ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΗΛΕΚΤΡΙΚΗΣ ΙΣΧΥΟΣ

Ανάλυση κυβερνοεπιθέσεων έγχυσης ψευδών δεδομένων στα συστήματα ρύθμισης φορτίου – συχνότητας και μελέτη ανίχνευσής τους μέσω παρατηρητή Luenberger

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Χρονόπουλος Γεώργιος

Επιβλέπων : Νικόλαος Χατζηαργυρίου
Καθηγητής Ε.Μ.Π.

Αθήνα, Οκτώβριος 2022

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΗΛΕΚΤΡΙΚΗΣ ΙΣΧΥΟΣ

Ανάλυση κυβερνοεπιθέσεων έγχυσης ψευδών δεδομένων στα συστήματα ρύθμισης φορτίου – συχνότητας και μελέτη ανίχνευσής τους μέσω παρατηρητών Luenberger

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Χρονόπουλος Γεώργιος

Επιβλέπων : Νικόλαος Χατζηαργυρίου
Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 19η Οκτωβρίου 2022.

.....	.....	……..
Νικόλαος Χατζηαργυρίου	Γεώργιος Κορρές	Παύλος Γεωργιλάκης
Καθηγητής Ε.Μ.Π	Καθηγητής Ε.Μ.Π	Αν. Καθηγητής Ε.Μ.Π

Αθήνα, Οκτώβριος 2022

.....

Χρονόπουλος Γεώργιος

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Ευχαριστίες

Με την υλοποίηση της παρούσας διπλωματικής εργασίας κλείνει ο κύκλος σπουδών μου στη σχολή Ηλεκτρολόγων Μηχανικών & Μηχανικών Υπολογιστών του Εθνικού Μετσόβιου Πολυτεχνείου και ολοκληρώνεται ένα ταξίδι γεμάτο προκλήσεις, προσπάθεια και αποτυχίες που έκαναν τις επιτυχίες και τις χαρές πιο όμορφες και πιο απολαυστικές.

Απόλυτο στήριγμά μου σε αυτό το ταξίδι αποτέλεσε η οικογένειά μου, ο πατέρας μου Βασίλης, η μητέρα μου Ρίτσα και η αδελφή μου Δήμητρα που με την αγάπη, τη στήριξη και τη συμπαράστασή τους σε όλα τα χρόνια των σπουδών μου, βοήθησαν τα μέγιστα ώστε να ολοκληρώσω τις σπουδές μου. Χωρίς αυτούς δε θα είχα καταφέρει όσα ήθελα και γι' αυτό τους ευχαριστώ θερμά.

Θα ήθελα στο σημείο αυτό να ευχαριστήσω πολύ τον επιβλέποντα της διπλωματικής μου εργασίας κ. Νικόλαο Χατζηαργυρίου για την ευκαιρία που μου έδωσε να προσεγγίσω ένα ιδιαίτερα ενδιαφέρον για μένα σύγχρονο πρόβλημα της επιστήμης του ηλεκτρολόγου μηχανικού και να το μελετήσω σε βάθος. Θα ήθελα επίσης να ευχαριστήσω και τον μεταπτυχιακό ερευνητή και υποψήφιο διδάκτορα Ανδρέα – Θεόδωρο Συρμακέση, συνεπιβλέποντα της διπλωματικής μου, που με τη συνεισφορά και τις υποδείξεις του συνέβαλε στην διαμόρφωση και την ολοκλήρωση της εργασίας μου.

Τέλος θα ήθελα να ευχαριστήσω τους φίλους μου Γιώργο, Φαίη, Χρήστο, Αλέξανδρο και Κωνσταντίνο για την αμέριστη συμπαράστασή τους καθ' όλη τη διάρκεια των σπουδών μου όπως επίσης τους συμφοιτητές και πλέον συναδέλφους μου Δημήτρη και Χάρη, τόσο για την ηθική υποστήριξη μέχρι το τέλος, όσο και για τις ατέλειωτες ώρες διαβάσματος που μοιραστήκαμε.

Γεώργιος Χρονόπουλος,

Οκτώβριος 2022

Περίληψη

Τα συστήματα ηλεκτρικής ενέργειας είναι πολύπλοκα συστήματα, τεράστιας σημασίας για όλον τον πλανήτη, καθώς ο κόσμος βασίζει την καθημερινότητά του στην τροφοδοσία ηλεκτρικής ισχύος. Για την ομαλή και ευσταθή λειτουργία των συστημάτων ισχύος, απαιτούνται αρκετές τεχνικές προστασίας και ελέγχου. Μεταξύ των διαφόρων ελέγχων, η ρύθμιση φορτίου - συχνότητας που απαιτείται για την ευστάθεια της συχνότητας είναι ένας σύνθετος μηχανισμός ελέγχου που περιλαμβάνει συνεργασία μηχανικών μερών με πληροφοριακά και τηλεπικοινωνιακά συστήματα. Καθώς οι αλγόριθμοι ελέγχου της σταθεροποίησης συχνότητας παρέχουν σήματα ελέγχου σε χρονική κλίμακα δευτερολέπτων, τα συστήματα ρύθμισης φορτίου - συχνότητας (LFC) δεν μπορούν να χειριστούν πολύπλοκους αλγόριθμους ελέγχου. Το γεγονός αυτό σε συνδυασμό με την πληθώρα καναλιών επικοινωνίας και ψηφιακών συστημάτων που διαθέτουν τα συστήματα αυτά, τα καθιστούν πιο ευάλωτα σε διαταραχές και επιθέσεις στον κυβερνοχώρο. Στο πλαίσιο αυτό, στην παρούσα εργασία μελετάται το σύστημα ρύθμισης φορτίου συχνότητας και πιθανά ευπαθή σημεία του σε επιθέσεις, καθώς και ο αντίκτυπος των επιθέσεων αυτών. Ακόμη μελετάται η ανίχνευση των παραπάνω επιθέσεων μέσω ενός παρατηρητή Luenberger και εξάγονται συμπεράσματα για όλα τα παραπάνω. Πιο συγκεκριμένα αρχικά παρουσιάζεται η δομή των συστημάτων ενέργειας και τα ευπαθή σε κυβερνοεπιθέσεις σημεία τους. Στη συνέχεια γίνεται αναλυτική περιγραφή και μοντελοποίηση του συστήματος ρύθμισης φορτίου - συχνότητας μίας και δύο περιοχών καθώς και των μεθόδων ελέγχου του, παρουσιάζονται η κυβερνοασφάλεια και οι κυβερνοεπιθέσεις σε αυτό και πραγματοποιούνται οι μαθηματικές μοντελοποιήσεις των επιθέσεων έγχυσης ψευδών δεδομένων στα παραπάνω συστήματα. Αμέσως μετά περιγράφονται οι παρατηρητές κατάστασης, παρουσιάζονται μέθοδοι ανίχνευσης κυβερνοεπιθέσεων και μοντελοποιείται η μέθοδος ανίχνευσης κυβερνοεπιθέσεων σε LFC συστήματα μιας και δύο περιοχών μέσω του παρατηρητή Luenberger. Έπειτα γίνονται προσομοιώσεις λειτουργίας του συστήματος ρύθμισης φορτίου – συχνότητας μιας και δύο περιοχών υπό την επίδραση διαταραχών, επιθέσεων έγχυσης ψευδών δεομένων και μελετάται τόσο ο αντίκτυπος των κυβερνοεπιθέσεων όσο και η ικανότητα του παρατηρητή Luenberger να τις ανιχνεύσει και να τις ξεχωρίσει σε σχέση με τις μεταβολές φορτίου. Τέλος εξάγονται τα τελικά συμπεράσματα της εργασίας και προτείνονται ιδέες για περαιτέρω ερεύνα και ανάλυση.

Λέξεις Κλειδιά

Ευστάθεια Συστήματος Ηλεκτρικής Ενέργειας, Αυτόματος Έλεγχος Παραγωγής, Ρύθμιση Φορτίου – Συχνότητας, Κυβερνοασφάλεια, Κυβερνοεπιθέσεις, Διασυνδεδεμένο Δίκτυο Ισχύος, Επιθέσεις Έγχυσης Ψευδών Δεδομένων, Παρατηρητές Κατάστασης, Παρατηρητής Luenberger, Ανίχνευση, Προσομοιώσεις.

Abstract

Power systems are complex systems that are of great importance to the entire planet, since the world relies on the supply of electric power for day-to-day life. For the smooth and stable operation of power systems, several protection and control techniques are necessary. Among the various controls, load frequency control, which is responsible for frequency stability, is a complex control mechanism which involves cooperation of mechanical parts with information and telecommunication systems. As frequency stabilization control algorithms provide control signals on a time scale of seconds, load-frequency control (LFC) systems cannot handle complex control algorithms. In addition to this, the complexity of communication channels and digital layers that these systems have, make them more vulnerable to disruptions and cyber-attacks. This thesis investigates the load frequency control system and its possible vulnerabilities to attacks, as well as the impact of these attacks. The detection of the attacks, described above, through a Luenberger observer is also being studied and therefore conclusions are drawn for all the above. More specifically, at first, the structure of power systems and the identification of attack points are presented. Then, the single and two-area load frequency control system and its control methods are described and modeled, cyber-security and cyber-attacks on it are presented, and false data injection attacks on single and two-area LFC systems are modeled too. Right after that, state observers are described, cyberattack detection methods are presented, and the cyberattack detection method in single and two-area LFC systems is modeled with the contribution of Luenberger observer. Then single and two-area LFC simulation results under load disturbances and false data injection attacks are carried out, and both the impact of cyber-attacks and the ability of the Luenberger observer to detect and distinguish them from load disturbances are studied. Finally, the final conclusions of this thesis are drawn and ideas for further research and analysis are proposed.

Key Words

Power System Stability, Automatic Generation Control, Load Frequency Control, Cyber-security, Cyber-attacks, Interconnected Power Grid, False Data Injection Attacks, State Observers, Luenberger Observer, Detection, Simulations.

Πίνακας περιεχομένων

1. Εισαγωγή 19

1.1. Συστήματα Ηλεκτρικής Ενέργειας 19

1.1.1. Ευσταθής Λειτουργεία ΣΗΕ 20

1.1.2. Δομή Ελέγχου Συστημάτων Ηλεκτρικής Ενέργειας 22

1.2. Κυβερνοασφάλεια και Ευπαθή Σημεία Συστημάτων Ηλεκτρικής Ενέργειας 33

1.2.1. Κυβερνοασφάλεια στα Συστήματα Ηλεκτρικής Ενέργειας 33

1.2.2. Ευπαθή Σημεία στα Συστήματα Ηλεκτρικής Ενέργειας 34

2. Μαθηματική μοντελοποίηση συστήματος ρύθμισης φορτίου συχνότητας ... 42

2.1. Μοντελοποίηση των στοιχείων των Συστημάτων Ισχύος 42

2.1.1. Μοντέλο Ρυθμιστή Στροφών (Governor) 43

2.1.2. Μοντέλο Στροβίλου (Turbine) 43

2.1.3. Μοντέλο Γεννήτριας (Generator) 44

2.1.4. Μοντέλο Φορτίου (Load) 45

2.2. Ανάλυση Ρύθμισης Φορτίου – Συχνότητας μέσω Συμβατικού Ελεγκτή 46

2.2.1. Μαθηματική Μοντελοποίηση Απομονωμένου Συστήματος LFC (Διάγραμμα Βαθμίδων) 46

2.2.2. Μαθηματική Μοντελοποίηση Συστήματος LFC Πολλαπλών Περιοχών (Διάγραμμα Βαθμίδων) 47

2.3. Ανάλυση Ρύθμισης Φορτίου – Συχνότητας στο Χώρο Κατάστασης (State Space Analysis) 52

2.3.1. Μοντελοποίηση στο χώρο κατάστασης απομονωμένου συστήματος Ρύθμισης Φορτίου – Συχνότητας (Single Area LFC) 53

2.3.2. Μοντελοποίηση στο χώρο κατάστασης συστήματος Ρύθμισης Φορτίου – Συχνότητας Δύο Περιοχών (Two Area LFC) 54

2.4. Μέθοδοι Ελέγχου στη Ρύθμιση Φορτίου – Συχνότητας 57

2.4.1. Συμβατικός Ολοκληρωτικός Ελεγκτής (Integral), PI και PID 58

2.4.2. Τεχνική Τοποθέτησης Πόλων 60

2.4.3. Βέλτιστος Έλεγχος (μέσω της μεθόδου Γραμμικού Τετραγωνικού Ρυθμιστή (LQR)) 61

2.5. Μοντέλο Προσομοιόσεων συστήματος Ρύθμισης Φορτίου – Συχνότητας Απομονωμένης Περιοχής (Single Area) με προσθήκη ελεγκτή 63

2.6. Μοντελο Προσομοιώσεων συστήματος Ρύθμισης Φορτίου - Συχνότητας Δύο Περιοχών (Two Area LFC) με προσθήκη ελεγκτή 64

3. Κυβερνοεπιθέσεις και Κυβερνοασφάλεια στο Σύστημα Ρύθμισης Φορτίου – Συχνότητας 65

3.1. Ευπαθή Σημεία στα Συστήματα Ρύθμισης Φορτίου – Συχνότητας..... 66

3.1.1. Ευπαθή σημεία συστημάτων ρύθμισης φορτίου – συχνότητας σε απομονωμένα συστήματα ισχύος (Single Area LFC)..... 66

3.1.2. Ευπαθή σημεία συστημάτων ρύθμισης φορτίου – συχνότητας σε διασυνδεδεμένα συστήματα ισχύος (Multi Area LFC)..... 66

3.2. Ανάλυση και Ταξινόμηση Επιθέσεων στο Σύστημα Ρύθμισης Φορτίου – Συχνότητας..... 68

3.2.1. Είδη Επιθέσεων (Strategic Attack)..... 69

3.2.2. Επιθέσεις Προτύπου (Template Attack)..... 71

3.2.3. Σημεία Επίθεσης (Location Attack)..... 72

3.3. Μοντελοποίηση Συστήματος Ρύθμισης Φορτίου – Συχνότητας παρουσία επιθέσεων..... 73

3.3.1. Μοντελοποίηση απομονωμένου συστήματος ρύθμισης φορτίου – συχνότητας (Single Area LFC) στον χώρο κατάστασης παρουσία επιθέσεων έγχυσης ψευδών δεδομένων (FDI)..... 73

3.3.2. Μοντελοποίηση συστήματος ρύθμισης φορτίου – συχνότητας Δύο Περιοχών (Two Area LFC) στον χώρο κατάστασης παρουσία επιθέσεων έγχυσης ψευδών δεδομένων (FDI)..... 74

4. Ανίχνευση Κυβερνοεπιθέσεων και ο ρόλος των Παρατηρητών Κατάστασης (State Observers)..... 77

4.1. Παρατηρητές Κατάστασης..... 77

4.1.1. Είδη Παρατηρητών Κατάστασης..... 79

4.2. Ανίχνευση Κυβερνοεπιθέσεων..... 87

4.2.1. Μέθοδοι Ανίχνευσης Κυβερνοεπιθέσεων τύπου FDI στο LFC..... 88

4.3. Μοντέλο Ανίχνευσης Επιθέσεων Έγχυσης Ψευδών Δεδομένων μέσω Παρατηρητή Luenberger..... 90

5. Προσομοιώσεις λειτουργίας LFC σε μεταβολές φορτίου και επιθέσεις Έγχυσης Ψευδών Δεδομένων - Ανίχνευσης επιθέσεων μέσω Παρατηρητή Luenberger..... 92

5.1. Προσομοιώσεις μελέτης Ρύθμισης Φορτίου – Συχνότητας υπό την επίδραση μεταβολών φορτίου..... 92

5.1.1. Προσομοιώσεις μεταβολής φορτίου σε σύστημα Ρύθμισης Φορτίου – Συχνότητάς Μιας Περιοχής με χρήση βηματικής απόκρισης 0.1 αμ..... 93

5.1.2. Προσομοιώσεις μεταβολής φορτίου σε σύστημα Ρύθμισης Φορτίου - Συχνότητας Δύο Περιοχών με χρήση βηματικής απόκρισης 0.1 αμ..... 97

5.2. Προσομοιώσεις και ανάλυση Επιθέσεων Έγχυσης Ψευδών Δεδομένων στο LFC104

5.2.1. Επιθέσεις σε Σύστημα Ρύθμισης Φορτίου – Συχνότητας Απομονωμένης Περιοχής 105

5.2.2. Επιθέσεις σε Σύστημα Ρύθμισης Φορτίου – Συχνότητας Δύο Περιοχών.....108

5.3. Προσομοιώσεις Ανίχνευσης Επιθέσεων Έγχυσης Ψευδών Δεδομένων στο σύστημα ρύθμισης Φορτίου – Συχνότητας 118
5.3.1. Ανάλυση Πειραματικής Μεθόδου 119
5.3.2. Μελέτη Ανίχνευσης (Detection) σε Απομονωμένο Σύστημα Ρύθμισης Φορτίου – Συχνότητας 120
5.3.3. Μελέτη Ανίχνευσης (Detection) Κυβερνοεπιθέσεων σε Σύστημα Ρύθμισης Φορτίου – Συχνότητας Δύο Περιοχών (Two Area LFC) 125
6. Γενικά συμπεράσματα και προτάσεις για περαιτέρω έρευνα 135
6.1. Γενικά Συμπεράσματα 135
6.2. Προτάσεις για περαιτέρω έρευνα 136
Βιβλιογραφία 138

Ευρετήριο Σχημάτων

ΣΧΗΜΑ 1. 1 : ΣΥΣΤΗΜΑ ΠΑΡΑΓΩΓΗΣ ΗΛΕΚΤΡΙΚΗΣ ΕΝΕΡΓΕΙΑΣ [1] 19
ΣΧΗΜΑ 1. 2 : ΚΑΤΗΓΟΡΙΟΠΟΙΗΣΗ ΜΟΡΦΩΝ ΕΥΣΤΑΘΕΙΑΣ 21
ΣΧΗΜΑ 1. 3 : ΣΧΗΜΑΤΙΚΟ ΔΙΑΓΡΑΜΜΑ ΑΥΤΟΜΑΤΗΣ ΡΥΘΜΙΣΗΣ ΤΑΣΗΣ ΚΑΙ ΡΥΘΜΙΣΗΣ ΦΟΡΤΙΟΥ – ΣΥΧΝΟΤΗΤΑΣ 22
ΣΧΗΜΑ 1. 4 : ΤΟΠΟΛΟΓΙΑ ΣΥΛΛΟΓΗΣ ΑΠΟΜΑΚΡΥΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΜΕΣΩ RTU [11] 24
ΣΧΗΜΑ 1. 5 : ΕΠΙΠΕΔΑ ΣΥΓΧΡΟΝΟΥ ΣΥΣΤΗΜΑΤΟΣ ΔΙΑΧΕΙΡΙΣΗΣ ΕΝΕΡΓΕΙΑΣ 25
ΣΧΗΜΑ 1. 6 : ΡΟΗ ΙΣΧΥΟΣ ΚΑΙ ΠΛΗΡΟΦΟΡΙΑΣ ΜΕΤΑΞΥ ΣΥΣΤΗΜΑΤΩΝ ΙΣΧΥΟΣ, SCADA ΚΑΙ EMS [10] 26
ΣΧΗΜΑ 1. 7 : ΠΡΑΓΜΑΤΙΚΗ ΑΠΕΙΚΟΝΙΣΗ ΣΥΣΤΗΜΑΤΩΝ ΙΣΧΥΟΣ, SCADA, EMS ΣΕ ΠΕΡΙΒΑΛΛΟΝ ΕΡΓΑΣΤΗΡΙΟΥ [10] 26
ΣΧΗΜΑ 1. 8 : ΣΤΟΙΧΕΙΑ ΚΑΙ ΔΟΜΗ ΣΥΣΤΗΜΑΤΩΝ ΙΣΧΥΟΣ, SCADA ΚΑΙ EMS [10] 26
ΣΧΗΜΑ 1. 9 : ΣΥΣΤΗΜΑ ΙΣΧΥΟΣ N – ΠΕΡΙΟΧΩΝ [19] 27
ΣΧΗΜΑ 1. 10 : ΣΥΣΤΗΜΑ ΕΠΟΠΤΙΚΟΥ ΕΛΕΓΧΟΥ ΗΛΕΚΤΡΙΚΗΣ ΕΝΕΡΓΕΙΑΣ 28
ΣΧΗΜΑ 1. 11 : ΧΑΡΑΚΤΗΡΙΣΤΙΚΗ ΚΑΜΠΥΛΗ ΣΤΑΤΙΣΜΟΥ 31
ΣΧΗΜΑ 1. 12 : ΣΧΗΜΑ ΠΡΩΤΕΥΟΥΣΑΣ ΚΑΙ ΔΕΥΤΕΡΕΥΟΥΣΑΣ ΡΥΘΜΙΣΗΣ 32
ΣΧΗΜΑ 1. 13 : ΤΟ ΤΡΙΓΩΝΟ ΔΙΑΘΕΣΙΜΟΤΗΤΑΣ - ΑΚΕΡΑΙΟΤΗΤΑΣ - ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑΣ 33
ΣΧΗΜΑ 1. 14 : ΚΥΒΕΡΝΟ – ΦΥΣΙΚΟ ΔΙΚΤΥΟ ΗΛΕΚΤΡΙΚΗΣ ΕΝΕΡΓΕΙΑΣ 35
ΣΧΗΜΑ 1. 15 : ΤΥΠΙΚΟ ΜΟΝΤΕΛΟ ΕΛΕΓΧΟΥ ΔΙΚΤΥΟΥ ΙΣΧΥΟΣ 36
ΣΧΗΜΑ 1. 16 : ΤΑΞΙΝΟΜΗΣΗ ΑΝΤΙΚΤΥΠΟΥ ΔΙΑΦΟΡΩΝ ΕΠΙΘΕΣΕΩΝ ΣΕ ΒΡΟΧΟΥΣ ΕΛΕΓΧΟΥ ΤΗΣ ΠΑΡΑΓΩΓΗΣ, ΤΗΣ ΜΕΤΑΦΟΡΑΣ ΚΑΙ ΤΗΣ ΔΙΑΝΟΜΗΣ ΙΣΧΥΟΣ [26]. 36
ΣΧΗΜΑ 1. 17 : ΤΑΞΙΝΟΜΗΣΗ ΕΛΕΓΧΟΥ ΠΑΡΑΓΩΓΗΣ [26] 37
ΣΧΗΜΑ 1. 18 : ΤΑΞΙΝΟΜΗΣΗ ΕΛΕΓΧΟΥ ΣΤΗ ΜΕΤΑΦΟΡΑ [26] 39
ΣΧΗΜΑ 1. 19 : ΤΑΞΙΝΟΜΗΣΗ ΕΛΕΓΧΟΥ ΣΤΗ ΔΙΑΝΟΜΗ [26] 41

ΣΧΗΜΑ 2. 1 : ΔΙΑΓΡΑΜΜΑ ΒΑΘΜΙΔΩΝ ΣΥΣΤΗΜΑΤΟΣ ΡΥΘΜΙΣΤΗ ΣΤΡΟΦΩΝ 43
ΣΧΗΜΑ 2. 2 : ΔΙΑΓΡΑΜΜΑ ΒΑΘΜΙΔΩΝ ΣΥΣΤΗΜΑΤΟΣ ΣΤΡΟΒΙΛΟΥ 44
ΣΧΗΜΑ 2. 3 : ΔΙΑΓΡΑΜΜΑ ΒΑΘΜΙΔΩΝ ΣΥΣΤΗΜΑΤΟΣ ΓΕΝΝΗΤΡΙΑΣ 44
ΣΧΗΜΑ 2. 4 : ΔΙΑΓΡΑΜΜΑ ΒΑΘΜΙΔΩΝ ΦΟΡΤΙΟΥ 45
ΣΧΗΜΑ 2. 5 : ΔΙΑΓΡΑΜΜΑ ΒΑΘΜΙΔΩΝ ΣΥΣΤΗΜΑΤΟΣ ΠΟΥ ΠΕΡΙΛΑΜΒΑΝΕΙ ΤΟ ΜΟΝΤΕΛΟ ΦΟΡΤΙΟΥ - ΓΕΝΝΗΤΡΙΑΣ, ΡΥΘΜΙΣΤΗ ΣΤΡΟΦΩΝ ΚΑΙ ΣΤΡΟΒΙΛΟΥ 45
ΣΧΗΜΑ 2. 6 : ΔΙΑΓΡΑΜΜΑ ΒΑΘΜΙΔΩΝ ΣΥΣΤΗΜΑΤΟΣ ΑΥΤΟΜΑΤΟΥ ΕΛΕΓΧΟΥ ΠΑΡΑΓΩΓΗΣ ΑΠΟΜΟΝΩΜΕΝΟΥ ΣΥΣΤΗΜΑΤΟΣ ΙΣΧΥΟΣ 46
ΣΧΗΜΑ 2. 7 : ΔΙΑΓΡΑΜΜΑ ΒΑΘΜΙΔΩΝ ΡΥΘΜΙΣΗΣ ΦΟΡΤΙΟΥ – ΣΥΧΝΟΤΗΤΑΣ ΑΠΟΜΟΝΩΜΕΝΟΥ ΣΥΣΤΗΜΑΤΟΣ ΙΣΧΥΟΣ ΜΕΣΩ ΣΥΜΒΑΤΙΚΟΥ ΟΛΟΚΛΗΡΩΤΙΚΟΥ ΕΛΕΓΚΤΗ 47
ΣΧΗΜΑ 2. 8 : ΙΣΟΔΥΝΑΜΟ ΔΙΚΤΥΟ ΓΙΑ ΣΥΣΤΗΜΑ ΙΣΧΥΟΣ ΔΥΟ ΠΕΡΙΟΧΩΝ (TWO AREA POWER SYSTEM) 48
ΣΧΗΜΑ 2. 9 : ΑΠΕΙΚΟΝΙΣΗ ΔΙΑΓΡΑΜΜΑΤΟΣ ΒΑΘΜΙΔΩΝ ΜΙΑΣ ΠΕΡΙΟΧΗΣ -Ι ΜΕ ΔΙΑΣΥΝΔΕΤΙΚΗ ΡΟΗ ΙΣΧΥΟΣ, ΣΕ ΕΝΑ ΔΙΑΣΥΝΔΕΔΕΜΕΝΟ ΣΥΣΤΗΜΑ ΙΣΧΥΟΣ N – ΠΕΡΙΟΧΩΝ ΕΛΕΓΧΟΥ ΜΕ ΣΥΜΒΑΤΙΚΟ ΕΛΕΓΚΤΗ K [19] 49
ΣΧΗΜΑ 2. 10 : ΔΙΑΓΡΑΜΜΑ ΒΑΘΜΙΔΩΝ ΣΥΣΤΗΜΑΤΟΣ ΔΥΟ ΠΕΡΙΟΧΩΝ ΑΠΟΤΕΛΟΥΜΕΝΟ ΜΟΝΟ ΑΠΟ ΠΡΩΤΕΥΟΝΤΑ ΕΛΕΓΧΟ [27] 50
ΣΧΗΜΑ 2. 11 : ΔΙΑΓΡΑΜΜΑ ΒΑΘΜΙΔΩΝ ΣΥΣΤΗΜΑΤΟΣ ΡΥΘΜΙΣΗΣ ΦΟΡΤΙΟΥ – ΣΥΧΝΟΤΗΤΑΣ ΔΥΟ ΠΕΡΙΟΧΩΝ ΜΕ ΧΡΗΣΗ ΟΛΟΚΛΗΡΩΤΙΚΟΥ ΕΛΕΓΚΤΗ [35] 51
ΣΧΗΜΑ 2. 12 : ΔΙΑΓΡΑΜΜΑ ΒΑΘΜΙΔΩΝ ΣΥΣΤΗΜΑΤΟΣ ΡΥΘΜΙΣΗΣ ΦΟΡΤΙΟΥ – ΣΥΧΝΟΤΗΤΑΣ ΔΥΟ ΠΕΡΙΟΧΩΝ ΜΕ **ΔΙΑΝΥΣΜΑΤΑ** ΤΟΥ ΧΩΡΟΥ ΚΑΤΑΣΤΑΣΗΣ (ΧΩΡΙΣ ΟΛΟΚΛΗΡΩΤΙΚΟ ΕΛΕΓΚΤΗ) [35] 54
ΣΧΗΜΑ 2. 13 : ΈΛΕΓΧΟΣ ΜΕ ΟΛΟΚΛΗΡΩΤΙΚΟ ΚΕΡΔΟΣ 58
ΣΧΗΜΑ 2. 14 : ΈΛΕΓΧΟΣ ΜΕ PI ΕΛΕΓΚΤΗ 59
ΣΧΗΜΑ 2. 15 : ΈΛΕΓΧΟΣ ΜΕ PID ΕΛΕΓΚΤΗ 59
ΣΧΗΜΑ 2. 17 : STATE FEEDBACK CONTROLLER 60

ΣΧΗΜΑ 3. 1 : ΓΕΝΙΚΟ ΔΙΑΓΡΑΜΜΑ ΒΑΘΜΙΔΩΝ ΣΥΣΤΗΜΑΤΟΣ ΡΥΘΜΙΣΗΣ – ΦΟΡΤΙΟΥ ΣΥΧΝΟΤΗΤΑΣ ΑΠΟΜΟΝΩΜΕΝΗΣ (SINGLE AREA) ΠΕΡΙΟΧΗΣ ΜΕ ΕΥΠΑΘΗ ΣΗΜΕΙΑ ΩΣ ΠΡΟΣ ΕΠΙΘΕΣΕΙΣ [32] 66

ΣΧΗΜΑ 3. 2 : ΓΕΝΙΚΟ ΔΙΑΓΡΑΜΜΑ ΒΑΘΜΙΔΩΝ ΣΥΣΤΗΜΑΤΟΣ ΡΥΘΜΙΣΗΣ – ΦΟΡΤΙΟΥ ΣΥΧΝΟΤΗΤΑΣ ΠΟΛΛΑΠΛΩΝ (MULIT AREA) ΠΕΡΙΟΧΩΝ ΜΕ ΕΥΠΑΘΗ ΩΣ ΠΡΟΣ ΕΠΙΘΕΣΕΙΣ ΣΗΜΕΙΑ [32] 67
ΣΧΗΜΑ 3. 3 : ΓΕΝΙΚΟ ΔΙΑΓΡΑΜΜΑ ΒΑΘΜΙΔΩΝ ΣΥΣΤΗΜΑΤΟΣ ΡΥΘΜΙΣΗΣ – ΦΟΡΤΙΟΥ ΣΥΧΝΟΤΗΤΑΣ ΔΥΟ (TWO AREA) ΠΕΡΙΟΧΩΝ ΜΕ ΕΥΠΑΘΗ ΩΣ ΠΡΟΣ ΕΠΙΘΕΣΕΙΣ ΣΗΜΕΙΑ [32] 68
ΣΧΗΜΑ 3. 4 : ΤΑΞΙΝΟΜΗΣΗ ΕΠΙΘΕΣΕΩΝ ΣΤΟ ΣΥΣΤΗΜΑ ΡΥΘΜΙΣΗΣ ΦΟΡΤΙΟΥ – ΣΥΧΝΟΤΗΤΑΣ 68
ΣΧΗΜΑ 3. 5 : ΔΙΑΓΡΑΜΜΑ ΕΠΙΘΕΣΕΩΝ ΣΤΟ ΣΥΣΤΗΜΑ ΡΥΘΜΙΣΗΣ ΦΟΡΤΙΟΥ - ΣΥΧΝΟΤΗΤΑΣ 72

ΣΧΗΜΑ 4. 1 : ΔΙΑΓΡΑΜΜΑ ΒΑΘΜΙΔΩΝ ΣΥΣΤΗΜΑΤΟΣ ΚΑΙ ΠΑΡΑΤΗΡΗΤΗ ΚΑΤΑΣΤΑΣΗΣ 77
ΣΧΗΜΑ 4. 2 : ΠΑΡΑΤΗΡΗΤΗΣ ΚΑΤΑΣΤΑΣΗΣ ΑΝΟΙΧΤΟΥ ΒΡΟΧΟΥ [78] 79
ΣΧΗΜΑ 4. 3 : ΠΑΡΑΤΗΡΗΤΗΣ LUENBERGER [85] 81
ΣΧΗΜΑ 4. 4 : ΑΠΕΙΚΟΝΙΣΗ ΠΟΛΩΝ ΕΝΕΡΓΕΙΑΚΟΥ ΣΥΣΤΗΜΑΤΟΣ ΚΑΙ ΠΑΡΑΤΗΡΗΤΗ ΚΑΤΑΣΤΑΣΗΣ ΣΤΟ ΜΙΓΑΔΙΚΟ ΕΠΙΠΕΔΟ . 82
ΣΧΗΜΑ 4. 5 : ΜΟΝΤΕΛΟ ΠΑΡΑΤΗΡΗΤΗ ΆΓΝΩΣΤΗΣ ΕΙΣΟΔΟΥ (UIO) [86] 84
ΣΧΗΜΑ 4. 6 : ΠΑΡΟΥΣΙΑΣΗ SLIDING MODE OBSERVER 86
ΣΧΗΜΑ 4. 7 : ΠΑΡΑΤΗΡΗΤΗΣ LUENBERGER ΣΤΟ ΜΟΝΤΕΛΟ ΤΩΝ ΠΡΟΣΟΜΟΙΩΣΕΩΝ 91
ΣΧΗΜΑ 4. 8 : ΣΥΣΤΗΜΑ ΡΥΘΜΙΣΗΣ ΦΟΡΤΙΟΥ – ΣΥΧΝΟΤΗΤΑΣ ΑΠΟΜΟΝΩΜΕΝΗΣ ΠΕΡΙΟΧΗΣ ΜΑΖΙ ΜΕ ΠΑΡΑΤΗΡΗΤΗ LUENBERGER 91
ΣΧΗΜΑ 4. 9 : ΣΥΣΤΗΜΑ ΡΥΘΜΙΣΗΣ ΦΟΡΤΙΟΥ – ΣΥΧΝΟΤΗΤΑΣ ΔΥΟ ΠΕΡΙΟΧΩΝ ΜΑΖΙ ΜΕ ΠΑΡΑΤΗΡΗΤΗ LUENBERGER 91

ΣΧΗΜΑ 5. 1 : ΜΟΝΤΕΛΟ ΡΥΘΜΙΣΗΣ ΦΟΡΤΙΟΥ – ΣΥΧΝΟΤΗΤΑΣ ΑΠΟΜΟΝΩΜΕΝΗΣ ΠΕΡΙΟΧΗΣ ΧΩΡΙΣ ΔΕΥΤΕΡΕΥΟΝΤΑ ΕΛΕΓΧΟ 94
ΣΧΗΜΑ 5. 2 : ΜΕΤΑΒΟΛΗ ΣΥΧΝΟΤΗΤΑΣ ΠΑΡΟΥΣΙΑ ΜΕΤΑΒΟΛΗΣ ΦΟΡΤΙΟΥ ΤΗ ΧΡΟΝΙΚΗ ΣΤΙΓΜΗ T = 3 SEC 94
ΣΧΗΜΑ 5. 3 : ΜΟΝΤΕΛΟ LFC ΑΠΟΜΟΝΩΜΕΝΗΣ ΠΕΡΙΟΧΗΣ ΜΕ ΠΡΟΣΘΗΚΗ ΔΕΥΤΕΡΕΥΟΝΤΑ ΒΡΟΧΟΥ 95
ΣΧΗΜΑ 5. 4 : ΜΕΤΑΒΟΛΗ ΣΥΧΝΟΤΗΤΑΣ ΣΤΟ LFC ΕΠΕΙΤΑ ΑΠΟ ΜΕΤΑΒΟΛΗ ΦΟΡΤΙΟΥ ΜΕΓΕΘΟΥΣ 0.1 ΑΜ, ΜΕ ΤΗΝ ΠΡΟΣΘΗΚΗ ΔΕΥΤΕΡΕΥΟΝΤΑ ΒΡΟΧΟΥ 96
ΣΧΗΜΑ 5. 5 : : ΜΕΤΑΒΟΛΗ ΜΗΧΑΝΙΚΗΣ ΙΣΧΥΟΣ ΣΤΟ LFC ΕΠΕΙΤΑ ΑΠΟ ΜΕΤΑΒΟΛΗ ΦΟΡΤΙΟΥ ΜΕΓΕΘΟΥΣ 0.1 ΑΜ, ΜΕ ΤΗΝ ΠΡΟΣΘΗΚΗ ΔΕΥΤΕΡΕΥΟΝΤΑ ΒΡΟΧΟΥ 96
ΣΧΗΜΑ 5. 6 : LFC ΜΟΝΤΕΛΟ ΔΥΟ ΠΕΡΙΟΧΩΝ 97
ΣΧΗΜΑ 5. 7 : ΜΕΤΑΒΟΛΗ ΣΥΧΝΟΤΗΤΑΣ ΠΕΡΙΟΧΗΣ 1 ΜΕ ΑΥΞΗΣΗ ΦΟΡΤΙΟΥ 0.5 ΑΜ ΤΗ ΧΡΟΝΙΚΗ ΣΤΙΓΜΗ T = 3 SEC 98
ΣΧΗΜΑ 5. 8 : ΜΕΤΑΒΟΛΗ ΣΥΧΝΟΤΗΤΑΣ ΠΕΡΙΟΧΗΣ 2 ΜΕ ΑΥΞΗΣΗ ΦΟΡΤΙΟΥ 0.5 ΑΜ ΣΤΗΝ ΠΕΡΙΟΧΗ 1 ΤΗ ΧΡΟΝΙΚΗ ΣΤΙΓΜΗ T = 3 SEC 99
ΣΧΗΜΑ 5. 9 : ΜΕΤΑΒΟΛΗ ΣΥΧΝΟΤΗΤΩΝ ΠΕΡΙΟΧΩΝ 1 ΚΑΙ 2 ΜΕ ΑΥΞΗΣΗ ΦΟΡΤΙΟΥ 0.5 ΑΜ ΤΗ ΧΡΟΝΙΚΗ ΣΤΙΓΜΗ T = 3 SEC ΣΤΗΝ ΠΕΡΙΟΧΗ 1 99
ΣΧΗΜΑ 5. 10 : ΜΕΤΑΒΟΛΗ ΔΙΑΣΥΝΔΕΤΙΚΗΣ ΡΟΗΣ ΠΕΡΙΟΧΗΣ 1 ΜΕ ΑΥΞΗΣΗ ΦΟΡΤΙΟΥ 0.5 ΑΜ ΤΗ ΧΡΟΝΙΚΗ ΣΤΙΓΜΗ T = 3 SEC 100
ΣΧΗΜΑ 5. 11 : ΣΦΑΛΜΑ ΕΛΕΓΧΟΥ ΠΕΡΙΟΧΗΣ 1 ΚΑΙ 2 ΜΕ ΑΥΞΗΣΗ ΦΟΡΤΙΟΥ 0.5 ΑΜ ΤΗ ΧΡΟΝΙΚΗ ΣΤΙΓΜΗ T = 3 SEC 100
ΣΧΗΜΑ 5. 12 : ΜΕΤΑΒΟΛΗ ΣΥΧΝΟΤΗΤΑΣ ΠΕΡΙΟΧΗΣ 1 ΜΕ ΑΥΞΗΣΗ ΦΟΡΤΙΟΥ 0.5 ΑΜ ΣΤΗΝ ΠΕΡΙΟΧΗ 2 ΤΗ ΧΡΟΝΙΚΗ ΣΤΙΓΜΗ T = 3 SEC 101
ΣΧΗΜΑ 5. 13 : : ΜΕΤΑΒΟΛΗ ΣΥΧΝΟΤΗΤΑΣ ΠΕΡΙΟΧΗΣ 2 ΜΕ ΑΥΞΗΣΗ ΦΟΡΤΙΟΥ 0.5 ΑΜ ΣΤΗΝ ΠΕΡΙΟΧΗ 2 ΤΗ ΧΡΟΝΙΚΗ ΣΤΙΓΜΗ T = 3 SEC 101
ΣΧΗΜΑ 5. 14 : ΜΕΤΑΒΟΛΗ ΣΥΧΝΟΤΗΤΩΝ ΠΕΡΙΟΧΩΝ 1 ΚΑΙ 2 ΜΕ ΑΥΞΗΣΗ ΦΟΡΤΙΟΥ 0.5 ΑΜ ΤΗ ΧΡΟΝΙΚΗ ΣΤΙΓΜΗ T = 3 SEC ΣΤΗΝ ΠΕΡΙΟΧΗ 2 101
ΣΧΗΜΑ 5. 15 : : ΜΕΤΑΒΟΛΗ ΔΙΑΣΥΝΔΕΤΙΚΗΣ ΡΟΗΣ ΠΕΡΙΟΧΗΣ 2 ΜΕ ΑΥΞΗΣΗ ΦΟΡΤΙΟΥ 0.5 ΑΜ ΤΗ ΧΡΟΝΙΚΗ ΣΤΙΓΜΗ T = 3 SEC 102
ΣΧΗΜΑ 5. 16 : ΣΦΑΛΜΑ ΕΛΕΓΧΟΥ ΠΕΡΙΟΧΗΣ 1 ΚΑΙ 2 ΜΕ ΑΥΞΗΣΗ ΦΟΡΤΙΟΥ 0.5 ΑΜ ΤΗ ΧΡΟΝΙΚΗ ΣΤΙΓΜΗ T = 3 SEC 102
ΣΧΗΜΑ 5. 17 : ΜΕΤΑΒΟΛΗ ΣΥΧΝΟΤΗΤΑΣ ΠΕΡΙΟΧΗΣ 1 ΜΕ ΜΕΙΩΣΗ ΦΟΡΤΙΟΥ 0.5 ΑΜ ΣΤΗΝ ΠΕΡΙΟΧΗ 1 ΤΗ ΧΡΟΝΙΚΗ ΣΤΙΓΜΗ T = 3 SEC 102
ΣΧΗΜΑ 5. 18 : ΜΕΤΑΒΟΛΗ ΣΥΧΝΟΤΗΤΑΣ ΠΕΡΙΟΧΗΣ 2 ΜΕ ΜΕΙΩΣΗ ΦΟΡΤΙΟΥ 0.5 ΑΜ ΣΤΗΝ ΠΕΡΙΟΧΗ 1 ΤΗ ΧΡΟΝΙΚΗ ΣΤΙΓΜΗ T = 3 SEC 103
ΣΧΗΜΑ 5. 19 : ΜΕΤΑΒΟΛΗ ΣΥΧΝΟΤΗΤΩΝ ΠΕΡΙΟΧΩΝ 1 ΚΑΙ 2 ΜΕ ΜΕΙΩΣΗ ΦΟΡΤΙΟΥ 0.5 ΑΜ ΣΤΗΝ ΠΕΡΙΟΧΗ 1 ΤΗ ΧΡΟΝΙΚΗ ΣΤΙΓΜΗ T = 3 SEC 103

