 15 moment. This configuration allows us to assess how well the observer structures, particularly GUIO and GOS, maintain their robustness under time-varying and oscillatory disturbances that more closely resemble real-world fluctuations in load demand.

As shown in the Figure 5.4 GUIO, the results remain nearly unchanged compared to the previous scenario. The residual norms are still on the order of 10^{-32}, which indicates an extremely low estimation error and confirms the robustness of the GUIO under the new disturbance input. Similarly, in the Figure 5.5 outputs of the observers within the GOS structure exhibit negligible differences, with residual magnitudes still in the range of 10^{-32} to 10^{-33}.

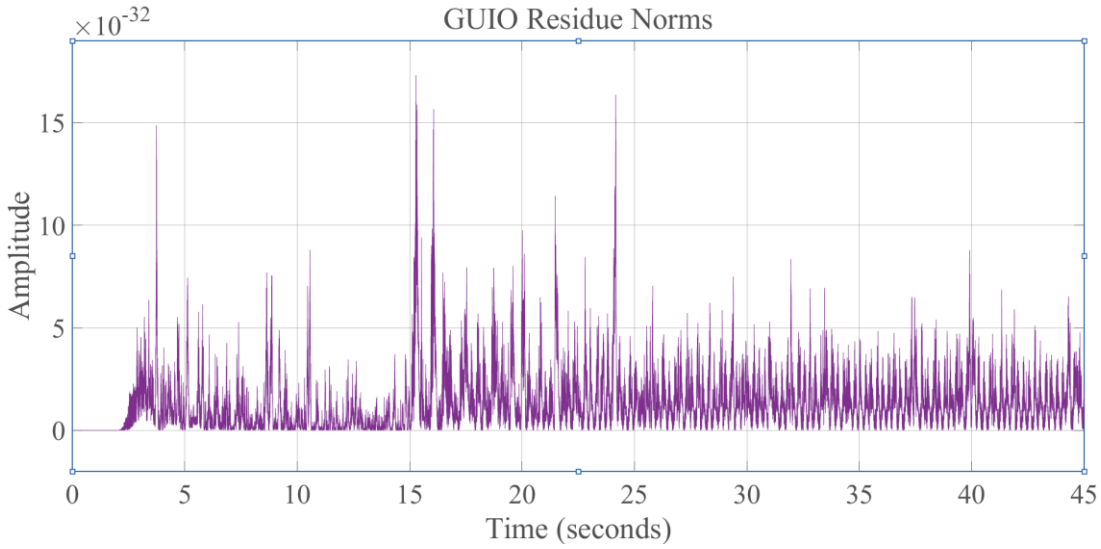

Figure 5.4 : Residual norms of GUIO under complex disturbances.

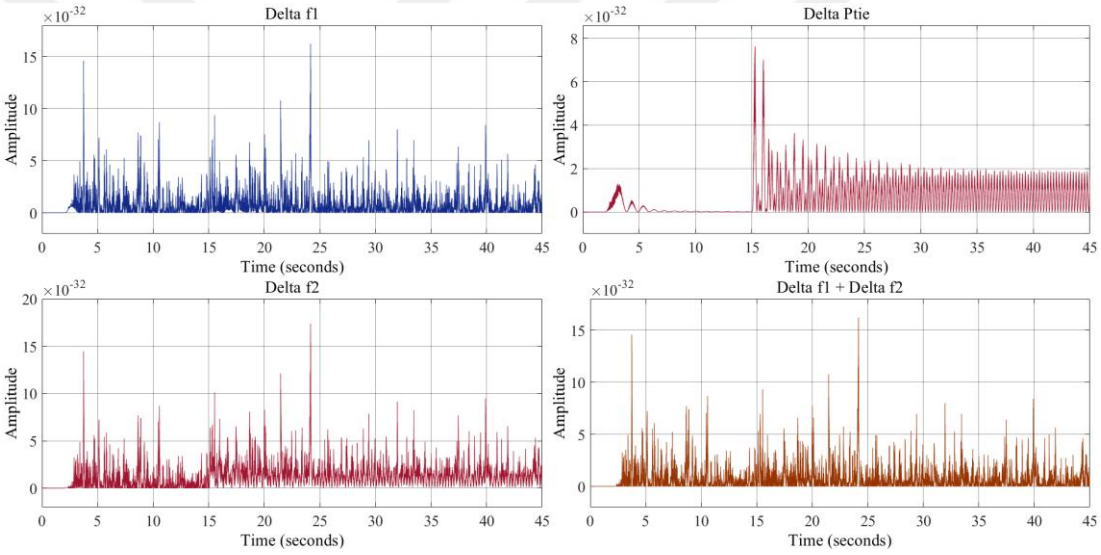

Figure 5.5 : Residual norms of observers in the GOS structure under complex disturbances.

Of particular note is the observer monitoring the ΔP_{tie} variable within the GOS structure. Its output clearly reflects the time instances where the disturbances are applied, making the influence of the injected noise distinguishable in the residual signal. However, due to the very low amplitude of these fluctuations, they are considered negligible in the context of FDIA detection. Therefore, the integrity and reliability of the proposed detection mechanism remain unaffected under these disturbance conditions.

Since both the GUIO and GOS observers have successfully passed the robustness test under disturbance conditions, the FDIA scenarios will be analyzed under the same

disturbance configuration used previously. In other words, a step disturbance with an amplitude of 0.1 will be applied to ΔP_{d2} at the $t = 2$ moment, while no disturbance will be introduced to ΔP_{d1}. Under this condition, various FDIAs will be implemented to evaluate the detection capabilities of the observer schemes.

In this case, an FDIA is applied to the first sensor Δf_1 at the 5th second in the form of a unit step signal with an amplitude of 0.1. The purpose is to observe how each observer structure GUIO, GOS, and DOS responds to this targeted cyber attack and whether the resulting residuals can reflect the anomaly clearly and effectively.

As shown in Figure 5.6 the GUIO structure, the attack is clearly detected. The injected FDIA appears almost identically in the residuals, with a magnitude around the order of 10^{-3}, matching the amplitude of the applied signal. This shows that the GUIO can effectively detect the attack without significant distortion or delay.

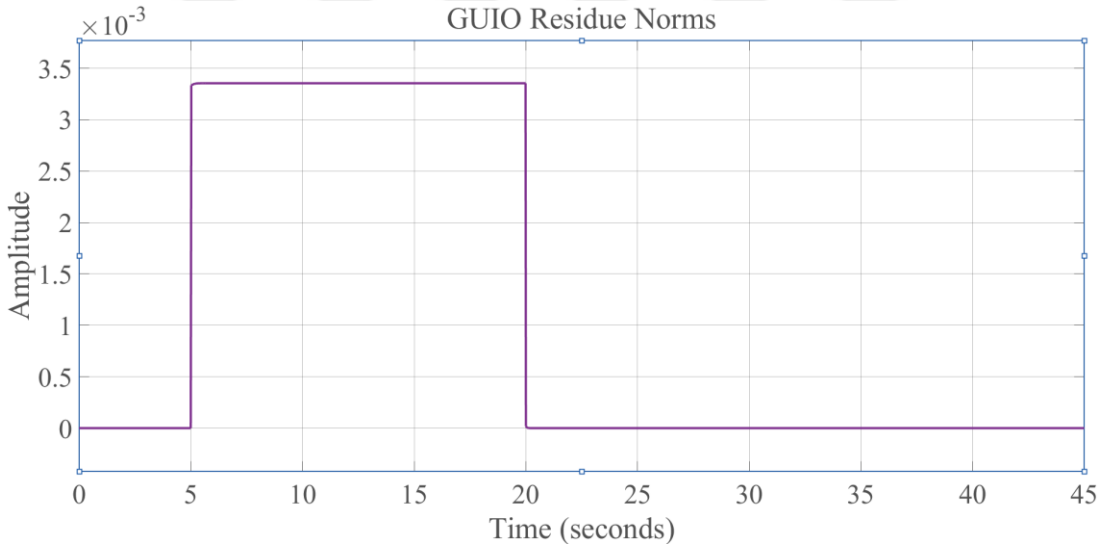

Figure 5.6 : Residual norms of GUIO under an FDIA (unit step with amplitude 0.1) on sensor 1.

Figure 5.7 shows the norms of the residuals from the GOS observers under the same FDIA. As seen in the figure, the observers assigned to the sensors that are not under attack behave very similarly to the GUIO, which is exactly what we expect. On the other hand, the observer associated with the attacked sensor does not demonstrate any noticeable change. This is actually the expected behavior from the GOS structure. Since the attacked sensor is excluded from that particular observer's input, the residual stays unaffected. However, the other observers, which still include the attacked sensor do react. This allows us to pinpoint the location of the attack by checking which

observer did not detect anything indicating that its corresponding sensor is the one under attack.

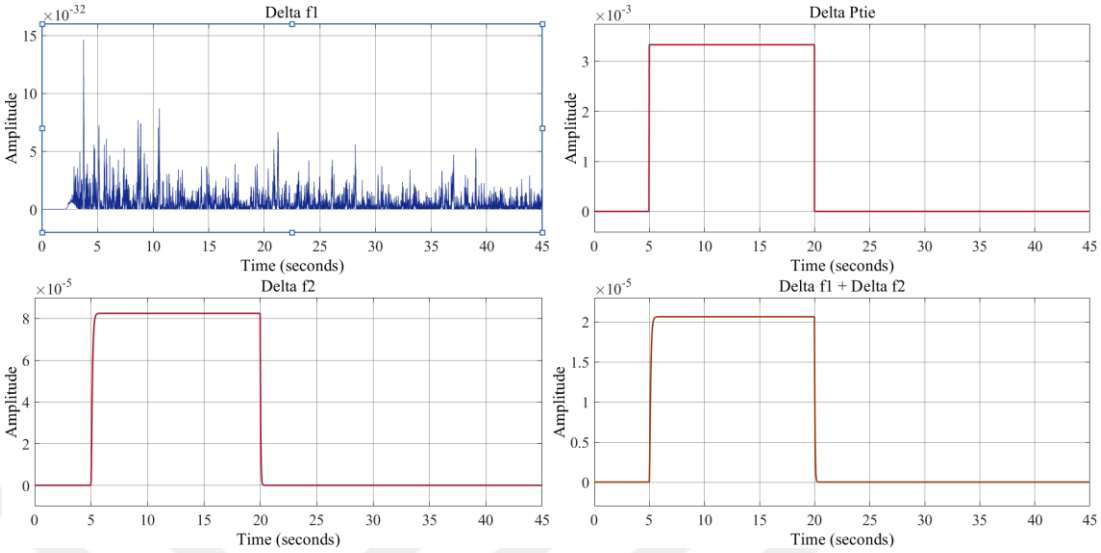

Figure 5.7 : Residual norms of GOS observers under an FDIA (unit step with amplitude 0.1) on sensor 1.

Due to the inherent limitations of the DOS architecture, this structure is excluded from the remaining analyses. As shown in Figure 5.8, the first and second observers in the DOS scheme fail to generate any meaningful residual signals, indicating a lack of sensitivity to the sensor anomalies under investigation. This inefficacy stems from the fact that the DOS observers do not fulfill the necessary design requirements outlined in section 3 and visualized in Figure 3.3. Specifically, the rank condition required for observability is not satisfied for the subsystems monitored by the DOS observers.