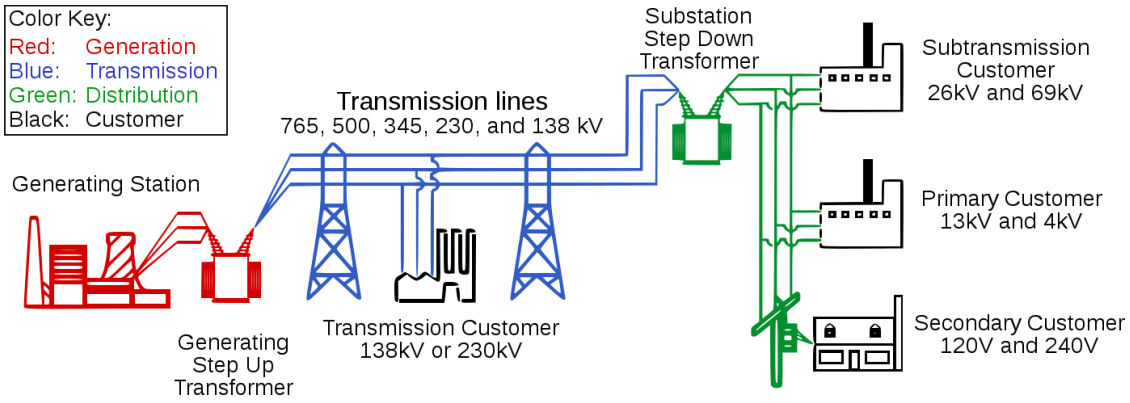
ΣΧΗΜΑ 5. 20 : ΜΕΤΑΒΟΛΗ ΔΙΑΣΥΝΔΕΤΙΚΗΣ ΡΟΗΣ ΠΕΡΙΟΧΗΣ 1 ΜΕ ΜΕΙΩΣΗ ΦΟΡΤΙΟΥ 0.5 ΑΜ ΤΗ ΧΡΟΝΙΚΗ ΣΤΙΓΜΗ T = 3 SEC 103
ΣΧΗΜΑ 5. 21 : ΣΦΑΛΜΑ ΕΛΕΓΧΟΥ ΠΕΡΙΟΧΗΣ 1 ΚΑΙ 2 ΜΕ ΜΕΙΩΣΗ ΦΟΡΤΙΟΥ 0.5 ΑΜ ΤΗ ΧΡΟΝΙΚΗ ΣΤΙΓΜΗ T = 3 SEC..... 104
ΣΧΗΜΑ 5. 22 : ΠΙΘΑΝΑ ΣΗΜΕΙΑ FDI ΕΠΙΘΕΣΕΩΝ ΣΤΟ ΣΥΣΤΗΜΑ ΡΥΘΜΙΣΗΣ ΦΟΡΤΙΟΥ – ΣΥΧΝΟΤΗΤΑΣ ΠΕΡΙΟΧΗΣ Ι..... 104
ΣΧΗΜΑ 5. 23 : ΣΥΣΤΗΜΑ ΡΥΘΜΙΣΗΣ ΦΟΡΤΙΟΥ -ΣΥΧΝΟΤΗΤΑΣ ΥΠΟ ΤΗΝ ΕΠΙΒΟΛΗ BIAS INJECTION ATTACK ΣΤΙΣ ΜΕΤΡΗΣΕΙΣ ΤΗΣ ΣΥΧΝΟΤΗΤΑΣ 106
ΣΧΗΜΑ 5. 24 : ΜΕΤΑΒΟΛΗ ΣΥΧΝΟΤΗΤΑΣ ΥΠΟ ΤΗΝ ΕΠΙΔΡΑΣΗ ΕΠΙΘΕΣΗΣ ΕΓΧΥΣΗΣ ΠΑΡΑΓΟΝΤΑ ΘΕΤΙΚΟΥ “BIAS”..... 106
ΣΧΗΜΑ 5. 25 : ΜΕΤΑΒΟΛΗ ΣΥΧΝΟΤΗΤΑΣ ΥΠΟ ΤΗΝ ΕΠΙΔΡΑΣΗ ΕΠΙΘΕΣΗΣ ΕΓΧΥΣΗΣ ΠΑΡΑΓΟΝΤΑ ΑΡΝΗΤΙΚΟΥ “BIAS”..... 107
ΣΧΗΜΑ 5. 26 : ΣΥΣΤΗΜΑ ΡΥΘΜΙΣΗΣ ΦΟΡΤΙΟΥ -ΣΥΧΝΟΤΗΤΑΣ ΥΠΟ ΤΗΝ ΕΠΙΒΟΛΗ ΠΡΟΣΘΕΤΙΚΗΣ ΑΡΜΟΝΙΚΗΣ ΕΠΙΘΕΣΗΣ ΣΤΟ ΚΑΝΑΛΙ ΕΠΙΚΟΙΝΩΝΙΑΣ ΚΕΝΤΡΟΥ ΕΛΕΓΧΟΥ ΚΑΙ ΡΥΘΜΙΣΤΗ ΣΤΡΟΦΩΝ..... 107
ΣΧΗΜΑ 5. 27 : ΜΕΤΑΒΟΛΗ ΣΥΧΝΟΤΗΤΑΣ ΥΠΟ ΤΗΝ ΕΠΙΔΡΑΣΗ ΠΡΟΣΘΕΤΙΚΗΣ ΑΡΜΟΝΙΚΗΣ ΕΠΙΘΕΣΗΣ ΣΤΟ ΚΑΝΑΛΙ ΕΠΙΚΟΙΝΩΝΙΑΣ ΚΕΝΤΡΟΥ ΕΛΕΓΧΟΥ ΚΑΙ ΡΥΘΜΙΣΤΗ ΣΤΡΟΦΩΝ..... 108
ΣΧΗΜΑ 5. 28 : ΣΥΣΤΗΜΑ ΡΥΘΜΙΣΗΣ ΦΟΡΤΙΟΥ -ΣΥΧΝΟΤΗΤΑΣ ΥΠΟ ΤΗΝ ΕΠΙΒΟΛΗ ΕΠΙΘΕΣΗΣ ΕΓΧΥΣΗΣ ΠΑΡΑΓΟΝΤΑ “BIAS” ΣΤΙΣ ΜΕΤΡΗΣΕΙΣ ΤΗΣ ΣΥΧΝΟΤΗΤΑΣ ΤΗΣ ΠΕΡΙΟΧΗΣ 1 109
ΣΧΗΜΑ 5. 29 : ΜΕΤΑΒΟΛΕΣ ΣΥΧΝΟΤΗΤΩΝ ΠΕΡΙΟΧΩΝ 1 ΚΑΙ 2 ΥΠΟ ΤΗΝ ΕΠΙΘΕΣΗ ΠΑΡΑΓΟΝΤΑ ΕΧΓΥΣΗΣ “BIAS”, ΜΕ Β =0.1 109
ΣΧΗΜΑ 5. 30 : ΜΕΤΑΒΟΛΗ ΔΙΑΣΥΝΔΕΤΙΚΗ ΡΟΗΣ ΥΠΟ ΤΗΝ ΕΠΙΔΡΑΣΗ ΕΠΙΘΕΣΗ ΠΑΡΑΓΟΝΤΑ ΕΧΓΥΣΗΣ “BIAS”, ΜΕ Β =0.1 10
ΣΧΗΜΑ 5. 31 : ΜΕΤΑΒΟΛΗ ΣΦΑΛΜΑΤΟΣ ΕΛΕΓΧΟΥ ΠΕΡΙΟΧΗΣ 1 ΚΑΙ 2 ΥΠΟ ΕΠΙΘΕΣΗ ΠΑΡΑΓΟΝΤΑ ΕΧΓΥΣΗΣ “BIAS”, ΜΕ Β =0.1 110
ΣΧΗΜΑ 5. 32 : ΣΥΣΤΗΜΑ ΡΥΘΜΙΣΗΣ ΦΟΡΤΙΟΥ -ΣΥΧΝΟΤΗΤΑΣ ΥΠΟ ΤΗΝ ΕΠΙΒΟΛΗ ΠΡΟΣΘΕΤΙΚΗΣ ΑΡΜΟΝΙΚΗΣ ΕΠΙΘΕΣΗΣ ΕΓΧΥΣΗΣ ΣΤΟ ΚΑΝΑΛΙ ΜΕΤΡΗΣΕΩΝ ΤΗΣ ΔΙΑΣΥΝΔΕΤΙΚΗΣ ΡΟΗΣ..... 111
ΣΧΗΜΑ 5. 33: ΜΕΤΑΒΟΛΕΣ ΣΥΧΝΟΤΗΤΩΝ ΠΕΡΙΟΧΩΝ 1 ΚΑΙ 2 ΥΠΟ ΠΡΟΣΘΕΤΙΚΗ ΑΡΜΟΝΙΚΗ ΕΠΙΘΕΣΗ ΠΛΑΤΟΥΣ 0.15 ΑΜ| 112
ΣΧΗΜΑ 5. 34 : : ΜΕΤΑΒΟΛΗ ΔΙΑΣΥΝΔΕΤΙΚΗ ΡΟΗΣ ΥΠΟ ΤΗΝ ΕΠΙΔΡΑΣΗ ΠΡΟΣΘΕΤΙΚΗΣ ΑΡΜΟΝΙΚΗΣ ΕΠΙΘΕΣΗΣ ΠΛΑΤΟΥΣ 0.15 ΑΜ..... 112
ΣΧΗΜΑ 5. 35 : : ΜΕΤΑΒΟΛΗ ΣΦΑΛΜΑΤΟΣ ΕΛΕΓΧΟΥ ΠΕΡΙΟΧΗΣ 1 ΚΑΙ 2 ΥΠΟ ΕΠΙΔΡΑΣΗ ΠΡΟΣΘΕΤΙΚΗΣ ΑΡΜΟΝΙΚΗΣ ΕΠΙΘΕΣΗΣ ΠΛΑΤΟΥΣ 0.15 ΑΜ..... 113
ΣΧΗΜΑ 5. 36 : ΣΥΣΤΗΜΑ ΡΥΘΜΙΣΗΣ ΦΟΡΤΙΟΥ -ΣΥΧΝΟΤΗΤΑΣ ΥΠΟ ΤΗΝ ΕΠΙΒΟΛΗ ΕΠΙΘΕΣΗΣ ΡΑΜΠΑΣ ΣΤΟ ΚΑΝΑΛΙ ΕΠΙΚΟΙΝΩΝΙΑΣ ΤΟΥ ΚΕΝΤΡΟΥ ΕΛΕΓΧΟΥ..... 114
ΣΧΗΜΑ 5. 37 : : ΜΕΤΑΒΟΛΕΣ ΣΥΧΝΟΤΗΤΩΝ ΠΕΡΙΟΧΩΝ 1 ΚΑΙ 2 ΥΠΟ ΕΠΙΘΕΣΗ ΡΑΜΠΑΣ ΜΕ $\Lambda_A = 0.5$ 114
ΣΧΗΜΑ 5. 38 : ΜΕΤΑΒΟΛΗ ΔΙΑΣΥΝΔΕΤΙΚΗ ΡΟΗΣ ΥΠΟ ΤΗΝ ΕΠΙΔΡΑΣΗ ΕΠΙΘΕΣΗΣ ΡΑΜΠΑΣ ΣΤΟ ΚΑΝΑΛΙ ΕΠΙΚΟΙΝΩΝΙΑΣ ΤΟΥ ΚΕΝΤΡΟΥ ΕΛΕΓΧΟΥ..... 115
ΣΧΗΜΑ 5. 39 : ΣΦΑΛΜΑΤΑ ΕΛΕΓΧΟΥ ΠΕΡΙΟΧΗΣ 1 ΚΑΙ 2 ΥΠΟ ΕΠΙΔΡΑΣΗ ΕΠΙΘΕΣΗΣ ΡΑΜΠΑΣ ΚΛΙΣΗΣ 0.5..... 115
ΣΧΗΜΑ 5. 40 : ΣΥΣΤΗΜΑ ΡΥΘΜΙΣΗΣ ΦΟΡΤΙΟΥ -ΣΥΧΝΟΤΗΤΑΣ ΥΠΟ ΤΗΝ ΕΠΙΒΟΛΗ ΚΛΙΜΑΚΟΥΜΕΝΗΣ ΕΠΙΘΕΣΗΣ ΣΤΟ ΚΑΝΑΛΙ ΕΠΙΚΟΙΝΩΝΙΑΣ ΤΟΥ ΚΕΝΤΡΟΥ ΕΛΕΓΧΟΥ ΤΗΣ 1ΗΣ ΠΕΡΙΟΧΗΣ..... 116
ΣΧΗΜΑ 5. 41: ΜΕΤΑΒΟΛΗ ΣΥΧΝΟΤΗΤΩΝ ΠΕΡΙΟΧΩΝ 1 ΚΑΙ 2 ΥΠΟ ΤΗΝ ΕΠΙΘΕΣΗ ΚΛΙΜΑΚΟΥΜΕΝΗΣ ΕΠΙΘΕΣΗΣ ΜΕ $\Lambda_A = 0.5$ ΠΑ T = 0 - 20 SEC..... 117
ΣΧΗΜΑ 5. 42 : ΜΕΤΑΒΟΛΗ ΣΥΧΝΟΤΗΤΩΝ ΠΕΡΙΟΧΩΝ 1 ΚΑΙ 2 ΥΠΟ ΤΗΝ ΕΠΙΘΕΣΗ ΚΛΙΜΑΚΟΥΜΕΝΗΣ ΕΠΙΘΕΣΗΣ ΜΕ $\Lambda_A = 0.5$ ΠΑ T = 0 - 50 SEC..... 117
ΣΧΗΜΑ 5. 43: ΣΦΑΛΜΑ ΕΛΕΓΧΟΥ ΠΕΡΙΟΧΩΝ 1 ΚΑΙ 2 ΥΠΟ ΤΗΝ ΕΠΙΘΕΣΗ ΚΛΙΜΑΚΟΥΜΕΝΗΣ ΕΠΙΘΕΣΗΣ ΜΕ $\Lambda_A = 0.5$ ΓΙΑ T = 0 - 20 SEC..... 117
ΣΧΗΜΑ 5. 44 : ΣΦΑΛΜΑ ΕΛΕΓΧΟΥ ΠΕΡΙΟΧΩΝ 1 ΚΑΙ 2 ΥΠΟ ΤΗΝ ΕΠΙΘΕΣΗ ΚΛΙΜΑΚΟΥΜΕΝΗΣ ΕΠΙΘΕΣΗΣ ΜΕ $\Lambda_A = 0.5$ ΓΙΑ T = 0 - 50 SEC..... 117
ΣΧΗΜΑ 5. 45 : ΜΕΤΑΒΟΛΗ ΔΙΑΣΥΝΔΕΤΙΚΗΣ ΡΟΗΣ ΥΠΟ ΤΗΝ ΕΠΙΘΕΣΗ ΚΛΙΜΑΚΟΥΜΕΝΗΣ ΕΠΙΘΕΣΗΣ ΜΕ $\Lambda_A = 0.5$ ΓΙΑ T = 0 - 20 SEC..... 118
ΣΧΗΜΑ 5. 46: ΜΕΤΑΒΟΛΗ ΔΙΑΣΥΝΔΕΤΙΚΗΣ ΡΟΗΣ ΥΠΟ ΤΗΝ ΕΠΙΘΕΣΗ ΚΛΙΜΑΚΟΥΜΕΝΗΣ ΕΠΙΘΕΣΗΣ ΜΕ $\Lambda_A = 0.5$ ΓΙΑ T = 0 - 50 SEC..... 118
ΣΧΗΜΑ 5. 47 : ΜΕΤΑΒΟΛΗ ΣΥΧΝΟΤΗΤΑΣ ΠΕΡΙΟΧΗΣ 1 ΕΠΕΙΤΑ ΑΠΟ ΜΕΤΑΒΟΛΗ ΦΟΡΤΙΟΥ $\Delta P_L = 0.1$ ΑΜ ΤΗΝ T = 5 SEC ΚΑΙ ΕΠΙΘΕΣΗ ΕΓΧΥΣΗΣ ΨΕΥΔΩΝ ΔΕΔΟΜΕΝΩΝ ΠΑΡΑΓΟΝΤΑ Β>0.05 ΤΗΝ T = 60 SEC..... 121
ΣΧΗΜΑ 5. 48 : ΧΑΡΑΚΤΗΡΙΣΤΙΚΗ ΣΦΑΛΜΑΤΟΣ ΕΞΟΔΟΥ ΠΑΡΑΤΗΡΗΤΗ ΕΠΕΙΤΑ ΑΠΟ ΜΕΤΑΒΟΛΗ ΦΟΡΤΙΟΥ $\Delta P_L = 0.05$ ΑΜ ΤΗΝ T = 5 SEC ΚΑΙ ΕΠΙΘΕΣΗ ΕΓΧΥΣΗΣ ΨΕΥΔΩΝ ΔΕΔΟΜΕΝΩΝ ΠΑΡΑΓΟΝΤΑ Β = 0.05 ΤΗΝ T = 60 SEC..... 122
ΣΧΗΜΑ 5. 49 : ΧΑΡΑΚΤΗΡΙΣΤΙΚΗ ΣΦΑΛΜΑΤΟΣ ΕΞΟΔΟΥ ΠΑΡΑΤΗΡΗΤΗ ΕΠΕΙΤΑ ΑΠΟ ΜΕΤΑΒΟΛΗ ΦΟΡΤΙΟΥ $\Delta P_L = 0.1$ ΑΜ ΤΗΝ T = 5 SEC ΚΑΙ ΕΠΙΘΕΣΗ ΕΓΧΥΣΗΣ ΨΕΥΔΩΝ ΔΕΔΟΜΕΝΩΝ ΠΑΡΑΓΟΝΤΑ Β>0.05 ΤΗΝ T = 60 SEC..... 122

Σχημα 5. 50 : Χαρακτηριστικη Σφαλματος Εξοδου Παρατηρητη επειτα απο μεταβολη φορτιου ΔP_L = 0.1 αμ την t = 5 sec και επιθεση εγχυσης ψευδων δεδομενων παραγοντα β<0.05 την t = 60 sec.....123
Σχημα 5. 51 : Μεταβολη Συχνοτητας Περιοχης 1, επειτα απο μεταβολη φορτιου ΔP_L = 0.1 αμ. τη χρονικη στιγμη t = 5 sec. και επιβολη ημιτονικης αρμονικης επιθεσης τη χρονικη στιγμη t = 60 sec.....124
Σχημα 5. 52: Χαρακτηριστικη Σφαλματος Εξοδου Παρατηρητη επειτα απο μεταβολη φορτιου ΔP_L = 0.1 αμ. τη χρονικη στιγμη t = 5 sec. και επιβολη ημιτονικης αρμονικης επιθεσης τη χρονικη στιγμη t = 60 sec.....124
Σχημα 5. 53 : Μεταβολη συχνοτητας περιοχης 1 επειτα απο μεταβολη φορτιου ΔP_L = 0.05 αμ την t = 5 sec και επιθεση εγχυσης ψευδων δεδομενων παραγοντα β>0.05 την t = 60 sec126
Σχημα 5. 54 : Χαρακτηριστικη Σφαλματος Εξοδου Παρατηρητη επειτα απο μεταβολη φορτιου ΔP_L = 0.05 αμ. τη χρονικη στιγμη t = 5 sec. και επιβολη επιθεσης εγχυσης ψευδων δεδομενων παραγοντα β = 0.1 τη χρονικη στιγμη t = 60 sec.....126
Σχημα 5. 55 : Χαρακτηριστικη Σφαλματος Εξοδου Παρατηρητη επειτα μονο απο επιβολη επιθεσης εγχυσης ψευδων δεδομενων παραγοντα β = 0.1 τη χρονικη στιγμη t = 60 sec..127
Σχημα 5. 56 : Μεταβολη συχνοτητας περιοχης 1 επειτα απο μεταβολη φορτιου ΔP_L = 0.05 αμ. τη χρονικη στιγμη t = 5 sec. και επιβολη επιθεσης εγχυσης ψευδων δεδομενων παραγοντα β = 0.1 τη χρονικη στιγμη t = 60 sec.....127
Σχημα 5. 57: Χαρακτηριστικη Σφαλματος Εξοδου Παρατηρητη επειτα απο μεταβολη φορτιου ΔP_L = 0.05 αμ. τη χρονικη στιγμη t = 5 sec. και επιβολη επιθεσης εγχυσης ψευδων δεδομενων παραγοντα β = 12 τη χρονικη στιγμη t = 60 sec.....128
Σχημα 5. 58: Μεταβολη συχνοτητας περιοχης 1 επειτα μονο απο επιβολη επιθεσης προσθετικης αρμονικης επιθεσης πλατους A = 0.15 τη χρονικη στιγμη t = 60 sec.....128
Σχημα 5. 59 Χαρακτηριστικη Σφαλματος Εξοδου Παρατηρητη επειτα μονο απο επιβολη προσθετικης αρμονικης πλατους A = 0.15 τη χρονικη στιγμη t = 60 sec.....129
Σχημα 5. 60: Μεταβολη συχνοτητας περιοχης 1 επειτα απο μεταβολη φορτιου ΔP_L = 0.05 αμ. τη χρονικη στιγμη t = 5 sec. και επιβολη προσθετικης ημιτονικης επιθεσης πλατους A = 0.15 τη χρονικη στιγμη t = 60 sec.....129
Σχημα 5. 61 : Χαρακτηριστικη Σφαλματος Παρατηρητη επειτα απο μεταβολη φορτιου ΔP_L = 0.05 αμ. τη χρονικη στιγμη t = 5 sec. και επιβολη προσθετικης αρμονικης επιθεσης πλατους A = 0.15 τη χρονικη στιγμη t = 60 sec.....130
Σχημα 5. 62: Μεταβολη συχνοτητας περιοχης 1 επειτα απο μεταβολη φορτιου ΔP_L = 0.00001 αμ. τη χρονικη στιγμη t = 5 sec. και επιβολη προσθετικης ημιτονικης επιθεσης πλατους A = 0.15 τη χρονικη στιγμη t = 60 sec.....130
Σχημα 5. 63: Χαρακτηριστικη Σφαλματος Εξοδου Παρατηρητη επειτα απο μεταβολη φορτιου ΔP_L = 0.00001 αμ. τη χρονικη στιγμη t = 5 sec. και επιβολη προσθετικης αρμονικης επιθεσης πλατους A = 0.15 τη χρονικη στιγμη t = 60 sec.....131
Σχημα 5. 64: Χαρακτηριστικη Σφαλματος Εξοδου Παρατηρητη επειτα απο μεταβολη φορτιου ΔP_L = 0.05 αμ. τη χρονικη στιγμη t = 5 sec. και επιβολη προσθετικης αρμονικης επιθεσης πλατους A = 700 τη χρονικη στιγμη t = 60 sec.....131
Σχημα 5. 65: Μεταβολη συχνοτητας περιοχης 1 επειτα απο μεταβολη φορτιου ΔP_L = 0.05 αμ. τη χρονικη στιγμη t = 5 sec. και επιβολη προσθετικης ημιτονικης επιθεσης πλατους A = 700 τη χρονικη στιγμη t = 60 sec.....132
Σχημα 5. 66: Μεταβολη συχνοτητας περιοχης 1 επειτα απο μεταβολη φορτιου ΔP_L = 0.05 αμ. τη χρονικη στιγμη t = 5 sec. και επιβολη επιθεσης ραμπας κλισης (slope) s = 2, τη χρονικη στιγμη t = 60 sec.....132
Σχημα 5. 67: Χαρακτηριστικη Σφαλματος Εξοδου Παρατηρητη επειτα απο μεταβολη φορτιου ΔP_L = 0.05 αμ. τη χρονικη στιγμη t = 5 sec. και επιβολη επιθεσης ραμπας, κλισης (slope) s = 2 τη χρονικη στιγμη t = 60 sec 133
Σχημα 5. 68: Μεταβολη συχνοτητας περιοχης 1 επειτα απο μεταβολη φορτιου ΔP_L = 0.05 αμ. τη χρονικη στιγμη t = 5 sec. και επιβολη κλιμακουμενης επιθεσης κλισης λ = 5, τη χρονικη στιγμη t = 40 sec.....134
Σχημα 5. 69: Χαρακτηριστικη Σφαλματος Εξοδου Παρατηρητη επειτα απο μεταβολη φορτιου ΔP_L = 0.05 αμ. τη χρονικη στιγμη t = 5 sec. και επιβολη κλιμακουμενης επιθεσης κλισης λ = 5 τη χρονικη στιγμη t = 40 sec 134

1. Εισαγωγή

1.1. Συστήματα Ηλεκτρικής Ενέργειας

Οι αυξημένες ανάγκες του 21ου αιώνα απαιτούν την κατανάλωση τεράστιων ποσοτήτων ενέργειας. Για την κάλυψη αυτών των αναγκών είναι απαραίτητη η δραστική αύξηση σε μέγεθος και πολυπλοκότητα των **Συστημάτων Ηλεκτρικής Ενέργειας**. Η παραδοσιακή δομή ενός ΣΗΕ αποτελείται από τρία υποσυστήματα. Το **Σύστημα Παραγωγής,** το **Σύστημα Μεταφοράς** και το **Σύστημα Διανομής.**



Σχήμα 1. 1 : Σύστημα Παραγωγής Ηλεκτρικής Ενέργειας [1]

Το Σύστημα Παραγωγής Ενέργειας περιλαμβάνει τους σταθμούς παραγωγής ηλεκτρικής ενέργειας, που είναι εγκαταστάσεις στις οποίες μια μορφή πρωτογενούς ενέργειας μετατρέπεται σε κινητική και κατόπιν σε ηλεκτρική με την βοήθεια των γεννητριών. Ανάλογα με την μορφή της πρωτογενούς αυτής ενέργειας οι σταθμοί παραγωγής διακρίνονται σε **θερμοηλεκτρικούς, υδροηλεκτρικούς και ανανεώσιμους.**

Οι αναδυόμενες ανανεώσιμες πηγές ενέργειας (Α.Π.Ε.) που εισάγονται στα δίκτυα για να προσφέρουν στα επίπεδα παραγόμενης ισχύος (ως μονάδες παραγωγής ισχύος φιλικές προς το περιβάλλον), καθώς και αβεβαιότητες, όπως οι περιβαλλοντικοί περιορισμοί λειτουργίας των δομών παραγωγής ενέργειας, αναγάγουν το πρόβλημα του ελέγχου και του σχεδιασμού τους σε μείζον [2]. Οι σύγχρονες αγορές και οι διαχειριστές της ηλεκτρικής ισχύος (πάροχοι), απαιτούν

αυξημένη ευφυΐα και ευελιξία στα συστήματα ελέγχου, για να εξασφαλίσουν ότι αυτά είναι σε θέση να διατηρήσουν την απαιτούμενη ισορροπία μεταξύ της παραγόμενης ισχύος και των φορτίων κατανάλωσης υπό την επίδραση εξωτερικών διαταραχών.

Τα σημερινά συστήματα ηλεκτρικής ενέργειας, πρέπει να χειρίζονται πολύπλοκα, και εκτεινόμενα σε πολλές περιοχές (multi-area) **προβλήματα βελτιστοποίησης** και **ρύθμισης ισχύος** για την ορθή και σταθερή λειτουργία των δικτύων. Τα προβλήματα αυτά χαρακτηρίζονται από υψηλό βαθμό διαφοροποίησης. Η διαφοροποίηση μπορεί να αφορά στις πολιτικές αγοράς ενέργειας (Tariffs), ενώ μάλιστα μπορεί να υπεισέρχεται στις στρατηγικές ελέγχου του δικτύου και τις τεχνικές ανάθεσης της απαιτούμενης ενέργειας προς τις πηγές κάλυψής της (π.χ. η κάλυψη των αναγκών ισχύος στα σύγχρονα δίκτυα πολλές φορές απαιτεί την αγορά ισχύος από εξωτερικούς παρόχους με δεδομένες τιμές χρέωσης και καθορισμένα διαθέσιμα ποσά ισχύος).

Προφανώς, τα συστήματα αυτά θα πρέπει να είναι αρκετά **ευφυή**, αξιοποιώντας τις νέες τεχνολογίες ώστε να ανταπεξέλθουν στα χαρακτηριστικά που αναφέρθηκαν. Ο πυρήνας αυτών των έξυπνων συστημάτων θα πρέπει να βασίζεται σε έξυπνους αλγορίθμους, που υλοποιούνται με την εφαρμογή τεχνολογιών πληροφορικής και τηλεπικοινωνιών.

1.1.1. Ευσταθής Λειτουργεία ΣΗΕ

Με την εφαρμογή όλων των σύγχρονων τεχνολογιών πληροφορικής και τηλεπικοινωνιών στα ΣΗΕ, βελτιώθηκαν η αποδοτικότητα και η αξιοπιστία των μεθόδων και των εξοπλισμών που χρησιμοποιούνταν στην παραγωγή, τη μεταφορά και τη διανομή της ηλεκτρικής ενέργειας, με πιο χαρακτηριστικό παράδειγμα την ευσταθή λειτουργίας τους.

Η **αξιόπιστη παροχή ηλεκτρισμού απαιτεί** την παρουσία όχι μόνο ικανοποιητικής παραγωγής για την κάλυψη των αναγκών των καταναλωτών, αλλά και εφεδρική παραγωγή για κάλυψη απρογραμμάτιστων απωλειών μονάδων παραγωγής ή/και γραμμών μεταφοράς υψηλής τάσεως. Όμως, το επιπλέον κόστος για τη διατήρηση εφεδρικής παραγωγής σε ετοιμότητα, απαιτεί τη συνεχή εξισορρόπηση του κόστους έναντι στο όφελος της αξιόπιστης παροχής ηλεκτρισμού [3], [4].

Ένα ΣΗΕ χαρακτηρίζεται γενικά ευσταθές, όταν ενώ λειτουργεί σε ορισμένη μόνιμη κατάσταση και αφού υποστεί διαταραχή από οποιαδήποτε αιτία, τείνει να επανέλθει σε μόνιμη κατάσταση λειτουργίας, ίδια ή παρόμοια με την αρχική. Ως μόνιμη κατάσταση λειτουργίας ορίζεται μια συνήθης κατάσταση λειτουργίας του συστήματος κατά την οποία το σύστημα εκτελεί τον προορισμό του, δηλαδή παράγει, μεταφέρει και διανέμει σε κάθε στιγμή την ζητούμενη ηλεκτρική ενέργεια.

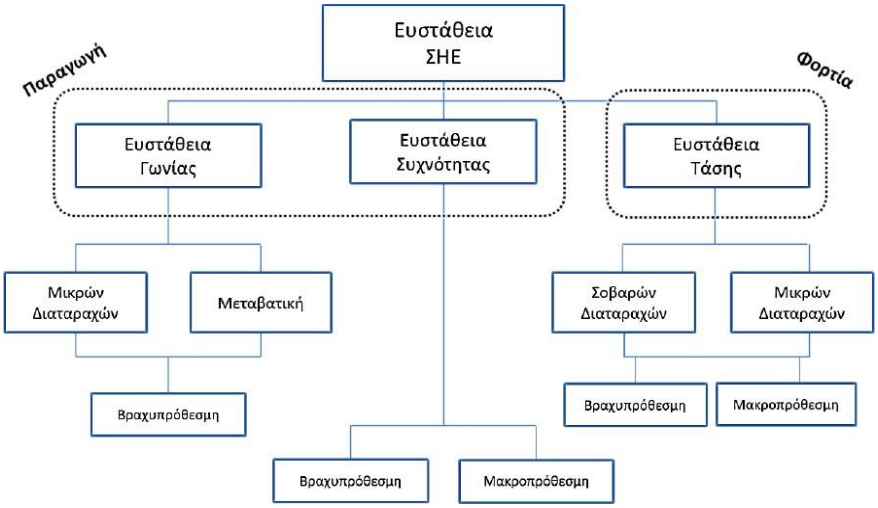
Τα ΣΗΕ είναι δυναμικά μη γραμμικά συστήματα τα οποία υφίστανται συνεχώς διάφορες μικρές ή σοβαρότερες διαταραχές προερχόμενες από μεταβολές της ζήτησης και της παραγωγής, από διακοπές ή ζεύξεις στοιχείων του συστήματος, από

βραχυκυκλώματα ή άλλα σφάλματα, ακόμη και από πιθανές επιθέσεις στο κυβερνοσύστημα.

Τα είδη ευστάθειας μπορούν να κατηγοριοποιηθούν στις εξής κατηγορίες [5], [6] :

- **Στατική ευστάθεια ή ευστάθεια μικρών διαταραχών.** Αφορά την απόκριση του συστήματος σε αργές και βαθμιαίες (μικρές) διαταραχές. Η στατική ευστάθεια εξαρτάται από το εξεταζόμενο σημείο λειτουργίας, αλλά όχι από τη διαταραχή, που θεωρείται υπερβολικά μικρή κατά την ανάλυση ευστάθειας.

- **Μεταβατική ευστάθεια ή ευστάθεια μεγάλων διαταραχών.** Αναφέρεται στην απόκριση του συστήματος σε μεγάλες (σοβαρές) και απότομες διαταραχές (συνήθεις διαταραχές αυτού του τύπου είναι τα βραχυκυκλώματα ή η απότομη μεταβολή μεγάλου φορτίου). Η μεταβατική ευστάθεια εξετάζει αν ένα σύστημα ηλεκτρικής ενέργειας είναι σε θέση να επανέλθει στην ονομαστική λειτουργία μετά από μια συγκεκριμένη μεγάλη διαταραχή και άρα εξαρτάται από το μέγεθος και το είδος της διαταραχής



Σχήμα 1. 2 : Κατηγοριοποίηση μορφών Ευστάθειας

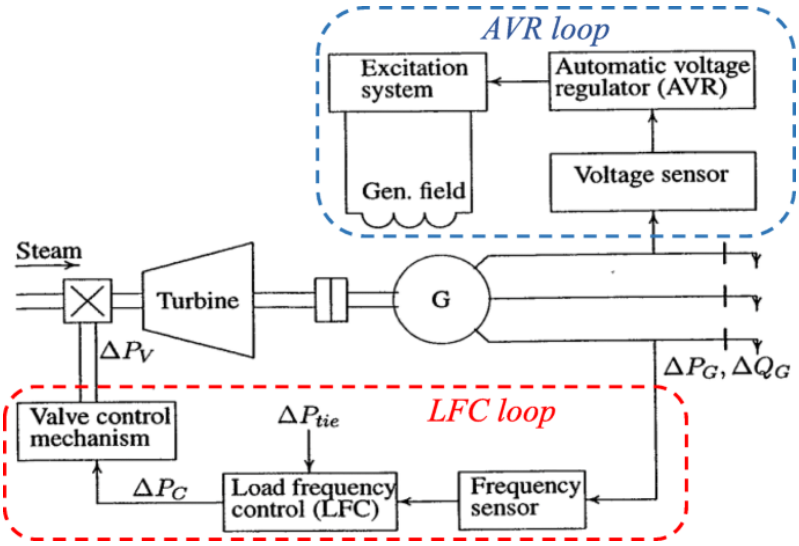
Αναλυτικότερα ανάλογα με τη φύση των εμπλεκόμενων φαινομένων τα είδη αστάθειας μπορούν να κατηγοριοποιηθούν στης εξής κατηγορίες [5], [6], [7] :

- **Ευστάθεια τάσεως** όπου αναφέρεται στην ικανότητα ενός συστήματος να διατηρήσει αποδεκτά επίπεδα τάσεων σε όλους τους ζυγούς του, μετά από μια διαταραχή. Αστάθεια τάσης προκαλείται από την αδυναμία του συστήματος να τροφοδοτήσει με την απαιτούμενη ισχύ τα φορτία που είναι ενταγμένα σε αυτό και λαμβάνει χώρα με τη μορφή μικρών (στατική) ή μεγάλων διαταραχών (μεταβατική).

- **Ευστάθεια γωνίας δρομέα** αναφέρεται στην ικανότητα ενός συνόλου συνδεδεμένων σύγχρονων μηχανών να παραμένουν σε συγχρονισμό μετά από την υποβολή τους σε κάποια διαταραχή. Αστάθεια εμφανίζεται στη μορφή μη αποσβενούμενων ηλεκτρομηχανικών ταλαντώσεων (στατική

αστάθεια) ή μονότονης επιτάχυνσης του δρομέα που οδηγεί σε απώλεια συγχρονισμού (μεταβατική αστάθεια). Το χρονικό πλαίσιο της ευστάθειας γωνίας είναι αυτό των ηλεκτρομηχανικών φαινόμενων, με διάρκεια μερικών δευτερολέπτων και άρα τα φαινόμενα αστάθειας γωνίας κατατάσσονται στη βραχυπρόθεσμη χρονική κλίμακα.

- **Ευστάθεια συχνότητας** αντιστοιχεί στην ικανότητα του συστήματος να διατηρεί τη συχνότητα κοντά στην ονομαστική τιμή μετά από μια σοβαρή διαταραχή (μεταβατική ευστάθεια). Αστάθεια συχνότητας προκαλείται λόγω αναντιστοιχίας μεταξύ της παραγόμενης και της καταναλισκόμενης ενεργού ισχύος. Σε μεγάλα διασυνδεδεμένα ΣΗΕ, η εμφάνιση αστάθειας συχνότητας είναι πιθανή μόνο σε «νησιδοποιημένα» τμήματα του συστήματος μετά από μεγάλη διαταραχή.



Σχήμα 1. 3 : Σχηματικό διάγραμμα Αυτόματης Ρύθμισης Τάσης και Ρύθμισης Φορτίου – Συχνότητας

1.1.2. Δομή Ελέγχου Συστημάτων Ηλεκτρικής Ενέργειας

Η αδυναμία αποθήκευσης μεγάλων ποσοτήτων ηλεκτρικής ενέργειας, οι συνεχείς μεταβολές του προς κάλυψη φορτίου καθώς και διάφορα προβλήματα που μπορεί αιφνιδιαστικά να προκληθούν, όπως πτώσεις κεραυνών, βραχυκυκλώματα, κ.α., επιβάλλουν τη συνεχή προσαρμογή της παραγωγής στις προκύπτουσες απαιτήσεις ενέργειας, έτσι ώστε να διατηρείται μια συνεχής ισορροπία ανάμεσα στην παραγωγή ηλεκτρικής ενέργειας και του μεταβαλλόμενου ηλεκτρικού φορτίου, διατηρώντας παράλληλα τις τιμές της τάσης και της συχνότητας στα ονομαστικά τους επίπεδα για τους λόγους που προαναφέρθηκαν [3], [4]. Αυτό το πρόβλημα αναλαμβάνουν να επιλύσουν ο **τοπικός** και ο **κεντρικός έλεγχος** των συστημάτων ηλεκτρικής ενέργειας, μέσω της συνολικής εποπτείας της λειτουργίας τους σε πραγματικό χρόνο καθώς και της οικονομικής κατανομής της παραγωγής ισχύος στο δίκτυο.

1.1.2.1. Κέντρο Ελέγχου Ενέργειας (Energy Management System)

Το Σύστημα Διαχείρισης Ενέργειας (ή Κέντρο Ελέγχου Ενέργειας) είναι ένα έξυπνο σύστημα απομακρυσμένου ελέγχου και διαχείρισης ενέργειας με υπολογιστή πραγματικού χρόνου (real time), που συλλέγει πληροφορίες και εκτελεί λειτουργίες ελέγχου. Επιπλέον, περιλαμβάνει μεγάλη υπολογιστική ισχύ, δυνατότητα αποθήκευσης μεγάλης ποσότητας πληροφοριών, καταγραφικά, οθόνες και διάφορα λογισμικά προγράμματα εξομοίωσης και επεξεργασίας δεδομένων. Σκοπός ενός EMS είναι η συνολική εποπτεία της λειτουργίας ενός συστήματος σε πραγματικό χρόνο και η οικονομική κατανομή της παραγωγής ηλεκτρικής ισχύος στο δίκτυο. Επιπρόσθετα, ένα σύγχρονο EMS είναι υπεύθυνο για τον έλεγχο της ασφάλειας του συστήματος, το οποίο εποπτεύει [8].

Πιο συγκεκριμένα, το EMS έχει τις παρακάτω λειτουργικές δυνατότητες [9], [10]:

1. Έλεγχος και κατανομή παραγωγής ενέργειας μεταξύ των μονάδων παραγωγής.
2. Ανάλυση και επιτήρηση της ασφάλειας του δικτύου μεταφοράς.
3. Πρόβλεψη ημερησίων και εβδομαδιαίων φορτίων κατανάλωσης και ανάπτυξης στρατηγικής για την ικανοποίηση των αναγκών με το χαμηλότερο δυνατό κόστος (βέλτιστος έλεγχος).
4. Οικονομική ανάλυση αγοράς και πώλησης (ανταλλαγή) ισχύος μεταξύ ηλεκτρικών εταιριών.
5. Ενημέρωση μιας βάσης δεδομένων με πληροφορίες.

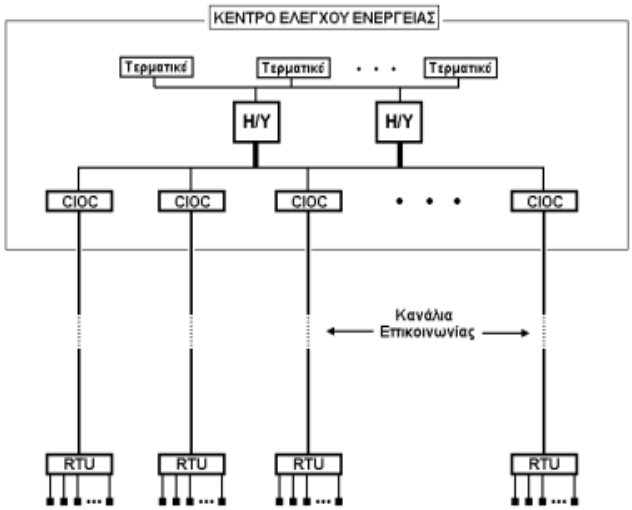
Η ελαχιστοποίηση του κόστους παραγωγής ηλεκτρισμού επιτυγχάνεται με μια σειρά ενεργειών [9], [10], [11]:

1. Βελτιστοποίηση της μίξης των διαφόρων πηγών ενέργειας, που γίνεται μακροχρόνια με τη βοήθεια υπολογιστικών μοντέλων σε Η/Υ. Τα μοντέλα αυτά καθορίζουν τον βέλτιστο συνδυασμό των διάφορων πηγών όπως υδάτων, λιγνίτη, πυρηνικής, γεωθερμικής, αιολικής ενέργειας και αγοράς ισχύος με χαμηλότερο ετήσιο κόστος. Η ανάλυση γίνεται βάσει προβλέψεων στις τιμές των πρωτογενών υλικών που απαιτούνται (καυσίμων και υδάτινου δυναμικού για παράδειγμα). Η διαδικασία αυτή επιφέρει την διαμόρφωση στρατηγικής σε ημερήσια, εβδομαδιαία και μηνιαία βάση, για την ελαχιστοποίηση του κόστους παραγωγής.
2. Η βελτιστοποίηση της διαδικασίας επιτυγχάνεται με την αντιστοίχιση της παραγωγής με την στιγμιαία ζήτηση των καταναλωτών. Αυτή η βελτιστοποίηση της παραγωγής και της μεταφοράς ηλεκτρικής ενέργειας σε πραγματικό χρόνο, είναι γνωστή ως **Αυτόματος Έλεγχος Παραγωγής (Automatic Generation Control)** και αποτελεί μέρος του Συστήματος Διαχείρισης Ενέργειας.

Στα Κέντρα Ελέγχου Ενέργειας των αυτόνομων συστημάτων και σε αντίθεση με τα διασυνδεδεμένα δίκτυα οι διαδικασίες της πρόβλεψης φορτίου, της βραχυχρόνιας (short-term) ένταξης μονάδων και της εκτίμησης της δυναμικής ασφάλειας είναι μείζονος σημασίας. Οι διακυμάνσεις της ζήτησης του φορτίου είναι μεγάλες και η πρόβλεψη τους δυσκολότερη από την αντίστοιχη πρόβλεψη σε ένα διασυνδεδεμένο

σύστημα. Η ένταξη των μονάδων εκτελείται συχνά, λόγω της ανάγκης κάλυψης του έντονα μεταβαλλόμενου φορτίου από ένα μεγάλο αριθμό μονάδων παραγωγής με μικρή ονομαστική ισχύ.

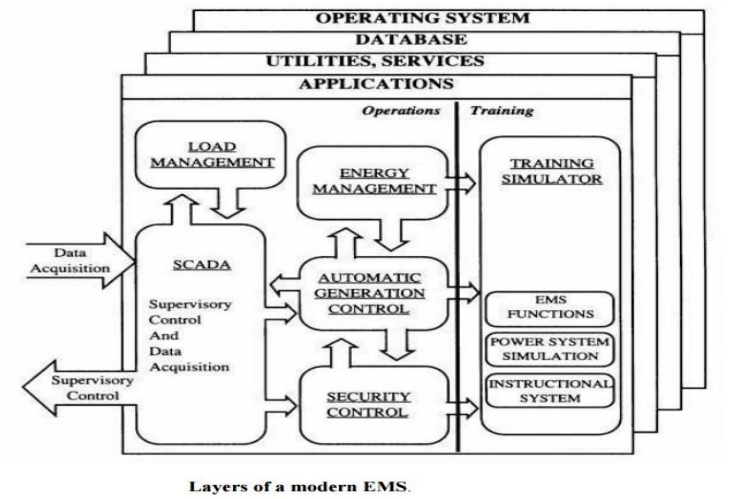
Μία από τις βασικές διαδικασίες κατά την εγκατάσταση ενός Κέντρου Ελέγχου Ενέργειας είναι η τοποθέτηση οργάνων μέτρησης και ελέγχου σε όλα τα σημαντικά σημεία του δικτύου. Οι συγκεκριμένες πληροφορίες μεταβιβάζονται από τα διάφορα σημεία του συστήματος στο κέντρο ελέγχου, μέσω τερματικών μονάδων επικοινωνίας (Remote Terminal Units-RTU). Οι συγκεκριμένες απομακρυσμένες τερματικές μονάδες βρίσκονται σε συνεχή επικοινωνία με τους ελεγκτές εισόδου-εξόδου (Communication Input/Output Controllers), οι οποίοι συνδέονται άμεσα με τους αντίστοιχους ηλεκτρονικούς υπολογιστές τους κέντρου [8].