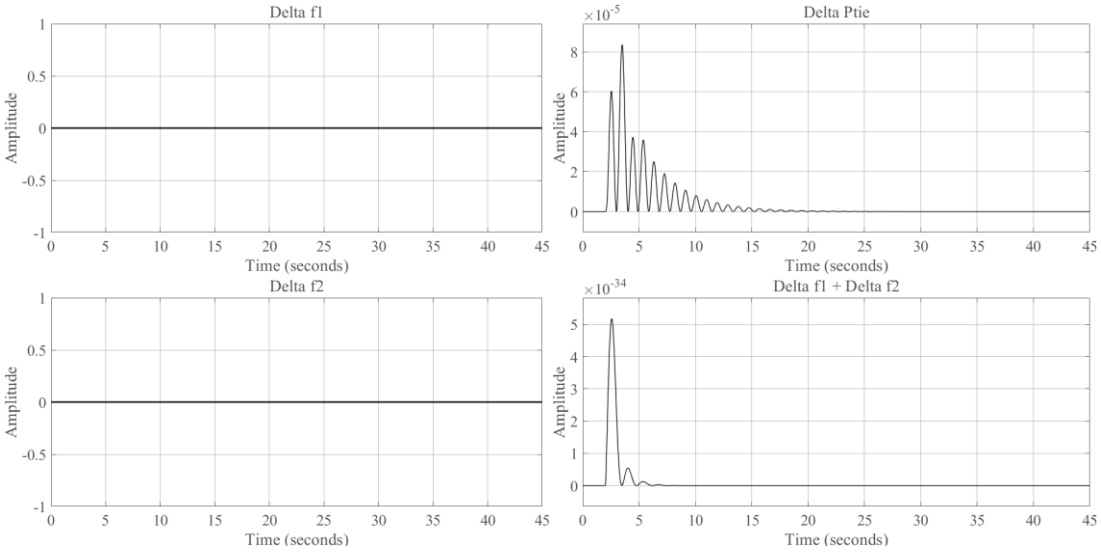

Figure 5.8 : Residual norms of DOS observers under an FDIA (unit step with amplitude 0.1) on sensor 1.

Although one might consider increasing the number of outputs by expanding the overall C matrix, such an adjustment proves ineffective in the DOS framework. Each observer in this scheme utilizes only a single-row output matrix c_j, and thus the individual observability properties of the observers remain unchanged regardless of the global output configuration. Consequently, the DOS structure fails to achieve the observability conditions necessary for UIO design, rendering it unsuitable for the current two-area LFC system.

In this scenario, the objective is to evaluate the sensitivity and effectiveness of the observer-based detection mechanism against low-magnitude cyberattacks. While a unit step FDIA with an amplitude of 0.1 was successfully identified in previous simulations, it is essential to investigate whether the same approach remains effective for much smaller disturbances.

To this end, an FDIA with a very small amplitude of 10^{-12} is injected into the Δf_2 sensor between 10 and 15 seconds. By analyzing the residual signals generated during this time window, the ability of the observers to detect such a subtle and short-duration intrusion is examined.

As illustrated in Figures 5.9 and 5.10, both the GUIO and the GOS demonstrate a remarkable sensitivity in detecting FDIAs, even when the injected data has an amplitude as low as 10^{-12}. Although such a signal is almost negligible in terms of its physical influence on the power system, the residuals generated by GUIO clearly indicate the presence of an abnormal condition. Moreover, the GOS structure enables the precise localization of the attack: while the observer associated with the compromised sensor remains unaffected due to its design, the remaining observers generate distinguishable residuals, allowing for accurate identification of the attacked sensor.

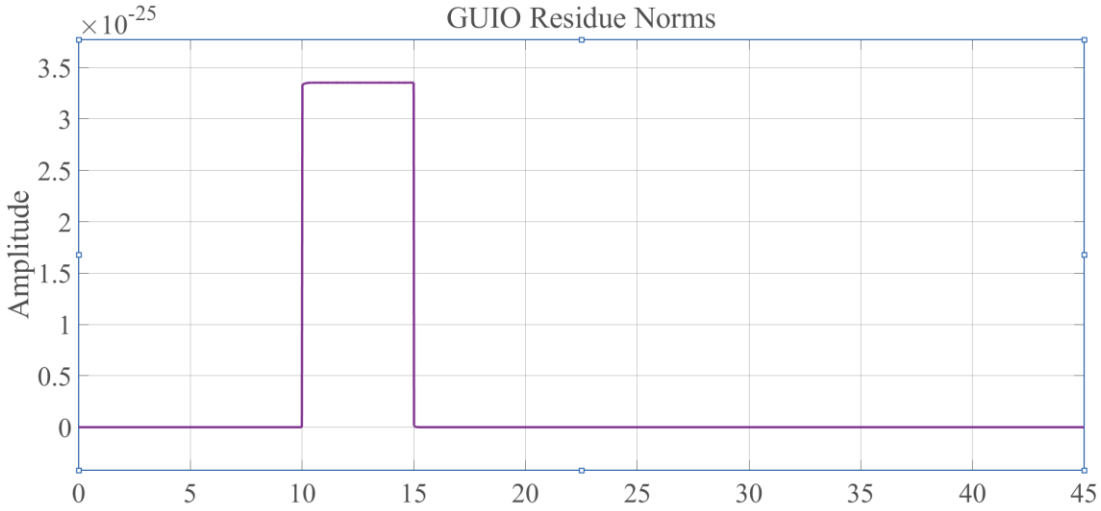

Figure 5.9 : Residual norms of GUIO under an FDIA (unit step with amplitude 1×10^{-12}) on sensor 2.