Σχήμα 1. 4 : Τοπολογία Συλλογής Απομακρυσμένων Πληροφοριών Μέσο RTU [11]

Τα συστήματα Αυτομάτου Ελέγχου Παραγωγής (Automatic Generation Control), ο έλεγχος ασφαλείας, ο εποπτικός έλεγχος και η απόκτηση δεδομένων (Supervisory Control and Data Acquisition - SCADA), καθώς και η διαχείριση φορτίου και η εκτίμηση κατάστασης (State Estimation) είναι οι κύριες μονάδες στο επίπεδο εφαρμογής ενός σύγχρονου συστήματος διαχείρισης ενέργειας, μέσω του οποίου πραγματοποιείται ο έλεγχος για την οικονομικότερη και αποδοτικότερη λειτουργία του ΣΗΕ.

Από τις παραπάνω λειτουργίες του EMS θα περιοριστούμε στην ανάλυση όσων είναι απαραίτητες για τη μελέτη σου συστήματος ρύθμισης φορτίου – συχνότητας, που θα αναλύσουμε στη συνέχεια. Αυτές είναι ο αυτόματος έλεγχος παραγωγής, κομμάτι του οποίου είναι η ρύθμιση φορτίου – συχνότητας καθώς και το σύστημα διαύλων SCADA που όπως θα αναλύσουμε παρακάτω αποτελούν το μέσο επικοινωνίας μεταξύ του αυτομάτου ελέγχου παραγωγής, του συστήματος ισχύος και του Κέντρου Διαχείρισης Ενέργειας.



Σχήμα 1. 5 : Επίπεδα Σύγχρονου Συστήματος Διαχείρισης Ενέργειας

1.1.2.2. Σύστημα Διαύλων SCADA

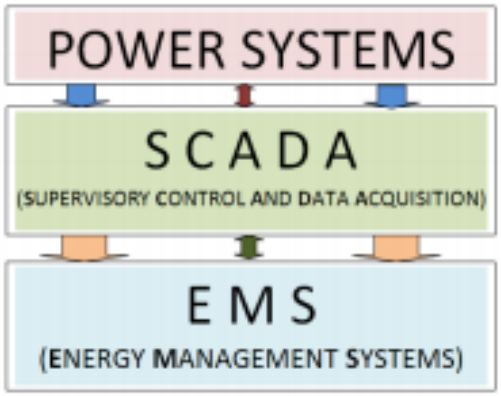
Ένα σύστημα **SCADA** αποτελείται από έναν κεντρικό σταθμό που επικοινωνεί με απομακρυσμένες τερματικές μονάδες (**Remote Telemetry Unit**) και έξυπνες ηλεκτρονικές συσκευές (**Intelligent Electronic Devices**), για ένα ευρύ φάσμα διαδικασιών παρακολούθησης και ελέγχου. με σκοπό να επιτρέπει στους χειριστές να παρατηρούν και να ελέγχουν τις φυσικές εγκαταστάσεις, όπως προαναφέραμε. Σε ένα σύγχρονο σύστημα SCADA, οι λειτουργίες παρακολούθησης, επεξεργασίας και ελέγχου διανέμονται μεταξύ τους σε διάφορους διακομιστές και υπολογιστές που επικοινωνούν με το κέντρο ελέγχου, χρησιμοποιώντας ένα τοπικό δίκτυο (LAN) σε πραγματικό χρόνο. Οι τερματικές μονάδες μεταδίδουν την κατάσταση και τις μετρήσεις του συστήματος και λαμβάνουν εντολές ελέγχου και set points από τον κεντρικό σταθμό. Η επικοινωνία γίνεται γενικά μέσω αποκλειστικών κυκλωμάτων που λειτουργούν στην περιοχή από 600 έως 4800 bit/s με το **RTU** να ανταποκρίνεται σε περιοδικά σήματα που ξεκινούν από τον κεντρικό σταθμό κάθε 2 έως 10 δευτερόλεπτα, ανάλογα με την κρισιμότητα των δεδομένων.

Οι βασικές λειτουργίες των συστημάτων SCADA συνοψίζονται στα παρακάτω [9]:

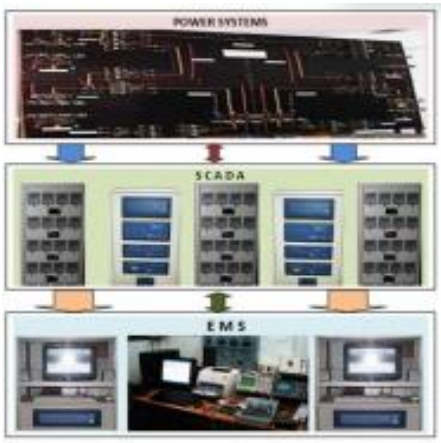
- Απόκτηση δεδομένων: Παρέχει μετρήσεις και πληροφορίες κατάστασης στον χειριστή από απόσταση.
- Εποπτικός έλεγχος: Επιτρέπει στον χειριστή να ελέγχει εξ αποστάσεως συσκευές, π.χ. να ανοίγει και να κλείνει διακόπτες κυκλώματος.
- Επισήμανση: Προσδιορίζει για μια συσκευή ότι υπόκειται σε συγκεκριμένους περιορισμούς λειτουργίας και αποτρέπει τη μη εξουσιοδοτημένη λειτουργία.
- Συναγερμοί: Ενημερώνει τον χειριστή για απρογραμμάτιστα συμβάντα και ανεπιθύμητες συνθήκες λειτουργίας. Οι συναγερμοί ταξινομούνται κατά κρισιμότητα, περιοχή ευθύνης και χρονολογία.
- Καταγραφή: Καταγράφει όλες τις καταχωρίσεις χειριστή, όλους τους συναγερμούς και τις επιλεγμένες πληροφορίες.

- Καταμερισμός φορτίου: Παρέχει αυτόματη ή από τον χειριστή διακοπή σε περίπτωση έκτακτης ανάγκης του συστήματος.
- Γενική κατεύθυνση: Σχεδιάζει μετρήσεις σε επιλεγμένες χρονικές κλίμακες.

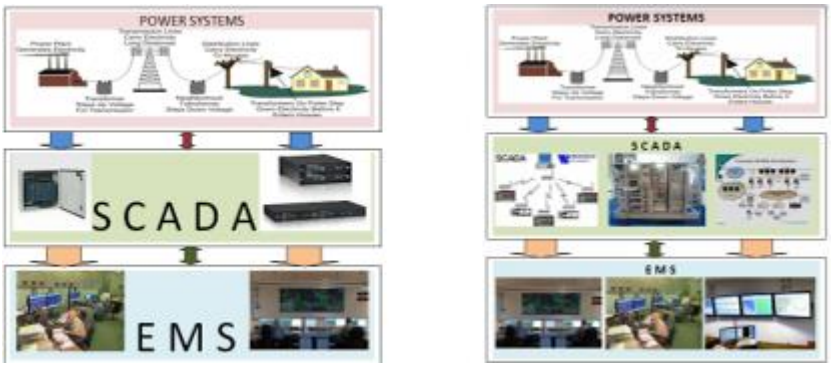
Στα Συστήματα Ηλεκτρικής Ενέργειας οι δίαυλοι επικοινωνίας SCADA, αποτελούν το μέσο επικοινωνίας μεταξύ του Αυτόματου Ελέγχου Παραγωγής, του συστήματος ισχύος και του Κέντρου Διαχείρισης Ενέργειας.



Σχήμα 1. 6 : Ροή Ισχύος και Πληροφορίας μεταξύ Συστημάτων Ισχύος, SCADA και EMS [10]



Σχήμα 1. 7 : Πραγματική απεικόνιση Συστημάτων Ισχύος, SCADA, EMS σε περιβάλλον εργαστηρίου [10]



Σχήμα 1. 8 : Στοιχεία και Δομή Συστημάτων Ισχύος, SCADA και EMS [10]

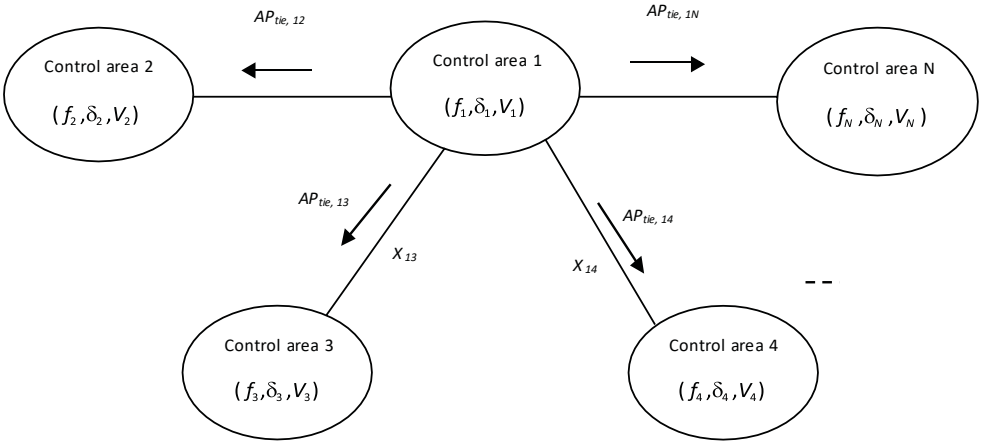
1.1.2.3. Αυτόματος Έλεγχος Παραγωγής (Automatic Generation Control)

Η μονάδα **Αυτόματου Ελέγχου Παραγωγής** (**AGC** - Automatic Generation Control) αποτελεί τη βάση ελέγχου για την παραγωγή και την εξισορρόπηση της ισχύος σε ένα δίκτυο. Η αρχική της εφαρμογή εμφανιζόταν στον απευθείας έλεγχο της παραγωγής ισχύος από τις ηλεκτρογεννήτριες. Αρχικά ήταν προσαρμοσμένη ως κύκλωμα αυτομάτου ελέγχου επί των γεννητριών, διασφαλίζοντας σε μικρή κλίμακα την ορθή λειτουργία των τοπικών συστημάτων παραγωγής. Η λειτουργία του AGC βασιζόταν στις αρχές ελέγχου λειτουργίας των γεννητριών με απευθείας μετρήσεις επί των εξόδων διανομής ισχύος αυτών [12].

Στις πρώτες εποχές, το AGC χρησιμοποιήθηκε βάσει στρατηγικής κεντρικού ελέγχου (centralized control model). Ένας σημαντικός περιορισμός της στρατηγικής κεντρικού ελέγχου AGC, είναι ότι απαιτεί την ανταλλαγή πληροφοριών μεταξύ του σταθμού λήψης αποφάσεων και των αισθητήρων μέτρησης, μεταφέροντας εντολές και πληροφορίες σε απομακρυσμένες γεωγραφικές περιοχές. Ο κεντρικός έλεγχος για την εφαρμογή του απαιτεί αυξημένη υπολογιστική και αποθηκευτική πολυπλοκότητα. Όμως, η κεντρική διασύνδεση των συστημάτων AGC παρέχει τη δυνατότητα συνολικού χειρισμού της παροχής ισχύος στους διασυνδεόμενους παρόχους – φορτία.

Από την άλλη, οι αποκεντρωμένες στρατηγικές αυτόματου ελέγχου παραγωγής (de-centralized control models) ασχολούνται πολύ αποτελεσματικά με τους περιορισμούς του κεντρικού συστήματος ισχύος. Οι ερευνητές πρότειναν τις μεθόδους σχεδιασμού συστηματικού κατανεμημένου ελέγχου και πέτυχαν σχεδόν ταυτόσημα αποτελέσματα με τις κεντρικές στρατηγικές ελέγχου. Οι αποκεντρωμένες τεχνικές ελέγχου με χρήση τοπικών AGC δίνουν τη δυνατότητα αυτόνομης λειτουργικότητας των υποσυστημάτων AGC για την επίτευξη της τοπικής ισορροπίας παροχής – ζήτησης φορτίου για την περιοχή την οποία χειρίζεται το υποσύστημα ελέγχου [13], [14], [15].

Η δράση του AGC μπορεί επίσης να κατηγοριοποιηθεί ανάλογα με το πλήθος των περιοχών ελέγχου, είτε σε σύστημα μιας περιοχής (Single Area) είτε σε συστήματα πολλαπλών περιοχών (Multi Area). Οι απλές περιοχές ελέγχου συνεπάγονται τη χρήση ενός αυτόνομου AGC συστήματος για τον έλεγχο μίας περιοχής. Οι πολλαπλές περιοχές ελέγχου συνδυάζουν τη χρήση πολλών συστημάτων AGC, τα οποία επικοινωνούν μεταξύ τους με μία ή περισσότερες γραμμές μεταφοράς που ονομάζονται γραμμές διασύνδεσης. Στόχος είναι η αγορά ή η πώληση ενέργειας με γειτονικά συστήματα των οποίων το λειτουργικό κόστος καθιστά τέτοιες συναλλαγές επικερδείς. Επίσης, ακόμα κι αν δεν μεταδίδεται ισχύς μέσω των γραμμών, εάν ένα σύστημα έχει ξαφνική απώλεια μιας μονάδας παραγωγής, οι μονάδες όλης της διασύνδεσης θα αντιμετωπίσουν την αλλαγή συχνότητας και θα βοηθήσουν στην αποκατάσταση της. Οι γεννήτριες απαιτείται να διατηρούν συγχρονισμό με τις γραμμές διασύνδεσης και τις συνδεδεμένες περιοχές [16 - 18].



Σχήμα 1. 9 : Σύστημα Ισχύος N – Περιοχών [19]

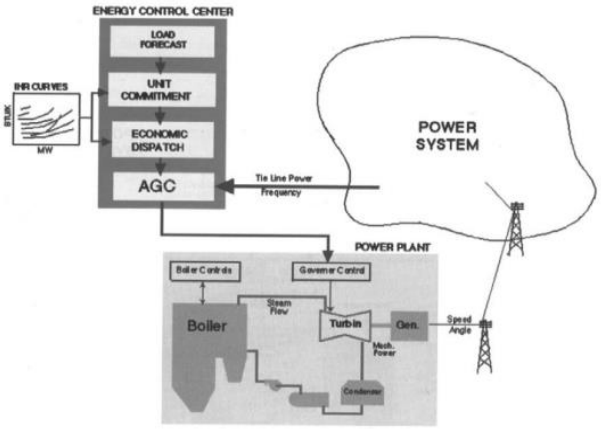
Τα πλεονεκτήματα ενός συστήματος πολλών περιοχών είναι [19]:

- Η αξιοπιστία
- Η βελτιστοποίηση της παραγωγής
- Η συνεχής παροχή ενέργειας
- Το χαμηλότερο Κόστος ανά KW για μεγαλύτερες γεννήτριες.

Η μονάδα **Αυτόματου Ελέγχου Παραγωγής** (**AGC** – Automatic Generation Control) είναι επιφορτισμένη με τις παρακάτω λειτουργικές αρμοδιότητες [11]:

- **Να διατηρεί την συχνότητα του συστήματος σταθερή (50/60 Hz)**
- **Να διατηρεί τη ροή ισχύος μεταξύ διασυνδεδεμένων ηλεκτρικών δικτύων σταθερή και σύμφωνα με τις προσυμφωνημένες δεσμεύσεις ή προγραμματισμένες ποσότητες.**
- Να διασφαλίσει ελάχιστο κόστος παραγωγής και μεταφοράς.
- Να εποπτεύει την εφεδρική παραγωγή, ώστε να εξασφαλίζεται η εύρυθμη λειτουργία.

Η διαδικασία των υποσυστημάτων AGC εκτελείται σε ένα κέντρο ελέγχου απομακρυσμένο από τα εργοστάσια παραγωγής, ενώ η παραγόμενη ισχύς ελέγχεται από ρυθμιστές ελέγχου των γεννητριών στο χώρο παραγωγής.



Σχήμα 1. 10 : Σύστημα Εποπτικού Ελέγχου Ηλεκτρικής Ενέργειας

Οι γεννήτριες παραγωγής ηλεκτρικής ισχύος αποθηκεύουν κινητική ενέργεια λόγω των μεγάλων περιστρεφόμενων τμημάτων τους. Όλη η κινητική ενέργεια που αποθηκεύεται σε ένα σύστημα ισχύος με περιστρεφόμενους άξονες είναι ένα μέρος της αδράνειας του δικτύου. Όταν αυξάνεται το φορτίο του συστήματος, η αδράνεια του δικτύου χρησιμοποιείται αρχικά, ως εσωτερική ενέργεια, για την τροφοδοσία του φορτίου. Αυτό, ωστόσο, οδηγεί σε μείωση της αποθηκευμένης κινητικής ενέργειας των γεννητριών. Δεδομένου ότι η μηχανική ισχύς αυτών των γεννητριών συσχετίζεται με την παραγόμενη ηλεκτρική ισχύ, οι γεννήτριες καταλήγουν σε μείωση της γωνιακής ταχύτητας περιστροφής των κινητών τμημάτων τους, το οποίο σημαίνει αυτομάτως μείωση της συχνότητας του δικτύου.

Η πραγματική ισχύς σε ένα σύστημα ισχύος ελέγχεται μέσω της μηχανικής ισχύος εξόδου του κινητήρα. Ανάλογα με τον τύπο της παραγωγής, ο κινητήρας μπορεί να είναι ένας ατμοστρόβιλος, ένας αεριοστρόβιλος, ένας υδροστρόβιλος ή ένας κινητήρας ντίζελ. Στην περίπτωση ενός ατμοστροβύλου ή υδροστρόβιλου, η μηχανική ισχύς ελέγχεται με το άνοιγμα ή το κλείσιμο των βαλβίδων που ρυθμίζουν την είσοδο ατμού ή τη ροή νερού στον στρόβιλο. Η είσοδος ατμού (ή νερού) στους στροβίλους πρέπει να ρυθμίζεται συνεχώς για να ανταποκρίνεται στην πραγματική ζήτηση ισχύος, διαφορετικά η ταχύτητα της μηχανής θα ποικίλλει με επακόλουθη αλλαγή στη συχνότητα.

Σε ένα σύστημα ηλεκτρικής ενέργειας θα πρέπει τόσο η τάση όσο και η συχνότητα να καθορίζονται στις επιθυμητές τιμές ανεξάρτητα από την αλλαγή των φορτίων που συμβαίνει τυχαία. Στην πραγματικότητα, είναι αδύνατο να διατηρηθεί τόσο η ενεργός όσο και η άεργος ισχύς χωρίς έλεγχο, καθώς κάτι τέτοιο θα οδηγούσε σε διακύμανση των επιπέδων τάσης και συχνότητας. Για να ακυρωθεί λοιπόν, η επίδραση της μεταβολής του φορτίου και να διατηρηθούν σταθερά η συχνότητα και το επίπεδο τάσης, απαιτείται ένα σύστημα ελέγχου. Συνήθως η ενεργός και η άεργος ισχύς έχουν συνδυασμένη επίδραση στη συχνότητα και την τάση, οπότε το πρόβλημα ελέγχου της συχνότητας και της τάσης μπορεί να διαχωριστεί. Η συχνότητα εξαρτάται κυρίως από την ενεργό ισχύ και η τάση εξαρτάται κυρίως από την άεργο ισχύ.

Η απόκλιση συχνότητας (frequency deviation) είναι άμεσο αποτέλεσμα της ανισορροπίας μεταξύ του ηλεκτρικού φορτίου και της παροχής ισχύος από τις συνδεδεμένες γεννήτριες στο δίκτυο και αποτελεί την πρωταρχική μετρική βάση για την ανίχνευση και τον έλεγχο της εξισορρόπησης. Έτσι, η απόκλιση συχνότητας παρέχει ένα χρήσιμο δείκτη για την ένδειξη της παραγόμενης ισχύος και της ανισορροπίας φορτίου - κατανάλωσης. Μία μόνιμη μεταβολή της ονομαστικής συχνότητας επηρεάζει άμεσα τη λειτουργία του συστήματος ισχύος, την ασφάλεια και την αξιοπιστία του.

Όταν η **συχνότητα** λειτουργίας του δικτύου ισχύος αυξάνεται, τότε παράγεται περισσότερη ισχύς από τη ζητούμενη, γεγονός που προκαλεί επιτάχυνση όλων των μηχανών που διασυνδέονται στο σύστημα. Εάν η συχνότητα του δικτύου παροχής ισχύος μειώνεται, τότε τα φορτία του συστήματος δεν καλύπτονται ικανοποιητικά από την παρεχόμενη ισχύ παραγωγής, γεγονός που προκαλεί επιβράδυνση σε όλες τις μηχανές που διασυνδέονται στο σύστημα. Το αποτέλεσμα των παραπάνω είναι κοινό και πολλές φορές καταστροφικό για τους σταθμούς παραγωγής. Η συχνότητα λοιπόν, θα πρέπει να διατηρείται στο $\pm 2{,}5$ % της ονομαστικής τιμής για τους εξής λόγους [8]:

- Οι διακυμάνσεις στη συχνότητα μπορεί να βλάψουν ή να καταστρέψουν τα πτερύγια του στροβίλου, που είναι κατασκευασμένα ώστε να λειτουργούν σε σταθερή ταχύτητα.
- Τα φορτία του εναλλασσόμενου τριφασικού κινητήρα συνδέονται άμεσα με τη συχνότητα και επομένως μια αλλαγή στη συχνότητα μπορεί να επηρεάσει την απόδοσή του κινητήρα γενικότερα.
- Η εφαρμογή τάσης με συχνότητα μικρότερη της επιθυμητής σε έναν μετασχηματιστή ισχύος μπορεί να προκαλέσει μία αύξηση στη ροή ρεύματος

και αυτή με τη σειρά της να επιφέρει χαμηλότερη απόδοση και υπερθέρμανση που μπορεί να οδηγήσει στην καταστροφή τους.

- Τα ηλεκτρικά ρολόγια συνδέονται με τους σύγχρονους κινητήρες και επομένως εξαρτώνται από τη συχνότητα και το ολοκλήρωμα του σφάλματος συχνότητας.
- Και τέλος, σε θερμοηλεκτρικούς σταθμούς οι αποκλίσεις στη συχνότητα μειώνουν την παραγωγή και αν αυτό το γεγονός γίνει συσσωρευτικά ο σταθμός παραγωγής καταρρέει (black out).

Δεδομένου ότι η συχνότητα που παράγεται στο ηλεκτρικό δίκτυο είναι ανάλογη προς την ταχύτητα περιστροφής της γεννήτριας, το πρωταρχικό πρόβλημα του ελέγχου συχνότητας συνεπώς, μπορεί να αναχθεί άμεσα σε ένα πρόβλημα ελέγχου της ταχύτητας περιστροφής της γεννήτριας. Αυτό αρχικά μπορεί να ξεπεραστεί με την προσθήκη ενός μηχανισμού ελέγχου που μετρά την ταχύτητα περιστροφής της γεννήτριας. Ο έλεγχος ρυθμίζει τη ροή καυσίμου (ή ποσότητα νερού, πυρηνικό καύσιμο, κλπ, ανάλογα τον σταθμό παραγωγής) για να αλλάξει το μηχανικό επίπεδο ισχύος στην έξοδο, παρακολουθώντας ταυτόχρονα τα φορτία, επαναφέροντας έτσι τη συχνότητα στην ονομαστική τιμή λειτουργίας για το δίκτυο.

Έτσι λοιπόν η εξισορρόπηση παραγόμενης ισχύος και φορτίου και η διατήρηση της επιθυμητής συχνότητας σε ένα σύστημα ηλεκτρικής ενέργειας γίνεται με τους ρυθμιστές στροφών των γεννητριών, οι οποίοι ελέγχουν τη μηχανική ισχύ που παράγεται στους κινητήρες.

Εάν το σύστημα είναι συνδεδεμένο με πολλά φορτία σε ένα σύστημα ισχύος, τότε η συχνότητα και η ταχύτητα του συστήματος αλλάζουν ανάλογα με τα χαρακτηριστικά του ρυθμιστή στροφών καθώς αλλάζει το φορτίο. Εάν δεν απαιτείται να διατηρείται σταθερή η συχνότητα σε ένα σύστημα, τότε ο χειριστής δεν απαιτείται να αλλάξει τη ρύθμιση της γεννήτριας. Εάν όμως απαιτείται σταθερή συχνότητα, τότε ο χειριστής μπορεί να ρυθμίσει την ταχύτητα του στροβίλου αλλάζοντας τα χαρακτηριστικά του ρυθμιστή στροφών.

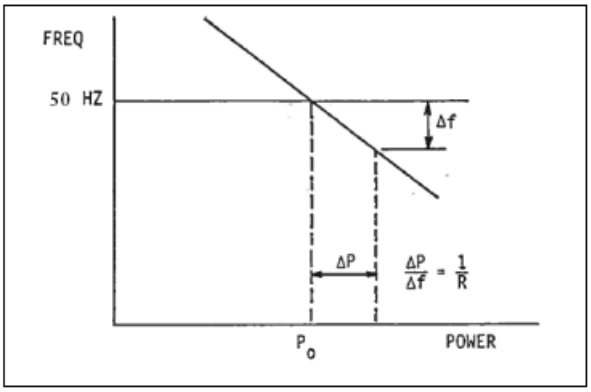
Οι ρυθμιστές στροφών μπορούν να χαρακτηριστούν είτε μηχανισμοί ελέγχου της συχνότητας, είτε μηχανισμοί ελέγχου της ισχύος. Αν μια γεννήτρια τροφοδοτεί ένα απομονωμένο φορτίο, τότε ο ρυθμιστής στροφών λειτουργεί ελέγχοντας τη συχνότητα, ενώ αν συνδέεται σε ένα μεγαλύτερο σύστημα, τότε η ταχύτητα περιστροφής της είναι δεσμευμένη από τη συχνότητα του συστήματος και ο ρυθμιστής στροφών ελέγχει στην ουσία την παραγόμενη ισχύ.

1.1.2.3.1. Πρωτεύουσα Ρύθμιση Συχνότητας

Ο ρυθμιστής στροφών διαθέτει δύο τύπους ρυθμίσεων. Η πρώτη είναι η **πρωτεύουσα Ρύθμιση** (δεν υπάρχει τηλεχειρισμός και SCADA), όπου η μεταβολή της ταχύτητας περιστροφής της γεννήτριας, γίνεται αντιληπτή από τον **φυγοκεντρικό ρυθμιστή**, που είναι συνδεδεμένος με τον άξονά της. Αυτή η μεταβολή μετατρέπεται σε **σήμα-εντολή** για μετακίνηση της δικλείδας του ατμοστροβίλου (ή πχ του ανοίγματος των πτερυγίων

του υδροστροβίλου για υδροηλεκτρικά), ώστε να προσαρμοστεί η μηχανική ισχύς που παράγεται.

Μία ορισμένη θέση του μηχανισμού αλλαγής στροφών, δηλαδή μια δεδομένη ταχύτητα αναφοράς, αντιστοιχεί σε μια ευθύγραμμη χαρακτηριστική Φορτίου-Συχνότητας. Η αρνητική κλίση λέγεται **στατισμός** και είναι στην ουσία το ποσοστό επί τοις εκατό της μόνιμης μεταβολής της συχνότητας λειτουργίας για μια μεταβολή του φορτίου ίση με την ονομαστική ισχύ της γεννήτριας.



Σχήμα 1. 11 : Χαρακτηριστική Καμπύλη Στατισμού

Μια μονάδα με μικρό στατισμό, για σχετικά μικρή μεταβολή συχνότητας μεταβάλλει σημαντικά το φορτίο της και λέγεται ρυθμίζουσα γιατί συμβάλλει καθοριστικά με τη μεταβολή της παραγωγής της στη Ρύθμιση της Συχνότητας, ενώ αντίθετα αν μια μονάδα έχει μεγάλο στατισμό, τότε μεταβάλλει ελάχιστα το φορτίο της όταν αλλάζει η συχνότητα και λέγεται μονάδα βάσεως [19].

1.1.2.3.2. Δευτερεύουσα Ρύθμιση (Ρύθμιση Φορτίου - Συχνότητας)

Το μόνιμο σφάλμα της συχνότητας έρχεται να διορθώσει η Δευτερεύουσα Ρύθμιση Φορτίου, κατά την οποία ενεργοποιείται ο μηχανισμός αλλαγής στροφών, μετρώντας το σφάλμα της συχνότητας, μέσω ενός συμπληρωματικού βρόχου, αλλά και τυχόν διαφορές στην διακινούμενη ισχύ των εξωτερικών διασυνδέσεων όταν έχουμε σύστημα πολλών περιοχών [20].

Ο συμπληρωματικός βρόχος παρέχει ανατροφοδότηση μέσω μέτρησης της απόκλισης συχνότητας επί της εξόδου της γεννήτριας και προσθέτει αυτήν την απόκλιση στον κύριο βρόχο ελέγχου, μέσω ενός δυναμικού ελεγκτή. Το αποτέλεσμα (σήμα ΔPc) χρησιμοποιείται για τη ρύθμιση της συχνότητας του συστήματος. Στα πραγματικά συστήματα παραγωγής ισχύος, ο δυναμικός ελεγκτής είναι συνήθως ένας απλός αναλογικός – ολοκληρωτικός ελεγκτής (Proportional – Integral Controller - PI). Μετά από μία αλλαγή στο φορτίο, ο μηχανισμός ανάδρασης παρέχει ένα κατάλληλο σήμα για την παραγωγή ισχύος στη γεννήτρια (σήμα ΔPm) για να αποδώσει τη ζητούμενη ισχύ στο φορτίο και να επαναφέρει τη συχνότητα του συστήματος.

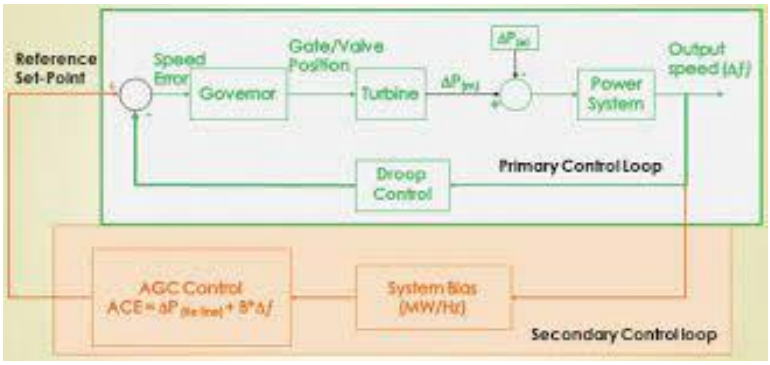
Κατά τη διάρκεια μίας ξαφνικής αύξησης του φορτίου περιοχής, η συχνότητα της περιοχής παρουσιάζει μία παροδική πτώση. Η πτώση αυτή μπορεί να διαδοθεί και στις

υπόλοιπες περιοχές χειρισμού, εφόσον πρόκειται για ένα σύστημα ελέγχου πολλαπλών περιοχών με κεντρικό έλεγχο. Κατά τη μεταβατική κατάσταση, προορίζονται ροές ισχύος από άλλες περιοχές για την κάλυψη του υπερβολικού φορτίου που προέκυψε στην περιοχή αυτή. Για να αποφευχθεί η διάδοση μίας τέτοιας διαταραχής σε ολόκληρο το δίκτυο, συνήθως, μόνο καθορισμένες μονάδες παραγωγής ισχύος σε κάθε περιοχή βρίσκονται σε κατάσταση ρύθμισης, καθώς το φορτίο αλλάζει. Σε σταθερή κατάσταση, η παρεχόμενη ισχύς από το δίκτυο ισορροπεί απόλυτα με τα φορτία ζήτησης, προκαλώντας σχεδόν μηδενικές αποκλίσεις ισχύος και συχνότητας.

Όταν όμως δεν υπάρχει αυτή η απόλυτη ισορροπία, στο σύστημα προκύπτει ένα σφάλμα. Ο συνδυασμός των σημάτων σφάλματος ονομάζεται Σφάλμα Ελέγχου Περιοχής (Area Control Error) και εκφράζει την ενεργειακή ανισορροπία μεταξύ παραγωγής και φορτίου. Είναι δηλαδή η διαφορά παραγόμενης ισχύος - καταναλισκόμενης ισχύος από τα φορτία και ενός κατωφλίου ισχύος (threshold). Με κατάλληλη στρατηγική ελέγχου, στέλνονται σήματα που αντιστοιχούν σε μια νέα ταχύτητα αναφοράς κάθε γεννήτριας.

Πιο συγκεκριμένα, ο ελεγκτής που βασίζει τη λειτουργία του στο σήμα ACE μπορεί να ενεργοποιηθεί για να στείλει υψηλότερους/χαμηλότερους παλμούς σήματος στις συμμετέχουσες γεννήτριες εφόσον το σήμα εισόδου του ACE υπερβαίνει ένα κατώφλι. Οι καθυστερήσεις, ο ρυθμός αύξησης/μείωσης και τα όρια ενεργοποίησης διαφέρουν ανά γεννήτρια που συνδέεται στο σύστημα και πρέπει να ρυθμιστούν ειδικά για διαφορετικές μονάδες παραγωγής.

Ο λόγος για τη χρήση κατωφλίων (thresholds) ενεργοποίησης είναι για να μην καθίσταται το σύστημα ελέγχου ευαίσθητο σε γρήγορες μεταβολές, οι οποίες οδηγούν σε γρήγορη λήψη αποφάσεων και κατά συνέπεια πολύ γρήγορη μεταβολή των ρυθμίσεων του συστήματος παραγωγής ισχύος (γεννήτριες).



Σχήμα 1. 12 : Σχήμα Πρωτεύουσας και Δευτερεύουσας Ρύθμισης

Σε καμία περίπτωση δεν είναι επιθυμητό, ακόμη και αν αυτό είναι δυνατό, να προσπαθήσουμε να μηδενίσουμε την παράμετρο. Ο λόγος είναι ότι αυτό θα απαιτούσε πολύ γρήγορες μεταβολές για τις μονάδες παραγωγής ισχύος μέσω των διαδιδόμενων σημάτων ελέγχου.

Συνήθως, η δευτερεύουσα ρύθμιση γίνεται κεντρικά για κάθε περιοχή ελέγχου ενός διασυνδεδεμένου συστήματος σε διακριτό χρόνο με σταθερή περίοδο λειτουργίας (2-10 sec). Ο υπολογισμός του **ΣΕΠ**, δηλαδή η διαφορά μεταξύ προγραμματισμένης και πραγματικής παραγωγής ηλεκτρικής ενέργειας σε μια περιοχή ελέγχου στο δίκτυο

ισχύος λαμβάνοντας υπόψη την πόλωση συχνότητας, γίνεται Περιφερειακό ή Κεντρικό Κέντρο Ελέγχου Ενέργειας, το οποίο στη συνέχεια αποστέλλει σε κάθε μονάδα της περιοχής ελέγχου τα Σήματα Επιθυμητής Παραγωγής. Επιθυμητή είναι η ελαχιστοποίηση του ΣΕΠ, όχι όμως ο μηδενισμός όπως αναφέραμε [8], [20].

Οι ροές στις διασυνδετικές γραμμές γίνονται βάσει προγράμματος, κατά τρόπο που να προκύπτει όφελος για όλα τα συνεργαζόμενα συστήματα (περιοχές). Ανάλογα τα ελεγχόμενα μεγέθη διακρίνονται τρείς τύποι ρύθμισης φορτίου-συχνότητας στα συστήματα με εξωτερική διασύνδεση [20]:

- **Επίπεδος Έλεγχος Συχνότητας** (flat frequency control) : Ρυθμίζεται μόνο η συχνότητα του συστήματος και δεν ελέγχεται η διασυνδετική ροή.
- **Επίπεδος Έλεγχος Διασύνδεσης** (flat tie-line control)**:** Ρυθμίζεται μόνο η ροή της εξωτερικής διασύνδεσης. Η παραγόμενη ισχύς αναπροσαρμόζεται, έτσι ώστε να παραμένει σταθερή η ανταλλαγή ισχύος με το εξωτερικό σύστημα, ανεξάρτητα από τις μεταβολές φορτίου στο ένα ή και στα δύο συστήματα.
- **Σύνθετος Έλεγχος με Συντελεστή Πολώσεως** (biased frequency tie-line control) : Ο πιο διαδεδομένος τύπος ρύθμισης φορτίου-συχνότητας για τα διασυνδεδεμένα συστήματα. Σε αυτόν τον έλεγχο, έχουμε δύο μετρήσεις, τόσο της συχνότητας όσο και της διασυνδετικής ροής, οι οποίες συντίθενται στο ΣΕΠ, όπως αναφέραμε.

1.2. Κυβερνοασφάλεια και Ευπαθή Σημεία Συστημάτων Ηλεκτρικής Ενέργειας

1.2.1. Κυβερνοασφάλεια στα Συστήματα Ηλεκτρικής Ενέργειας

Ως κυβερνοασφάλεια του έξυπνου δικτύου ή οποιουδήποτε άλλου συστήματος ισχύος, θεωρούμε τα μέτρα (τεχνικά ή μη) και τις διαδικασίες που εφαρμόζει ένας οργανισμός για να προστατέψει τη "Διαθεσιμότητα" (Availability), "Ακεραιότητα" (Integrity) και "Εμπιστευτικότητα" (Confidentiality). Οι κυβερνοεπιθέσεις του συστήματος ισχύος μπορούν να ταξινομηθούν βάσει αυτών των τριών απαιτήσεων ασφαλείας υψηλού επιπέδου [21], [22].

Σχήμα 1. 13 : Το τρίγωνο Διαθεσιμότητας - Ακεραιότητας - Εμπιστευτικότητας

Η διαθεσιμότητα (Availability) διασφαλίζει την έγκαιρη και αξιόπιστη διαθεσιμότητα των πληροφοριών στο δίκτυο μετάδοσης του συστήματος ισχύος. Από την άποψη του ελέγχου, είναι δουλεία του συστήματος ελέγχου ή των εξαρτημάτων του συστήματος, όπως αισθητήρες, ενεργοποιητές και ελεγκτές, να είναι προσβάσιμα και να λειτουργούν από εξουσιοδοτημένο φορέα κατόπιν αιτήματος. Οι επιθέσεις όπως η άρνηση εξυπηρέτησης (DoS), τις οποίες θα εξετάσουμε αναλυτικότερα στη συνέχεια, επηρεάζουν τη διαθεσιμότητα πληροφοριών στα κανάλια επικοινωνίας και αποτελούν απειλή για μια τέτοια απαίτηση ασφάλειας [21], [22].

Η ακεραιότητα (Integrity) ενός συστήματος αναφέρεται στην ικανότητα επίτευξης επιχειρησιακών στόχων μέσω της πρόληψης και της ανίχνευσης επιθέσεων σε κανάλια επικοινωνίας μεταξύ ενεργοποιητών, αισθητήρων και ελεγκτών. Οι επιθέσεις του συστήματος ισχύος που απειλούν την ακεραιότητα τροποποιούν γενικά τα δεδομένα που μεταφέρονται μέσω των καναλιών επικοινωνίας του συστήματος ισχύος. Τα δεδομένα τηλεμετρίας από το RTU των συστημάτων ισχύος όπως οι γραμμές διασύνδεσης των περιοχών ή τα σήματα ισχύος στα κανάλια επικοινωνίας των συστημάτων είναι ευάλωτα κυρίως σε επιθέσεις ακεραιότητας. Οι επιθέσεις ακεραιότητας δεδομένων είναι σοβαρές απειλές που μπορούν να θέσουν σε κίνδυνο τη σταθερή λειτουργία των δικτύων ή των συστημάτων ισχύος και θα τις αναλύσουμε εκτενώς στην παρούσα εργασία [21], [22].

Η εμπιστευτικότητα (Confidentiality) αναφέρεται στην ικανότητα του συστήματος να διατηρεί τις πληροφορίες απρόσιτες σε μη εξουσιοδοτημένους χρήστες. Αυτό εμποδίζει διείσδυση στα φυσικά συστήματα μέσω της υποκλοπής της επικοινωνίας αισθητήρων, ενεργοποιητών και ελεγκτών [21], [22].

Επομένως, για να διασφαλιστούν τα τρία χαρακτηριστικά ασφαλείας, απαιτούνται πολύ αποτελεσματικοί μηχανισμοί ανίχνευσης και άμυνας κατά των κυβερνοεπιθέσεων.

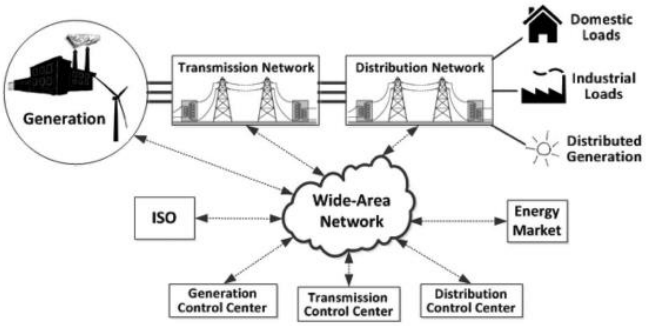
1.2.2. Ευπαθή Σημεία στα Συστήματα Ηλεκτρικής Ενέργειας

Οι έξυπνες τεχνολογίες που χρησιμοποιούνται κατά κόρον στις μέρες μας είναι επιρρεπείς σε κυβερνοεπιθέσεις καθώς υποστηρίζουν τεχνολογίες πληροφορικής όπως αναλύσαμε και μπορεί εύκολα να επηρεαστεί η σταθερότητα του συστήματος ισχύος. Επιπλέον, τεχνικές ελέγχου ευρείας παρακολούθησης, βασισμένες στο Διαδίκτυο Πραγμάτων (Internet of Things) έχουν αναπτυχθεί για έξυπνα δίκτυα ηλεκτρικής ενέργειας με Διαχείριση Διανεμημένων Ενεργειακών Πόρων (Distributed Energy Resources), τα οποία επίσης συμβάλουν στην μεγαλύτερη ευπάθεια των συστημάτων σε επιθέσεις.

Στον τομέα της ενέργειας γενικά, έχουν παρατηρηθεί περίπου 800 κυβερνοεπιθέσεις από τη δεκαετία του 1980. Περίπου 250 περιπτώσεις παρατηρήθηκαν στις ΗΠΑ που είναι ακούσιες, όπως η Διακοπή παροχής δημόσιας υπηρεσίας της Αριζόνα (2007) και η Διακοπή ρεύματος και φωτός στη Φλόριντα (2008) [23] Ωστόσο, πιθανώς η πρώτη σκόπιμη μεγάλη επίθεση στον τομέα της ηλεκτρικής ενέργειας παρατηρήθηκε στις 23 Δεκεμβρίου 2015 στην Ουκρανία όπου το ουκρανικό δίκτυο ηλεκτρικής ενέργειας

υπέστη διακοπή ρεύματος (black out) και επηρεάζοντας περίπου 225.000 πελάτες για αρκετές ώρες [24]. Η επίθεση πραγματοποιήθηκε από κακόβουλο λογισμικό μέσω phishing email. Αυτό το περιστατικό άνοιξε τα μάτια των ερευνητών ώστε να αναζητήσουν κάποιο μηχανισμό ελέγχου που να ενσωματώνει την κυβερνο-φυσική προσέγγιση για την ασφάλεια του.

Ως εκ τούτου, από την άποψη της λειτουργίας του συστήματος ισχύος, η βελτίωση της σταθερότητας και ο ανθεκτικός στην επίθεση έλεγχος του συστήματος ισχύος (Resilient Control) είναι εξαιρετικά σημαντικά πεδία που απαιτούν συνεχή έρευνα.



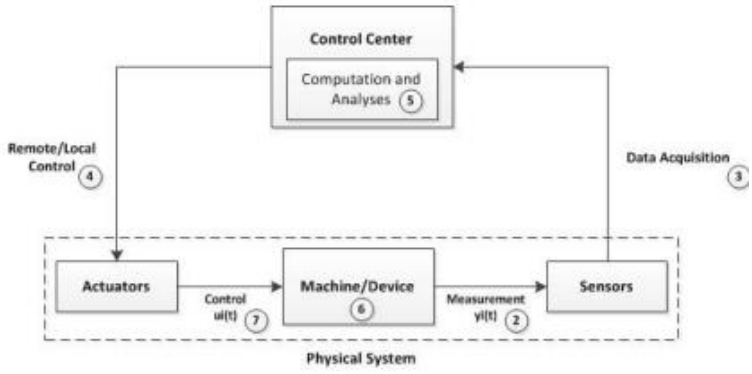
Σχήμα 1. 14 : Κυβερνο – φυσικό Δίκτυο Ηλεκτρικής Ενέργειας

Τα σύγχρονα συστήματα ηλεκτρικής ενέργειας αποτελούνται από ηλεκτρονικές συσκευές πεδίου, δίκτυα επικοινωνιών, συστήματα αυτοματισμού υποσταθμών και κέντρα ελέγχου για να επιτύχουν αποτελεσματική και αξιόπιστη παραγωγή, μετάδοση και διανομή ισχύος.

Το κέντρο ελέγχου είναι υπεύθυνο για την παρακολούθηση, τον έλεγχο και τη λήψη επιχειρησιακών αποφάσεων σε πραγματικό χρόνο. Οι ανεξάρτητοι χειριστές συστημάτων συντονίζουν τις επιχειρήσεις παροχής ενέργειας και αποστέλλουν εντολές στα κέντρα ελέγχου τους. Οι επιχειρήσεις κοινής ωφέλειας που συμμετέχουν σε αγορές ηλεκτρικής ενέργειας αλληλεπιδρούν επίσης με τους ανεξάρτητους χειριστές ενέργειας για να υποστηρίξουν τις λειτουργίες της αγοράς με βάση την παραγωγή, τη μεταφορά και τη ζήτηση ενέργειας σε πραγματικό χρόνο [9], [10].

Τα **κέντρα ελέγχου** λαμβάνουν μετρήσεις από αισθητήρες (**sensors**) που αλληλεπιδρούν με συσκευές πεδίου (γραμμές μετάδοσης, μετασχηματιστές κ.λπ.). Οι αλγόριθμοι που εκτελούνται στο κέντρο ελέγχου επεξεργάζονται αυτές τις μετρήσεις για να λάβουν επιχειρησιακές αποφάσεις. Στη συνέχεια, οι αποφάσεις μεταδίδονται στους ενεργοποιητές (**actuators**) για να εφαρμόσουν αυτές τις αλλαγές σε συσκευές πεδίου [22].

Στο σύστημα ισχύος, οι μετρούμενες φυσικές παράμετροι μπορεί να αναφέρονται σε ποσότητες όπως η τάση, η ισχύς και η συχνότητα. Αυτές οι μετρήσεις από υποσταθμούς, γραμμές μεταφοράς και άλλα μηχανήματα αποστέλλονται στο κέντρο ελέγχου χρησιμοποιώντας ειδικά πρωτόκολλα επικοινωνίας.



Σχήμα 1. 15 : Τυπικό Μοντέλο Ελέγχου Δικτύου Ισχύος

Στη συνέχεια, οι μετρήσεις επεξεργάζονται από ένα σύνολο υπολογιστικών αλγορίθμων, που εκτελούνται στο κέντρο ελέγχου. Έπειτα, τα σήματα που προκύπτουν από το κέντρο ελέγχου μεταδίδονται σε ενεργοποιητές (actuators) που σχετίζονται με συσκευές πεδίου.

Κάποιος επιτιθέμενος θα μπορούσε να εκμεταλλευτεί ευπάθειες κατά μήκος των συνδέσμων επικοινωνίας και να δημιουργήσει πρότυπα επίθεσης σχεδιασμένα είτε να καταστρέφουν το περιεχόμενο (π.χ. επιθέσεις ακεραιότητας), είτε να εισάγουν χρονική καθυστέρηση ή άρνηση στην επικοινωνία (π.χ. άρνηση υπηρεσίας (Denial of Service), στα σήματα ελέγχου/μέτρησης [22], [26].

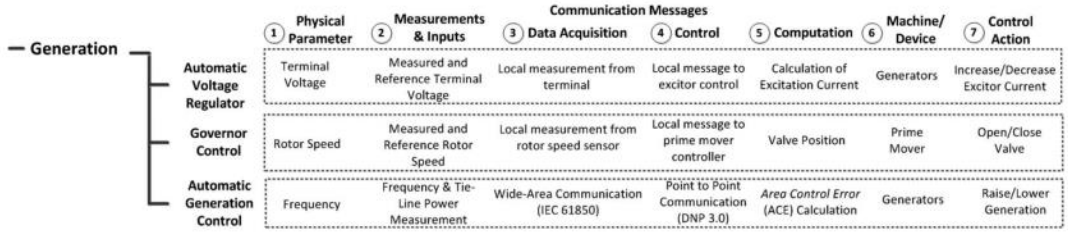
Είναι σημαντικό να μελετηθούν και να αναλυθούν οι επιπτώσεις τέτοιων επιθέσεων στο σύστημα ηλεκτρικής ενέργειας, καθώς θα μπορούσαν να επηρεάσουν σοβαρά την ασφάλεια και την αξιοπιστία του. Αυτές οι επιπτώσεις μπορούν να αφορούν την απώλεια φορτίου ή τις παραβιάσεις και τις αλλαγές στη συχνότητα και την τάση λειτουργίας του συστήματος. Οι μελέτες επιθέσεων θα βοηθήσουν επίσης στην ανάπτυξη αντίμετρων που μπορούν να αποτρέψουν επιθέσεις ή να μετριάσουν τις επιπτώσεις από τις επιθέσεις. Τα αντίμετρα περιλαμβάνουν τεχνικές ανίχνευσης κακών δεδομένων και αλγόριθμους ελέγχου ανθεκτικούς στην επίθεση.

Power System Control Loop \ Impact from Attack Type		Data Integrity	Denial of Service	Replay and Timing	Malware	De-Sync
Generation	Automatic Voltage Regulator	NA	NA	NA	Yes	NA
	Governor Control	NA	NA	NA	Yes	NA
	Automatic Generation Control	Yes	Maybe	Yes	Yes	Maybe
Transmission	State Estimation	Maybe	Maybe	Maybe	Yes	No
	VAR Compensation	Yes	Yes	Yes	Yes	Yes
	Wide-Area Measurement Systems	Yes	Yes	Yes	Yes	Yes
Distribution	Load Shedding	Yes	Maybe	Maybe	Yes	NA
	Advanced Metering Infrastructure	Yes	Yes	Yes	Yes	NA

Σχήμα 1. 16 : Ταξινόμηση Αντικτύπου διαφόρων επιθέσεων σε βρόχους ελέγχου της παραγωγής, της μεταφοράς και της διανομής ισχύος [26].

1.2.2.1. Ευπαθή Σημεία Ελέγχου στην Παραγωγή

Οι βρόχοι ελέγχου στην παραγωγή αφορούν κυρίως τον έλεγχο της ισχύος εξόδου της γεννήτριας και της τάσης ακροδεκτών. Η παραγωγή ελέγχεται τόσο από τοπικά (αυτόματος ρυθμιστής τάσης - AVR) και ρυθμιστής στροφών) όσο και από συστήματα ελέγχου ευρείας περιοχής (αυτόματος έλεγχος παραγωγής - AGC) [26].



Σχήμα 1. 17 : Ταξινόμηση Ελέγχου Παραγωγής [26]

- Αυτόματος ρυθμιστής τάσης (AVR):

Ο έλεγχος διεγέρτη γεννήτριας χρησιμοποιείται για τη βελτίωση της σταθερότητας του συστήματος ισχύος ελέγχοντας την ποσότητα άεργου ισχύος που απορροφάται ή εγχέεται στο σύστημα. Ο ψηφιακός εξοπλισμός ελέγχου για τον διεγέρτη επιτρέπει τη δοκιμή διαφορετικών αλγορίθμων για τη βελτίωση της σταθερότητας του συστήματος. Ως εκ τούτου, αυτή η οικονομικά αποδοτική προσέγγιση προτιμάται ευρέως και χρησιμοποιείται από επιχειρήσεις κοινής ωφελείας. Η μονάδα ελέγχου ψηφιακού διεγέρτη συνδέεται με το κέντρο ελέγχου της εγκατάστασης μέσω Ethernet και επικοινωνεί χρησιμοποιώντας πρωτόκολλα όπως το Modbus. Αυτή η σύνδεση Ethernet χρησιμοποιείται για τον προγραμματισμό του ελεγκτή με τιμές σημείου ρύθμισης τάσης. Ο βρόχος ελέγχου AVR λαμβάνει ανάδραση της τάσης της γεννήτριας από το τερματικό και τη συγκρίνει με το σημείο ρύθμισης τάσης που είναι αποθηκευμένο στη μνήμη. Με βάση τη διαφορά μεταξύ της παρατηρούμενης μέτρησης και του σημείου ρύθμισης, το ρεύμα μέσω του διεγέρτη τροποποιείται για να διατηρείται η τάση στο επιθυμητό επίπεδο.

- Έλεγχος του ρυθμιστή στροφών:

Ο έλεγχος του ρυθμιστή στροφών είναι ο πρωταρχικός μηχανισμός ελέγχου συχνότητας. Αυτός ο μηχανισμός χρησιμοποιεί έναν αισθητήρα που ανιχνεύει αλλαγές στην ταχύτητα που συνοδεύουν τις διαταραχές και κατά συνέπεια αλλάζει τις ρυθμίσεις στη βαλβίδα ατμού για να αλλάξει την ισχύ εξόδου από τη γεννήτρια. Οι ελεγκτές που χρησιμοποιούνται στις σύγχρονες μονάδες ελέγχου ψηφιακού ρυθμιστή χρησιμοποιούν το πρωτόκολλο Modbus για να επικοινωνούν με υπολογιστές στο κέντρο ελέγχου μέσω Ethernet. Όπως και στην περίπτωση του AVR, αυτή η σύνδεση επικοινωνίας χρησιμοποιείται για τον καθορισμό του σημείου ρύθμισης λειτουργίας για τον έλεγχο του ρυθμιστή .

Το AVR και ο έλεγχος του ρυθμιστή στροφών είναι βρόχοι τοπικού ελέγχου. Δεν εξαρτώνται από τα συστήματα SCADA για τις λειτουργίες τους, καθώς τόσο η τάση

τερματικού όσο και η ταχύτητα του ρότορα ανιχνεύονται τοπικά. Ως εκ τούτου, η επιφάνεια επίθεσης για αυτούς τους βρόχους ελέγχου είναι περιορισμένη.

- Αυτόματος έλεγχος παραγωγής:

Ο βρόχος αυτόματης παραγωγής ελέγχου (AGC) είναι ένας δευτερεύων βρόχος ελέγχου συχνότητας που ασχολείται με τη ρύθμιση της συχνότητας του συστήματος στην ονομαστική του τιμή. Η λειτουργία του βρόχου AGC είναι να κάνει διορθώσεις στη διασυνδετική ροή μεταξύ περιοχών και στην απόκλιση της συχνότητας. Ο αλγόριθμος συσχετίζει την απόκλιση συχνότητας και τις μετρήσεις της ροής διασύνδεσης για τον προσδιορισμό του σφάλματος ελέγχου περιοχής. Η διόρθωση αποστέλλεται σε κάθε σταθμό παραγωγής για την προσαρμογή των σημείων λειτουργίας μία φορά κάθε πέντε δευτερόλεπτα.

Πιο αναλυτικά γνωρίζουμε πως μεταξύ των διαφόρων ελέγχων, ο έλεγχος συχνότητας είναι ο πιο σημαντικός αλλά και ο πιο χρονοβόρος μηχανισμός ελέγχου των συστημάτων, λόγω της εμπλοκής των μηχανικών εξαρτημάτων. Τα σήματα ελέγχου που αποστέλλονται κατά την προσπάθεια του συστήματος να διατηρήσει την συχνότητα σταθερή, χρειάζονται αρκετά δευτερόλεπτα και επομένως, στα πλαίσια της ρύθμισης φορτίου-συχνότητας (LFC), δεν είναι εφικτή η διατήρηση πολλών δεδομένων και η διαχείριση πολύπλοκων αλγορίθμων επικύρωσης δεδομένων. Το γεγονός αυτό καθιστά τη ρύθμιση φορτίου-συχνότητας, το πιο ευάλωτο σημείο ελέγχου σε διαταραχές και επιθέσεις στον κυβερνοχώρο.

Τα σύγχρονα συστήματα LFC χρησιμοποιούν ανοιχτή υποδομή επικοινωνίας σε αντίθεση με τα συμβατικά LFC, τα οποία χρησιμοποιούσαν ειδικά κανάλια επικοινωνίας για τη μετάδοση σημάτων, μεταξύ απομακρυσμένων τερματικών μονάδων (RTU), κέντρου ελέγχου και μονάδας γεννητριών. Το αποκεντρωμένο σύστημα LFC με ανοιχτό δίκτυο επικοινωνίας είναι πιο ευαίσθητα σε διάφορες κακόβουλες επιθέσεις, όπως μπλοκάρισμα καναλιών επικοινωνίας, έγχυση ψευδών δεδομένων (injection of false data), αλλοιώσεις στο φορτίο του συστήματος ισχύος κ.λπ. Επιπλέον, τα σχήματα LFC πρέπει να παράγουν σήματα ελέγχου στο χρονοδιάγραμμα των δευτερολέπτων. Επομένως, ο βρόχος LFC δεν μπορεί να χρησιμοποιήσει σύνθετους αλγόριθμους επικύρωσης δεδομένων για την επικύρωση και την εκτίμηση των δεδομένων μέτρησης. Οι εισβολείς μπορούν να επωφεληθούν από αυτό και να χειριστούν τα δεδομένα μέτρησης με λιγότερο λεπτομερή μαθηματικά.

1.2.2.2. Ευπαθή Σημεία Ελέγχου στην Μεταφορά

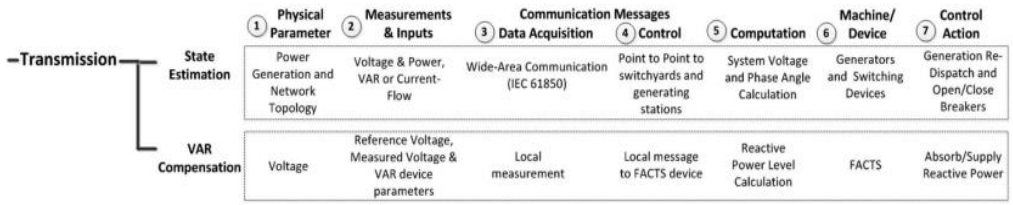
Το σύστημα μεταφοράς λειτουργεί συνήθως σε τάσεις άνω των 13 KV και τα ελεγχόμενα εξαρτήματα περιλαμβάνουν συσκευές μεταγωγής και υποστήριξης αέργου ισχύος. Είναι ευθύνη του χειριστή να διασφαλίσει ότι η ισχύς που ρέει μέσω των γραμμών είναι εντός των ασφαλών περιθωρίων λειτουργίας και ότι διατηρείται η σωστή τάση. Οι παρακάτω βρόχοι ελέγχου βοηθούν τον χειριστή σε αυτήν τη λειτουργία [26].

- Εκτίμηση κατάστασης:

Η εκτίμηση κατάστασης του συστήματος ισχύος είναι μια τεχνική με την οποία πραγματοποιούνται εκτιμήσεις μεταβλητών του συστήματος, όπως το μέγεθος της τάσης και η γωνία φάσης (μεταβλητές κατάστασης) με βάση τις εικαζόμενες λανθασμένες μετρήσεις από συσκευές πεδίου. Η διαδικασία παρέχει μια εκτίμηση των μεταβλητών κατάστασης όχι μόνο όταν οι συσκευές πεδίου παρέχουν ατελείς μετρήσεις, αλλά και όταν το κέντρο ελέγχου αποτυγχάνει να λάβει μετρήσεις είτε λόγω δυσλειτουργίας της συσκευής είτε του καναλιού επικοινωνίας. Αυτό δίνει στον χειριστή λεπτομέρειες σχετικά με τις ροές ισχύος και τα μεγέθη τάσης κατά μήκος διαφορετικών τμημάτων του δικτύου μεταφοράς και ως εκ τούτου βοηθά στη λήψη αποφάσεων. Το κέντρο ελέγχου εκτελεί υπολογισμούς χρησιμοποιώντας χιλιάδες μετρήσεις που λαμβάνει. Αυτές οι τεχνικές παρέχουν καλές εκτιμήσεις των μεταβλητών κατάστασης παρά τα σφάλματα που εισάγονται από τυχόν ατέλειες των συσκευών και των καναλιών επικοινωνίας.

- Αντιστάθμιση VAR:

Η αντιστάθμιση άεργου βολτ-αμπέρ (VAR) είναι η διαδικασία ελέγχου της έγχυσης ή της απορρόφησης άεργου ισχύος σε ένα σύστημα ισχύος για τη βελτίωση της απόδοσης του συστήματος μετάδοσης. Ο πρωταρχικός στόχος τέτοιων συσκευών είναι να ελαχιστοποιούν τις διακυμάνσεις τάσης σε ένα δεδομένο άκρο μιας γραμμής μεταφοράς. Αυτές οι συσκευές μπορούν επίσης να αυξήσουν τη μεταβιβάσιμη ισχύ μέσω μιας δεδομένης γραμμής μεταφοράς και έχουν επίσης τη δυνατότητα να βοηθήσουν στην αποφυγή καταστάσεων συσκότισης. Οι σύγχρονοι πυκνωτές και επαγωγείς με μηχανική εναλλαγή ήταν οι συμβατικές συσκευές αντιστάθμισης VAR. Ωστόσο, με την πρόσφατη πρόοδο στους ελεγκτές που βασίζονται σε θυρίστορ, συσκευές όπως αυτές που ανήκουν στην οικογένεια των ευέλικτων συστημάτων μετάδοσης εναλλασσόμενου ρεύματος (FACTS), κερδίζουν δημοτικότητα. Οι συσκευές FACTS αλληλεπιδρούν μεταξύ τους για την ανταλλαγή επιχειρησιακών πληροφοριών. Αν και αυτές οι συσκευές λειτουργούν αυτόνομα, εξαρτώνται από την επικοινωνία με άλλες συσκευές FACTS, πράγμα που τις κάνει ευπάθειες στον κυβερνοχώρο.



Σχήμα 1. 18 : Ταξινόμηση Ελέγχου στη Μεταφορά [26]

1.2.2.3. Ευπαθή Σημεία Ελέγχου στη Διανομή

Το σύστημα διανομής είναι υπεύθυνο για την παροχή ενέργειας στον πελάτη. Με την εμφάνιση του έξυπνου δικτύου, οι πρόσθετοι βρόχοι ελέγχου που επιτρέπουν τον άμεσο έλεγχο του φορτίου σε επίπεδο τελικού χρήστη γίνονται όλο και πιο συνηθισμένοι [26].

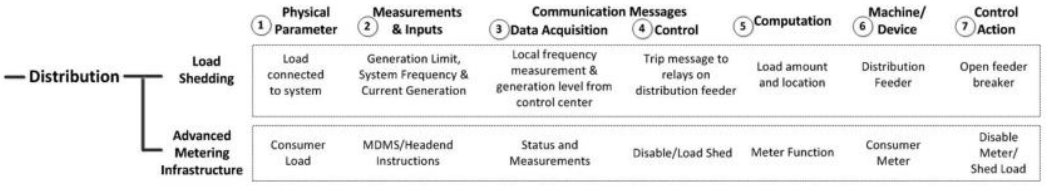
- Απόρριψη φορτίου (Load Shedding) :

Τα προγράμματα μείωσης φορτίου είναι χρήσιμα για την πρόληψη της κατάρρευσης του συστήματος κατά τις συνθήκες λειτουργίας έκτακτης ανάγκης. Αυτά τα σχήματα μπορούν να ταξινομηθούν σε προληπτικά, αντιδραστικά και χειροκίνητα. Τα ενεργά και προληπτικά σχήματα είναι συστήματα αυτόματης απόρριψης φορτίου που λειτουργούν με τη βοήθεια ρελέ. Για παράδειγμα, σε περιπτώσεις όπου η παραγωγή συστήματος είναι ανεπαρκής για να ανταποκριθεί στο φορτίο, θα μπορούσαν να χρησιμοποιηθούν συστήματα αυτόματης απόρριψης φορτίου για τη διατήρηση της συχνότητας του συστήματος εντός ασφαλών ορίων λειτουργίας και την προστασία του εξοπλισμού που είναι συνδεδεμένος στο σύστημα. Όταν παραστεί ανάγκη, το φορτίο απορρίπτεται από ένα βοηθητικό πρόγραμμα στο επίπεδο διανομής από τα ρελέ χαμηλής συχνότητας που είναι συνδεδεμένα στον τροφοδότη διανομής. Τα σύγχρονα ρελέ ακολουθούν το πρωτόκολλο Διαδικτύου (IP) και υποστηρίζουν πρωτόκολλα επικοινωνίας όπως το IEC 61850. Μια επίθεση στην υποδομή επικοινωνίας του ρελέ ή μια κακόβουλη αλλαγή στη λογική ελέγχου θα μπορούσε να οδηγήσει σε απρογραμμάτιστη ενεργοποίηση των τροφοδοτών διανομής για μη εξυπηρετούμενα τμήματα φόρτωσης.

- AMI και διαχείριση από πλευράς ζήτησης:

Τα μελλοντικά συστήματα διανομής θα βασίζονται σε μεγάλο βαθμό στην AMI για να αυξήσουν την αξιοπιστία, να ενσωματώσουν ανανεώσιμες πηγές ενέργειας και να παρέχουν στους καταναλωτές λεπτομερή παρακολούθηση της κατανάλωσης. Η AMI βασίζεται κυρίως στην ανάπτυξη μετρητών στις τοποθεσίες των καταναλωτών για την παροχή μετρήσεων σε πραγματικό χρόνο. Οι έξυπνοι μετρητές παρέχουν στις επιχειρήσεις κοινής ωφελείας τη δυνατότητα να εφαρμόζουν μεταγωγή ελέγχου φορτίου (Load Control Switching) για να απενεργοποιούν τις συσκευές καταναλωτών όταν η ζήτηση αυξάνεται. Η διαχείριση από την πλευρά της ζήτησης εισάγει μια cyber-physical σύνδεση μεταξύ της μετρητικής υποδομής στον κυβερνοχώρο και της ισχύος που παρέχεται στους καταναλωτές. Η τρέχουσα διαμόρφωση του μετρητή ελέγχεται από ένα σύστημα διαχείρισης δεδομένων μετρητή (MDMS) το οποίο βρίσκεται υπό έλεγχο κοινής ωφέλειας. Το MDMS συνδέεται με μια συσκευή κεφαλής AMI που προωθεί εντολές και συγκεντρώνει δεδομένα που συλλέγονται από τους μετρητές σε όλη την υποδομή. Η δικτύωση εντός της υποδομής AMI πιθανότατα θα βασίζεται σε πολλές διαφορετικές τεχνολογίες, συμπεριλαμβανομένων των δικτύων ραδιοσυχνοτήτων, του WiMax, του WiFi και του φορέα παροχής ηλεκτρικού δικτύου. Είναι προφανές επομένως, πως ο έλεγχος για το εάν ο μετρητής είναι ενεργοποιημένος ή απενεργοποιημένος και η δυνατότητα απομακρυσμένης απενεργοποίησης συσκευών μέσω εναλλαγής ελέγχου φορτίου αποτελούν πιθανές απειλές από τους εισβολείς. Η

προσθήκη πρόσθετης ασφάλειας σε αυτές τις λειτουργίες παρουσιάζει ενδιαφέρουσες προκλήσεις.



Σχήμα 1. 19 : Ταξινόμηση Ελέγχου στη Διανομή [26]

Στα πλαίσια της παρούσας διπλωματικής γίνεται μελέτη και ανάλυση κυβερνοεπιθέσεων στον τομέα της παραγωγής και συγκεκριμένα στον αυτόματο έλεγχο παραγωγής και δη στη ρύθμιση φορτίου συχνότητας, που όπως είδαμε, η μελέτη και ανάλυση των επιπτώσεων επίθεσης στο σύστημα LFC είναι εξαιρετικά σημαντική.

2. Μαθηματική μοντελοποίηση συστήματος ρύθμισης φορτίου συχνότητας

2.1. Μοντελοποίηση των στοιχείων των Συστημάτων Ισχύος

Η μελέτη της απόκρισης των συστημάτων ισχύος σε διαταραχές και λειτουργικές αλλαγές γίνεται σε μεγάλο βαθμό με τη βοήθεια μαθηματικών μοντέλων και προσομοιώσεων υπολογιστή. Η μαθηματικοποίηση των περιγραφών αποτελεί τη βάση για την εφαρμογή προσομοιώσεων με χρήση Η/Υ για τον έλεγχο της λειτουργίας των δικτύων ισχύος μεγάλης κλίμακας. Οι συνθήκες που επιβάλλονται στο μαθηματικό μοντέλο μπορεί να είναι ακραίες, ανάλογα με το επιθυμητό σενάριο προσομοίωσης. Τα αποτελέσματα προσομοίωσης δίνουν τη δυνατότητα για εξαγωγή συμπερασμάτων ως προς τη λήψη αποφάσεων και δράσεων στο σύστημα. Επίσης αποτελούν χρήσιμα εργαλεία για την ανάλυση λειτουργίας των δικτύων ισχύος σε φάσεις επιθέσεων, όπως θα παρουσιασθεί και στις επόμενες ενότητες της εργασίας.

Τα μαθηματικά μοντέλα που περιλαμβάνουν μικρές διαταραχές αναπτύσσονται με γραμμικοποίηση του συστήματος γύρω από ένα τρέχον σημείο λειτουργίας, αλλά για μεγαλύτερες διαταραχές θα πρέπει να γίνει επίλυση μη γραμμικών διαφορικών εξισώσεων. Η μελέτη LFC βασίζεται βασικά στην ανάλυση μικρού σήματος. Τα γραμμικά μοντέλα στροβίλων, ρυθμιστών, συστημάτων ισχύος και σχετικών εξισώσεων είναι αποδεκτά και έχουν χρησιμοποιηθεί από πολλούς ερευνητές για μοντελοποίηση συστημάτων LFC σε απομονωμένα και διασυνδεδεμένα συστήματα ισχύος.

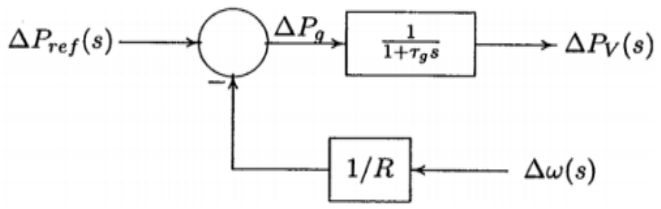
Το πρώτο βήμα για την ανάλυση του συστήματος ελέγχου είναι η μαθηματική μοντελοποίηση των στοιχείων του. Στην παρούσα εργασία χρησιμοποιήσαμε το μοντέλο ενός θερμοηλεκτρικού σταθμού, επομένως μοντελοποιήσαμε το Ρυθμιστή Στροφών, το Στρόβιλο καθώς και τη Γεννήτρια – Φορτίο [16].

2.1.1. Μοντέλο Ρυθμιστή Στροφών (Governor)

Όταν το ηλεκτρικό φορτίο αυξάνεται ξαφνικά, τότε η ηλεκτρική ισχύς υπερβαίνει τη μηχανική ισχύ εισόδου. Αυτή η έλλειψη ισχύος στην πλευρά του φορτίου αντισταθμίζεται από την κινητική ενέργεια του στροβίλου. Λόγω αυτού η αποθηκευμένη ενέργεια μειώνεται και ο ρυθμιστής στέλνει σήμα για παροχή περισσότερων όγκων νερού, ατμού ή αερίου ανάλογα τον σταθμό παραγωγής, ώστε να αυξήσει την ταχύτητα του στροβίλου και να αντισταθμιστεί η διαφορά στην ταχύτητα.

Ο ρυθμιστής Στροφών έχει δύο εισόδους :

- ΔP_{ref_i} : Συχνότητα αναφοράς εκφρασμένη σε ισχύ (MW)
- Δf_i : Μεταβολή της συχνότητας ή $\Delta \omega_i$: μεταβολή γωνιακής ταχύτητας



Σχήμα 2. 1 : Διάγραμμα Βαθμίδων Συστήματος Ρυθμιστή Στροφών

Μια αύξηση λοιπόν του ΔP_{ref} ή μια μείωση στο Δf προκαλούν αύξηση της παραγωγής, όπως φαίνεται και από τη σχέση (2.1).

$$\Delta P_g = \Delta P_{ref} - \frac{1}{R} \cdot \Delta_f \tag{2.1}$$

Η εντολή ΔP_g μετατρέπεται μέσω του κέρδους του ρυθμιστή (K_g) στην εντολή θέσης βαλβίδας ατμού ΔP_v. Εάν T_g είναι η χρονική σταθερά και το K_g το κέρδος του ρυθμιστή, τότε η έξοδος του ρυθμιστή ΔP_V μπορεί να εκφραστεί ως :

$$\Delta P_v = \frac{1}{1+T_g} \cdot \Delta P_g \tag{2.2}$$

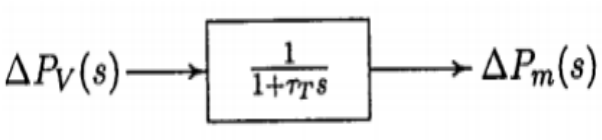
2.1.2. Μοντέλο Στροβίλου (Turbine)

Η πηγή της παραγωγής ενέργειας προέρχεται από το κομμάτι που είναι γνωστό ως στρόβιλος. Ο στρόβιλος αυτός, μιλώντας για συμβατικούς σταθμούς παραγωγής, μπορεί να είναι υδροστρόβιλος, οπότε η ενέργεια προέρχεται από την πτώση νερού ή ατμοστρόβιλος του οποίου η ενέργεια προέρχεται από την καύση του άνθρακα, του αερίου και άλλων καυσίμων. Το μοντέλο για τον στρόβιλο συσχετίζει τις αλλαγές στη μηχανική ισχύ εξόδου ΔP_m με τις αλλαγές στη θέση της βαλβίδας ατμού ΔP_v.

$$\Delta P_m = \frac{1}{1+T_t} \cdot \Delta P_v \tag{2.3}$$

T_t : σταθερά χρόνου στροβίλου (0.2 – 2 sec)

ΔP_m : αλλαγή στην ισχύ που αναπτύσσεται από τον στρόβιλο



Σχήμα 2. 2 : Διάγραμμα Βαθμίδων Συστήματος Στροβίλου

2.1.3. Μοντέλο Γεννήτριας (Generator)

Μια αλλαγή στο φορτίο σημαίνει αλλαγή στην ηλεκτρική ροπή εξόδου της γεννήτριας T_e. Όπως γνωρίζουμε σύμφωνα με την εξίσωση ταλάντωσης μηχανής η ηλεκτρική ροπή και η μηχανική ροπή πρέπει να είναι ίσες για να είναι το σύστημα σε ισορροπία.

$$\frac{2\,H}{\omega}\,\frac{d^2\Delta\delta}{dt^2} = \Delta P_m - \Delta P_e \qquad (2.4)$$

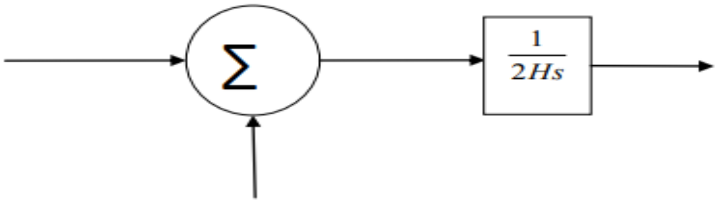
Σε περίπτωση μεταβολής της ταχύτητας :

$$\frac{d\Delta\omega}{dt} = \frac{1}{2H}\,(\Delta P_m - \Delta P_e) \qquad (2.5)$$

- H = Σταθερά Αδράνειας (MW-sec/MVA)
- Δω = Μεταβολή γωνιακής ταχύτητας ρότορα (pu)

Η αλλαγή στην ισχύ που αναπτύσσεται από τον στρόβιλο προκαλεί μια αλλαγή στην έξοδο του εναλλάκτη ΔP_G. Η διαφορά μεταξύ της αλλαγής στην έξοδο του εναλλάκτη και της αλλαγής στο φορτίο (ΔP_L) τείνει να αλλάζει τη συχνότητα του συστήματος.

$$\Delta f = \frac{1}{1+T_t}\cdot \Delta P_v \qquad (2.6)$$



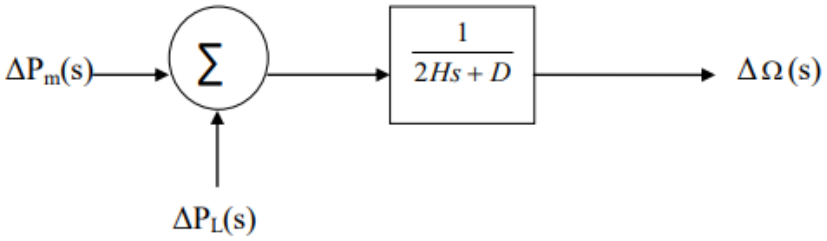
Σχήμα 2. 3 : Διάγραμμα Βαθμίδων Συστήματος Γεννήτριας

2.1.4. Μοντέλο Φορτίου (Load)

Το φορτίο ενός συστήματος αποτελείται από πληθώρα ηλεκτρικών μηχανισμών. Η χαρακτηριστική του φορτίου δίνεται ως εξής :

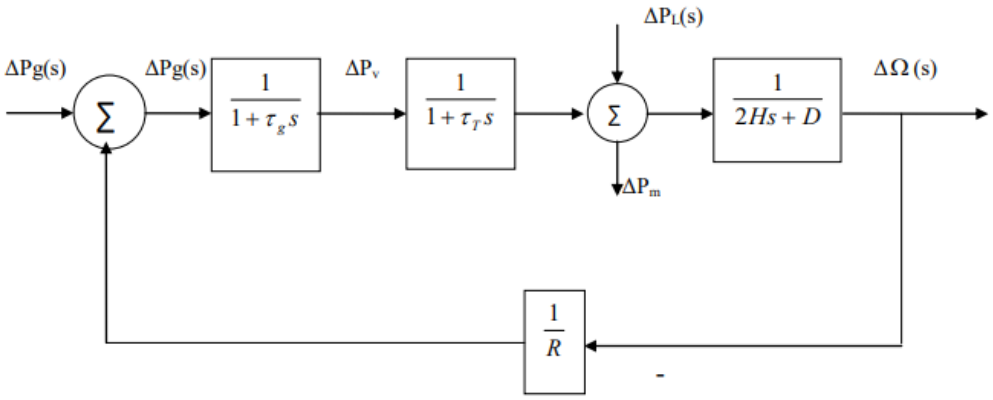
$$\Delta P_e = \Delta P_L + D \cdot \Delta\omega \quad (2.7)$$

- ΔP_L : η μεταβολή του φορτίου που δεν είναι ευαίσθητη στη συχνότητα
- $D \cdot \Delta\omega$: η μεταβολή φορτίου ευαίσθητου στη συχνότητα.
- D : συντελεστής απόσβεσης φορτίου. Είναι το ποσοστό αλλαγής φορτίου σε σχέση με το 1 % της αλλαγής στη συχνότητα.



Σχήμα 2. 4 : Διάγραμμα Βαθμίδων Φορτίου

Συνδυάζοντας όλες τις παραπάνω χαρακτηριστικές, για ένα σύστημα μίας περιοχής παίρνουμε το διάγραμμα βαθμίδων που παρουσιάζεται στο σχήμα 2.5:



Σχήμα 2. 5 : Διάγραμμα Βαθμίδων Συστήματος που περιλαμβάνει το μοντέλο φορτίου - γεννήτριας, ρυθμιστή στροφών και στροβίλου

Από τη θεωρία ελέγχου, είναι γνωστό ότι ο κλειστός βρόχος είναι πιο χρήσιμος, για τη διατήρηση της ευστάθειας. Η συνολική χρονική απόκριση του συστήματος αποτελείται από δύο αποκρίσεις, την μεταβατική και την απόκριση μόνιμης κατάστασης [16].

Η μεταβατική απόκριση είναι η απόκριση ενός συστήματος ως συνάρτηση του χρόνου, δηλαδή ο χρόνος στον οποίο το σύστημα περνά από την αρχική κατάσταση στην τελική κατάσταση, και είναι ένα σημαντικό χαρακτηριστικό του συστήματος.

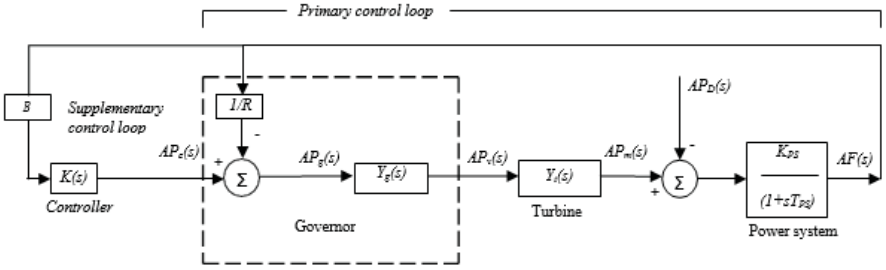
Η απόκριση μόνιμης κατάστασης είναι ο τρόπος με τον οποίο το σύστημα συμπεριφέρεται σε άπειρο χρόνο. Τα χαρακτηριστικά απόδοσης του συστήματος πρέπει να προσδιορίζονται από την μεταβατική απόκριση. Η τιμή σταθερής κατάστασης μιας μεταβλητής δίνεται από το παρακάτω θεώρημα της τελικής τιμής [28]:

$$\lim_{t\to\infty} T(t) = \lim_{s\to 0} T(s) \tag{2.8}$$

2.2. Ανάλυση Ρύθμισης Φορτίου – Συχνότητας μέσω Συμβατικού Ελεγκτή

2.2.1. Μαθηματική Μοντελοποίηση Απομονωμένου Συστήματος LFC (Διάγραμμα Βαθμίδων)

Η λειτουργία συστήματος ρύθμισης φορτίου - συχνότητας είναι να επαναφέρει τη συχνότητα στην καθορισμένη ονομαστική τιμή, δηλαδή οι αποκλίσεις συχνότητας να διευθετούνται με μηδενικό σφάλμα μόνιμης κατάστασης. Για να επιτευχθεί αυτό, ο συμπληρωματικός βρόχος ελέγχου πρέπει να κλείσει και ο ρυθμιστής στροφών να προσαρμοστεί σύμφωνα με κάποια κατάλληλη ενέργεια του ελεγκτή, μέσω της αναφοράς φορτίου ώστε να αλλάξει το set point της ταχύτητας. Το ενσωματωμένο κέρδος του ελεγκτή πρέπει να ρυθμιστεί για μια ικανοποιητική μεταβατική απόκριση.



Σχήμα 2. 6 : Διάγραμμα Βαθμίδων Συστήματος Αυτομάτου Ελέγχου Παραγωγής Απομονωμένου Συστήματος Ισχύος

Η συνάρτηση μεταφοράς κλειστού βρόχου δίνεται από την παρακάτω σχέση [31]:

$$\frac{\Delta\Omega(s)}{-\Delta PL(s)} = \frac{s(1+\tau_g s) + (1+\tau_T s)}{s(2Hs+D)(1+\tau_g s)(1+\tau_T) + K_1 + {}^{s}/_{R}} \tag{2.9}$$

Το σήμα που τροφοδοτείται στον ελεγκτή αναφέρεται ως σφάλμα ελέγχου περιοχής (ACE). Το ACE σε ένα απομονωμένο (Single Area) σύστημα ισχύος μπορεί να οριστεί ως:

$$ACE = B_i \cdot \Delta f_i \tag{2.10}$$

όπου B : ο συντελεστής πόλωσης της συχνότητας, (α.μ MW/Hz)

Ο ρυθμιστής στροφών μπορεί να λάβει εντολή από ένα σήμα ελέγχου ΔPc που προκύπτει από μια κατάλληλη ενέργεια ελέγχου στο σήμα σφάλματος.

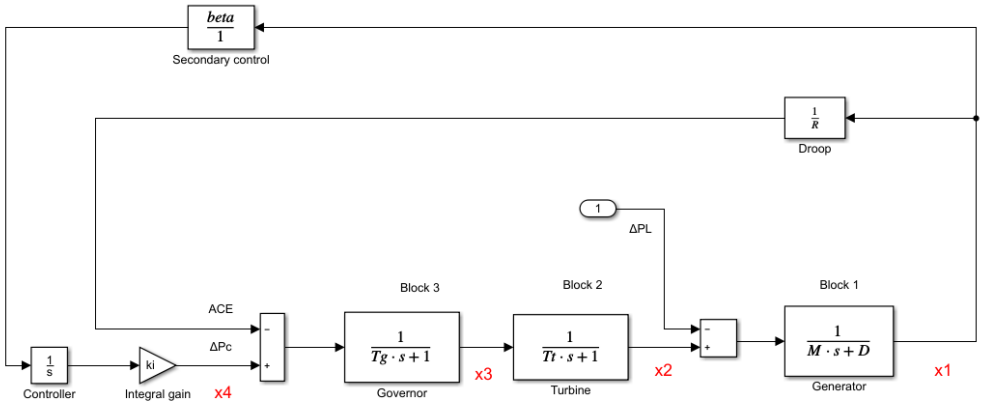
$$\Delta P_c = K(s) \cdot ACE \tag{2.10}$$

όπου K(s) : το κέρδος του ελεγκτή.

Για ολοκληρωτικό ελεγκτή : $K(s) = -\frac{KI}{s}$, το σήμα ΔP_c γίνεται:

$$\Delta P_c = -K_I \cdot \int B \cdot \Delta f \, dt \tag{2.11}$$

Το πρόσημο του ολοκληρωτικού ελεγκτή είναι αρνητικό έτσι ώστε να προκαλέσει ένα θετικό σφάλμα στη συχνότητα που οδηγεί σε μια εντολή μείωσης. Όσο το σφάλμα παραμένει, η έξοδος του ελεγκτή θα αυξάνεται, προκαλώντας κίνηση στον ρυθμιστή στροφών. Η έξοδος του ελεγκτή και επομένως η θέση του ρυθμιστή στροφών επιτυγχάνει σταθερή τιμή μόνο όταν το σφάλμα συχνότητας έχει μειωθεί στο μηδέν. Η σταθερά κέρδους K_I ελέγχει τον ρυθμό ολοκλήρωσης και επομένως την ταχύτητα απόκρισης του βρόχου [29], [30].



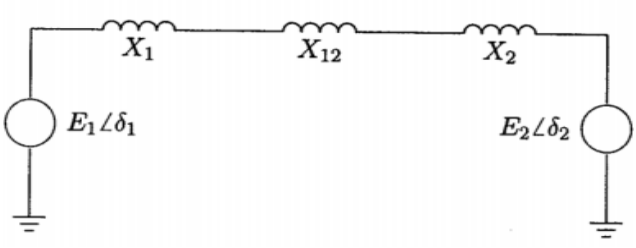
Σχήμα 2. 7 : Διάγραμμα βαθμίδων ρύθμισης φορτίου – συχνότητας απομονωμένου συστήματος ισχύος μέσω συμβατικού ολοκληρωτικού ελεγκτή

2.2.2. Μαθηματική Μοντελοποίηση Συστήματος LFC Πολλαπλών Περιοχών (Διάγραμμα Βαθμίδων)

Σε ένα απομονωμένο σύστημα ισχύος, η ρύθμιση της ισχύος διασύνδεσης δεν αποτελεί ζήτημα ελέγχου και η ρύθμιση φορτίου – συχνότητας (Load Frequency Control) περιορίζεται στην επαναφορά της συχνότητας του συστήματος στην καθορισμένη ονομαστική τιμή.

Ένα σύστημα ισχύος πολλαπλών περιοχών περιλαμβάνει περιοχές που διασυνδέονται με γραμμές μεταφοράς υψηλής τάσης. Το σύστημα Ρύθμισης Φορτίου - Συχνότητας σε κάθε περιοχή ελέγχου των διασυνδεδεμένων συστημάτων ισχύος πολλαπλών περιοχών θα πρέπει να ελέγχει τη διασυνδετική ροή ισχύος με τις άλλες περιοχές ελέγχου καθώς και την τοπική συχνότητά του [27].

Για μια απλή μοντελοποίηση ενός συστήματος **δύο** περιοχών, θεωρούμε ότι οι δύο περιοχές απεικονίζονται με μια ισοδύναμη μονάδα παραγωγής που συνδέεται με μια γραμμή διασύνδεσης χωρίς απώλειες και αντίδραση X_{tie}. Κάθε περιοχή αποτελείται από μια πηγή τάσης και μια ισοδύναμη αντίδραση όπως φαίνεται στο παρακάτω σχήμα.