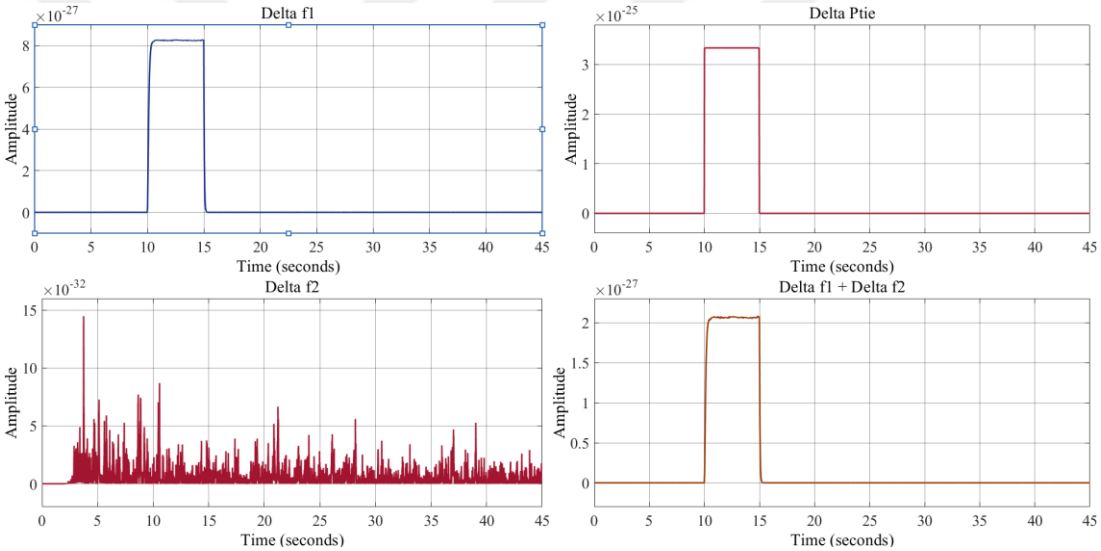

Figure 5.10 : Residual norms of GOS observers under an FDIA (unit step with amplitude 1×10^{-12}) on sensor 2.

These results confirm that the proposed observer-based framework is not only robust under normal operating disturbances but also highly sensitive to even extremely subtle cyberattacks.

In the following simulation, a sequence of false data injection attacks (FDIAs) is applied to each of the four sensors at different time intervals within a single run. The goal is to evaluate the performance of the observer-based detection framework in identifying and localizing attacks occurring at various times and across different sensors.

Specifically, a unit step FDIA (amplitude of 1) is injected into:

- Sensor 1 between 5 and 10 seconds,
- Sensor 2 between 15 and 20 seconds,
- Sensor 3 between 25 and 30 seconds,
- Sensor 4 between 35 and 40 seconds.

By analyzing the residual outputs of the observers during these intervals, we aim to verify whether the GUIO can consistently detect each attack and whether the GOS structure can accurately isolate which sensor is under attack at each stage.

In this scenario, the residual responses corresponding to the sequential FDIAs applied to each sensor reveal an important observation. As shown in Figure 5.11 and 5.12, except for the attack targeting the third sensor (ΔP_{tie}), the observer residuals for the other sensors exhibit similar behaviors in response to the injected attacks. However, since ΔP_{tie} inherently represents a derivative-related signal, the FDIA in unit step form applied to this sensor induces sharp transient responses at the moments of activation and deactivation resembling dirac function impulses.

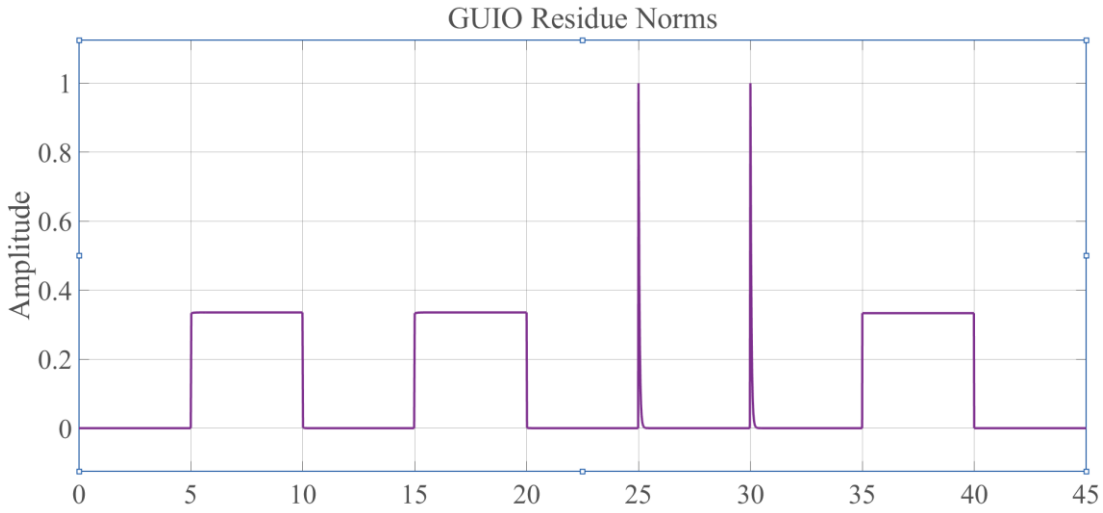

Figure 5.11 : Residual norms of GUIO under sequential single-sensor FDIAs (unit step with amplitude 1) on all sensors.