Σχήμα 2. 8 : Ισοδύναμο Δίκτυο για σύστημα ισχύος Δύο Περιοχών (Two Area Power System)

Για ένα σύστημα δύο περιοχών, κατά την κανονική λειτουργία, η πραγματική ισχύς που μεταφέρεται μέσω της γραμμής διασύνδεσης δίνεται από τη σχέση [16-19]:

$$P_{tie,12} = \frac{|E_1||E_2|}{X_{12}} \cdot \sin\delta_{12} \tag{2.11}$$

Όπου :

- P_{12}: η ενέργεια που ανταλλάσσεται μεταξύ των δύο περιοχών μέσω των γραμμών διασύνδεσης,
- X_{12}: η επαγωγική ηλεκτρική αντίδραση των γραμμών διασύνδεσης
- δ_1 και δ_2 οι γωνίες ισχύος των τάσεων V_1 και V_2
- $\delta_{12} = \delta_1 - \delta_2$

Για μια μικρή απόκλιση της διασυνδετικής ροής :

$$\Delta P_{tie,12} = \frac{dP_{12}}{d\delta_{12}}\Big|_{\delta_{120}} = \frac{|E_1||E_2|}{X_{12}} \cdot \cos(\delta 1 - \delta 2)(\Delta\delta_1 - \Delta\delta_2) \tag{2.12}$$

Και τελικά η απόκλιση της διασυνδετικής ροής παίρνει τη μορφή :

$$\Delta P_{tie,12} = T_{12}(\Delta\delta_1 - \Delta\delta_2) \tag{2.13}$$

$$\text{όπου } T_{12} = \frac{|E_1||E_2|}{X_{12}} \cdot \cos(\delta_1 - \delta_2) \tag{2.14}$$

Η απόκλιση συχνότητας Δf σχετίζεται με τη γωνία αναφοράς δ από τον τύπο:

$$\Delta\delta = 2\pi \int_0^t \Delta f \, dt \tag{2.15}$$

Εκφράζοντας τις αποκλίσεις της γραμμής διασύνδεσης ως Δf, παίρνουμε :

$$\Delta P_{tie,12} = 2\pi T_{12}\left(\int_0^t \Delta f_1 \, dt - \int_0^t \Delta f_{\,2} dt\right) \tag{2.16}$$

Και μέσω του μετασχηματισμού Laplace :

$$\Delta P_{tie,12}(s) = \frac{2\pi T_{12}}{s}(\Delta F_1(s) - \Delta F_2(s)) \tag{2.17}$$

Αντίστοιχα, η διασυνδετική ροή από την περιοχή 2 στην περιοχή 1 :

$$\Delta P_{tie,21} = \frac{2\pi T_{21}}{s}(\Delta F_2(s) - \Delta F_1(s))$$

όπου $T_{21} = \frac{|E_1||E_2|}{X_{12}} \cdot \cos(\delta_2 - \delta_1)$ (2.18)

Επομένως προκύπτει η ισοδυναμία :

$$\Delta P_{tie,12} = -\Delta P_{tie,21} \quad (2.19)$$

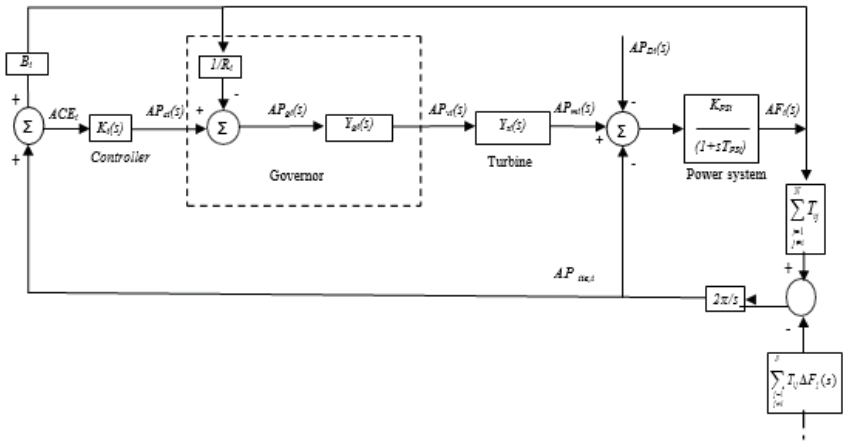
Ομοίως, μεταξύ των περιοχών 1 και 3 η διασυνδετική ροή θα είναι :

$$\Delta P_{tie,13} = \frac{2\pi T_{13}}{s}(\Delta F_1(s) - \Delta F_3(s)) \quad (2.20)$$

Επομένως, ανάγοντας τις παραπάνω σχέσεις για N–περιοχές ελέγχου, η συνολική διασυνδετική ροή ισχύος μεταξύ της περιοχής i και των υπολοίπων περιοχών θα είναι [32]:

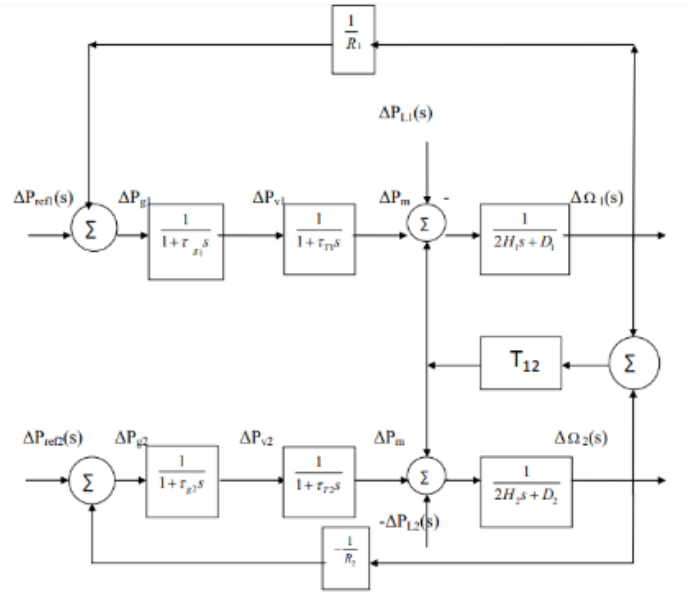
$$\Delta P_{tie,i}(s) = \Delta P_{tie,i1}(s) + \ldots + \Delta P_{tie,in}(s) = \sum_{\substack{j=1 \\ j\neq i}}^{N} \Delta P_{tie,ij}(s) = \frac{2\pi}{s}\left(\sum_{\substack{j=1 \\ j\neq i}}^{N} T_{ij}\Delta F_i(s) - \sum_{\substack{j=1 \\ j\neq i}}^{N} T_{ij}\Delta F_j(s)\right)$$

(2.21)



Σχήμα 2. 9 : Απεικόνιση διαγράμματος βαθμίδων μιας περιοχής -i με διασυνδετική ροή ισχύος, σε ένα διασυνδεδεμένο σύστημα ισχύος N – περιοχών ελέγχου με συμβατικό ελεγκτή Κ [19]

Το αποτέλεσμα της αλλαγής της ισχύος της γραμμής διασύνδεσης για μια περιοχή είναι ισοδύναμο με την αλλαγή του φορτίου αυτής της περιοχής. Επομένως, το $\Delta Ptie_{,i}$ πρέπει να προστεθεί στη μεταβολή της μηχανικής ισχύος ΔPm_i και στην αλλαγή φορτίου της περιοχής ελέγχου ΔPL_i χρησιμοποιώντας το κατάλληλο πρόσημο.



Σχήμα 2. 10 : Διάγραμμα βαθμίδων συστήματος δύο περιοχών αποτελούμενο μόνο από πρωτεύοντα έλεγχο [27]

Το επόμενο σημείο που πρέπει να λάβουμε υπόψη είναι ο συμπληρωματικός βρόχος ελέγχου με την ταυτόχρονη παρουσία γραμμών διασύνδεσης. Στην περίπτωση μιας απομονωμένης περιοχής ελέγχου, αυτός ο βρόχος κλείνει μέσα από μια ανάδραση από την απόκλιση συχνότητας περιοχής ελέγχου με τη βοήθεια ενός απλού δυναμικού ελεγκτή [27].

Σε ένα σύστημα πολλών περιοχών, εκτός από τη ρύθμιση της συχνότητας περιοχής, ο συμπληρωματικός έλεγχος θα πρέπει να διατηρεί την διασυνδετική ροή ισχύος της γραμμής διασύνδεσης με τις γειτονικές περιοχές στις προγραμματισμένες τιμές. Αυτό γενικά επιτυγχάνεται προσθέτοντας την απόκλιση της διασυνδετικής ροής ισχύος και την απόκλιση συχνότητας στον συμπληρωματικό βρόχο ανάδρασης.

Μέσω λοιπόν του γραμμικού συνδυασμού της μεταβολής της συχνότητας και της διασυνδετικής ροής ισχύος για τη συγκεκριμένη περιοχή, παίρνουμε το Σφάλμα Ελέγχου Περιοχής, το οποίο περιγράφεται από την παρακάτω σχέση [16-19]:

$$\mathrm{ACE_i} = \Delta \mathrm{P_{tie,i}} + \mathrm{B_i} \Delta \mathrm{f_i} \tag{2.22}$$

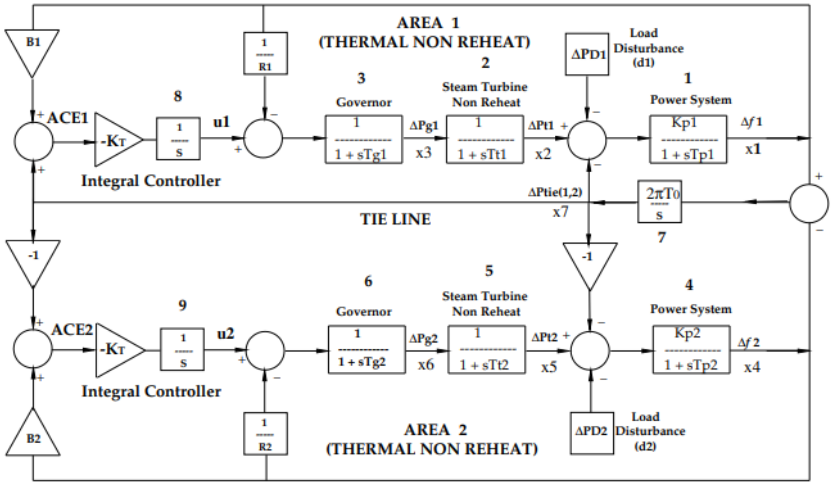
$$\text{Όπου : } \mathrm{B_i} = \beta_\mathrm{i} = \mathrm{D_i} + \frac{1}{\mathrm{R_i}}, \tag{2.23}$$

ο συντελεστής πόλωσης που αναπαριστά την αναμενόμενη απόκριση συχνότητας της παραγωγής και του φορτίου σε μια διασυνδεδεμένη περιοχή.

Σε ένα διασυνδεδεμένο σύστημα που αποτελείται από πολλές περιοχές, το καθήκον του AGC είναι να κατανείμει το φορτίο μεταξύ του συστήματος, των σταθμών και των γεννητριών έτσι ώστε να επιτευχθεί η μέγιστη οικονομία και η κοινή συχνότητα.

Τα αποτελέσματα των τοπικών αλλαγών φορτίου και οι αλληλεπιδράσεις με άλλες περιοχές ελέγχου θεωρούνται ως δύο σήματα εισόδου. Κάθε περιοχή ελέγχου παρακολουθεί τη δική της ροή ισχύος και συχνότητα στο κέντρο ελέγχου της. Στη συνέχεια, το σήμα ACE υπολογίζεται και εκχωρείται στον ελεγκτή K(s). Πιο συγκεκριμένα, το σήμα σφάλματος, δηλαδή τα Δf και ΔPtie ενισχύονται, αναμειγνύονται και μετατρέπονται σε σήμα εντολής πραγματικής ισχύος, το οποίο αποστέλλεται στον ρυθμιστή στροφών για να ζητήσει αύξηση ή μείωση της ροπής. Έτσι θα επέλθει μια αλλαγή στην έξοδο της γεννήτριας κατά ένα ποσό ΔPG που θα αλλάξει τις τιμές των Δf και ΔPtie εντός των καθορισμένων ορίων [32].

Έτσι, αναμένεται ότι ο συμπληρωματικός έλεγχος μπορεί ιδανικά να ανταποκριθεί στους βασικούς στόχους της ρύθμισης φορτίου - συχνότητας και να διατηρήσει τη συχνότητα περιοχής καθώς και τη διασυνδετική ροή ισχύος στις προγραμματισμένες τιμές.



Σχήμα 2. 11 : Διάγραμμα βαθμίδων συστήματος ρύθμισης φορτίου – συχνότητας Δύο Περιοχών με χρήση ολοκληρωτικού ελεγκτή [35]

Κατά την αναπαράσταση γεννητριών σε μία περιοχή ελέγχου με ένα ισοδύναμο ανά μονάδα σύστημα μηχανής - φορτίου, το δυναμικό μοντέλο μπορεί να περιγραφεί με τις ακόλουθες μαθηματικές εξισώσεις [33] :

- **Δυναμική εξίσωση Στροβίλου :**

$$\Delta\dot{P}_{m_1} = -\frac{1}{T_{t_i}} \cdot \Delta P_{m_i} + \frac{1}{T_{t_i}} \cdot \Delta P_{v_i} \tag{2.24}$$

όπου, το ΔP_{m_i} είναι η απόκλιση της μηχανικής ισχύος της γεννήτριας, το ΔP_{v_i}είναι η απόκλιση της θέσης της βαλβίδας του στροβίλου και το T_t είναι η σταθερά χρόνου του στροβίλου i.

- **Δυναμική εξίσωση Ρυθμιστή Στροφών :**

$$\Delta\dot{P}_{v_i} = -\frac{1}{T_{g_i} \cdot R_i} \cdot \Delta f_i - \frac{1}{T_{g_i}} \cdot \Delta P_{v_i} + \frac{1}{T_{g_i}} \cdot \Delta P_{c_i} \tag{2.25}$$

όπου, Δf_i είναι η απόκλιση συχνότητας της περιοχής i, ΔP_{c_i} είναι το set point αναφοράς φορτίου, T_g είναι η χρονική σταθερά του ρυθμιστή στροφών i και R_i είναι ο συντελεστής ρύθμισης ταχύτητας.

- **Δυναμική εξίσωσης συνολικού Φορτίου – Γεννήτριας :**

$$\dot{\Delta f_i} = -\frac{D_i}{M_i} \cdot \Delta f_i + \frac{1}{M_i} \cdot \Delta P_{m_i} - \frac{1}{M_i} \cdot \Delta P_{L_i} - \frac{1}{M_i} \cdot \Delta P^i{}_{tie} \qquad (2.26)$$

όπου, $\Delta P^i{}_{tie}$ είναι η διασυνδετική ροή ισχύος στην περιοχή i, ΔP_{L_i} είναι η απόκλιση φορτίου, M_i η ισοδύναμη σταθερά αδράνειας της περιοχής i και D_i είναι ο ισοδύναμος συντελεστής απόσβεσης της περιοχής i.

- **Δυναμική εξίσωση Διασυνδετικής Ροής Ισχύος :**

$$\dot{\Delta P^i}_{tie} = \sum_{j=1, j\neq i}^{N} 2\pi T_{ij}(\Delta f_i - \Delta f_j) \qquad (2.27)$$

όπου Tij είναι ο συντελεστής ταυτοχρονισμού και Δf_j είναι η απόκλιση συχνότητας της περιοχής j.

2.3. Ανάλυση Ρύθμισης Φορτίου – Συχνότητας στο Χώρο Κατάστασης (State Space Analysis)

Ο σύγχρονος σχεδιασμός ελέγχου βασίζεται αρκετά στο διανυσματικό σύστημα πολλαπλών μεταβλητών κατάστασης. Σε αυτόν τον αλγόριθμο σχεδίασης χρησιμοποιούμε τις παραμέτρους των μεταβλητών κατάστασης που μπορούν να ληφθούν από το σύστημα.

Οι ακόλουθες εξισώσεις απεικονίζουν το μοντέλο ρύθμισης φορτίου συχνότητας στον χώρο κατάστασης για την περιοχή ελέγχου i σε ένα σύστημα ισχύος με N περιοχές ελέγχου [34-36]:

$$\dot{x}_i = A_{ii}\, x_i + B_i\, u_i + \sum_{j=1, j\neq i}^{N} A_{ij} x_j + F_i \Delta P_{Li}, \qquad x_i(0) = x_0$$

$$y_i = C_i\, x_i \qquad (2.28)$$

ή πιο απλά :

$$\dot{x} = A\, x(t) + B\, u(t) + F\, d(t)$$

$$y = Cx \qquad (2.29)$$

Όπου x(t), u(t), d(t), τα διανύσματα κατάστασης, εισόδου και μεταβολής φορτίου αντίστοιχα.

2.3.1. Μοντελοποίηση στο χώρο κατάστασης απομονωμένου συστήματος Ρύθμισης Φορτίου – Συχνότητας (Single Area LFC)

Με βάση τις εξισώσεις που χρησιμοποιήσαμε για να μοντελοποιήσουμε τον στρόβιλο, τον ρυθμιστή στροφών, τη γεννήτρια και το φορτίο, ορίζουμε [37] :

Μεταβλητές κατάστασης :

$$x = [\Delta f_1 \;\; \Delta P_{m1} \;\; \Delta P_{v1} \;\; \int ACE_1]^T \tag{2.30}$$

με : $x_1 = \Delta f_1$ $x_2 = \Delta P_m$ $x_3 = \Delta P_v$ $x_4 = \int ACE \, dt$ (2.31)

Μεταβλητές Ελέγχου Εισόδου :

$$u = [u_1] \tag{2.32}$$

με : $u_1 = \Delta P_{c1}$ (2.33)

Μεταβλητές Εισόδου Διαταραχών :

$$d = [d_1] \tag{2.34}$$

με : $d_1 = \Delta P_{d1}$ (2.35)

Οι εξισώσεις κατάστασης προκύπτουν από τη συνάρτηση μεταφοράς των Blocks, 1 έως 4 το Σχήματος 2.7, μια εξίσωση για κάθε μπλοκ. Οι εξισώσεις στον χώρο κατάστασης θα είναι :

- Block 1 (Γεννήτρια-Φορτίο):

$$\dot{x}_1 = -\frac{D_1}{M_1} \cdot x_1 + \frac{1}{M_1} \cdot x_2 - \frac{1}{M_1} \cdot d_1 \tag{2.36}$$

- Block 2 (Στρόβιλος):

$$\dot{x}_2 = -\frac{1}{T_{t1}} \cdot x_2 + \frac{1}{T_{t1}} \cdot x_3 \tag{2.37}$$

- Block 3 (Ρυθμιστής Στροφών):

$$\dot{x}_3 = -\frac{1}{T_{g1} \cdot R_1} \cdot x_1 - \frac{1}{T_{g1}} \cdot x_3 + \frac{1}{T_{g1}} \cdot u_1 \tag{2.38}$$

- Block 4 (Ανάδρασης):

$$\dot{x_4} = B_1 \cdot x_4 \tag{2.39}$$

Οι παραπάνω εξισώσεις μπορούν να γραφούν στο χώρο κατάστασης με τη μορφή πινάκων ως εξής :

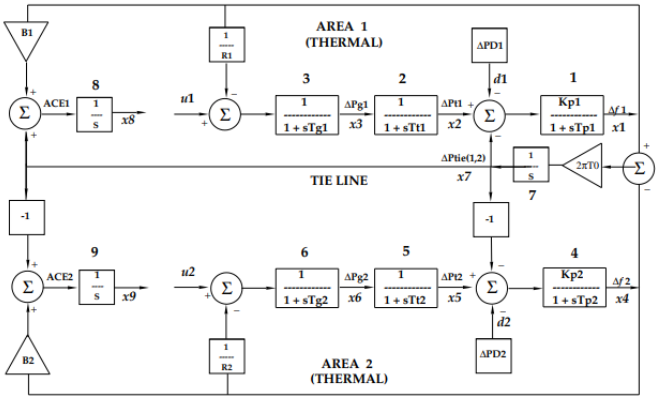
$$\dot{x} = \begin{bmatrix} -\frac{D_1}{M_1} & \frac{1}{M_1} & 0 & 0 \\ 0 & -\frac{1}{T_{t_1}} & \frac{1}{T_{t_1}} & 0 \\ -\frac{1}{R_1 T_{g_1}} & 0 & -\frac{1}{T_{g_1}} & 0 \\ B_1 & 0 & 0 & 0 \end{bmatrix} \cdot x + \begin{bmatrix} 0 \\ 0 \\ \frac{1}{T_{g_1}} \\ 0 \end{bmatrix} \cdot u + \begin{bmatrix} -\frac{1}{M_1} \\ 0 \\ 0 \\ 0 \end{bmatrix} \cdot d \qquad (2.40)$$

$$\text{όπου : } A = \begin{bmatrix} -\frac{D_1}{M_1} & \frac{1}{M_1} & 0 & 0 \\ 0 & -\frac{1}{T_{t_1}} & \frac{1}{T_{t_1}} & 0 \\ -\frac{1}{R_1 T_{g_1}} & 0 & -\frac{1}{T_{g_1}} & 0 \\ B_1 & 0 & 0 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 0 \\ 0 \\ \frac{1}{T_{g_1}} \\ 0 \end{bmatrix}, \quad F = \begin{bmatrix} -\frac{1}{M_1} \\ 0 \\ 0 \\ 0 \end{bmatrix} \qquad (2.41)$$

2.3.2. Μοντελοποίηση στο χώρο κατάστασης συστήματος Ρύθμισης Φορτίου – Συχνότητας Δύο Περιοχών (Two Area LFC)

Οι εξισώσεις κατάστασης του συστήματος δύο περιοχών για έναν θερμικό σταθμό παραγωγής με μη αναθερμενόμενο στρόβιλο, παράγονται μέσω του διαγράμματος βαθμίδων του συστήματος ισχύος με ολοκληρωτικό ελεγκτή του σχήματος 2.11, με τη βοήθεια των blocks 1 έως 7. Το διάγραμμα βαθμίδων απεικονίζει ένα σύστημα ελέγχου δύο περιοχών, αποτελούμενο από δύο εισόδους ελέγχου u_1 και u_2, που συνδέονται μεταξύ τους μέσω μιας γραμμής, που προκύπτει από την έξοδο του 7ου μπλοκ. Από το σχήμα, φαίνεται ότι κάθε περιοχή αποτελείται από τρία μπλοκ, αυτά του ρυθμιστή στροφών, του στροβίλου και του φορτίου, όπως ακριβώς και στο σύστημα ελέγχου για μία περιοχή. Επομένως υπάρχουν συνολικά 9 μπλοκς για ολόκληρο το σύστημα, που σημαίνει ότι προκύπτουν και 9 εξισώσεις μεταβλητών κατάστασης.

Για το σύστημα δύο περιοχών σύμφωνα με τα παραπάνω καθώς και από το ακόλουθο σχήμα, προκύπτει το μοντέλο στον χώρο καταστάσεων (χωρίς την παρουσία ολοκληρωτικού ελεγκτή) με 9 μεταβλητές κατάστασης ως εξής :



*Σχήμα 2. 12 : Διάγραμμα βαθμίδων συστήματος ρύθμισης φορτίου – συχνότητας Δύο Περιοχών με **διανύσματα** του χώρου κατάστασης (χωρίς ολοκληρωτικό ελεγκτή) [35]*

Μεταβλητές κατάστασης :

$$x_i = [\Delta f_1 \ \Delta P_{m_1} \ \Delta P_{v_1} \ \Delta f_2 \ \Delta P_{m_2} \ \Delta P_{v_2} \Delta P_{tie_{12}} \int ACE_1 \int ACE_2]^T$$

με: $x_1 = \Delta f_1$ $x_2 = \Delta P_{m1}$ $x_3 = \Delta P_{v1}$ $x_4 = \Delta f_2$ $x_5 = \Delta P_{m2}$ $x_6 = \Delta P_{v2}$
$x_7 = \Delta P_{tie}$ $x_8 = \int ACE_1 \, dt$ $x_9 = \int ACE_2 \, dt$

(2.42)

Μεταβλητές Ελέγχου Εισόδου :

$$u = \begin{bmatrix} u_1 \\ u_2 \end{bmatrix}$$

$u_1 = \Delta P_{c1}$ & $u_2 = \Delta P_{c2}$

(2.43)

Μεταβλητές Εισόδου Διαταραχών :

$$d = \begin{bmatrix} d_1 \\ d_2 \end{bmatrix}$$

$d_1 = \Delta P_{d1}$ & $d_2 = \Delta P_{d2}$

(2.44)

Οι εξισώσεις κατάστασης προκύπτουν από τις συναρτήσεις μεταφοράς των Blocks, 1 έως 9. Οι εξισώσεις στον χώρο κατάστασης θα είναι :

- Block 1 :

$$\dot{x}_1 = -\frac{1}{T_{p1}} \cdot x_1 + \frac{K_{p1}}{T_{p1}} \cdot x_2 + \frac{K_{p1}}{T_{p1}} x_1 - \frac{K_{p1}}{T_{p1}} \cdot d_1 \quad (2.45)$$

- Block 2 :

$$\dot{x}_2 = -\frac{1}{T_{t1}} \cdot x_2 + \frac{1}{T_{t1}} \cdot x_3 \quad (2.46)$$

- Block 3 :

$$\dot{x}_3 = -\frac{1}{T_{g1} \cdot R_1} \cdot x_1 - \frac{1}{T_{g1}} \cdot x_3 + \frac{1}{T_{g1}} \cdot u_1 \quad (2.47)$$

- Block 4:

$$\dot{x}_4 = -\frac{1}{T_{p2}} \cdot x_4 + \frac{K_{p1}}{T_{p1}} \cdot x_5 + \frac{K_{p2}}{T_{p2}} x_7 - \frac{K_{p2}}{T_{p2}} \cdot d_2 \quad (2.48)$$

- Block 5 :

$$\dot{x}_5 = -\frac{1}{T_{t2}} \cdot x_2 + \frac{1}{T_{t2}} \cdot x_3 \quad (2.49)$$

- Block 6 :

$$\dot{x}_3 = -\frac{1}{T_{g2} \cdot R_2} \cdot x_4 - \frac{1}{T_{g2}} \cdot x_6 + \frac{1}{T_{g2}} \cdot u_2 \quad (2.50)$$

- Block 7 :

$$\dot{x_7} = 2\pi T^0 x_1 - 2\pi T^0 x_4 \quad (2.51)$$

- Block 8 :

$$\dot{x_8} = B_1 \cdot x_1 + x_7 \quad (2.52)$$

- Block 9 :

$$\dot{x_9} = B_2 \cdot x_4 - x_7 \quad (2.53)$$

Οι παραπάνω εξισώσεις όπως αναφέραμε και στη σχέση (2.29) μπορούν να γραφούν στο χώρο κατάστασης ως εξής :

$$\dot{x} = A\,x(t) + B\,u(t) + F\,d(t)$$

Όπου για τις δύο περιοχές, το A είναι ένας τετραγωνικός πίνακας διαστάσεων 9×9, που ονομάζεται Πίνακας Καταστάσεων, B και Γ είναι οι ορθογώνιοι πίνακες διαστάσεων 9×2 που ονομάζονται πίνακας ελέγχου και πίνακας διαταραχής αντίστοιχα. Το «x» είναι το διάνυσμα κατάστασης 9×1, το «u» είναι το διάνυσμα ελέγχου 2×1 και το «d» είναι το διάνυσμα διαταραχής 2×1.

Οι πίνακες A(9×9), B(9×2) και F(9×2) είναι οι παρακάτω :

$$A = \begin{bmatrix} \frac{-1}{T_{p1}} & \frac{K_{p1}}{T_{p1}} & 0 & 0 & 0 & 0 & \frac{-K_{p1}}{T_{p1}} & 0 & 0 \\ 0 & \frac{-1}{T_{t1}} & \frac{1}{T_{t1}} & 0 & 0 & 0 & 0 & 0 & 0 \\ \frac{-1}{R_1 T_{g1}} & 0 & \frac{-1}{T_{g1}} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{-1}{T_{p2}} & \frac{K_{p2}}{T_{p2}} & 0 & \frac{K_{p2}}{T_{p2}} & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{-1}{T_{t2}} & \frac{1}{T_{t2}} & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{-1}{R_2 T_{g2}} & 0 & \frac{-1}{T_{g2}} & 0 & 0 & 0 \\ 2\pi T^0 & 0 & 0 & -2\pi T^0 & 0 & 0 & 0 & 0 & 0 \\ B_1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & B_2 & 0 & 0 & -1 & 0 & 0 \end{bmatrix}$$

$$B = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ \frac{1}{T_{g1}} & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & \frac{1}{T_{g2}} \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix} \qquad F = \begin{bmatrix} \frac{-K_{p1}}{T_{p1}} & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & \frac{-K_{p2}}{T_{p2}} \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}$$

(2.54)

2.4. Μέθοδοι Ελέγχου στη Ρύθμιση Φορτίου – Συχνότητας

Ο έλεγχος αποτελεί το πιο σημαντικό κομμάτι της ρύθμισης φορτίου - συχνότητας, καθώς είναι ο μηχανισμός μέσω του οποίου μηδενίζεται στην ουσία η διαφορά των ονομαστικών (συνεχώς απαιτούμενων) τιμών της συχνότητας και των τιμών που παίρνουμε έπειτα από μεταβολές.

Υπάρχουν αρκετά είδη ελέγχου για τη ρύθμιση φορτίου-συχνότητας, κυριότερα εκ των οποίων είναι τα εξής [38]:

Α) Κλασικοί Μέθοδοι Ελέγχου

1) Συμβατικός Ολοκληρωτικός Ελεγκτής (I), PI και PID
2) Τοποθέτηση Πόλων
3) Μέθοδοι βασισμένοι στο Γραμμικό Τετραγωνικό Ρυθμιστή (LQR)

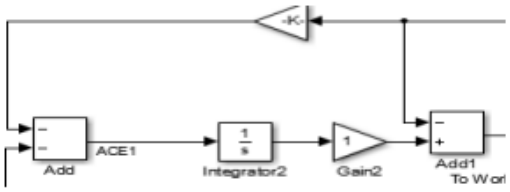
Β) Μέθοδοι με χρήση αλγορίθμων

4) Fuzzy Logic Controllers
5) Νευρωνικά Δίκτυα
6) Γενετικοί Αλγόριθμοι,
7) Υβριδικά συστήματα
8) Αλγόριμοι βελτιστοποίησης με σμήνος σωματιδίων (Particle Swarm Optimization, PSO)

Οι μέθοδοι της κατηγορίας Β, αποτελούν μεθόδους προηγμένης τεχνικής ελέγχου που παρέχουν μεγάλη βοήθεια στο σύστημα ρύθμισης φορτίου - συχνότητας των συστημάτων ισχύος στις μέρες μας. Καινοτόμος και βελτιωμένος έλεγχος απαιτείται για οικονομική, ασφαλή και σταθερή λειτουργία. Οι προηγμένες τεχνικές ελέγχου έχουν την ικανότητα να παρέχουν υψηλή προσαρμογή στις μεταβαλλόμενες συνθήκες και να λαμβάνουν γρήγορες αποφάσεις. Οι μέθοδοι αυτές αναλύονται στο [38]. Στην παρούσα εργασία θα αναλύσουμε κλασικές μεθόδους ελέγχου, δύο εκ των οποίων χρησιμοποιούμε στις μοντελοποιήσεις μας (1, 2).

2.4.1. Συμβατικός Ολοκληρωτικός Ελεγκτής (Integral), PI και PID

Ο **ολοκληρωτικός έλεγχος** αποτελείται από έναν αισθητήρα συχνότητας και έναν ολοκληρωτή. Ο αισθητήρας μετρά τη μεταβολή της συχνότητας Δf και στέλνει το προκύπτον σφάλμα στον ολοκληρωτή. Η είσοδος του ολοκληρωτή ονομάζεται Σφάλμα Ελέγχου Περιοχής (ACE) και είναι στην ουσία η αλλαγή στη συχνότητα περιοχής, η οποία στον κλειστό βρόχο του ολοκληρωτικού ελέγχου, οδηγεί το σφάλμα μόνιμης κατάστασης της συχνότητας στο μηδέν [39]



Σχήμα 2. 13 : Έλεγχος με ολοκληρωτικό κέρδος

Ο ολοκληρωτής παράγει ένα σήμα ενεργού ισχύος που δίνεται από τον τύπο [30]:

$$\Delta P_c = -K_i \int \Delta f \, dt = -K_i \int (ACE) dt \tag{2.55}$$

Όπου :

ΔP_c = είσοδος του ρυθμιστή στροφών και

K_i = το κέρδος του ολοκληρωτικού ελεγκτή

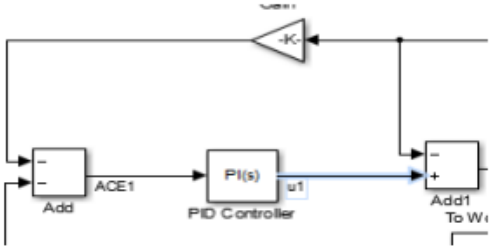
Η τιμή του K_i δίνεται από την παρακάτω εξίσωση [30]:

$$K_i = {}^1\!/_4 \, \tau_p K_{ps} \left(1 + \frac{K_{ps}}{R}\right)^2 = K_{crit} \tag{2.56}$$

Η τιμή του K_i επιλέγεται έτσι ώστε η απόκριση να είναι αποσβενύμενη και όχι αμείωτη ταλάντωση. Έτσι :

$$K_i < K_{crit}$$

Οι **PI** ελεγκτές χρησιμοποιούνται συνήθως σε βιομηχανικά συστήματα ελέγχου. Αποτελούνται από δύο βασικούς όρους, τον αναλογικό (K_p) και τον ολοκληρωτικό (K_i). Ο συνδυασμός των δύο αυτών όρων έχει ως αποτέλεσμα τόσο την αύξηση της ταχύτητας της απόκρισης, όσο και την εξάλειψη του σφάλματος μόνιμης κατάστασης της συχνότητας, το οποίο πιθανώς να έμενε αν είχαμε μόνο έναν ολοκληρωτικό ελεγκτή. Ο ολοκληρωτικός ελεγκτής παρέχει μηδενική απόκλιση συχνότητας μόνιμης κατάστασης και ο αναλογικός ελεγκτής μειώνει το την ακραία αρχική μεταβολή [39-40].

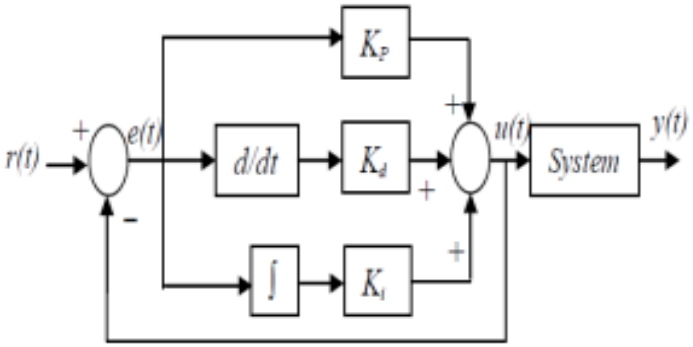


Σχήμα 2. 14 : Έλεγχος με PI ελεγκτή

Το τελικά παραγόμενο σήμα αυτού του τύπου ελέγχου δίνεται από τον τύπο :

$$\Delta P_c = -K_p(ACE) - K_i \int (ACE)\, dt \qquad (2.57)$$

Ο ελεγκτής τύπου **PID** χρησιμοποιείται επίσης ευρέως στην επίλυση του προβλήματος της ρύθμισης φορτίου-συχνότητας και λόγω της απλότητάς του αλλά και λόγω της επιτυχίας του σε μεγάλο αριθμό βιομηχανικών εφαρμογών. Η προσθήκη του διαφορικού όρου αυξάνει την απόσβεση και βελτιώνει την ευστάθεια χωρίς να επηρεάζει το μόνιμο σφάλμα [39-42].



Σχήμα 2. 15 : Έλεγχος με PID ελεγκτή

Οι συμβατικοί ολοκληρωτικοί ελεγκτές παρόλα αυτά έχουν ορισμένα μειονεκτήματα που με το πέρασμα των χρονών μας οδήγησαν στη χρησιμοποίηση και άλλων μεθόδων ελέγχου.

Μερικά από αυτά τα μειονεκτήματα είναι τα παρακάτω [30], [39]:

- Σχετικά αργοί στη λειτουργία τους
- Υπάρχουν μερικά μη γραμμικά φαινόμενα τα οποία ο ολοκληρωτικός ρυθμιστής αγνοεί, όπως τα φαινόμενα νεκρής ζώνης ή η παρουσία μη γραμμικών φαινομένων από τη χρήση στροβίλων.
- Δεν ακολουθούν με ακριβή συνέπεια τις συνεχείς αλλαγές στο φορτίο, καθώς για τα καλύτερα αποτελέσματα θα πρέπει να αλλάζει συνεχώς το κέρδος του ολοκληρωτή, το οποίο θα πρέπει να έχει τέτοια τιμή, ώστε να συνδυάζει και τη γρήγορη επαναφορά του συστήματος αλλά και το χαμηλό overshoot κατά τη μεταβολή, πράγμα ιδιαίτερα δύσκολο.

2.4.2. Τεχνική Τοποθέτησης Πόλων

Ο σύγχρονος σχεδιασμός ελέγχου βασίζεται κυρίως στο διανυσματικό σύστημα πολλαπλών μεταβλητών κατάστασης που είδαμε προηγουμένως. Σε αυτόν τον αλγόριθμο σχεδίασης χρησιμοποιούμε τις παραμέτρους της μεταβλητής κατάστασης που μπορούν να ληφθούν από το σύστημα. Είναι αναγκαίο, επομένως, να αναλύσουμε το σύστημα μας στο χώρο κατάστασης χρησιμοποιώντας τις εξισώσεις κατάστασης [36].

Βασικό εργαλείο ελέγχου του συστήματος είναι η ανάδραση της κατάστασης (state feedback). Με τον όρο ανάδραση (feedback) ορίζουμε τη διαδικασία εκείνη κατά την οποία ανατροφοδοτούμε το σύστημα μας διαρκώς με τα δεδομένα της κατάστασης στην οποία βρίσκεται το σύστημα την κάθε στιγμή. Ο έλεγχος επιτυγχάνεται με ανάδραση των μεταβλητών κατάστασης μέσω ενός ρυθμιστή με σταθερά κέρδη [43-45].

Το πρώτο βήμα στο σχεδιασμό ενός state feedback ελεγκτή είναι ο η εφαρμογή της μεθόδου της **τοποθέτησης πόλων**, κατά την οποία επιλέγονται οι θέσεις των επιθυμητών πόλων κλειστού βρόχου.

Η ιδέα της επανατοποθέτησης των πόλων του συστήματος βασίζεται στο γεγονός ότι η θέση όλων των πόλων του συστήματος χαρακτηρίζει την ασυμπωτική ευστάθεια μιας κατάστασης ισορροπίας ενός γραμμικού και χρονικά αναλλοίωτου συστήματος συνεχούς χρόνου. Η έννοια «πόλοι του συστήματος» αναφέρεται στις ιδιοτιμές του πίνακα A και όχι στους πόλους της συνάρτησης μεταφοράς [46].

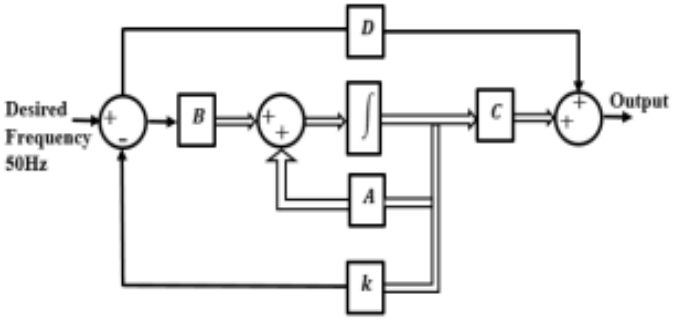
Ο νόμος ελέγχου δίνεται ως εξής:

$$\mathbf{U} = -\mathbf{K}\,\mathbf{x} \tag{2.58}$$

Όπου K ορίζεται ως πίνακας - διάνυσμα κέρδους διάστασης 1×n.

Η παραπάνω εξίσωση υποδεικνύει ότι το σήμα ελέγχου u ορίζεται από στιγμιαίες καταστάσεις (δηλαδή ανάδραση κατάστασης). Έτσι, ο πίνακας K, μεγλέθους 1×n ονομάζεται πίνακας κέρδους ανάδρασης κατάστασης.

Η είσοδος του συστήματος ελέγχου r(t) θεωρείται ότι είναι μηδέν. Σκοπός της μεθόδου είναι να μειώσει όλες τις μεταβολές των μεταβλητών κατάστασης στο μηδέν όταν αυτές έχουν διαταραχθεί.



Σχήμα 2. 16 : State Feedback Controller

Από τις εξισώσεις κατάστασης της σχέσης (2.52), αντικαθιστώντας με τον παραπάνω νόμο και δεδομένου πως ο πίνακας D στον έλεγχο ανάδρασης θεωρείται μηδέν, έχουμε την εξής σχέση :

$$\dot{x}(t) = (A - BK)x(t)$$

$$y(t) = C\,x(t) \tag{2.59}$$

Η λύση της παραπάνω εξίσωσης δίνεται ως εξής :

$$x(t) = e^{(A-BK)t} \cdot x(0) \tag{2.60}$$

Οι ιδιοτιμές του πίνακα (A-BK) είναι οι επιθυμητοί πόλοι του κλειστού συστήματος. Οι πίνακες A,B είναι οι πίνακες του συστήματος και το P είναι ο πίνακας σειρά που περιέχει τους επιθυμητούς πόλους κλειστού βρόχου. Η συνάρτηση επιστρέφει τον πίνακα κέρδους K και τον πίνακα κλειστού βρόχου Af [27].

Οι πόλοι του συστήματος θα πρέπει να μεταφερθούν κατά 10-15% πιο αριστερά στο αριστερό μιγαδικό επίπεδο. Οι δύο κυρίαρχοι πόλοι που είναι πιο αργοί και τείνουν να κυριαρχούν στην απόκριση, θα κρατηθούν κατά το δυνατό πιο κοντά στον φανταστικό άξονα, ώστε με αυτόν τον τρόπο να συμπεριφέρεται το σύστημα ως ένα σύστημα δευτέρου βαθμού. Οι άλλοι πόλοι τοποθετούνται μακριά από τους δύο κυρίαρχους πόλους. Με αυτόν τον τρόπο εγγυάται η ευστάθεια του κλειστού συστήματος. Εάν μετακινήσουμε τους πόλους πολύ αριστερά ώστε να πάρουμε μια γρηγορότερη απόκριση, κινδυνεύουμε να κινηθούμε σε πλαίσια εκτός πραγματικότητας, καθώς οι ενεργοποιητές πιθανόν να μην μπορούν να ανταποκριθούν σε αυτές τις ταχύτητες [43-47].

2.4.3. Βέλτιστος Έλεγχος (μέσω της μεθόδου Γραμμικού Τετραγωνικού Ρυθμιστή (LQR))

Στον κλασικό έλεγχο προσπαθούμε να ελαχιστοποιήσουμε το σφάλμα σε καθορισμένα χρονικά σημεία, π.χ. σφάλμα μόνιμης κατάστασης. Στο βέλτιστο έλεγχο ελαχιστοποιούμε το σφάλμα παντού. Ο βέλτιστος Έλεγχος (Optimal Control) πρωτοεμφανίστηκε το 1960, όταν ΗΠΑ και πρώην Σοβιετική Ένωση, έδειχναν μεγάλο ενδιαφέρον στην έρευνα για καθοδήγηση (guidance) και ελιγμούς (maneuvering) κυρίως για στρατιωτικές και διαστημικές εφαρμογές. Σκοπός του ελέγχου αυτού είναι η απόδοση του συστήματος, εκτός από αποδεκτή να είναι και η βέλτιστη. Η διαφορά του βέλτιστου ελέγχου σε σχέση με τον κλασικό είναι ότι στον βέλτιστο, εκτός από την ελαχιστοποίηση του σφάλματος σε καθορισμένα σημεία, ελαχιστοποιούμε το σφάλμα παντού.

Ο γραμμικός τετραγωνικός ρυθμιστής (Linear Quadratic Regulator) ως μέθοδος βέλτιστου ελέγχου, χρησιμοποιείται για να δώσει καλύτερες δυναμικές και στατικές αποκρίσεις, βρίσκοντας το ιδανικό K του ελεγκτή, επιλέγοντας συνδυαστικά ορισμένα

χαρακτηριστικά, όπως η απόδοση του συστήματος και η προσπάθεια που απαιτείται για την απόδοση του [34-36].

Ο LQR είναι ένας βέλτιστος ελεγκτής που είναι πολύ γνωστός λόγω της ευρείας χρήσης του σε συστήματα ελέγχου. Ο λόγος που ονομάζεται γραμμικός (linear) είναι ότι ισχύει για γραμμικά συστήματα. Το τετραγωνικό (quadratic) δηλώνει την ύπαρξη μιας τετραγωνικής αντικειμενικής συνάρτησης που πρέπει να ελαχιστοποιηθεί [34-36].

Η ρύθμιση φορτίου - συχνότητας του συστήματος ισχύος είναι βασικά ένα μη γραμμικό σύστημα. Έτσι για την εφαρμογή του Γραμμικού Τετραγωνικού Ρυθμιστή (LQR), το σύστημα γραμμικοποιείται γύρω από ένα μόνο σημείο λειτουργίας. Χρησιμοποιείται λοιπόν το μοντέλο του χώρου κατάστασης που είναι η γραμμική μορφή του μη γραμμικού συστήματος, ώστε να εφαρμοστεί ο Γραμμικός Τετραγωνικός Ρυθμιστής.

Σκοπός είναι να βρούμε τον πίνακα κέρδους ανάδρασης «K», έτσι η συνάρτηση κόστους **J** να ελαχιστοποιείται ενώ το σύστημα μεταφέρεται από την αρχική κατάσταση $x(0)\neq 0$ στο σημείο ισορροπίας στην αρχή καθώς ο χρόνος τείνει στο άπειρο($t\rightarrow \infty$, $x(\infty)=0$) [30], [34-36].

Η συνάρτηση κόστους στην τετραγωνική μορφή είναι:

$$J = \frac{1}{2}\int_0^{\infty} (x^T Q x + u^T R u)\, dt \tag{2.61}$$

όπου,

Q≥ 0: ο είναι πραγματικός, συμμετρικός και θετικά ημιπεπερασμένος πίνακας κατάλληλων διαστάσεων

R≥ 0 : ο πραγματικός, συμμετρικός και θετικά πεπερασμένος πίνακας κατάλληλων διαστάσεων.

Οι πίνακες βάρους Q, R επιδρούν με τις μεταβλητές x, u και αποτελούν επιλογές των μηχανικών που ρυθμίζουν τον έλεγχο.

Ο LQR προκύπτει με ανατροφοδότηση κατάστασης

$$u = -K\, x(t) \tag{2.62}$$

Ο πίνακας κέρδους K δίνεται από τον τύπο :

$$K = R^{-1} B^T S \tag{2.63}$$

Όπου S είναι ένας πραγματικός, συμμετρικός και θετικά πεπερασμένος πίνακας που προκύπτει από την επίλυση της εξίσωσης Riccatti του πίνακα που δίνεται από:

$$A^T S + SA - SBR^{-1}B^T S + Q = 0 \tag{2.64}$$

Έτσι το σύστημα κλειστού βρόχου παίρνει την τελική μορφή :

$$\dot{x} = (A - BK)\cdot x \;=\; A_c x \tag{2.65}$$

2.5.Μοντέλο Προσομοιόσεων συστήματος Ρύθμισης Φορτίου – Συχνότητας Απομονωμένης Περιοχής (Single Area) με προσθήκη ελεγκτή

Για το μοντέλο που θα χρησιμοποιήσουμε, από τις σχέσεις (2.29) και (2.59) έχουμε :

$$\dot{x}(t) = (A - BK) \cdot x(t) + F \cdot d(t) \tag{2.66}$$

Όπου $K = [k_1 \quad k_2 \quad k_3 \quad k_4]$ και σε μορφή πινάκων :

$$\dot{x} = \begin{bmatrix} -\frac{D_1}{M_1} & \frac{1}{M_1} & 0 & 0 \\ 0 & -\frac{1}{T_{t_1}} & \frac{1}{T_{t_1}} & 0 \\ -\frac{1}{R_1 T_{g_1}} & 0 & -\frac{1}{T_{g_1}} & 0 \\ B_1 & 0 & 0 & 0 \end{bmatrix} \cdot x + \begin{bmatrix} 0 \\ 0 \\ \frac{1}{T_{g_1}} \\ 0 \end{bmatrix} \cdot [k_1 \quad k_2 \quad k_3 \quad k_4] \cdot x + \begin{bmatrix} -\frac{1}{M_1} \\ 0 \\ 0 \\ 0 \end{bmatrix} \cdot d$$

(2.67)

Όμως : $\mathbf{u = -k_4 \cdot \int ACE}$, επομένως :

$$\dot{x} = \begin{bmatrix} -\frac{D_1}{M_1} & \frac{1}{M_1} & 0 & 0 \\ 0 & -\frac{1}{T_{t_1}} & \frac{1}{T_{t_1}} & 0 \\ -\frac{1}{R_1 T_{g_1}} & 0 & -\frac{1}{T_{g_1}} & 0 \\ B_1 & 0 & 0 & 0 \end{bmatrix} \cdot x + \begin{bmatrix} 0 \\ 0 \\ \frac{1}{T_{g_1}} \\ 0 \end{bmatrix} \cdot [0 \quad 0 \quad 0 \quad -k_4] \cdot x + \begin{bmatrix} -\frac{1}{M_1} \\ 0 \\ 0 \\ 0 \end{bmatrix} \cdot d$$

(2.68)

Και τελικά : $\dot{x} = \begin{bmatrix} -\frac{D_1}{M_1} & \frac{1}{M_1} & 0 & 0 \\ 0 & -\frac{1}{T_{t_1}} & \frac{1}{T_{t_1}} & 0 \\ -\frac{1}{R_1 T_{g_1}} & 0 & -\frac{1}{T_{g_1}} & \frac{k_1}{T_{g_1}} \\ B_1 & 0 & 0 & 0 \end{bmatrix} \cdot x + \begin{bmatrix} -\frac{1}{M_1} \\ 0 \\ 0 \\ 0 \end{bmatrix} \cdot d$

(2.69)

με: $A_{new} = \begin{bmatrix} -\frac{D_1}{M_1} & \frac{1}{M_1} & 0 & 0 \\ 0 & -\frac{1}{T_{t_1}} & \frac{1}{T_{t_1}} & 0 \\ -\frac{1}{R_1 T_{g_1}} & 0 & -\frac{1}{T_{g_1}} & \frac{k_1}{T_{g_1}} \\ B_1 & 0 & 0 & 0 \end{bmatrix}$, $B_{new} = \begin{bmatrix} -\frac{1}{M_1} \\ 0 \\ 0 \\ 0 \end{bmatrix}$

(2.70)

2.6.Μοντελο Προσομοιώσεων συστήματος Ρύθμισης Φορτίου - Συχνότητας Δύο Περιοχών (Two Area LFC) με προσθήκη ελεγκτή

Από τον κανόνα της ανατροφοδότησης, για τον έλεγχο του συστήματος δύο περιοχών, όπως έχουμε αναλύσει ήδη για μία περιοχή, προκύπτει η σχέση (2.58) :

$$\dot{x}(t) = (A - BK) \cdot x(t) + F \cdot d(t)$$

Και αφού :

$$u_1 = -K_{18} \cdot x_8 = -K_{18} \cdot \int ACE_1 \quad \text{και} \quad u_2 = -K_{29} \cdot x_9 = -K_{29} \cdot \int ACE_2 \qquad (2.71)$$

ο πίνακας K θα είναι : $K = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & K_{18} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & K_{29} \end{bmatrix}$

(2.72)

Και τελικά λαμβάνουμε τους πίνακες A_c = [A-BK] και [F] :

$$A_c = \begin{bmatrix} \frac{-1}{T_{p1}} & \frac{K_{p1}}{T_{p1}} & 0 & 0 & 0 & 0 & \frac{-K_{p1}}{T_{p1}} & 0 & 0 \\ 0 & \frac{-1}{T_{t1}} & \frac{1}{T_{t1}} & 0 & 0 & 0 & 0 & 0 & 0 \\ \frac{-1}{R_1 T_{g1}} & 0 & \frac{-1}{T_{g1}} & 0 & 0 & 0 & 0 & -\frac{K_{18}}{T_{g1}} & 0 \\ 0 & 0 & 0 & \frac{-1}{T_{p2}} & \frac{K_{p2}}{T_{p2}} & 0 & \frac{K_{p2}}{T_{p2}} & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{-1}{T_{t2}} & \frac{1}{T_{t2}} & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{-1}{R_2 T_{g2}} & 0 & \frac{-1}{T_{g2}} & 0 & 0 & \frac{K_{29}}{T_{g2}} \\ 2\pi T^0 & 0 & 0 & -2\pi T^0 & 0 & 0 & 0 & 0 & 0 \\ B_1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & B_2 & 0 & 0 & -1 & 0 & 0 \end{bmatrix} \text{και } F = \begin{bmatrix} \frac{-K_{p1}}{T_{p1}} & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & \frac{-K_{p2}}{T_{p2}} \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}$$

(2.73)

3. Κυβερνοεπιθέσεις και Κυβερνοασφάλεια στο Σύστημα Ρύθμισης Φορτίου – Συχνότητας

Αν και τα συστήματα LFC διασφαλίζουν τη ευστάθεια του συστήματος με αξιόπιστη ηλεκτρική ισχύ εγγυημένης ποιότητας και μηδενικής απόκλισης συχνότητας, εξαρτώνται σε μεγάλο βαθμό από τα δίκτυα επικοινωνίας. Το LFC μιας περιοχής ή διασυνδεδεμένων περιοχών που περιλαμβάνουν πολλαπλές γεννήτριες γίνεται με τη βοήθεια κέντρων ελέγχου ενέργειας που κάνουν χρήση ηλεκτρονικών υπολογιστών και συστημάτων απομακρυσμένης απόκτησης δεδομένων όπως το SCADA. Επομένως είναι προφανές ότι αναπόφευκτα η χρήση των παραπάνω δικτύων θα επιφέρει κινδύνους για την ασφάλεια του δικτύου [48].

Επιπλέον, τα σχήματα LFC πρέπει να παράγουν σήματα ελέγχου σε χρονική κλίμακα δευτερολέπτων. Επομένως, ο βρόχος LFC δεν έχει την πολυτέλεια να χρησιμοποιεί σύνθετους αλγόριθμους επαλήθευσης δεδομένων για την επικύρωση και την εκτίμηση των δεδομένων μέτρησης. Οι εισβολείς μπορούν να επωφεληθούν από αυτό και να χειριστούν τα δεδομένα μέτρησης με λιγότερο λεπτομερή μαθηματικά. Αυτές οι συνθήκες υποδεικνύουν την ευπάθεια του συστήματος LFC σε κυβερνοεπιθέσεις [49].

Ως εκ τούτου, η μελέτη και η ανάλυση των επιπτώσεων επίθεσης στο σύστημα LFC είναι εξαιρετικά σημαντική. Οι ερευνητικές δραστηριότητες στον τομέα της κυβερνοασφάλειας του συστήματος αυτού βοηθούν επίσης στην ανάπτυξη αντιμέτρων όπως οι μηχανισμοί ανίχνευσης και άμυνας που μπορούν να μετριάσουν τις επιπτώσεις των κυβερνοεπιθέσεων.

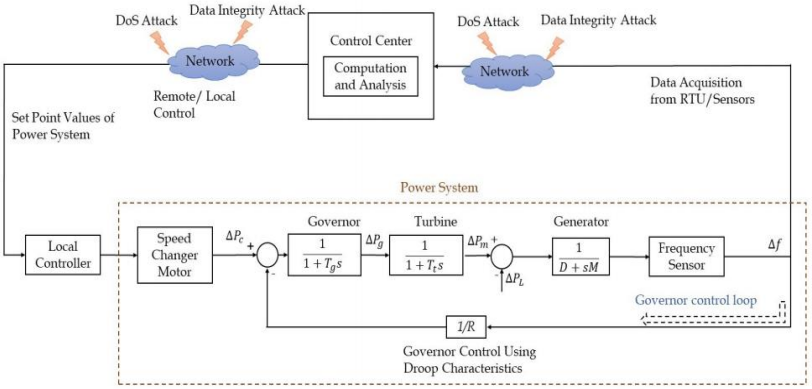
Ο στόχος της κυβερνοασφάλειας της λειτουργίας LFC έχει να κάνει κυρίως με [50]:

- το πρόβλημα της εύρεσης των κακόβουλων μετρήσεων και την αποτροπή του ελεγκτή από εκτέλεση λανθασμένων κινήσεων λόγω πειραγμένων υπολογισμών σφάλματος ελέγχου περιοχής (ACE).
- τη διατήρηση της ισορροπίας μεταξύ παραγωγής και ζήτησης, παρουσία αναξιόπιστων μετρήσεων.

3.1.Ευπαθή Σημεία στα Συστήματα Ρύθμισης Φορτίου – Συχνότητας

3.1.1. Ευπαθή σημεία συστημάτων ρύθμισης φορτίου – συχνότητας σε απομονωμένα συστήματα ισχύος (Single Area LFC)

Ο στόχος του συστήματος LFC μιας περιοχής περιορίζεται μόνο στη σταθεροποίηση της συχνότητας λειτουργίας στην ονομαστική τιμή, καθώς δεν απαιτείται ρύθμιση της διασυνδετικής ροής.



Σχήμα 3. 1 : Γενικό Διάγραμμα Βαθμίδων Συστήματος Ρύθμισης – Φορτίου Συχνότητας Απομονωμένης (Single Area) Περιοχής με ευπαθή σημεία ως προς επιθέσεις [32]

Τα κυβερνο-φυσικά επίπεδα του LFC είναι ελκυστικά σημεία για τους εισβολείς. Τα σημεία επίθεσης για το απομονωμένο σύστημα περιλαμβάνουν κανάλια μετάδοσης του δικτύου επικοινωνίας, υπολογιστικούς αλγόριθμους στο κέντρο ελέγχου και φυσικούς αισθητήρες (sensors) ή ενεργοποιητές (actuators) [16], [26].

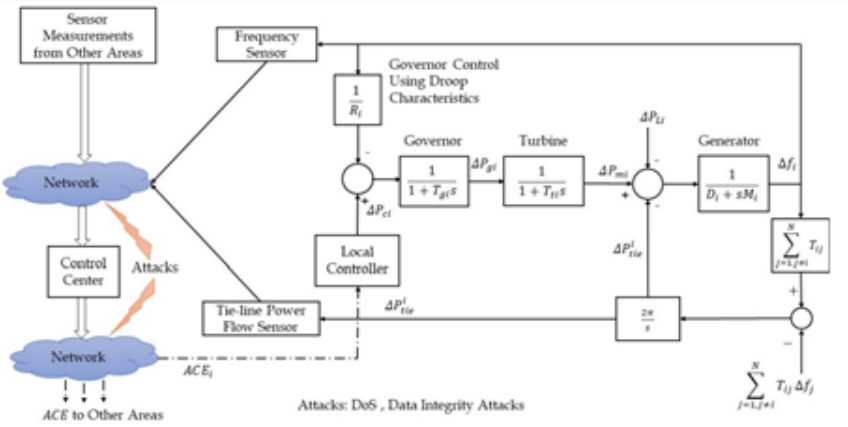
Για τη μελέτη των επιθέσεων στον κυβερνοχώρο μέσω του συστήματος LFC, το βασικό μοντέλο τροποποιείται για να ενσωματώσει τα χαρακτηριστικά επίθεσης. Τα κανάλια αισθητήρα και ενεργοποιητή είναι τα κύρια κανάλια-στόχος για τους επιτιθέμενους. Στην περίπτωση του συστήματος LFC μιας περιοχής, οι επιθέσεις υλοποιούνται είτε μέσω του χειρισμού της συχνότητας του συστήματος, της πραγματικής ισχύος εξόδου των γεννητριών και του σήματος ελέγχου του ρυθμιστή είτε μη επιτρέποντας στις εξουσιοδοτημένες πηγές την πρόσβαση σε αυτά τα σήματα [26].

3.1.2. Ευπαθή σημεία συστημάτων ρύθμισης φορτίου – συχνότητας σε διασυνδεδεμένα συστήματα ισχύος (Multi Area LFC)

Στα διασυνδεδεμένα σύστημα ισχύος, το PMU του ηλεκτρικού δικτύου ή το RTU ενός παραδοσιακού συστήματος SCADA στέλνει τις μετρήσεις του αισθητήρα όπως η συχνότητα του συστήματος ισχύος, οι ροές ισχύος, η χρονική απόκλιση του συστήματος και τα σήματα ισχύος της γεννήτριας στο κέντρο ελέγχου. Ο Αυτόματος Έλεγχος Παραγωγής (AGC) βασίζεται στις μετρήσεις της συχνότητας και της ισχύος

διασύνδεσης και οποιαδήποτε μεταβολή αυτών των μετρήσεων λόγω επιθέσεων ή διαταραχής φορτίου μπορεί να έχει άμεσο αντίκτυπο στην ευστάθεια του συστήματος και την οικονομική λειτουργία του [26], [32], [51].

Επομένως, κατά τη λειτουργία του Αυτομάτου Ελέγχου Παραγωγής, το κέντρο ελέγχου εκχωρεί τα Σφάλματα Ελέγχου Περιοχής (ACE) σε αντίστοιχους τοπικούς ελεγκτές και ελέγχει την απόκλιση συχνότητας και της διασυνδετικής ροής ισχύος των γεννητριών κάθε περιοχής με βάση τα δεδομένα που συλλέγει [51].

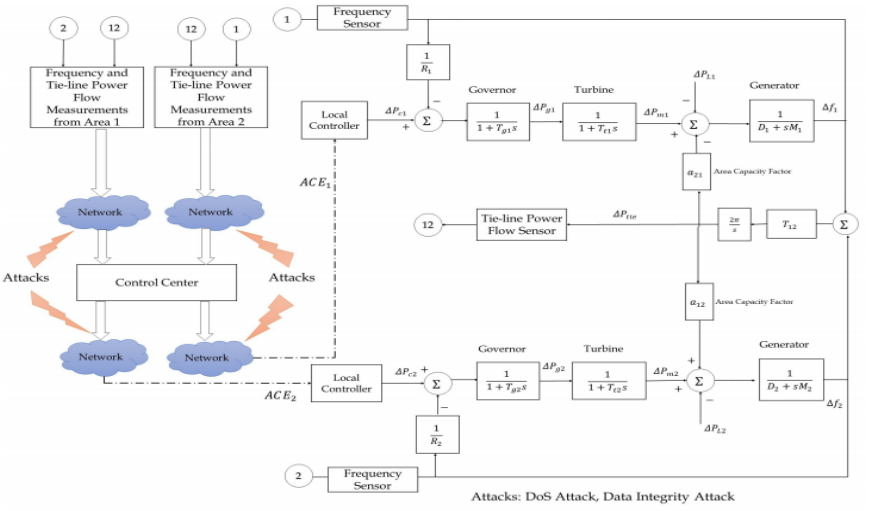


Σχήμα 3. 2 : Γενικό Διάγραμμα Βαθμίδων Συστήματος Ρύθμισης – Φορτίου Συχνότητας Πολλαπλών (Mulit Area) Περιοχών με ευπαθή ως προς επιθέσεις σημεία [32]

Παρόλο που η διασύνδεση των περιοχών βελτιώνει την απόδοση του συστήματος, αυξάνει την ευπάθεια σε κυβερνοεπιθέσεις μέσω της εισόδου της γραμμής διασύνδεσης. Στην περίπτωση διασυνδεδεμένου συστήματος με πολλές περιοχές η επίθεση επικεντρώνεται κυρίως στην παραποίηση των τιμών του Σφάλματος Ελέγχου Περιοχής (ACE), μέσω του χειρισμού της συχνότητας ή της διασυνδετικής ροής ισχύος [52].

Η επίθεση σε μία περιοχή LFC μπορεί να είναι αρκετά ισχυρή για να δημιουργήσει γενική κατάρρευση (blackout) σε ολόκληρο το δίκτυο ισχύος [60]. Η επίθεση πάνω στο κανάλι των ενεργοποιητων (actuator) ή των αισθητήρων (sensor) του συστήματος LFC πολλαπλών περιοχών μπορεί να οδηγήσει σε μη προσβασιμότητα ή σε κακόβουλο χειρισμό σημάτων όπως στο σύστημα της συχνότητας, της διασυνδεδεμένης ισχύος, της ισχύος εξόδου της γεννήτριας ενεργοποίησης και των τιμών του Σφάλματος Ελέγχου Περιοχής (ΣΕΠ) κάθε περιοχής ελέγχου.

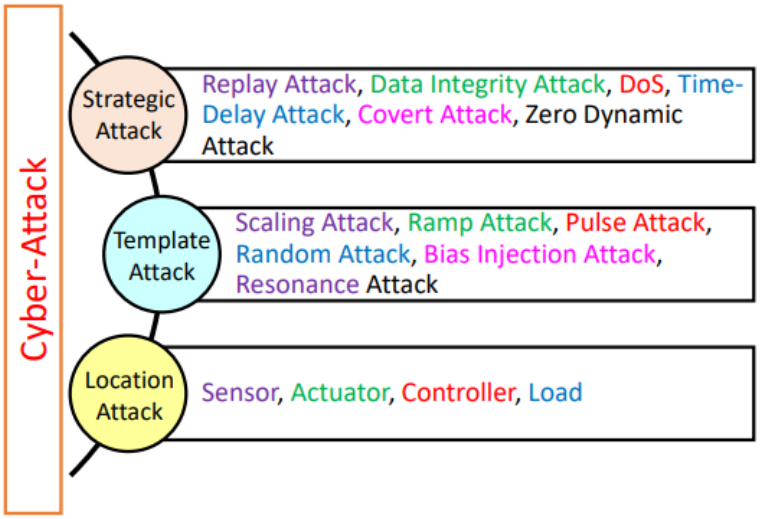
Το σύστημα LFC δύο περιοχών χρησιμοποιείται ευρέως για τη μελέτη της επίδρασης των επιθέσεων στον κυβερνοχώρο σε συστήματα LFC πολλαπλών περιοχών λόγω της απλότητας του. Ο αριθμός των καναλιών μετάδοσης είναι μεγαλύτερος σε σύγκριση με το σύστημα LFC μιας περιοχής κι επομένως, ο αντίκτυπος της επίθεσης και η υποβάθμιση της απόδοσης του συστήματος εντείνονται στο σύστημα LFC δύο περιοχών, αφού αυξάνεται ο αριθμός των διασυνδεδεμένων περιοχών. Παρόμοια συμβαίνει με τα συστήματα ισχύος τριών, τεσσάρων και περισσοτέρων περιοχών [53-55].



Σχήμα 3. 3 : Γενικό Διάγραμμα Βαθμίδων Συστήματος Ρύθμισης – Φορτίου Συχνότητας Δύο (Two Area) Περιοχών με ευπαθή ως προς επιθέσεις σημεία [32]

3.2.Ανάλυση και Ταξινόμηση Επιθέσεων στο Σύστημα Ρύθμισης Φορτίου – Συχνότητας

Θα ορίσουμε τις επιθέσεις στη ρύθμιση φορτίου συχνότητας κινούμενοι σε τρείς άξονες, με βάση τα είδη (Στρατηγική) των επιθέσεων, το πρότυπο Επίθεσης και το σημείο Επίθεσης, όπως παρουσιάζεται στο σχήμα 3.4 [50].



Σχήμα 3. 4 : Ταξινόμηση Επιθέσεων στο σύστημα Ρύθμισης Φορτίου – Συχνότητας

3.2.1. Είδη Επιθέσεων (Strategic Attack)

3.2.1.1.Επιθέσεις Άρνησης Εξυπηρέτησης (DoS Attacks)

Η DoS είναι μία από τις πιο κακόβουλες επιθέσεις, που μπορούν να μπλοκάρουν το κανάλι επικοινωνίας στέλνοντας τεράστιες ποσότητες μη αυθεντικών πακέτων. Πρόκειται για επίθεση στον κυβερνοχώρο που προκαλεί μεγάλο φόρτο μετάδοσης και καταναλώνει υπερβολικές ποσότητες εύρους ζώνης δικτύου και υπολογιστικών πόρων γενικότερα, προκαλώντας διακοπές στο δίκτυο [48] [56].

Για το σύστημα LFC, τα κανάλια επικοινωνίας ((α) που συνδέουν **RTU / PMU** και το **κέντρο ελέγχου** και (β) που συνδέουν το **κέντρο ελέγχου** και τον **ρυθμιστή στροφών**) είναι τα κύρια τρωτά σημεία του συστήματος για επιθέσεις DoS. Οι επιθέσεις DoS μπορούν να εμποδίσουν τα δεδομένα μέτρησης που θα μεταφερθούν στο κέντρο ελέγχου και να επηρεάσουν την ενημέρωση της εντολής ελέγχου από το κέντρο ελέγχου ή να καθυστερήσουν τα σήματα ελέγχου που αποστέλλονται στον ενεργοποιητή κάνοντας την απόδοση του συστήματος ισχύος χειρότερη [51].

Τα συστήματα LFC είναι επίσης επιρρεπή σε επιθέσεις DDoS (Coordinated attacks) και η καθυστέρηση επικοινωνίας που προκαλείται από το DDoS μπορεί να επηρεάσει δυσμενώς τη σταθερότητα της συχνότητας [57].

3.2.1.2. Επιθέσεις Ακεραιότητας (Data Integrity Attacks)

Οι επιθέσεις ακεραιότητας πραγματοποιούνται μέσω του χειρισμού σημάτων μέτρησης και ελέγχου που μεταδίδονται μεταξύ των τμημάτων του κυβερνοχώρου του συστήματος ισχύος [58]. Ο επιτιθέμενος παραποιεί τις πληροφορίες που αποστέλλονται από τους αισθητήρες προς τον ελεγκτή (Διαχειριστή Δικτύου EMS) ή από τον EMS προς τους ενεργοποιητές (actuators), οι οποίοι επιβάλλουν τις αποφάσεις ελέγχου στο δίκτυο. Οι ψευδείς πληροφορίες μπορεί να είναι παραποιημένες μετρήσεις/σήματα ελέγχου ή ψευδείς ακολουθίες για συστήματα με διάφορους αισθητήρες και ενεργοποιητές. Οι επιθέσεις ακεραιότητας μπορεί να προκύψουν με τη λήψη των μυστικών κλειδιών που χρησιμοποιούνται από τις συσκευές ή με τη διακύβευση αισθητήρων ή ελεγκτών. Επιθέσεις αυτού του τύπου είναι παρουσιάζονται παρακάτω:

3.2.1.2.1. Επιθέσεις Έγχυσης Ψευδών Δεδομένων - False Data Injection (FDI) Attacks

Οι επιθέσεις έγχυσης ψευδών δεδομένων (False Data Injection Attacks) είναι μία σημαντική κατηγορία επιθέσεων. Στις επιθέσεις FDI ο επιτιθέμενος στέλνει ψευδείς πληροφορίες από αισθητήρες στο κέντρο ελέγχου ή από το κέντρο ελέγχου στις γεννήτριες που ελέγχονται από το AGC. Οι FDIA είναι καταστροφικές για τα

συστήματα AGC, καθώς μπορούν να επηρεάσουν τη σταθερότητα και την οικονομική λειτουργία τους. Οι FDIA φαίνεται να είναι πιθανές αιτίες που να οδηγούν σε καταστάσεις υποβιβασμού συχνότητας και θα μπορούσαν να οδηγήσουν σε μη αναγκαία απόρριψη φορτίου (load shedding) [59].

Οι επιθέσεις FDI εφαρμόζονται στα κανάλια μέτρησης και ελέγχου του συστήματος LFC με τη μορφή διανυσμάτων επίθεσης εισόδου που έχουν διαμορφωθεί χρησιμοποιώντας στρατηγικές διαφθοράς δεδομένων ή πρότυπα επίθεσης. Το AGC είναι ένας ελκυστικός στόχος για FDI επιθέσεις, καθώς ελέγχει τη **συχνότητα δικτύου**, την κρίσιμη παγκόσμια παράμετρο του συστήματος ισχύος. Οι επιθέσεις FDI ξεκινούν στο σύστημα LFC με τους ακόλουθους τρόπους [61-63]:

- Μέσω επίθεσης σε φυσικούς αισθητήρες, παραποιώντας τις μετρήσεις τους.
- Χρησιμοποιώντας κανάλια επικοινωνίας δεδομένων αισθητήρα και ενεργοποιητή (Actuator/Sensor).
- Διαμορφώνοντας τους υπολογιστικούς αλγορίθμους του κέντρου ελέγχου.
- Χρησιμοποιώντας VPNs για την απόκρυψη IP συνδεόμενου χρήστη από τους κατανεμημένους αισθητήρες.
- Δίνοντας ψευδές στίγμα στο Παγκόσμιο Σύστημα Εντοπισμού Θέσης (GPS), επιτρέποντας έτσι τη διείσδυση στις μονάδες μέτρησης φάσης (PMU) και επηρεάζοντας το συγχρονισμό ρολογιών των υποσταθμών που οδηγεί σε λανθασμένες μετρήσεις γωνίας φάσης.

3.2.1.2.2. Επίθεση επανάληψης (Replay Attack)

Πριν από την επίθεση, ο επιτιθέμενος καταγράφει τις μετρήσεις κατά την κανονική κατάσταση λειτουργίας του δικτύου ισχύος για κάποιο χρονικό διάστημα. Κατά τη διάρκεια της επίθεσης, οι πραγματικές μετρήσεις που παρατηρούνται από τους αισθητήρες αντικαθίστανται από τις καταγεγραμμένες μετρήσεις και αποστέλλονται, σκόπιμα, λανθασμένες τιμές στο κέντρο ελέγχου [64]. Επιθέσεις αυτού του είδους δεν απαιτούν προηγούμενη γνώση του μοντέλου του συστήματος, ούτε των ελεγκτών και των εκτιμητών [59].

3.2.1.2.3. Κρυφή επίθεση (Covert Attack)

Οι κρυφές επιθέσεις δημιουργούν μια κρυφή και ισχυρή στρατηγική επίθεσης από την πλήρη γνώση του συστήματος και τη χρήση της δυνατότητας πρόσβασής τους σε σήματα ελέγχου και μετρήσεις που μεταδίδονται μέσω των καναλιών επικοινωνίας [65-66].

Οι κρυφές επιθέσεις λειτουργούν ακυρώνοντας την επίδραση των σημάτων επίθεσης, υπολογίζοντας την απόκριση εξόδου του συστήματος και αφαιρώντας την από τις

μετρήσεις που καταγράφονται. Κατά συνέπεια, το σύστημα διάγνωσης από την πλευρά του ελεγκτή, λαμβάνει τα δεδομένα μέτρησης χωρίς πληροφορίες σχετικά με την επίθεση. Αυτό κάνει την επίθεση κρυφή. Επιπλέον, εκμεταλλεύεται την οριακή τιμή που υπάρχει στη λογική των συστημάτων ανίχνευσης για τη μείωση των ψευδών συναγερμών λόγω της ύπαρξης αβεβαιοτήτων του μοντέλου καθώς και άγνωστων διαταραχών. Ως εκ τούτου, η επίθεση θα παραμείνει κρυφή παρά τις ασυμφωνίες του μοντέλου που συμβαίνουν μεταξύ του μοντέλου εγκατάστασης του εισβολέα και του πραγματικού [65].

3.2.1.3. Επιθέσεις Χρονοκαθυστέρησης (Time-Delay – TD Attacks)

Ο επιτιθέμενος καθυστερεί τα σήματα μέτρησης που αποστέλλονται από τους αισθητήρες ή τα σήματα ελέγχου που αποστέλλονται από τον ελεγκτή. Κατά συνέπεια, η λήψη αποφάσεων από τον EMS, αν και σωστή, αναφέρεται σε λανθασμένα χρονικά δεδομένα (παλαιότερα χρονικά διαστήματα). Επομένως, όλοι οι επαγόμενοι χειρισμοί αφορούν σε διαφορετική κατάσταση για το δίκτυο ισχύος. Οι επιθέσεις χρονοκαθυστέρησης αποτελούν τον ευκολότερο τύπο επιθέσεων.

Ένα σύστημα LFC με επίθεση TD διαμορφώνεται ως υβριδικό σύστημα με τη δράση διακόπτη (γι' αυτό και αναφέρεται ως Time-Delay Switch Attack), "Off / Delay-by-τ", όπου τ, ο τυχαίος χρόνος καθυστέρησης που εισάγεται στην κατάσταση μέτρησης ή στα σήματα ελέγχου. Η εισαγωγή χρονικών καθυστερήσεων στις δυναμικές καταστάσεις του συστήματος μπορεί να μεταφέρουν το σύστημα σε ασταθή κατάσταση [67].

3.2.1.4. Zero Dynamics Attack (Επίθεση Μηδενικής Δυναμικής)

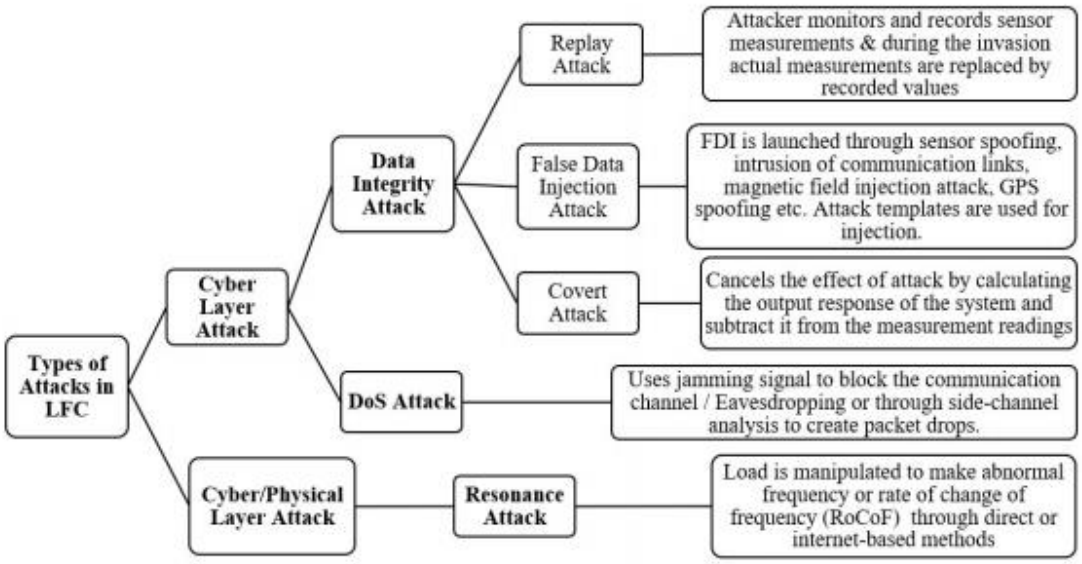
Για την επιτυχή εκτέλεση της επίθεσης μηδενικής δυναμικής, ο εισβολέας θα πρέπει να έχει τέλεια γνώση της δυναμικής των εγκαταστάσεων που υπολογίζονται από πίνακες εξισώσεων κατάστασης και εξόδου [64-65]. Σε αυτήν την επίθεση, η έξοδος του γραμμικού συστήματος αποσυνδέεται και χρησιμοποιεί τα μηδενικά στη συνάρτηση μεταφοράς για να αναπτύξει μια συγκεκριμένη στρατηγική επίθεσης.

3.2.2. Επιθέσεις Προτύπου (Template Attack)

Η επίθεση προτύπου, μπορεί να εισαχθεί τροποποιώντας το πλάτος του σήματος του μηνύματος. Μια τέτοια επίθεση μπορεί να χωριστεί γενικά στους ακόλουθους τύπους [50], [68-71]:

- **Scaling Attack** (Κλιμακούμενη Επίθεση): οι πραγματικές μετρήσεις τροποποιούνται σε υψηλότερες ή χαμηλότερες τιμές, ανάλογα με την παράμετρο της επίθεσης κλιμακωτά.

- **Ramp Attack** (επίθεση Ράμπας): οι πραγματικές μετρήσεις τροποποιούνται σταδιακά με την προσθήκη μίας συνάρτησης ράμπας (ramp function) που σταδιακά αυξάνεται/μειώνεται με το χρόνο.
- **Pulse Attack** (Επίθεση παλμών): Σε αντίθεση με την scaling attack, όπου οι μετρήσεις τροποποιούνται σε υψηλότερες/χαμηλότερες τιμές καθ' όλη τη διάρκεια της επίθεσης, σε αυτόν τον τύπο επίθεσης, οι πραγματικές μετρήσεις τροποποιούνται μέσω παλμών μικρής διάρκειας με καθορισμένη ή μεταβαλλόμενη παράμετρο επίθεσης.
- **Random Attack** (Τυχαία Επίθεση): Αυτή η επίθεση περιλαμβάνει την προσθήκη θετικών τιμών που επιστρέφονται με μία ομοιόμορφη τυχαία λειτουργία στις πραγματικές μετρήσεις. Τα ανώτερα και κατώτερα όρια αυτής της επίθεσης διαμορφώνουν τις μεταβολές στις παραποιημένες από τον επιτιθέμενο τιμές για το δίκτυο ισχύος.
- **Bias injection attack** (Επίθεση έγχυσης παράγοντα Bias) : Η επίθεση αυτή είναι η απλούστερη επίθεση, στην οποία ο αισθητήρας ή τα σήματα ελέγχου του καναλιού που δέχεται επίθεση, εγχέονται με ένα σταθερό σήμα πόλωσης .



Σχήμα 3. 5 : Διάγραμμα επιθέσεων στο σύστημα Ρύθμισης Φορτίου - Συχνότητας

3.2.3. Σημεία Επίθεσης (Location Attack)

Με βάση τη θέση της επίθεσης, η επίθεση (από άποψη δικτυακού ελέγχου) του συστήματος LFC μπορεί να είναι [50], [63]:

1. Επίθεση στον αισθητήρα: Οι μεταδιδόμενες μετρήσεις αλλάζουν μετά από επίθεση.

2. Επίθεση στον έλεγχο: Το σήμα ελέγχου διαφέρει.

3. Επίθεση στον ενεργοποιητή: Το σήμα του ενεργοποιητή παραμορφώνεται.

4. Επίθεση μέσω Φορτίου: Στη λειτουργία LFC, ο εισβολέας μπορεί επίσης να διεισδύσει μέσω της διαταραχή φορτίου ΔP_d.

3.3.Μοντελοποίηση Συστήματος Ρύθμισης Φορτίου – Συχνότητας παρουσία επιθέσεων

Τα μεγάλα συστήματα ισχύος συνήθως περιέχουν πολλές περιοχές που συνδέονται με γραμμές διασύνδεσης. Το σύστημα LFC είναι ένα δικτυωμένο σύστημα ελέγχου μεγάλης κλίμακας που ρυθμίζει τη ροή ισχύος μεταξύ διαφορετικών περιοχών ισχύος, διατηρώντας παράλληλα την επιθυμητή συχνότητα και τη διασυνδετική ροή ισχύος στο επιθυμητό επίπεδο. Τα ψευδή δεδομένα μπορούν να εγχυθούν στις μετρήσεις διασύνδεσης και συχνότητας εισχωρώντας στα ευαίσθητα κανάλια επικοινωνίας. Αυτήν την περίπτωση θα μελετήσουμε.

Η εξίσωση στο χώρο κατάστασης κατά τη διάρκεια επιθέσεων μπορεί να τροποποιηθεί ως εξής [68], [72-74], :

$$\dot{x} = A\,x(t) + B\,u(t) + E\,d(t) + F\,f(t)$$

$$y = Cx \tag{3.1}$$

Όπου όπως έχουμε αναφέρει ήδη x(t), u(t), d(t), τα διανύσματα κατάστασης, εισόδου και μεταβολής φορτίου (ή οποιασδήποτε διαταραχής αντίστοιχα και A, B, C οι αντίστοιχοι πίνακες κατάστασης, εισόδου και μεταβολής φορτίου. Επιπλέον τώρα f(t) το διάνυσμα επίθεσης και F ο αντίστοιχος πίνακας

3.3.1. Μοντελοποίηση απομονωμένου συστήματος ρύθμισης φορτίου – συχνότητας (Single Area LFC) στον χώρο κατάστασης παρουσία επιθέσεων έγχυσης ψευδών δεδομένων (FDI)

Μεταβλητές κατάστασης :

$$x = \left[\Delta f_1 \;\; \Delta P_{m1} \;\; \Delta P_{v1} \;\; \int ACE_1\right]^T$$

με : $x_1 = \Delta f_1$ $x_2 = \Delta P_m$ $x_3 = \Delta P_v$ $x_4 = \int ACE\,dt$

(3.2)

Μεταβλητές Ελέγχου Εισόδου :

$$u = [u_1]$$

με : $u_1 = \Delta P_{c1}$ (3.3)

Μεταβλητές Εισόδου Διαταραχών :

$$d = [d_1]$$

με : $d_1 = \Delta P_{d1}$ (3.4)

Μεταβλητές Εισόδου Επίθεσης :

$$f = [f_1] \quad (3.5)$$

$$\dot{x} = \begin{bmatrix} -\frac{D_1}{M_1} & \frac{1}{M_1} & 0 & 0 \\ 0 & -\frac{1}{T_{t_1}} & \frac{1}{T_{t_1}} & 0 \\ -\frac{1}{R_1 T_{g_1}} & 0 & -\frac{1}{T_{g_1}} & 0 \\ B_1 & 0 & 0 & 0 \end{bmatrix} \cdot x + \begin{bmatrix} 0 \\ 0 \\ \frac{1}{T_{g_1}} \\ 0 \end{bmatrix} \cdot u + \begin{bmatrix} -\frac{1}{M_1} \\ 0 \\ 0 \\ 0 \end{bmatrix} \cdot d + \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \cdot f \quad (3.6)$$

όπου : $A = \begin{bmatrix} -\frac{D_1}{M_1} & \frac{1}{M_1} & 0 & 0 \\ 0 & -\frac{1}{T_{t_1}} & \frac{1}{T_{t_1}} & 0 \\ -\frac{1}{R_1 T_{g_1}} & 0 & -\frac{1}{T_{g_1}} & 0 \\ B_1 & 0 & 0 & 0 \end{bmatrix}$, $B = \begin{bmatrix} 0 \\ 0 \\ \frac{1}{T_{g_1}} \\ 0 \end{bmatrix}$, $E = \begin{bmatrix} -\frac{1}{M_1} \\ 0 \\ 0 \\ 0 \end{bmatrix}$, $F = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$ (3.7)

3.3.2. Μοντελοποίηση συστήματος ρύθμισης φορτίου – συχνότητας Δύο Περιοχών (Two Area LFC) στον χώρο κατάστασης παρουσία επιθέσεων έγχυσης ψευδών δεδομένων (FDI)

Μεταβλητές κατάστασης :

$$x_i = [\Delta f_1 \ \Delta P_{m_1} \ \Delta P_{v_1} \ \Delta f_2 \ \Delta P_{m_2} \ \Delta P_{v_2} \Delta P_{tie_{12}} \int ACE_1 \int ACE_2]^T, \text{με}$$

$x_1 = \Delta f_1$ $x_2 = \Delta P_{m1}$ $x_3 = \Delta P_{v1}$ $x_4 = \Delta f_2$

$x_5 = \Delta P_{m2}$ $x_6 = \Delta P_{v2}$ $x_7 = \Delta P_{tie}$ $x_8 = \int ACE_1 \, dt$ $x_9 = \int ACE_2 \, dt$ (3.8)

Μεταβλητές Ελέγχου Εισόδου :

$$u = \begin{bmatrix} u_1 \\ u_2 \end{bmatrix}$$

με : $u_1 = \Delta P_{c1}$ & $u_2 = \Delta P_{c2}$ (3.9)

Μεταβλητές Εισόδου Διαταραχών :

$$d = \begin{bmatrix} d_1 \\ d_2 \end{bmatrix}$$

με : $d_1 = \Delta P_{d1}$ & $d_2 = \Delta P_{d2}$ (3.10)

Μεταβλητές Εισόδου Επίθεσης :

$$f = \begin{bmatrix} f_1 \\ f_2 \end{bmatrix}$$

(3.11)

Οι παραπάνω εξισώσεις μπορούν να γραφούν στο χώρο κατάστασης στη μορφή της σχέσης (3.1) :

$$\dot{x} = A\,x(t) + B\,u(t) + E\,d(t) + F\,f(t)$$

(3.12)

Όπου, το A είναι ένας τετραγωνικός πίνακας διαστάσεων 9×9, που ονομάζεται Πίνακας Καταστάσεων, B και E είναι οι ορθογώνιοι πίνακες διαστάσεων 9×2 που ονομάζονται πίνακας ελέγχου και πίνακας διαταραχής αντίστοιχα. Το «x» είναι το διάνυσμα κατάστασης 9×1, το «u» είναι το διάνυσμα ελέγχου 2×1 και το «d» είναι το διάνυσμα διαταραχής 2×1.