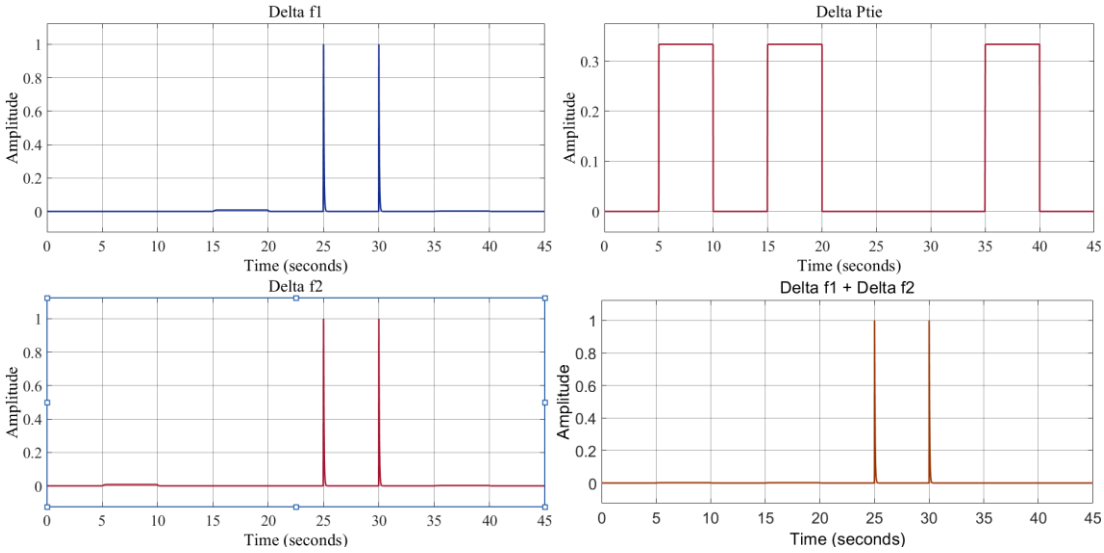

Figure 5.12 : Residual norms of GOS under sequential single-sensor FDIAs (unit step with amplitude 1) on all sensors.

Due to the significantly higher amplitude of these transient spikes, the residual signal associated with sensor 3 dominates the overall residual response. As a result, the residual signals generated by attacks on sensors 1, 2, and 4 become comparatively less distinguishable. Despite this, the attack intervals can still be inferred from the behavior of the sensor 3 observer, whose residual output reacts clearly at each attack instance.

This issue can be solved in practice by introducing thresholding logic or comparator circuits to normalize and filter the residual responses. To better visualize the detection capability across all sensors, the FDIA amplitude applied to sensor 3 is reduced to 0.1 in the following simulation, while the same attack amplitudes are preserved for the remaining sensors. The attack sequence is then re-applied to evaluate the detection clarity under more balanced residual magnitudes.

When the FDIAs are applied in this manner using unit step signals with amplitude 1 for all sensors except the third, which receives an injection with amplitude 0.1 as shown in Figure 5.13 they become clearly distinguishable in the residual norm plots. Although the previous simulation already demonstrated that the observer structure was capable of detecting all attacks, the visual distinction of some attacks was limited due to the dominant residual generated by the third sensor. With the reduced amplitude, the visibility of all injected attacks in the residuals has improved.

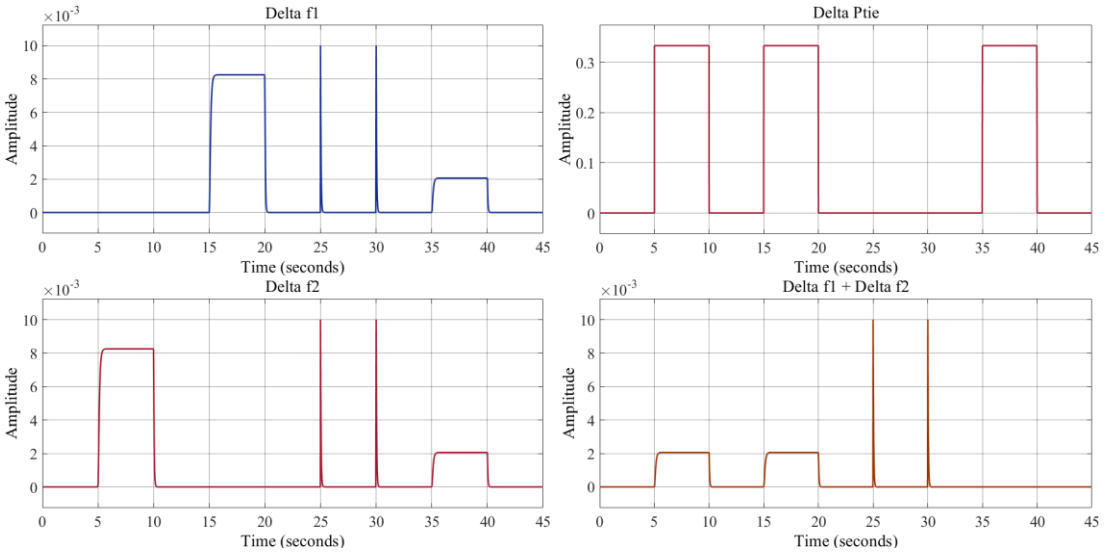

Figure 5.13 : Residual norms of GOS under sequential single-sensor FDIAs (unit step, amplitude 1; amplitude 0.1 for sensor 3).

To further evaluate the detection capability of the observer structure under more dynamic and different attack scenarios, the same sequence of FDIAs is now applied using sinusoidal bias signals instead of unit steps. Each sensor is targeted in the same time intervals as before: sensor 1 between 5–10 seconds, sensor 2 between 15–20 seconds, sensor 3 between 25–30 seconds, and sensor 4 between 35–40 seconds.

In this setup, sinusoidal false data injections with a frequency of 1 Hz and an amplitude of 1 are applied to all sensors except the third. For sensor 3, the attack signal is also sinusoidal with a frequency of 1 Hz, but its amplitude is reduced to 0.1 in order to prevent its dominant residual response from masking the effects of the other attacks. This adjustment helps to better visualize and assess the residual responses of all GOS observers and ensures a more balanced evaluation of the scheme's sensitivity to subtle attack signatures across different sensors.

In contrast to previous cases where unit step FDIAs were applied, the residual signals generated by the sinusoidal attacks in this scenario exhibit a markedly different behavior. As shown in Figure 5.14, the false data injections applied to each sensor appear as smooth sinusoidal waveforms in the output signals, clearly reflecting the nature of the injected disturbances.

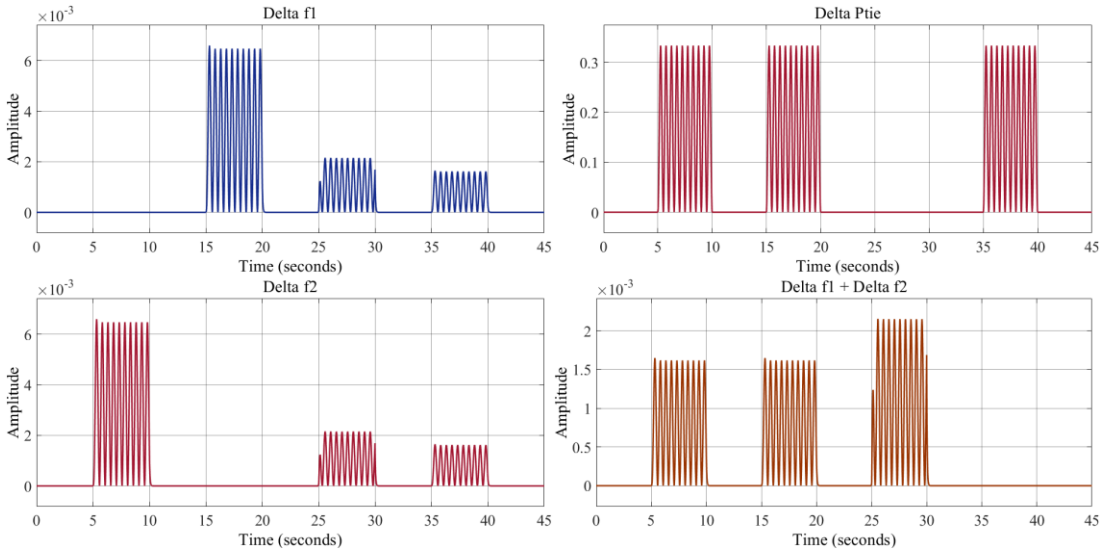

Figure 5.14 : Residual norms of GOS under sequential single-sensor sinusoidal FDIAs (1 Hz, amplitude 1; amplitude 0.1 for sensor 3).

Notably, the third sensor (ΔP_{tie}), which previously responded with sharp spikes only at the onset and termination of step-based attacks due to its derivative-dependent structure, now exhibits a full sinusoidal pattern throughout the attack interval. This outcome is entirely expected, as the derivative of a sinusoidal function is itself a sinusoidal function.

As demonstrated in the previous scenario, the observer structure is capable of clearly detecting FDIA signals regardless of changes in their shape or amplitude. Even when the injected datas are sinusoidal and of relatively low magnitude, the generated residuals effectively reflect the presence of anomalies in the corresponding sensors.

In the next experiment, we extend the analysis to evaluate how the observer-based detection mechanism responds when multiple sensors are attacked simultaneously. Specifically, an FDIA with an amplitude of 1 is applied to sensor 1 during the interval from 5 to 20 seconds, while another FDIA of equal amplitude is injected into sensor 2 between 10 and 15 seconds. This setup allows us to observe how the residual responses evolve when two different sensors are compromised within overlapping time frames, and whether the observers can still isolate and detect each anomaly accurately.

Figure 5.15 illustrates the residual signals of the GOS observers under a multiple FDIA scenario. A unit step FDIA with an amplitude of 1 is injected into sensor 1 between 5 and 20 seconds, and another attack with the same amplitude is applied to sensor 2 between 10 and 15 seconds. No attack is introduced to sensors 3 and 4. The visualized

signals reflect the cumulative effects of these attacks, with noticeable deviations in both individual sensor channels and the combined $\Delta f_1 + \Delta f_2$ measurement. The overlapping time interval (10–15 seconds) allows for observing the system's behavior under simultaneous compromise of multiple sensor nodes.