Οι πίνακες A(9×9), B(9×2), E(9×2) και F(9×2) είναι οι παρακάτω:

$$A = \begin{bmatrix} \frac{-1}{T_{p1}} & \frac{K_{p1}}{T_{p1}} & 0 & 0 & 0 & 0 & \frac{-K_{p1}}{T_{p1}} & 0 & 0 \\ 0 & \frac{-1}{T_{t1}} & \frac{1}{T_{t1}} & 0 & 0 & 0 & 0 & 0 & 0 \\ \frac{-1}{R_1 T_{g1}} & 0 & \frac{-1}{T_{g1}} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{-1}{T_{p2}} & \frac{K_{p2}}{T_{p2}} & 0 & \frac{K_{p2}}{T_{p2}} & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{-1}{T_{t2}} & \frac{1}{T_{t2}} & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{-1}{R_2 T_{g2}} & 0 & \frac{-1}{T_{g2}} & 0 & 0 & 0 \\ 2\pi T^0 & 0 & 0 & -2\pi T^0 & 0 & 0 & 0 & 0 & 0 \\ B_1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & B_2 & 0 & 0 & -1 & 0 & 0 \end{bmatrix}$$

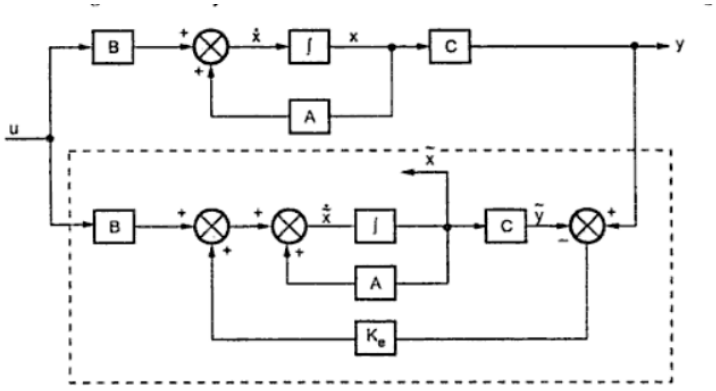
$$B = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ \frac{1}{T_{g1}} & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & \frac{1}{T_{g2}} \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix} \qquad E = \begin{bmatrix} \frac{-K_{p1}}{T_{p1}} & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & \frac{-K_{p2}}{T_{p2}} \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix} \qquad F = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$$

(3.13)

4. Ανίχνευση Κυβερνοεπιθέσεων και ο ρόλος των Παρατηρητών Κατάστασης (State Observers)

4.1.Παρατηρητές Κατάστασης

Στον έλεγχο με ανατροφοδότηση καταστάσεων είναι απαραίτητη προϋπόθεση ότι θα είναι διαθέσιμες οι καταστάσεις του συστήματος. Κάτι τέτοιο είναι πολλές φορές δύσκολο (δαπανηρό λόγω μεγάλου κόστους πολλών αισθητήρων) ή αδύνατο (λόγω θέσης μέτρησης του μεγέθους) [75]. Τη λύση σε αυτό το πρόβλημα δίνουν οι εκτιμητές κατάστασης. Οι εκτιμητές επίσης, προσφέρουν λύση στο πρόβλημα της στοχαστικότητας σε περιπτώσεις διαταραχών ή ακόμη και επιθέσεων στο σύστημα, δηλαδή σε απρόβλεπτα φαινόμενα με αποτέλεσμα να μπορεί ο χειριστής να προλάβει ανεπιθύμητες εντολές χειρισμού που μπορεί να προκύψουν από διαταραχές ή επιθέσεις στα δεδομένα των αισθητήρων [76].



Σχήμα 4. 1 : Διάγραμμα Βαθμίδων Συστήματος και Παρατηρητή Κατάστασης

Όπως θα αναλύσουμε και στο δεύτερο μέρος του κεφαλαίου, για την ανίχνευση κυβερνοεπιθέσεων στο σύστημα ρύθμισης φορτίου - συχνότητας, σύχνα χρησιμοποιούνται παρατηρητές κατάστασης. Έτσι, σε περίπτωση αλλοίωσης ορισμένων μετρήσεων που θα ληφθούν από τους αισθητήρες, με τη βοήθεια των παρατηρητών θα είναι δυνατή η ανίχνευση της εξωτερικής παρέμβασης και συνεπώς η αντιμετώπιση αυτής.

Πιο αναλυτικά, για να αντιμετωπιστούν τα φαινόμενα που αναφέραμε παραπάνω, οι καταστάσεις του συστήματός μας εκτιμώνται μέσω παρατηρητών (observers). Αυτοί αποτελούνται από ένα μαθηματικό μοντέλο (παρόμοιο με το σύστημα), λαμβάνοντας ως είσοδο την έξοδο y και την εντολή ελέγχου u, δίνοντας ως $\hat{x}$, την εκτίμηση του x. Μερικοί, όπως θα δούμε αναλυτικότερα στη συνέχεια, διαθέτουν κατάλληλο κέρδος **L** που υπολογίζεται έτσι ώστε το σφάλμα μεταξύ των καταστάσεων του συστήματος και των εκτιμώμενων καταστάσεων να συγκλίνει γρήγορα και σταθερά στο μηδέν.

Η εκτίμηση της κατάστασης μπορεί να μπορεί να εκτιμήσει σημαντικές μεταβλητές όταν αυτές για διάφορους λόγους δεν είναι διαθέσιμες, όπως η μεταβολή της συχνότητας και η διασυνδετική ροή στο σύστημα ρύθμισης φορτίου - συχνότητας. Όσο περισσότερες πληροφορίες έχει ένας ελεγκτής για τη διαδικασία που ελέγχει, τόσο καλύτερα (με μεγαλύτερη ακρίβεια) μπορεί να την ελέγξει. Αν όμως για παράδειγμα θέλουμε να προλάβουμε τυχόν εντολές ελέγχου που έχουν δοθεί έπειτα από εσφαλμένες εισροές στοιχείων, μπορούμε να χρησιμοποιήσουμε τις εκτιμήσεις των μεταβλητών, αρκεί το σφάλμα μεταξύ πραγματικών και εκτιμώμενων καταστάσεων να συγκλίνει όπως αναφέραμε γρήγορα και σταθερά (συνδυαστικά) στο μηδέν [75-78]

Ο παρατηρητής εκπληρώνει το σκοπό του με τον υπολογισμό του σφάλματος, δηλαδή της διαφοράς της μέτρησης της πραγματικής εξόδου και της εξόδου του παρατηρητή. Το σφάλμα αυτό όπως θα δούμε και στη συνέχεια στο σύστημά μας, πολλαπλασιασμένο με ένα κέρδος L χρησιμοποιείται σαν είσοδος στο σύστημα. Η σωστή επιλογή του κέρδους L θα δώσει ένα σταθερό δυναμικό σύστημα με την εκτίμηση του σφάλματος να συγκλίνει στο μηδέν και άρα οι εκτιμώμενες καταστάσεις να συγκλίνουν στις πραγματικές. Στην περίπτωση που ο παρατηρητής εκτιμά όλο το πλήθος των καταστάσεων ονομάζεται παρατηρητής πλήρους τάξης (full order observer), ενώ αν εκτιμά κάποιες από τις καταστάσεις ονομάζεται παρατηρητής μειωμένης τάξης (reduced order observer) [75-78].

Απαραίτητη προϋπόθεση για να εκτιμηθούν οι καταστάσεις που δεν είναι διαθέσιμες, είναι το σύστημα να είναι παρατηρήσιμο (observable). Αν το σύστημα δεν είναι παρατηρήσιμο, τότε είναι αδύνατο να σχεδιαστεί πάνω του παρατηρητής. Ένα σύστημα καλείται πλήρως παρατηρήσιμο αν γνωρίζοντας τις τιμές των εξόδων y(t) και εισόδων u(t) για ένα πεπερασμένο χρονικά διάστημα t, $0 < t < \infty$, μπορούμε να ανακτήσουμε τις τιμές των μεταβλητών κατάστασης x(t) για οποιαδήποτε χρονική στιγμή του διαστήματος [0,t]. Αυτό σημαίνει ότι παρατηρώντας τις σχέσεις του συστήματος με το περιβάλλον (είσοδοι-έξοδοι) μπορούμε να υπολογίσουμε την εσωτερική συμπεριφορά του συστήματος

Ένα σύστημα είναι πλήρως παρατηρήσιμο αν και μόνο αν ο πίνακας παρατηρησιμότητας $\Theta = \begin{bmatrix} C \\ CA \\ CA^2 \\ \vdots \\ CA^{n-1} \end{bmatrix}$ είναι πλήρους βαθμού, δηλαδή βαθμός $[\Theta] = n$.

Εάν ο βαθμός του παραπάνω πίνακα είναι μικρότερος από n τότε το σύστημα δεν είναι παρατηρήσιμο και δεν παρατηρείται.

4.1.1. Είδη Παρατηρητών Κατάστασης

Στο κεφάλαιο αυτό παρουσιάζονται οι τύποι των παρατηρητών που χρησιμοποιούνται κατά κόρον στην εκτίμηση καταστάσεων, ικανότητα που είναι απαραίτητη στην ανίχνευση επιθέσεων, κομμάτι στο οποίο θα αναφερθούμε εκτενώς στη συνέχεια.

4.1.1.1. Παρατηρητής Ανοιχτού Βρόχου (Open Loop Observer)

Στον παρατηρητή «ανοικτού βρόχου» τα μετρούμενα δεδομένα εισόδου τροφοδοτούνται στο μαθηματικό μοντέλο, το οποίο παράγει τις δικές του εσωτερικές εκτιμήσεις κατάστασης. Ωστόσο, οι μετρήσεις εξόδου y(t) δεν χρησιμοποιούνται για τη διόρθωση του μοντέλου [75-78].

Έστω το σύστημα μας στο χώρο κατάστασης όπως έχουμε ήδη δει:

$$\dot{x} = A\,x(t) + B\,u(t)$$

$$y = Cx$$

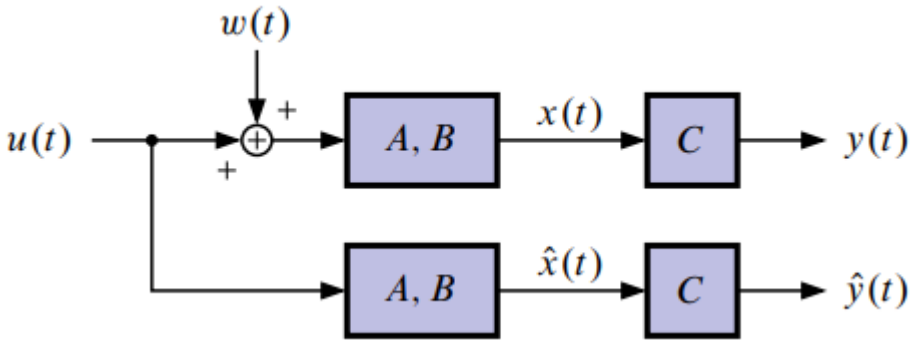
Η εκτίμηση κατάστασης ανοιχτού βρόχου θα είναι :

$$\dot{\hat{x}} = A\hat{x} + Bu$$

$$\hat{y} = C\hat{x} \tag{4.1}$$

Όπου : x : η πραγματική κατάσταση

$\hat{\mathrm{x}}$: η εκτίμηση κατάσασης



Σχήμα 4. 2 : Παρατηρητής Κατάστασης Ανοιχτού Βρόχου [78]

Εξετάζουμε το σφάλμα :

$$\tilde{\mathrm{x}} = \mathrm{x} - \hat{\mathrm{x}} \tag{4.2}$$

Θέλουμε : $\tilde{\mathrm{x}}(\mathrm{t}) = 0.$

Για τον εκτιμητή μας :

$$\dot{\tilde{x}}(t) = \dot{x}(t) - \dot{\hat{x}}(t) = A\,x(t) + B\,u(t) - A\,\hat{x}(t) - Bu(t) = A\,\tilde{x}(t) \quad (4.3)$$

Έτσι : $\tilde{x}(t) = e^{At}\tilde{x}(0)$ (4.4)

Η εξίσωση αυτή δείχνει ότι το σφάλμα εκτίμησης θα συγκλίνει στο μηδέν αν ο πίνακας A είναι ευσταθής. Το πρόβλημα είναι ότι αφενός ο A μπορεί να είναι ασταθής, αφετέρου η σύγκλιση να επιτυγχάνεται με ρυθμό που μπορεί να μην είναι επαρκής για το σύστημά μας. Και τα δύο αυτά προβλήματα λύνονται με τη χρήση ανατροφοδότησης και στον παρατηρητή μέσω ενός όρου διόρθωσης.

Ο παρατηρητής αυτός είναι γνωστός ως Παρατηρητής Luenberger.

4.1.1.2.Παρατηρητής Luenberger

Ο σχεδιασμός του παρατηρητή Luenberger βασίζεται στην εκχώρηση ιδιοτιμών (τοποθέτηση πόλων) και είναι γνωστός ως παρατηρητής Luenberger. Πήρε το όνομά του από τον David Gilbert Luenberger, καθηγητή στη Διοίκηση Επιστήμης και Μηχανικής στο Πανεπιστήμιο του Στάνφορντ, ο οποίος εισήγαγε για πρώτη φορά αυτές τις μεθόδους για την κατασκευή κρατικών παρατηρητών στη διδακτορική του διατριβή στο Caltech.

Έστω λοιπόν οι εξισώσεις κατάστασης του συστήματός μας που είδαμε και προηγουμένως :

$$\dot{x} = A\,x(t) + B\,u(t)$$

$$y = Cx$$

Το μαθηματικό μοντέλο του παρατηρητή Luenberger θα χρησιμοποιήσει ένα αντίγραφο του ενεργειακού συστήματος με την προσθήκη ενός όρου ανατροφοδότησης κέρδους L [75-77]:

$$\dot{\hat{x}} = A\hat{x} + Bu + L(y - \hat{y})$$

$$\hat{y} = C\hat{x} \quad (4.5)$$

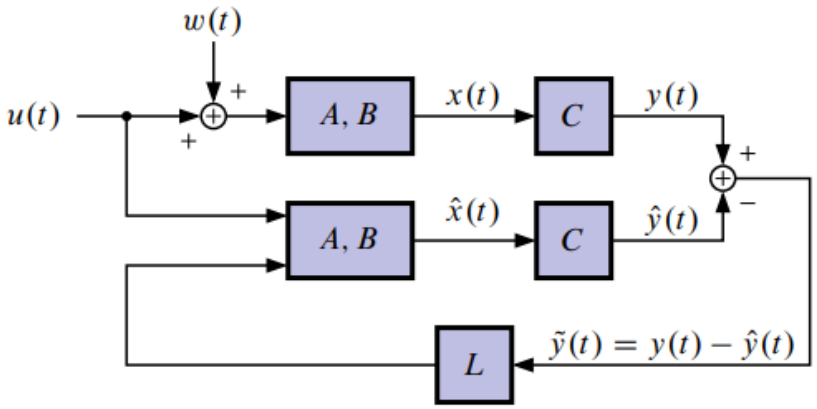
Ελέγχοντας το σφάλμα :

$$\dot{\tilde{\boldsymbol{x}}}(\boldsymbol{t}) = \dot{x}(t) - \dot{\hat{x}}(t) = A\,x(t) + B\,u(t) - A\,\hat{x}(t) - Bu(t) - L(y(t) - C\hat{x}(t))$$
$$= A\,\tilde{x}(t) - L(C\,x(t) - C\,\hat{x}(t)) = (\boldsymbol{A} - \boldsymbol{LC})\tilde{\boldsymbol{x}}(\boldsymbol{t}) \quad (4.6)$$

Έτσι : $\tilde{\boldsymbol{x}}(\boldsymbol{t}) = \boldsymbol{e}^{(\boldsymbol{A}-\boldsymbol{LC})\boldsymbol{t}}\tilde{\boldsymbol{x}}(\boldsymbol{0})$ (4.7)

Η δυναμική συμπεριφορά του διανύσματος σφάλματος λαμβάνεται από τις ιδιοτιμές του πίνακα (A-LC). Αν ο πίνακας αυτός είναι ευσταθής τότε το διάνυσμα σφάλματος θα συγκλίνει στο μηδέν για κάθε αρχική τιμή x(0). Έτσι $\hat{x}(t) \rightarrow$ x(t) ανεξάρτητα από το x(0) και $\hat{x}(0)$.

Έτσι $\tilde{x}(t) \to 0$ ή $\hat{x}(t) \to$ x(t) καθώς t $\to \infty$, όπου η ταχύτητα σύγκλισης χαρακτηρίζεται από τις ιδιοτιμές του (A − LC).



Σχήμα 4. 3 : Παρατηρητής Luenberger [85]

Το σύστημα είναι ασυμπτωτικά ευσταθές εάν επιλέξουμε το L έτσι ώστε οι ιδιοτιμές του (A − LC) να έχουν αρνητικά πραγματικά μέρη. Δηλαδή, μπορούμε να επιλέξουμε τις ιδιοτιμές με τέτοιο τρόπο ώστε η δυναμική συμπεριφορά του συστήματός μας να είναι ασυμπτωτικά ευσταθής και επαρκώς γρήγορη κι έτσι το διάνυσμα σφάλματος να τείνει στο μηδέν με ικανοποιητική ταχύτητα.

Αξίζει να σημειωθεί ότι [75-77]:

$$eig\{A - LC\} = eig\{(A - LC)^T\} = eig(A^T - C^T L^T), \tag{4.8}$$

οπότε μπορούμε να συμπεράνουμε ότι το πρόβλημα τοποθέτησης πόλων του παρατηρητή είναι παρόμοιο με το πρόβλημα τοποθέτησης πόλων του ελεγκτή.

$$eig\{A\text{-}BK\}$$

Αν αντικαταστήσουμε το A με το A^T, το B με το C^T, μπορούμε να χρησιμοποιήσουμε τις ίδιες μεθόδους για την τοποθέτηση πόλων που αναλύθηκαν στο πρόβλημα της ανατροφοδότησης. Έτσι μπορούμε να λάβουμε τον πίνακα L ως $L = K^T$.

Εάν το σύστημα είναι παρατηρήσιμο, τότε είναι δυνατόν να επιλέξουμε τον πίνακα L με τέτοιο τρόπο ώστε οι ιδιοτιμές του (A − LC) να μπορούν να τοποθετηθούν αυθαίρετα στο μιγαδικό επίπεδο.

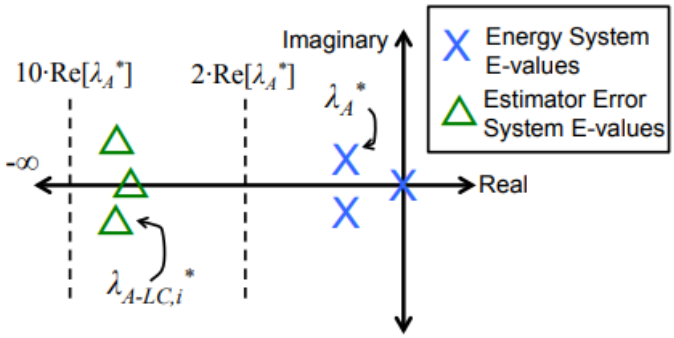
Ένας γενικός εμπειρικός κανόνας είναι ότι οι ιδιοτιμές του παρατηρητή πρέπει να τοποθετούνται 2-10 φορές πιο γρήγορα (πιο αριστερά) από την πιο αργή σταθερή ιδιοτιμή του ίδιου του ενεργειακού συστήματος.

Έστω λοιπόν $\lambda *_A$ η πιο αργή ιδιοτιμή του συστήματος, δηλαδή [77] :

$Re[\lambda *_A] = max_i\{Re[\lambda_{A,i}] \mid \lambda_{A,i} \in eig(A), Re[\lambda_{A,i}] < 0\}$. Εμπειρικά λοιπόν θα ισχύει:

$$-\infty < 10 \cdot Re[\lambda *_A] \leq Re[\lambda_{A-LC,i}] \leq 2 \cdot Re[\lambda *_A] < 0 \tag{4.9}$$

όπου $\lambda_{A\text{-}LC,i}$ είναι οι ιδιοτιμές του A-LC. Αυτός ο εμπειρικός κανόνας επιτυγχάνει γρήγορη σύγκλιση των εκτιμήσεων κατάστασης, χωρίς να είναι υπερευαίσθητος στον θόρυβο της μέτρησης.



Σχήμα 4. 4 : Απεικόνιση Πόλων Ενεργειακού Συστήματος και Παρατηρητή Κατάστασης στο μιγαδικό επίπεδο

Η τοποθέτηση των ιδιοτιμών του εκτιμητή πιο κοντά στο αρνητικό άπειρο αυξάνει την ευαισθησία στο θόρυβο της μέτρησης. Αυτός είναι και ο λόγος για τον οποίο δεν επιλέγουμε τόσο αρνητικό πραγματικό μέρος στις ιδιοτιμές. Σχεδιάζουμε επομένως τον L έτσι ώστε να εξισορροπείται η ταχύτητα σύγκλισης και η αντοχή των αισθητήρων του παρατηρητή έναντι του θορύβου

Η ιδανική ισορροπία ανάμεσα στην ευαισθησία στα δεδομένα μέτρησης και στην αβεβαιότητα του μοντέλου επιτυγχάνει με τη χρήση ενός φίλτρο ονόματι Kalman [75].

4.1.1.3.Φίλτρο Kalman

Το φίλτρο Kalman (KF), γνωστό και ως γραμμικός τετραγωνικός εκτιμητής, είναι μια από τις πιο σημαντικές εξελίξεις στα συστήματα και την τεχνολογία ελέγχου. Το KF έχει πολυάριθμες εφαρμογές, ειδικά στα ενεργειακά συστήματα. Πήρε το όνομά του από τον Rudolf E. Kalman, έναν Ούγγρο-Αμερικανό μηχανικό και μαθηματικό επιστήμονα. Το KF εξισορροπεί βέλτιστα την εμπιστοσύνη στο μοντέλο μας και την εμπιστοσύνη στα δεδομένα μας για τη δημιουργία εκτιμήσεων κατάστασης.

Όταν υπάρχουν διαταραχές ή/και θόρυβοι μέτρησης στο σύστημα, το φίλτρο Kalman θεωρείται ως εναλλακτικός παρατηρητής. Αυτός ο τύπος φίλτρου χρησιμοποιεί τη γνώση των στατιστικών ιδιοτήτων του συστήματος στο σχεδιασμό του. Είναι μια βέλτιστη εκτίμηση με την έννοια ότι η μέση τιμή του αθροίσματος των σφαλμάτων εκτίμησης παίρνει μια ελάχιστη τιμή [80-83]

Ο θόρυβος παίζει σημαίνοντα ρόλο στην χρήση των φίλτρων Kalman. Το σύστημα στο χώρο κατάστασης με την προσθήκη θορύβου είναι το εξής [32], [75]:

$$\dot{x}(t) = A\,x(t) + B\,u(t) + w(t),\ x(0) = x_0,\ x, w \in \mathbb{R}^n, u \in \mathbb{R}^p \qquad (4.10)$$

$$\mathrm{y(t)} = \mathrm{Cx(t)} + \mathrm{Du(t)} + \mathrm{n(t)},\quad \mathrm{y_m}, \mathrm{n} \in \mathbb{R}^{\mathrm{q}} \qquad (4.11)$$

όπου w(t) και n(t) οι «θόρυβοι» του συστήματος που στην ουσία αντιπροσωπεύουν τις διάφορες ανακρίβειες του συστήματος.

Στα πλαίσια της διπλωματικής μας, θεωρούμε το μοντέλο μας απελευθερωμένο από θορύβους ή διαταραχές μέτρησης και γι' αυτό χρησιμοποιούμε παρατηρητή Luenberger όπως θα αναλύσουμε στην συνέχεια με σκοπό να μας βοηθήσει στην ανίχνευση των επιθέσεων. Για μη γραμμικά συστήματα ή προχωρημένου επιπέδου και τεχνολογίας συστήματα είναι συχνή η χρήση των παρακάτω παρατηρητών.

4.1.1.4.Unknown Input Observer

Στο σημείο αυτό εισάγουμε την έννοια του παρατηρητή άγνωστης εισόδου (Unknown Input Observer). Ο παρατηρητής αυτός είναι σημαντικός για την αντιμετώπιση της αυξημένης αβεβαιότητας που αντιμετωπίζει η υψηλή διείσδυση των ανανεώσιμων πηγών ενέργειας αλλά και σε περιπτώσεις διαχείρισης κυβερνοεπιθέσεων μέσω της χρήσης τους στην ανίχνευση αυτών [79].

Ένας παρατηρητής άγνωστης εισόδου (UIO) είναι ένα δυναμικό σύστημα που εκτιμά την άγνωστη κατάσταση (ή ένα μέρος) ενός δεδομένου συστήματος, ανεξάρτητα από τις άγνωστες εισόδους. Το πρόβλημα της UIO έχει ξεκινήσει από τους Basile και Marro (1969) [91] και Guidorzi και Marro (1971) [85]. Έκτοτε, έχουν προταθεί αρκετές συνεισφορές για το σχεδιασμό UIO μειωμένης και πλήρους τάξης: η γεωμετρική προσέγγιση από τον Bhattacharyya (1978) [86]. Η έννοια της ισχυρής ανιχνευσιμότητας και η χρήση της στην κατασκευή UIO εισήχθη από τον Hautus (1983) [87]. Ο αλγόριθμος αντιστροφής και οι αλγεβρικές προσεγγίσεις, από Darouach, Zasadzinski και Xu (1994) [88] και Hou and Muller (1992) [89].

Οι παρατηρητές για συστήματα με άγνωστες εισόδους διαδραματίζουν ουσιαστικό ρόλο στην ανίχνευση σφαλμάτων. Ξεκινώντας από τους Watanabe και Himmelblau (1982) [90], αυτό το πρόβλημα έχει επεκταθεί στην ανίχνευση σφαλμάτων τόσο των αισθητήρων (sensors) όσο και των ενεργοποιητών (actuators) από τους Patton και Chen (1993) [91] και Wunnenberg και Frank (1982) [92]. Ο γραμμικός παρατηρητής που βασίζεται στην ανίχνευση και την απομόνωση σφαλμάτων συνίσταται στο σχεδιασμό ενός παρατηρητή, που ονομάζεται υπολειπόμενο φίλτρο, δημιουργώντας μια έξοδο που γίνεται ευαίσθητη σε ορισμένα σφάλματα και πιθανώς μη ευαίσθητη σε ένα άλλο (FDI).

Σε ένα σύστημα ρύθμισης φορτίου – συχνότητας, που συχνά υπάρχουν διαταραχές και αβεβαιότητες, έχουμε θεωρητικά άγνωστες – ή στοχαστικές – μεταβλητές εισόδου. Έτσι λόγω των άγνωστων εισόδων, ο σχεδιασμός των παραδοσιακών παρατηρητών κατάστασης Luenberger παρουσιάζει αρκετές δυσκολίες. Ως εκ τούτου, στα σύγχρονα συστήματα έχει σχεδιαστεί ένας ειδικός παρατηρητής καταστάσεων, που ονομάζεται παρατηρητής άγνωστης εισόδου (UIO) για να παρακολουθεί τις δυναμικές καταστάσεις των διασυνδεδεμένων συστημάτων ισχύος λαμβάνοντας υπόψη τις άγνωστες εισόδους και τις αβεβαιότητές τους [93-95], [79].

Για το σύστημα [96-97]:

$$\dot{x} = A\,x(t) + B\,u(t) + E\,d(t)$$

$$y = Cx$$

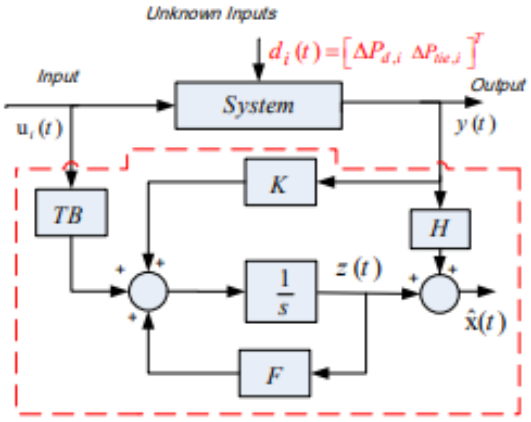
η δομή του δυναμικού συστήματος που παρουσιάζεται παρακάτω είναι ένας παρατηρητής εάν και μόνο εάν το σφάλμα εκτίμησης κατάστασής του $\dot{\boldsymbol{e}}(\boldsymbol{t}) = \dot{x}(t) - \dot{\hat{x}}(t)$ τείνει ασυμπτωτικά στο μηδέν, ανεξάρτητα από το διάνυσμα άγνωστης εισόδου d (t).

$$\dot{z} = Fz(t) + T\,B\,u(t) + K\,y(t)$$

$$\hat{\dot{x}}(t) = z(t) + H\,y(t)$$

(4.12)

Όπου : $\hat{\dot{x}}(t)$ η εκτιμητέα μεταβλητή κατάστασης του αρχικού συστήματος, $\hat{\dot{x}}(t)$ το διάνυσμα σφάλματος της εκτίμησης, z η μεταβλητή κατάσταση του συστήματος άγνωστης εισόδου και F, T, H και K πίνακες κατάλληλου μεγέθους ώστε να επιτυγχάνεται διαχωρισμός των άγνωστων εισόδων.



Σχήμα 4. 5 : Μοντέλο Παρατηρητή Άγνωστης Εισόδου (UIO) [86]

Το πλεονέκτημα που προκύπτει από το παραπάνω διάγραμμα βαθμίδων είναι ο διαχωρισμός της εκτίμησης των δυναμικών μεταβλητών κατάστασης από τις διαταραχές στο κύριο σύστημα.

Επεκτείνοντας το σφάλμα εκτίμησης δυναμικής κατάστασης $\dot{e}(t) = \dot{x}(t) - \hat{\dot{x}}(t)$λαμβάνουμε τα εξής :

$$\dot{e}(t) = (A - HCA - K_1C)\,e(t) + [F - (A - HCA - K_1C]\,z(t) + [K_2 - HCA - K_1C]\,y(t) + [T - (I - HC)]\,B\,u(t) + (HC - I)\,E\,d(t)$$

(4.13)

Το UIO υπάρχει, εάν και μόνο εάν, το σφάλμα εκτίμησης κατάστασης συγκλίνει στο μηδέν ασυμπτωτικά, ανεξάρτητα από το άγνωστο διάνυσμα εισόδου d. Για να

εκφραστεί η δυναμική του σφάλματος εκτίμησης κατάστασης $\dot{e}$ ως συνάρτηση του e, θα πρέπει να ισχύουν οι συνθήκες που δίνονται παρακάτω [96-97]:

$$(\mathrm{HC}-\mathrm{I})\mathrm{E}=0$$
$$\mathrm{T}=\mathrm{I}-\mathrm{HC}$$
$$\mathrm{F}=\mathrm{A}_2-\mathrm{K}_1\,\mathrm{C}$$
$$\mathrm{K}_2=\mathrm{FH}$$
$$\mathrm{K}=\mathrm{K}_1+\mathrm{K}_2$$
$$\mathrm{A}_2=\mathrm{A}-\mathrm{HCA}$$

(4.14)

Από τις παραπάνω σχέσεις, είναι προφανές ότι η εκτίμηση κατάστασης είναι αποσυνδεδεμένη από το άγνωστο διάνυσμα εισόδου d.

Η εξίσωση $\dot{e}(t) = F\,e(t)$ δείχνει ότι το σφάλμα εκτίμησης κατάστασης e, πλησιάζει ασυμπτωτικά το μηδέν, εάν ο πίνακας F είναι σταθερός. Κατά συνέπεια, ο πίνακας K_1 θα πρέπει να εκχωρηθεί έτσι ώστε ο πίνακας F να είναι Hurwitz που αποδεικνύει τη σταθερότητα UIO [98]. Αποδεικνύεται στα [99], [100] ότι οι επαρκείς και απαραίτητες συνθήκες ώστε το δυναμικό σύστημα που δίνεται στην (4.12) να είναι σύστημα UIO για την περιοχή του συστήματος ισχύος :

i) rank(CE) = rank€
ii) Το ζεύγος (C,A_1) να είναι ανιχνεύσιμο,

Όπου : $A_1 = A - E[(CE)^T CE]^{-1}(CE)^T CA$ (4.15)

Οι αποδείξεις αυτών των επαρκών και απαραίτητων συνθηκών του UIO που βασίζονται σε ορισμένα θεωρήματα γραμμικής άλγεβρας, αναλύονται στο [99-101]. Ως περαιτέρω αποτέλεσμα και επέκταση του UIO, οι διαταραχές που μοντελοποιούνται ως άγνωστες εισροές, μπορούν να εκτιμηθούν. Ας πάρουμε την παράγωγο της εκτιμώμενης παραγωγής, ως εξής

$$\dot{\hat{y}}(t) = C\,\dot{\hat{x}}(t) \quad (4.16)$$

Ξαναγράφοντας στις σχέσεις του συστήματος βασιζόμενοι στις εκτιμήσεις και αντικαθιστώντας το $\dot{\hat{x}}(t)$ στην παραπάνω σχέση, έχουμε :

$$\dot{y}(t) = C[A\,\hat{x}(t) + B\,u(t) + E\,d(t)$$
$$\hat{d} = (CE)^{+}[\dot{\hat{y}} - CA\,\hat{x} - CB\,u]$$

(4.17)

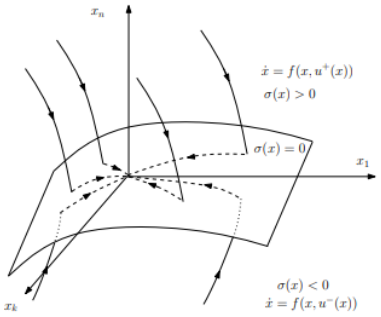
4.1.1.5. Sliding Mode Observer

Ο παρατηρητής λειτουργίας ολίσθησης χρησιμοποιεί μη γραμμική ανάδραση υψηλού κέρδους για να οδηγήσει τις εκτιμώμενες καταστάσεις σε μια υπερεπιφάνεια όπου δεν υπάρχει διαφορά μεταξύ της εκτιμώμενης εξόδου και της μετρούμενης εξόδου. Το μη γραμμικό κέρδος που χρησιμοποιείται στον παρατηρητή υλοποιείται συνήθως με μια

κλιμακούμενη συνάρτηση, όπως αυτή του προσήμου (sgn) του εκτιμώμενου – μετρούμενου σφάλματος εξόδου.

Οι παρατηρητές λειτουργίας ολίσθησης (Sliding Mode Observers) έχουν μοναδικές ιδιότητες, όπως η ικανότητα δημιουργίας μιας ολισθαίνουσας κίνησης στο σφάλμα μεταξύ της μετρούμενης εξόδου του συστήματος και της εξόδου του παρατηρητή που διασφαλίζει ότι ο παρατηρητής παράγει ένα σύνολο εκτιμήσεων κατάστασης που είναι ακριβώς ανάλογες με την πραγματική έξοδο του συστήματος [102]. Τα σφάλματα εξόδου ανατροφοδοτούνται τόσο με γραμμικό όσο και με ασυνεχές τρόπο για μη γραμμικά συστήματα με στόχο να διασφαλιστεί ότι το λεγόμενο «sliding patch» (το οποίο καθορίζει την περιοχή στην οποία είναι δυνατό το σύστημα δυναμικού παρατηρητή να εμφανίζει συμπεριφορά ολίσθησης) μεγιστοποιείται.

Η ανάλυση της μέσης τιμής του σήματος του παρατηρητή, το λεγόμενο ισοδύναμο σήμα έγχυσης, προσφέρει χρήσιμες πληροφορίες σχετικά με την απόκλιση του μοντέλου που χρησιμοποιείται για να ορίσουμε τον παρατηρητή του πραγματικού μοντέλου μας.



Σχήμα 4. 6 : Παρουσίαση Sliding Mode Observer

Επιπλέον, είναι διαισθητικά προφανές ότι από τη στιγμή που είναι γνωστό μόνο ένα υποσύνολο πληροφοριών κατάστασης (οι έξοδοι του συστήματος), η ικανότητα οποιουδήποτε συστήματος να επιτύχει και να διατηρήσει την ολίσθηση θα είναι πιο περιορισμένη απ' ότι στην περίπτωση που είναι διαθέσιμες πληροφορίες όλων των καταστάσεων.

Για το σύστημα [103] :

$$\dot{x} = A\,x(t) + B\,u(t)$$

$$y = Cx$$

ο παρατηρητής λειτουργίας ολίσθησης είναι :

$$\hat{x}(t) = A\,\hat{x}(t) + B\,u(t) + L\,\tilde{y}(t) + M\,\mathrm{sign}(\tilde{y}(t))$$

$$\hat{y}(t) = C\hat{x}(t)$$

(4.18)

Όπου : $\dot{\hat{x}}(t)$ η εκτιμητέα μεταβλητή κατάστασης του αρχικού συστήματος, $\hat{y}$ το εκτιμητέο διάνυσμα εξόδου, L ο πίνακας κέρδους του παρατηρητή, M η μήτρα πλάτους, $\tilde{y}$ το ολισθένον διάνυσμα επιφάνειας, όπου $\tilde{y} = y(t) - \hat{y}(t)$ και sign(.) το διάνυσμα συνάρτησης sign ορισμένης ως [103] :

$$\text{sign}\,(\tilde{y}(t)) = \begin{bmatrix} \text{sign}\,(\widetilde{y_1}(t) \\ \text{sign}(\widetilde{y_2}(t) \\ \vdots \\ \text{sign}(\widetilde{y_p}(t) \end{bmatrix} \tag{4.19}$$

με $\text{sign}\,(\tilde{y}_i(t)) = f(x) = \begin{cases} +1, & \tilde{y}_i(t) > 0 \\ -1, & \tilde{y}_i(t) < 0 \end{cases}$

Το σφάλμα ορίζεται ως εξής:

$$\tilde{x}(t) = x\,(t) - \hat{x}\,(t)$$

Αντικαθιστώντας τα x, $\hat{x}$ από τις αντίστοιχες σχέσεις τους :

$$\dot{\hat{x}}(t) = (A - LH)\tilde{x}(t) - M\text{sign}(\tilde{y}(t)) \tag{4.20}$$

4.2.Ανίχνευση Κυβερνοεπιθέσεων

Ως βασικό κομμάτι του συστήματος ισχύος, το LFC πρέπει να χρησιμοποιεί τεράστιες ποσότητες μετρούμενων δεδομένων για να διατηρεί τη σταθερότητα της συχνότητας του συστήματος. Οι εξελιγμένοι τεχνολογικά εισβολείς μπορούν να παρέμβουν στα μετρούμενα δεδομένα εξαπολύοντας κυβερνοεπιθέσεις και να αναγκάσουν τον ρυθμιστή φορτίου - συχνότητας να δώσει λανθασμένες οδηγίες, γεγονός που μπορεί να οδηγήσει σε απρόβλεπτη διακύμανση συχνότητας, όπως έχουμε αναλύσει σε προηγούμενες ενότητες. Ως εκ τούτου, για την αντιμετώπιση αυτών των συνεπειών έχουν χρησιμοποιηθεί κυρίως δύο μέθοδοι σύμφωνα με τη βιβλιογραφία :

(i) η βασισμένη στην **ανίχνευση** άμυνα και

(ii) η άμυνα βασισμένη στην **προστασία**

Πρακτικά, λόγω κόστους, δεν είναι δυνατή η προστασία όλων των μετρητών/αισθητήρων σε ένα ηλεκτρικό δίκτυο και μόνο ένα επιλεγμένο σημαντικό σύνολο μπορεί να προστατεύεται ώστε να υπάρχει ισορροπία μεταξύ της ανάγκης για προστασία και του κόστους [104]. Από την άλλη, οι μέθοδοι που βασίζονται στην ανίχνευση αναλύουν τα δεδομένα του μετρητή [105-106] για τον εντοπισμό επιθέσεων FDI και δεν έχουν το κόστος τα προηγούμενης κατηγορίας. Αυτή είναι και η κατηγορία που μελετάμε.

Οι επιθέσεις FDI μπορούν εύκολα να αλλοιώσουν τις κανονικές ενέργειες ενός κέντρου ελέγχου, θέτοντας σε κίνδυνο τα δεδομένα των ευαίσθητων μεταβλητών. Ως εκ τούτου,

για τον εντοπισμό επιθέσεων FDI και για τη διασφάλιση της λειτουργικής αξιοπιστίας των συστημάτων ισχύος, η παρακολούθηση του συστήματος μέσω μετρητών και τεχνικών εκτίμησης κατάστασης είναι ευρέως διαδεδομένη [107].

4.2.1. Μέθοδοι Ανίχνευσης Κυβερνοεπιθέσεων τύπου FDI στο LFC

Τα συστήματα ανίχνευσης που χρησιμοποιούνται σε συστήματα LFC περιλαμβάνουν **αλγόριθμους** που ελέγχουν εάν οι μετρήσεις που λαμβάνονται για τις παραμέτρους του συστήματος ισχύος βρίσκονται εντός αποδεκτών ορίων [108]. Όταν αυτές αποκλίνουν σημαντικά από τις προβλεπόμενες, ενεργοποιούνται συναγερμοί, καθώς το δίκτυο σε συνδυασμό με το σύστημα ελέγχου AGC θεωρεί ότι δέχεται επίθεση [109]. Ένας καλός αλγόριθμος ανίχνευσης θα πρέπει να είναι ικανός να παρέχει πληροφορίες σχετικά με την τοποθεσία, το μέγεθος και τον χρόνο της επίθεσης σε πραγματικό χρόνο [110].

Οι μηχανισμοί ανίχνευσης στο δικτυακό σύστημα ελέγχου ονομάζονται γενικά ανιχνευτές ανωμαλιών (**anomaly detectors**) και συνυπάρχουν με τους ελεγκτές [108]. Οι ανιχνευτές ανωμαλιών εντοπίζουν μη ομαλές μετρήσεις του συστήματος, όπως η εμφάνιση κάποιας ανεπιθύμητης κατάστασης στο σύστημα [111], μία κυβερνοεπίθεση [112] ή συνδυασμός και των δύο, συγκρίνοντας την μη ομαλή συμπεριφορά με την επιθυμητή συμπεριφορά του συστήματος. Η ανίχνευση της επίθεσης καθορίζεται αρχικά με την ανάλυση της διαφοράς που υπάρχει ανάμεσα στα κανονικά και τα αλλοιωμένα σήματα. Η μέθοδος που αναπτύχθηκε στο [113] προβλέπει το φορτίο και στη συνέχεια, κατά τη λειτουργία σε πραγματικό χρόνο, οι προβλεπόμενες τιμές χρησιμοποιούνται για την λειτουργία του συστήματος AGC και τον εντοπισμό FDI επιθέσεων. Ωστόσο, λόγω της μη διαθεσιμότητας των τιμών των φορτίων σε πραγματικό χρόνο στο σύστημα, και οι δύο προαναφερθείσες μέθοδοι χρησιμοποιούν τις εκτιμώμενες ή προβλεπόμενες αλλαγές φορτίου στο σύστημα - οι οποίες μπορεί να μην είναι απόλυτα ακριβείς.

Στην τρέχουσα βιβλιογραφία, ο σχεδιασμός **παρατηρητών** και η χρήση **αλγορίθμων μηχανικής μάθησης** είναι δύο σημαντικές μέθοδοι για την εξαγωγή των δυναμικών χαρακτηριστικών των μεταβλητών [114-116]. Στο [117], η διαταραχή της ενεργού ισχύος παρακολουθείται χρησιμοποιώντας μια λειτουργία ολίσθησης δεύτερης τάξης σε ένα σύστημα LFC. Στο [118], τα σήματα σφάλματος στο σύστημα LFC παρατηρούνται χρησιμοποιώντας τον παρατηρητή λειτουργίας ολισθαίνουσας.

Μια προσέγγιση ανίχνευσης βασισμένη σε νευρωνικό δίκτυο για επιθέσεις FDI στον βρόχο ανίχνευσης του συστήματος διανομής δύο περιοχών παρουσιάζεται στο [119]. Κατά τη μέθοδο αυτή χρησιμοποιείται και ένας παρατηρητής Luenberger. Οι μετρούμενες είσοδοι και έξοδοι ελέγχου αποστέλλονται στον παρατηρητή Luenberger για την εκτίμηση της κατάστασης. Η μονάδα ανίχνευσης νευρωνικού δικτύου λαμβάνει αυτές τις εκτιμήσεις για τον εντοπισμό και την παρακολούθηση επιθέσεων FDI. Η ικανότητα του νευρωνικού δικτύου να εκτιμά τη μη γραμμική συμπεριφορά του συστήματος προσθέτει επίσης πλεονεκτήματα σε αυτή τη μέθοδο.