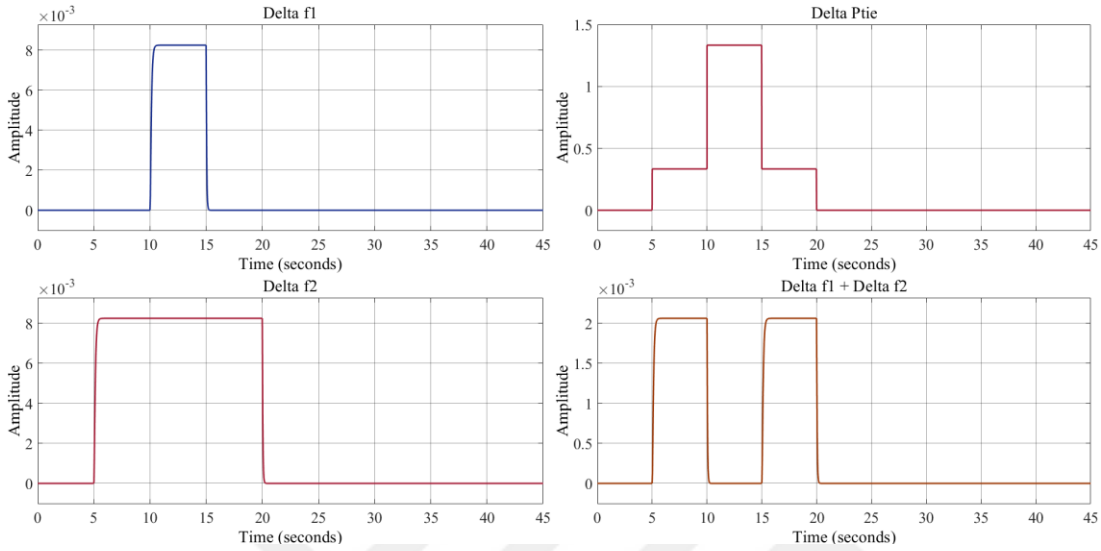

Figure 5.15 : Residual norms of GOS under multiple FDIAs (unit step with amplitude 1) on sensors 1 and 2.

The GOS operates by constructing each observer to monitor the system using all sensor outputs except one. In this way, fault or attack isolation is achieved based on the principle of insensitivity: when an anomaly occurs, the residual of the observer that excludes the compromised sensor remains unaffected, while others show significant deviations. This allows for identifying the attacked sensor by detecting which residual signal remains stable.

However, in cases where multiple sensors are simultaneously compromised, this insensitivity-based strategy becomes less effective. Since each observer omits only one sensor and includes the rest, if more than one sensor is under attack, none of the observers remain fully insulated from the compromised measurements. As a result, all residuals tend to deviate, and it becomes difficult to identify exactly which sensors are under attack.

This behavior is clearly illustrated in Figure 5.16, where overlapping FDIA scenarios lead to complex residual outputs. While the GOS structure still successfully detects the presence of anomalies under multiple attacks, a different observer scheme or extended framework is needed to achieve accurate isolation in such scenarios.

6. CONCLUSIONS AND RECOMMENDATIONS

6.1 Conclusion

In this study, a comprehensive simulation analysis was conducted to evaluate the performance of observer-based detection schemes against FDIAs targeting sensor measurements in a two-area LFC system. The primary focus was on the application of UIO-based methods, particularly the GOS and the DOS, which were initially designed for fault detection in control systems.

The DOS which employs an individual observer for each sensor using only that sensor's output, proved ineffective for the tested system. This ineffectiveness stems from the fact that DOS observers fail to meet the necessary observability conditions required for UIO design. Particularly for critical system states like frequency deviations (Δf_1 and Δf_2), the observers could not produce meaningful residuals, effectively rendering them blind to injected anomalies. Attempts to increase observability by expanding the C matrix also failed because each observer in DOS still operates on a single-row output matrix. Consequently, the DOS structure was categorized under "UIO does not exist" and excluded from further analysis. Its poor performance highlights the importance of structural observability in multi-variable control systems and the limitations of overly simplified observer assignments.

In contrast, the GUIO demonstrated excellent robustness under various disturbance conditions, including different load demand shapes in two areas. The GUIO consistently produced residuals in the order of 10^{-32} when no attack was present, and successfully detected FDIAs even when the injected signal amplitude was as small as 10^{-12}. These findings confirm that GUIO is highly sensitive and reliable for detecting subtle, stealthy cyber threats without generating false alarms under normal operating disturbances.

The GOS composed of multiple UIOs where each observer excludes one sensor from its input, provided an effective solution not only for detecting but also isolating FDIA incidents. In single-sensor attack scenarios, the GOS allowed accurate identification

of the compromised sensor based on which observer's residual remained unchanged. Furthermore, even when the attack signal's shape was modified from step to sinusoidal the GOS structure continued to perform well in localizing and detecting the intrusions.

However, the isolation capability of GOS is compromised under simultaneous multi-sensor attack scenarios. Since each observer includes all but one sensor, the residuals become interdependent when multiple sensors are corrupted simultaneously. In such cases, none of the observers remains completely insulated from the attack, leading to ambiguous residual outputs that hinder precise localization. Although the detection of an anomaly is still successful, the source of the attack becomes harder to identify. This limitation suggests the necessity of alternative observer architectures or extended framework for improved isolation in more complex threat environments.

It is also worth emphasizing that in the case of simultaneous multi-sensor attacks, precisely identifying which specific sensors have been compromised may not always be of primary importance. If the attacker has already gained access to manipulate multiple sensor channels, it implies a significant security breach within the system. In such a scenario, the priority should shift from detailed isolation toward immediate mitigation, such as revoking access, reconfiguring network privileges, or initiating predefined cyber-defense protocols. Therefore, the primary goal becomes the rapid detection of the presence of a coordinated attack, rather than an exact localization of every compromised node.

In conclusion, this study has demonstrated the potential of adapting fault detection observers as cybersecurity tools in power systems, validating their performance through various practical FDIA conditions. While current implementations effectively detect and isolate single-sensor attacks, further improvements are necessary to extend their applicability to more complex and coordinated cyberattack scenarios, as outlined in the following section.

6.2 Future Work

This study demonstrated that observer-based residual generation methods, originally developed for fault detection, can be effectively adapted for identifying FDIA-type cyber threats targeting sensor measurements in LFC systems. In particular, the GOS

structure not only detects the presence of an attack but also successfully identifies which specific sensor has been targeted, assuming only one is affected.

However, in realistic scenarios where multiple sensors may be simultaneously targeted, the current scheme struggles to maintain accurate isolation. Therefore, one key direction for future research is the development of an extended observer framework that can detect multiple concurrent sensor attacks and still determine which specific sensors are under attack. This may involve designing logic-based diagnostic layers or utilizing redundant observer networks that allow cross-verification among residuals, even in multi-fault conditions.

Beyond simply detecting and localizing attacks, future studies could focus on estimating the characteristics of the injected false data such as its amplitude, duration, and waveform. By identifying these features, it would be possible to reconstruct the original, unaffected sensor signal or apply real-time filtering to cancel out the malicious interference. In this way, the system would not just recognize that an attack has occurred, but could actively respond to it by restoring clean data for control processes. This is particularly valuable in load-frequency control applications, where even small disruptions in measurement signals can lead to larger imbalances across the grid.

Finally, combining model-based observer methods with data-driven techniques such as machine learning could increase detection accuracy and reduce false alarms. Such hybrid approaches could offer more flexible and reliable cyber defense solutions for future smart grids.

REFERENCES

[1] **J. Chen and R. J. Patton,** *Robust Model-Based Fault Diagnosis for Dynamic Systems*, Springer, 1999.

[2] **S. X. Ding,** *Model-Based Fault Diagnosis Techniques: Design Schemes, Algorithms, and Tools*, Springer, 2008.

[3] **F. Çalışkan and İ. Genç,** "A robust fault detection and isolation method in load frequency control loops," *IEEE Trans. Power Syst.*, vol. 23, no. 4, pp. 1756–1767, Nov. 2008, doi:10.1109/TPWRS.2008.2004831.

[4] **Y. Liu, P. Ning, and M. K. Reiter,** "False data injection attacks against state estimation in electric power grids," in *Proc. 16th ACM Conf. Computer and Communications Security*, 2009, pp. 21–32.

[5] **A. Teixeira, H. Sandberg, and K. H. Johansson,** "Cyber security of SCADA systems — A survey," *IFAC Proc. Volumes*, vol. 45, no. 22, pp. 1124–1131, 2012.

[6] **F. Pasqualetti, F. Dörfler, and F. Bullo,** "Attack detection and identification in cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 58, no. 11, pp. 2715–2729, Nov. 2013, doi:10.1109/TAC.2013.2266831.

[7] **J. Giraldo *et al.*,** "A survey of physics-based attack detection in cyber-physical systems," *ACM Comput. Surveys*, vol. 51, no. 4, art. 76, 2018, doi:10.1145/3203245.

[8] **P. Kundur,** *Power System Stability and Control*, New York, NY, USA: McGraw-Hill, 1994, Bölüm 11, ss. 581–691.

[9] **R. DiPippo,** *Geothermal Power Plants: Principles, Applications and Case Studies*, 1st ed., Elsevier Science, 2005.

[10] **S. A. Kamilu and H.-P. Beck,** "Steady-state operating points of islanded virtual synchronous machine-based microgrids: closed-form fundamental-frequency models," *Energy Sci. Eng.*, vol. 11, no. 2, pp. 342–355, 2024, doi: 10.1002/ese3.1739.

[11] **T. Ackermann,** *Wind Power in Power Systems*, Wiley, 2012.

[12] **R. DiPippo,** *Geothermal Power Plants: Principles, Applications and Case Studies*, 2nd ed., Butterworth-Heinemann, 2008.

[13] **S. J. Chapman,** *Elektrik Makinalarının Temelleri*, 5. Baskı, İstanbul, Türkiye: Çağlayan Kitap & Yayıncılık & Eğitim, Bölüm 5, pp. 267–345.

[14] **A. Demirören and L. Zeynelgil**, *Elektrik Enerji Sistemlerinin Kararlılığı: Kontrolü ve Çalışması*, Birsen Yayınevi, Bölüm 6, pp. 163–203, 2004.

[15] **S. Hui and S. H. Zak**, "Observer design for systems with unknown inputs," *Int. J. Appl. Math. Comput. Sci.*, vol. 15, no. 4, pp. 431–444, 2005.

[16] **R. Isermann**, "Model-based fault-detection and diagnosis — Status and applications," *Annu. Rev. Control*, vol. 29, no. 1, pp. 71–85, 2005, doi: 10.1016/j.arcontrol.2004.12.002.

[17] **R. N. Clark**, "A simplified instrument detection scheme," *IEEE Trans. Aerospace Electron. Syst.*, vol. 14, pp. 456–465, 1978.

[18] **P. M. Frank**, "Fault diagnosis in dynamic systems via state estimation — A survey," in *System Fault Diagnostics,* S. Tzafestas *et al.* (Eds.), Dr. Reidel Publ. Comp., Dordrecht, pp. 35–98, 1987.

[19] **D. Maquin,** "On the unknown input observer design: A decoupling-class approach with application to sensor fault diagnosis," in *Proc. 1st Int. Conf. Automation and Mechatronics (CIAM'2011)*, 2011.

[20] **K. Adjallah, D. Maquin, and J. Ragot**, "Non-linear observer-based fault detection," in *Proc. 3rd IEEE Conf. Control Applications (CCA'94)*, Glasgow, 1994, pp. 1115–1120.

CURRICULUM VITAE

Name Surname : Arslan Mete BAYBARS

EDUCATION :

- **B.Sc. :** 2020, Atatürk University, Engineering Faculty, Electrical and Electronics Engineering Department

PROFESSIONAL EXPERIENCE AND REWARDS:

- 2020 - 2022 İM Mühendislik İnşaat Taahhüt Ltd. Şti. – Site Electrical Engineer *Participated in the 154 kV Yeniçates–Bartın high-voltage transmission line renovation project.*
- 2024 – İstanbul Technical University, Research Assistant.

PUBLICATIONS, PRESENTATIONS AND PATENTS ON THE THESIS:

- **Baybars A. M.,** Caliskan F., Genc V. M. I, 2025: Adaptation of a Generalized Observer Scheme for False Data Injection Detection in Load Frequency Control Systems. *IGRS 2025 | 4th International Graduate Research Symposium*, May 12-14, 2025 İstanbul, Turkey.