Μια μέθοδος βασισμένη στο επαναλαμβανόμενο νευρωνικό δίκτυο (**RNN**) προτείνεται για την ανίχνευση επίθεσης FDI στο σύστημα AGC με μη γραμμικότητες όπως η νεκρή ζώνη του ρυθμιστή στροφών στο [120]. Μια άλλη τεχνική ανίχνευσης που βασίζεται στη βαθιά μάθηση (**Deep Learning**) προτείνεται στο [121]. Η μέθοδος βαθιάς μάθησης χρησιμοποιεί ιστορικά δεδομένα μετρήσεων συχνότητας και ροής ισχύος για την εκμάθηση των μοτίβων δεδομένων και την πρόβλεψη των τιμών ACE μέσω των διαβασμένων προτύπων.

Όσον αφορά τη χρήση παρατηρητών, ένας **παρατηρητής Luenberger** υιοθετήθηκε επίσης [122] και [123] για την παρακολούθηση του συστήματος ισχύος και του μικροδικτύου, αντίστοιχα. Στο [124], σχεδιάστηκε ένας προσαρμοστικός παρατηρητής λειτουργίας ολίσθησης (**Sliding Mode Observer**) για την ανίχνευση κυβερνοεπίθεσης σε συστήματα ισχύος. Επιπλέον, το **φίλτρο Kalman** αποδεικνύεται ότι είναι αποτελεσματικό στην ανίχνευση διαφόρων επιθέσεων, συμπεριλαμβανομένων βραχυπρόθεσμων και μακροπρόθεσμων τυχαίων επιθέσεων [125]. Τέλος, μεθοδολογίες βασισμένες σε παρατηρητές για βέλτιστη λειτουργία LFC υπό κυβερνοεπίθεση εισάγονται ακόμη στο [126].

Αξίζει τέλος να κάνουμε μια αναφορά σε μερικές μεθόδους που βασίζονται σε στατιστικές αναλύσεις. Είναι αρχικά οι μέθοδοι που βασίζονται σε υδατογράφηση (**Watermarking-based defense techniques**) [127-128] είναι εξαιρετικά δημοφιλή σχήματα που στην πραγματικότητα ορίζουν την αναγνώριση της επίθεσης αντιστοιχίζοντας τις μετρήσεις του τεχνητά εγχυόμενου θορύβου του αισθητήρα που βασίζεται σε πιθανότητες με τις αλλοιωμένες μετρήσεις. Η μέθοδος που χρησιμοποιεί **μηχανές διανυσματικής υποστήριξης** μπορούν να ανιχνεύσουν μία κλιμακούμενη επίθεση (Scaling attack) και μία επίθεση άγνωστης διαταραχής [129], ενώ τέλος μέσω μιας προσέγγισης της **θεωρίας συνόλων** για την ανίχνευση ψευδών δεδομένων μπορεί να χρησιμοποιηθεί για την παρατήρηση ενός επιτιθέμενου [130].

Οι υπάρχουσες μέθοδοι για τον εντοπισμό επιθέσεων FDI σε συστήματα LFC έχουν τα ακόλουθα ελαττώματα [131]:

1. Οι τρέχουσες μέθοδοι που βασίζονται σε δεδομένα δεν επαρκούν για τον εντοπισμό επιθέσεων σε συγκεκριμένες συνθήκες. Οι εισβολείς μπορούν να εισάγουν ψευδή δεδομένα με βάση τα δεδομένα ιστορικού στο σύστημα LFC. Για παράδειγμα, σε μια συνθήκη λειτουργίας, οι εισβολείς μπορούν να χρησιμοποιήσουν ιστορικά δεδομένα για να δημιουργήσουν σήματα επίθεσης που ικανοποιούν τα χαρακτηριστικά των μεταβλητών σε άλλες συνθήκες.

2. Λόγω της καθυστέρησης επικοινωνίας και του θορύβου, υπάρχει διαφορά μεταξύ των παρατηρούμενων δεδομένων και των αληθινών δεδομένων. Οι αμυνόμενοι συχνά δεν μπορούν να ορίσουν το εύλογο όριο της διαφοράς. Η ακατάλληλη ρύθμιση του ορίου θα οδηγήσει σε λανθασμένη εκτίμηση.

4.3. Μοντέλο Ανίχνευσης Επιθέσεων Έγχυσης Ψευδών Δεδομένων μέσω Παρατηρητή Luenberger

Στα πλαίσια της παρούσας διπλωματικής, για την διαδικασία της ανίχνευσης κυβερνοεπιθέσεων και συγκεκριμένα επιθέσεων έγχυσης ψευδών δεδομένων (FDIAs) σε συγκεκριμένα σημεία του συστήματος ρύθμισης φορτίου – συχνότητας των συστημάτων ισχύος μιας ή δύο περιοχών, χρησιμοποιήθηκε ο παρατηρητής Luenberger, που αναλύθηκε προηγουμένως. Ο συγκεκριμένος παρατηρητής είναι εύκολος στην υλοποίησή του, οικονομικός και μπορεί να παρέχει τις πληροφορίες που χρειαζόμαστε σχετικά με την ανίχνευση των επιθέσεων με τη μέθοδό μας, την οποία θα αναλύσουμε στο κεφάλαιο των προσομοιώσεων.

Οι εξισώσεις που περιγράφουν το σύστημά μας στο χώρο κατάστασης, παρουσία πιθανών επιθέσεων και διαταραχών όπως οι μεταβολές φορτίων σύμφωνα με την (3.1), είναι οι εξής:

$$\dot{\mathrm{x}}(\mathrm{t}) = \mathrm{A}\,\mathrm{x}(\mathrm{t}) + \mathrm{B}\,\mathrm{u}(\mathrm{t}) + \mathrm{E}\,\mathrm{d}(\mathrm{t}) + \mathrm{F}\,f_{FDI}(\mathrm{t})$$

$$y(t) = Cx$$

Το μοντέλο του παρατηρητή Luenberger για τις παραπάνω εξισώσεις που περιγράφουν το σύστημά μας είναι το παρακάτω:

$$\dot{\hat{x}}(t) = A\hat{x}(t) + Bu(t) + F\,\hat{f}_{FDI}(t) + L(y(t) - \hat{y}(t))$$

$$\hat{y}(t) = C\hat{x}(t) \tag{4.23}$$

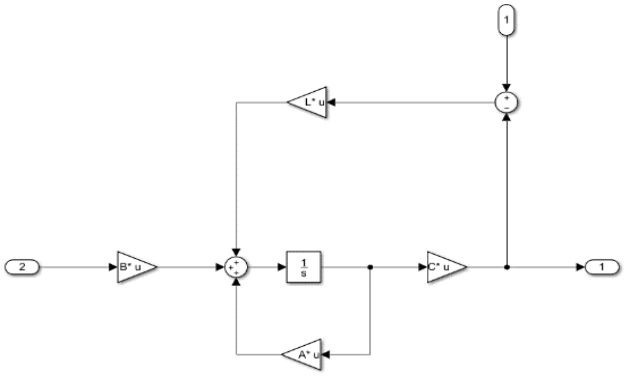
όπου $\hat{x}(t)$ και $\hat{f}_{FDI}$ είναι τα διανύσματα εκτίμησης κατάστασης και επίθεσης και L ο πίνακας κέρδους του παρατηρητή.

Το σφάλμα εκτίμησης κατάστασης $e_x(t)$ και το σφάλμα εκτίμησης εξόδου $e_y(t)$ είναι :

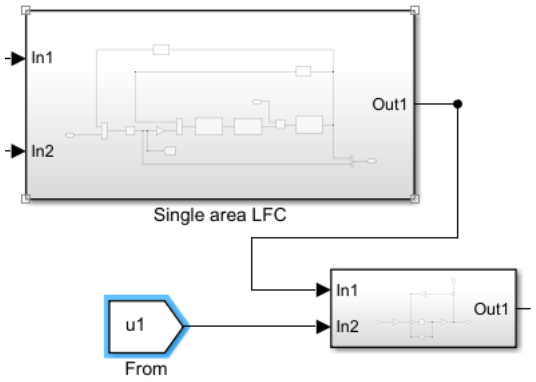
$$\mathrm{e}_x(\mathrm{t}) = \mathrm{x}(\mathrm{t}) - \hat{x}(t)$$

$$e_y(t) = y(t) - \hat{y}(t) \tag{4.24}$$

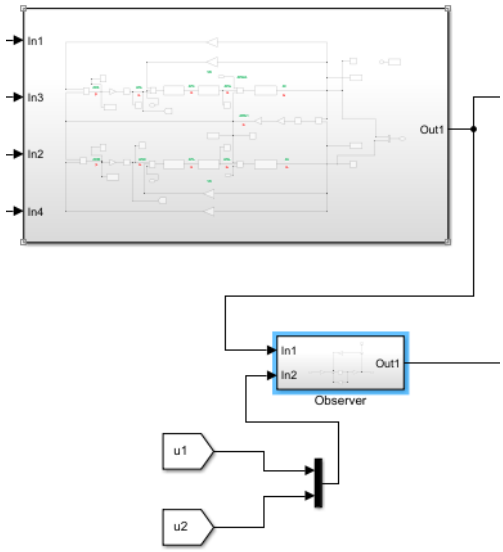
Τα συστήματα ρύθμισης φορτίου συχνότητας, ο παρατηρητής Luenberger, και ο συνδυασμός τους, που θα χρησιμοποιήσουμε στις προσομοιώσεις με σκοπό την ανίχνευση κυβερνοεπιθέσεων (θα αναλύσουμε περισσότερα για τη μέθοδο αυτή στο κεφάλαιο των προσομοιώσεων) παρουσιάζεται στα Σχήματα 4.6 – 4.8. Η επιλογή του πίνακα L γίνεται μέσω της μεθόδου τοποθέτησης πόλων και όσα αναφέρθηκαν στο κεφάλαιο 4.1.1.2. για τον παρατηρητή Luenberger (οι ιδιοτιμές του πίνακα A-LC βρίσκονται στο αριστερό μιγαδικό επίπεδο και το σύστημα είναι ευσταθές). Με αυτόν τον τρόπο το σφάλμα εκτίμησης του παρατηρητή είναι ασυμπτωτικά ευσταθές και θα συγκλίνει στο μηδέν σε βάθος χρόνου, πράγμα που μας επιτρέπει να χρησιμοποιήσουμε το σφάλμα αυτό ως μέσο ανίχνευσης για καταστάσεις στις οποίες το σύστημα δέχεται επιθέσεις (και δεν συγκλίνει στο μηδέν).



Σχήμα 4. 7 : Παρατηρητής Luenberger στο μοντέλο των προσομοιώσεων



Σχήμα 4. 8 : Σύστημα Ρύθμισης Φορτίου – Συχνότητας Απομονωμένης Περιοχής μαζί με Παρατηρητή Luenberger



Σχήμα 4. 9 : Σύστημα Ρύθμισης Φορτίου – Συχνότητας Δύο Περιοχών μαζί με Παρατηρητή Luenberger

5. Προσομοιώσεις λειτουργίας LFC σε μεταβολές φορτίου και επιθέσεις Έγχυσης Ψευδών Δεδομένων - Ανίχνευσης επιθέσεων μέσω Παρατηρητή Luenberger

Βασιζόμενοι στα μοντέλα ρύθμισης φορτίου συχνότητας για μία και δύο περιοχές που αναφέραμε στα προηγούμενα κεφάλαια, στο κεφάλαιο αυτό θα προχωρήσουμε σε προσομοιώσεις που αφορούν τόσο απλές διαταραχές φορτίου, όσο και περιπτώσεις επιθέσεων και θα εξετάσουμε την απόκριση των συστημάτων μας.

Στα πλαίσια της παρούσας διπλωματικής κατασκευάστηκε μοντέλο ρύθμισης φορτίου - συχνότητας (τόσο για μία όσο και για δύο περιοχές), σύμφωνα με όσα αναφέραμε σε προηγούμενες ενότητες, ενώ έγινε και χρήση παρατηρητή κατάστασης Luenberger με σκοπό τη μελέτη ανίχνευσης των επιθέσεων. Με την προσθήκη του παρατηρητή/εκτιμητή θα προβούμε σε πειράματα επιθέσεων στο σύστημά μας και θα εξετάσουμε τις δυνατότητες που μας δίνει ο συγκεκριμένος παρατηρητής προκειμένου να αναγνωριστούν οι επιθέσεις και να χρησιμοποιηθούν ως μέσο καταπολέμησής τους.

5.1. Προσομοιώσεις μελέτης Ρύθμισης Φορτίου – Συχνότητας υπό την επίδραση μεταβολών φορτίου

Στο παρόν κεφάλαιο εξετάζεται η απόκριση των συστημάτων τόσο της μιας όσο και των δύο περιοχών έπειτα από διαταραχές φορτίου (απότομη αύξηση/μείωση). Πιο συγκεκριμένα μελετάται αρχικά ο πρωτεύοντας έλεγχος του συστήματος μιας περιοχής και το μόνιμο σφάλμα που αυτός αφήνει στη συχνότητά της. Στη συνέχεια μελετάται πρώτα στη μία και μετά στις δύο περιοχές ο δευτερεύοντας έλεγχος. Πιο συγκεκριμένα, έπειτα από μία απότομη αύξηση/μείωση φορτίου -μέσω μιας συνάρτησης step, ελέγχεται εάν καταπολεμάται το μόνιμο σφάλμα που αφήνει ο πρωτεύοντας έλεγχος στη συχνότητα, πόσο απότομη είναι η μεταβολή αυτή και πόσο γρήγορα επιτυγχάνεται ο τελικός έλεγχος για κάθε περιοχή. Ελέγχεται επιπλέον η διασυνδετική ροή των δύο περιοχών καθώς και το σφάλμα ελέγχου περιοχής τους και κατά πόσο και έπειτα από

πόσο χρονικό διάστημα αυτό συγκλίνει στο μηδέν. Τέλος γίνεται σχολιασμός των αποτελεσμάτων αυτών καθώς και συσχέτιση τους με τα αναμενόμενα.

Όλες οι αριθμητικές προσομοιώσεις εκτελούνται στο MATLAB R2018a.

5.1.1. Προσομοιώσεις μεταβολής φορτίου σε σύστημα Ρύθμισης Φορτίου – Συχνότητάς Μιας Περιοχής με χρήση βηματικής απόκρισης 0.1 αμ

Έπειτα από την εκτενή ανάλυση στο κεφάλαιο 2, το σύστημα μιας περιοχής που θα χρησιμοποιήσουμε για τις προσομοιώσεις μας έχει την εξής μορφή στον χώρο κατάστασης :

$$\dot{x} = \begin{bmatrix} -\frac{D_1}{M_1} & \frac{1}{M_1} & 0 & 0 \\ 0 & -\frac{1}{T_{t_1}} & \frac{1}{T_{t_1}} & 0 \\ -\frac{1}{R_1 T_{g_1}} & 0 & -\frac{1}{T_{g_1}} & \frac{k_1}{T_{g_1}} \\ B_1 & 0 & 0 & 0 \end{bmatrix} \cdot x + \begin{bmatrix} -\frac{1}{M_1} \\ 0 \\ 0 \\ 0 \end{bmatrix} \cdot d$$

Οι τιμές των παραμέτρων του μοντέλου μας είναι οι εξής :

Ισχύς Παραγωγής P_{ref} = 2000 MW, **Συχνότητα** (f) = 60 Hz, **Συντελεστής Απόσβεσης** (D) = 1 αμ MW/Hz, **Σταθερά Αδράνειας** (M) = 10 sec, **Χρονική Σταθερά Ρυθμιστή Στροφών** (Tg) = 0.1 sec, **Σταθερά Χρόνου Στροβίλου** (Tt) = 0.3 sec, **Στατισμός Πρωτεύουσας Ρύθμισης** (R) = 0.05 αμ Hz/MW, **Συντελεστής Πόλωσης** (beta) = 20, **Ολοκληρωτικό** Κέρδος (ki) = 0.1

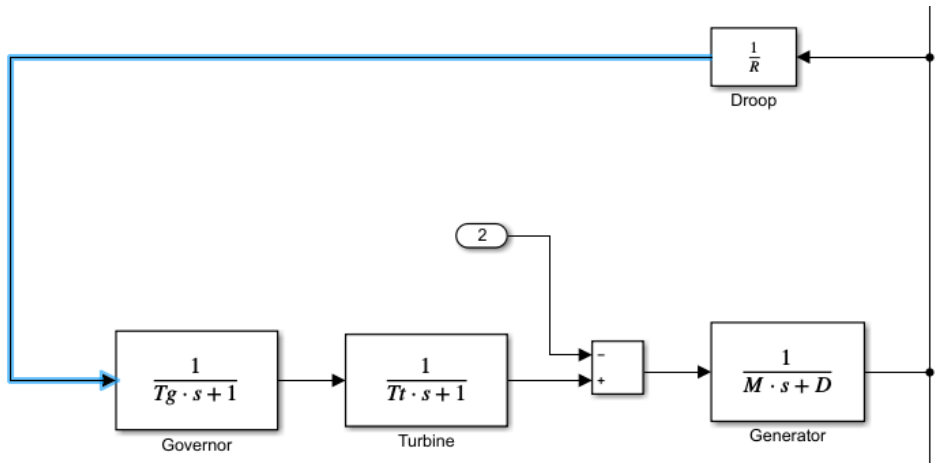
Από τις παραπάνω τιμές προκύπτουν τελικά και οι πίνακες A, B του χώρου κατάστασης του συστήματός μας.

$$A = \begin{bmatrix} -0{,}1 & 0{,}1 & 0 & 0 \\ 0 & -3.33 & 3.33 & 0 \\ -200 & 0 & -10 & 0.33 \\ 20 & 0 & 0 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} -0{,}1 \\ 0 \\ 0 \\ 0 \end{bmatrix},$$

Ο στόχος της **ρύθμισης φορτίου συχνότητας** (Δευτερεύον Έλεγχος) είναι η μείωση του σφάλματος μόνιμης κατάστασης της συχνότητας, της διακύμανσης της διασυνδετικής ροής, της υψηλής απόσβεσης των ταλαντώσεων συχνότητας καθώς και

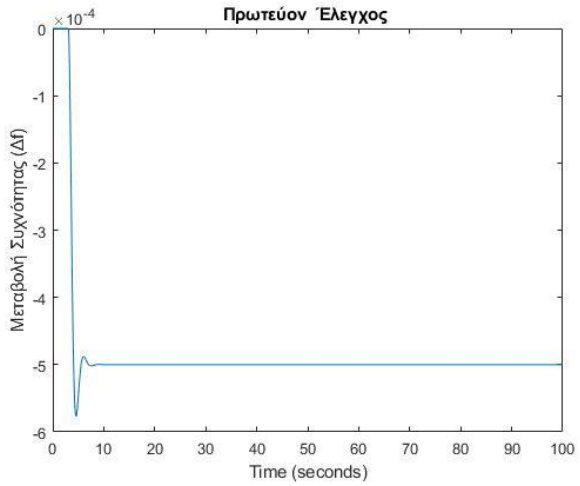
η μείωση της απότομης μεταβολής της διαταραχής, έτσι ώστε το σύστημα να παραμένει ευσταθές. Αυτό θα επιβεβαιώσουμε στη συνέχεια.

Το μοντέλο που χρησιμοποιήσαμε για την πραγματοποίηση των πειραμάτων είναι το παρακάτω. Η είσοδος **2** απεικονίζει την απότομη μεταβολή του φορτίου (βηματική απόκριση μεγέθους 0.1 αμ).



Σχήμα 5. 1 : Μοντέλο Ρύθμισης Φορτίου – Συχνότητας Απομονωμένης περιοχής χωρίς δευτερεύοντα έλεγχο

Το παρακάτω σχήμα απεικονίζει την απόκριση της απόκλισης στη συχνότητα για ένα σύστημα ισχύος μιας περιοχής (Single Area). Η μεταβολή στο φορτίο είναι μια βηματική απόκριση μεγέθους 0.1 αμ, η οποία ενεργείται στο σύστημα τη χρονική μηιγμή t = 3 sec.



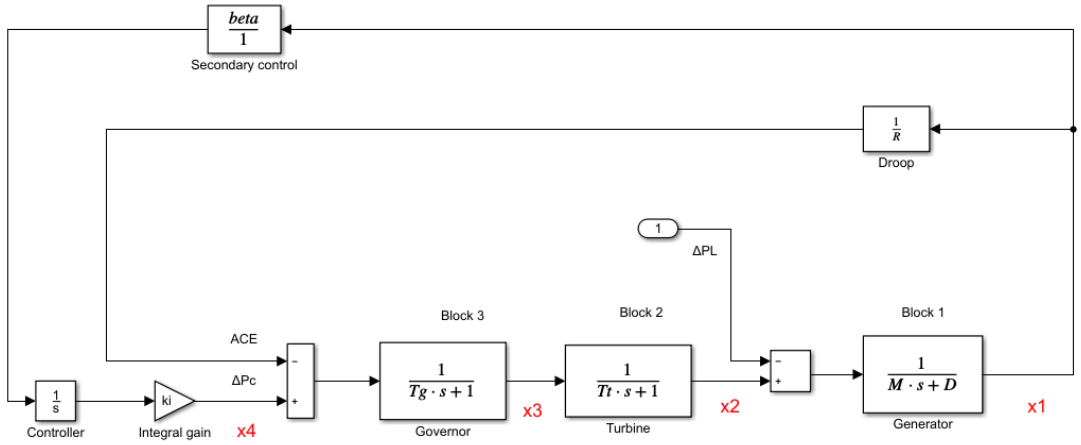
Σχήμα 5. 2 : Μεταβολή Συχνότητας παρουσία μεταβολής φορτίου τη χρονική στιγμή t = 3 sec

Όπως φαίνεται από την παραπάνω γραφική παράσταση, η αλλαγή στο φορτίο επιφέρει την αλλαγή στην ταχύτητα που προκαλεί τη μεταβολή της συχνότητας τη χρονική στιγμή t = 3 sec. Παρατηρούμε επίσης ότι ναι μεν σταθεροποιείται η συχνότητα, αλλά σταθεροποιείται με ένα μόνιμο σφάλμα μεγέθους $5x10^{-4}$.

Για τον λόγο αυτόν όπως έχουμε αναφέρει πρέπει να εισαχθεί ένας ελεγκτής στο σύστημα ώστε να επαναφέρει το σύστημα στην αρχική του συχνότητα λειτουργίας σε

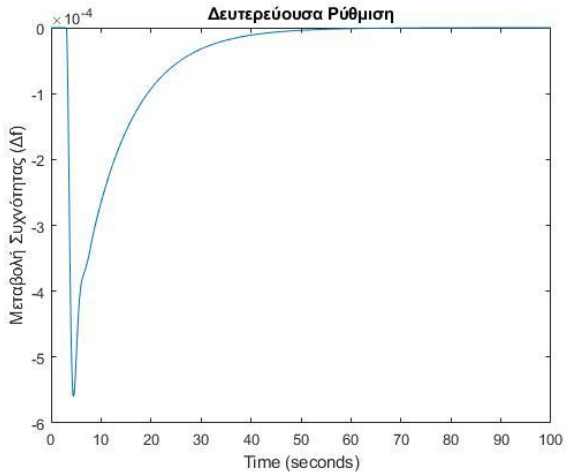
σύντομο χρονικό διάστημα και χωρίς να θέτει σε κίνδυνο την ακεραιότητα των μηχανών του συστήματος.

Μπορούν να χρησιμοποιηθούν πολλοί τύποι ελεγκτών για να διασφαλιστεί η σταθερότητα και η επιθυμητή απόδοση. Σε προηγούμενα κεφάλαια έχουμε αναφέρει τους διάφορους ελεγκτές. Για τις προσομοιώσεις μας χρησιμοποιούμε έναν συμβατικό ολοκληρωτικό ελεγκτή , ολοκληρωτικού κέρδους ki. Ο ελεγκτής αυτός μας προσφέρει την απλότητα που ζητάμε για τα πειράματα μας. Δεν είναι ο βέλτιστος, καθώς δεν είναι σκοπός της παρούσας διπλωματικής η εύρεση του βέλτιστου λειτουργικά και οικονομικά ελεγκτή, είναι όμως αρκετά απλός και εύκολος στην κατασκευή του και επιλέγεται για τα πειράματά μας. Το μοντέλο που χρησιμοποιούμε παρουσιάζεται παρακάτω:



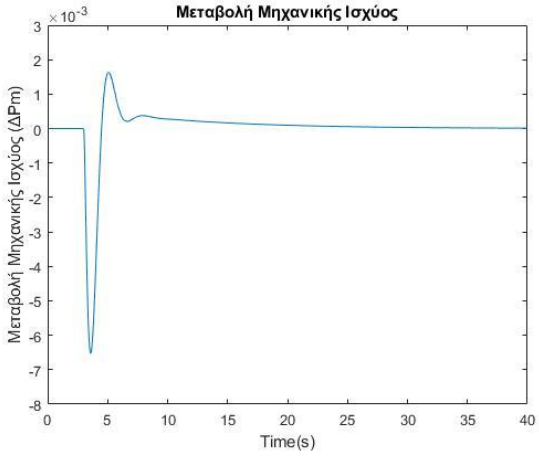
Σχήμα 5. 3 : Μοντέλο LFC απομονωμένης περιοχής με προσθήκη δευτερεύοντα βρόχου

Το παραπάνω σχήμα δείχνει το σύστημα μιας περιοχής που μελετάμε με δευτερεύοντα έλεγχο με χρήση ενός ενιαίου ελεγκτή με ολοκληρωτικό κέρδος Ki = 0.1 για τη ρύθμιση του σήματος αναφοράς ταχύτητας έτσι ώστε η μεταβολή της συχνότητας Δf να συγκλίνει στο μηδέν, δηλαδή η συχνότητα να επανέρχεται στην αρχική της τιμή.



Σχήμα 5. 4 : Μεταβολή Συχνότητας στο LFC έπειτα από μεταβολή φορτίου μεγέθους 0.1 αμ, με την προσθήκη δευτερεύοντα βρόχου

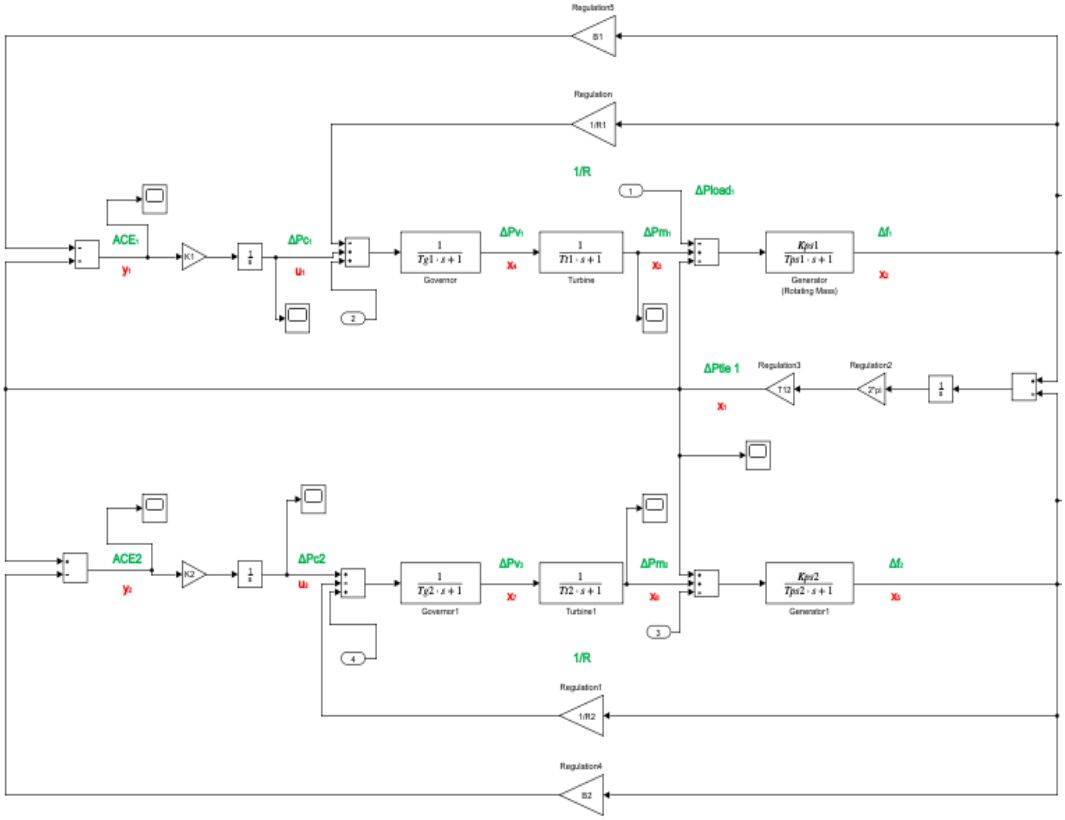
Από τα παραπάνω πράγματι παρατηρούμε ότι μετά από ένα χρονικό διάστημα περίπου 40 sec, η συχνότητα του συστήματος επανέρχεται στην αρχική της τιμή, ενώ από το παρακάτω σχήμα παρατηρούμε ότι η μεταβατική μεταβολή της μηχανικής ισχύος είναι ανεπαίσθητη ($6.5x10^{-3}$ αμ) και γρήγορα η ζήτηση του φορτίου καλύπτεται από το σύστημά μας χωρίς οι μηχανές του να τεθούν σε κίνδυνο αποσυγχρονισμού η μόνιμων βλαβών λόγω πολλών ταλαντωσεων (παφλασμών).



Σχήμα 5. 5 : : Μεταβολή Μηχανικής Ισχύος στο LFC έπειτα από μεταβολή φορτίου μεγέθους 0.1 αμ, με την προσθήκη δευτερεύοντα βρόχου

5.1.2. Προσομοιώσεις μεταβολής φορτίου σε σύστημα Ρύθμισης Φορτίου - Συχνότητας Δύο Περιοχών με χρήση βηματικής απόκρισης 0.1 αμ

Το μοντέλο που χρησιμοποιήσαμε για τις προσομοιώσεις σε ένα σύστημα ρύθμισης φορτίου – συχνότητας δύο περιοχών (Two Area LFC), σύμφωνα με όσα αναφέραμε στο κεφάλαιο 2, απεικονίζεται στο παρακάτω σχήμα.



Σχήμα 5. 6 : LFC μοντέλο Δύο περιοχών

Οι τιμές των παραμέτρων του συστήματος που χρησιμοποιήθηκαν σύμφωνα με την [37] είναι οι εξής:

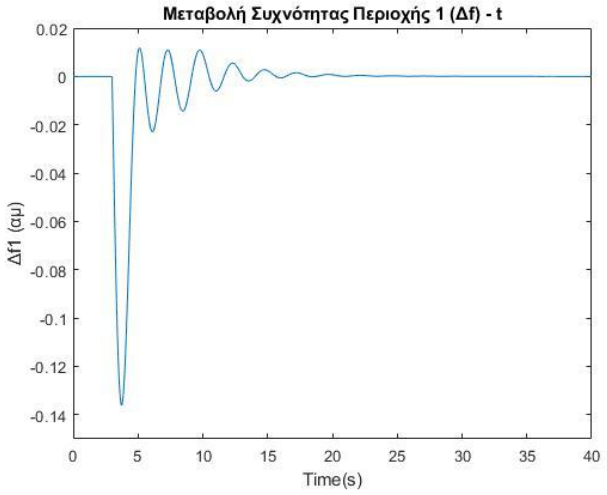
Σταθέρα Κέρδους Συστήματος Ισχύος : $Kps_1 = Kps_2 = 120$, **Συχνότητα** : $f_1 = f_2 = 60$ Hz, **Συντελεστής Απόσβεσης** : $D_1 = D_2 = 0.00834$ αμ MW/HZ, **Χρονική Σταθερά Συστήματος Ισχύος** : $Tps_1 = Tps_2 = 20$ sec, **Χρονική Σταθερά Ρυθμιστή Στροφών** : $Tg_1 = Tg_2 = 0.04$ sec, **Σταθερά Χρόνου Στροβίλου** : $Tt_1 = 0.5$ sec, $Tt_2 = 0.6$ sec **Στατισμός Πρωτεύουσας Ρύθμισης** : $R_1 = R_2 = 2.5$ Hz/MW, **Συντελεστής Πόλωσης** : $beta_1 = beta_2 = 20$, **Ολοκληρωτικό Κέρδος** : $k_1 = k_2 = 0.2$

Στις επόμενες ενότητες παρουσιάζονται τα αποτελέσματα των προσομοιώσεων μεταβολής φορτίου τόσο στην περιοχή 1 όσο και στην περιοχή 2, καθώς και η επιρροή της μεταβολής αυτής στις συχνότητες κάθε συστήματος αλλά και της διασυνδετικής ροής των διασυνδεδεμένων περιοχών.

Καθώς τα δύο συστήματα είναι διασυνδεδεμένα, οι μετατοπίσεις συχνότητας των δύο θα σταθεροποιηθούν σε ίση τιμή μετά από κάποιες ταλαντώσεις.

5.1.2.1.Προσομοιώσεις απότομης αύξησης φορτίου στην περιοχή 1 με χρήση βηματικής απόκρισης step (+0.05 pu ή 5%) την χρονική στιγμή t = 3 sec.

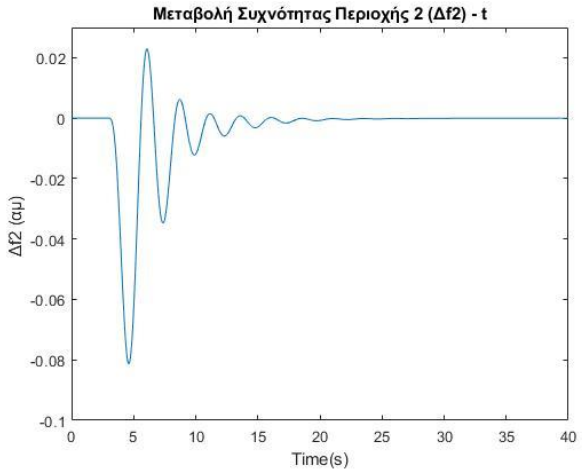
Το παρακάτω σχήμα απεικονίζει τη μεταβολή της συχνότητας λειτουργίας της περιοχής 1, έπειτα από μια απότομη αύξηση του φορτίου στην ίδια περιοχή την χρονική στιγμή t = 3 sec. Η ξαφνική αύξηση του ηλεκτρικού φορτίου οδηγεί σε μία απότομη πτώση της συχνότητας, καθώς η ηλεκτρική ισχύς άρα και η μηχανική είναι μικρότερη από το φορτίο, γεγονός που οδηγεί σε πτώση της συχνότητας όπως αναλύσαμε σε προηγούμενα κεφάλαια.



Σχήμα 5. 7 : Μεταβολή Συχνότητας Περιοχής 1 με αύξηση φορτίου 0.5 αμ τη χρονική στιγμή t = 3 sec

Η απότομη μεταβολή που παρατηρούμε την χρονική στιγμή t = 3 sec οφείλεται στην ξαφνική αύξηση του φορτίου. Οι ταλαντώσεις που γίνονται μέχρι την τελική ισορροπία δεν είναι ικανές να προκαλέσουν μόνιμη βλάβη στο σύστημα, καθώς έχουν αρκετά μικρό πλάτος και εξαλείφονται στα πρώτα 20sec. Έπειτα από αυτήν την χρονική στιγμή παρατηρούμε ότι η συχνότητα της περιοχής επανέρχεται στην αρχική της τιμή χωρίς το μόνιμο σφάλμα που αφήνει ο πρωτεύον έλεγχος κι επομένως ο δευτερεύοντας έλεγχος μέσω του ολοκληρωτή λειτουργεί επιτυχώς.

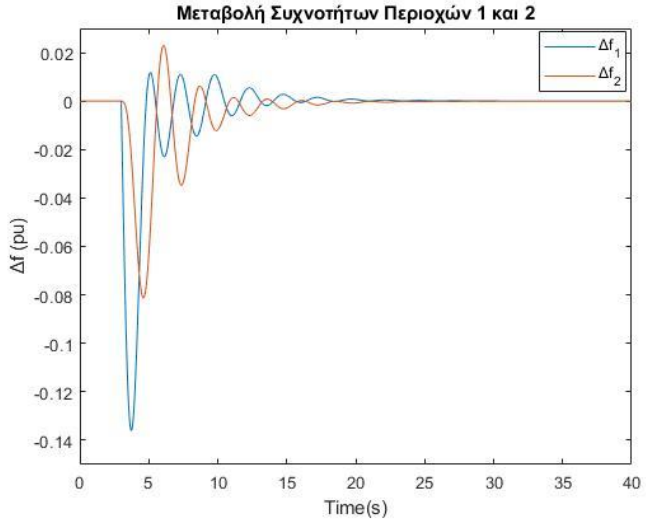
Η πτώση της συχνότητας όπως θα δούμε και στο επόμενο σχήμα, διαδίδεται και στην περιοχή 2. Καθώς τα δύο συστήματα είναι διασυνδεδεμένα, οι μεταβολές της συχνότητας των δύο θα σταθεροποιηθούν σε ίση τιμή μετά από κάποιες ταλαντώσεις, όπως παρατηρούμε και από το παραπάνω σχήμα.



Σχήμα 5. 8 : Μεταβολή Συχνότητας Περιοχής 2 με αύξηση φορτίου 0.5 αμ στην περιοχή 1 τη χρονική στιγμή t = 3 sec

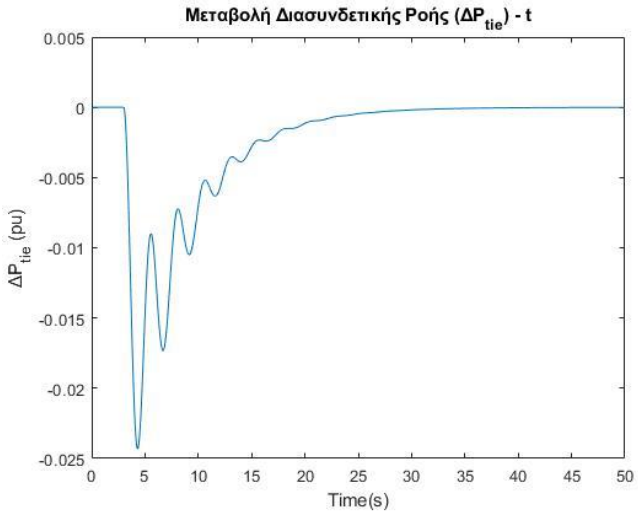
Παρατηρούμε πως η μεταβολή της συχνότητας της περιοχής 2, ακολουθεί την ίδια πορεία με τη συχνότητα της περιοχής 1, όπως περιμέναμε. Η απότομη μεταβολή στην περιοχή 2 είναι λιγότερο απότομη και εμφανώς μικρότερη απ΄ ότι στην περιοχή 1, όπως και το πλάτος και ο αριθμός των ταλαντώσεων μέχρι την τελική σταθεροποίηση στο μηδεν, γεγονός που εξηγείται από το γεγονός ότι η περιοχή 2 επενεργεί βοηθητικά στην απότομη μεταβολή που συμβαίνει στην περιοχή 1.

Στο παρακάτω σχήμα φαίνεται πιο καθαρά η πιο ομαλή και πιο μικρού πλατους μεταβολή της συχνότητας στην διασυνδεδεμένη περιοχή 2 σε σχέση με την περιοχή 1.

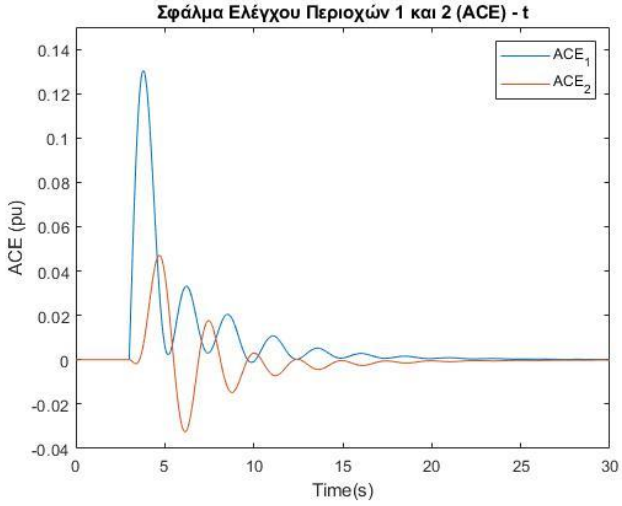


Σχήμα 5. 9 : Μεταβολή Συχνοτήτων περιοχών 1 και 2 με αύξηση φορτίου 0.5 αμ τη χρονική στιγμή t = 3 sec στην περιοχή 1

Στα επόμενα διαγράμματα παρουσιάζουμε τόσο τη διασυνδετική ροή μεταξύ των δύο περιοχών, όσο και τα Σφάλματα Ελέγχου Περιοχών 1 και 2.



Σχήμα 5. 10 : Μεταβολή Διασυνδετικής Ροής Περιοχής 1 με αύξηση φορτίου 0.5 αμ τη χρονική στιγμή t = 3 sec

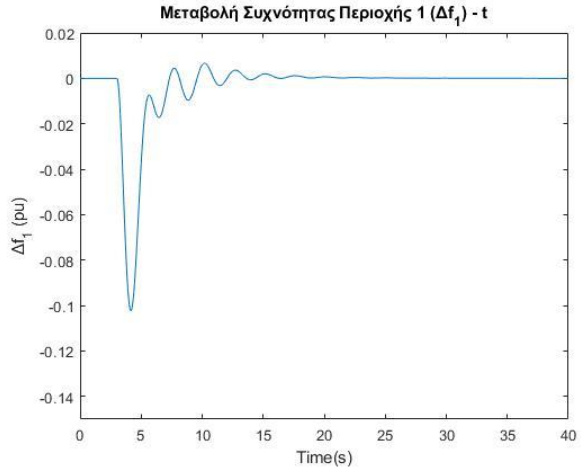


Σχήμα 5. 11 : Σφάλμα Ελέγχου Περιοχής 1 και 2 με αύξηση φορτίου 0.5 αμ τη χρονική στιγμή t = 3 sec

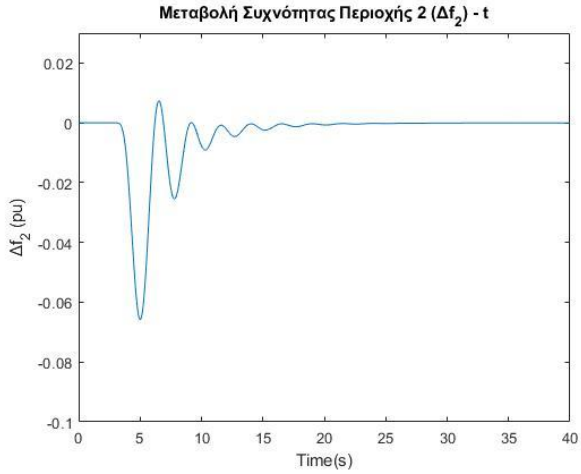
Παρατηρούμε πως συγκλίνουν ταυτόχρονα στο μηδέν (μετά το πέρας περίπου 25 sec), όπως επίσης και την διαφορετική πολικότητα που έχουν κάθε χρονική στιγμή, πράγμα που είναι φυσικό σύμφωνα με τη διαδικασία που ακολουθεί ο αλγόριθμος του ΣΕΠ.

5.1.2.2.Προσομοιώσεις απότομης αύξησης φορτίου στην περιοχή 2 με χρήση βηματικής απόκρισης step (+0.05 pu) την χρονική στιγμή t = 3 sec.

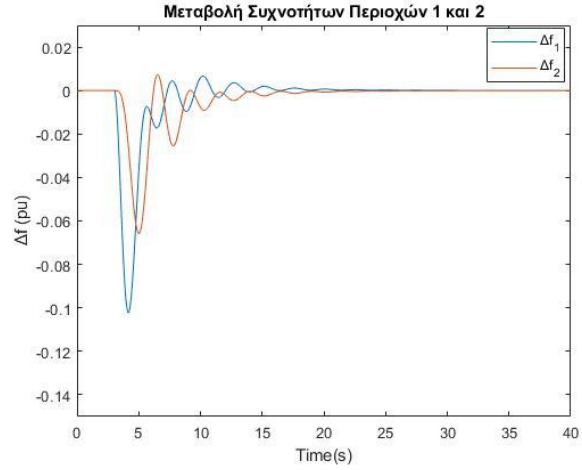
Επιβάλουμε στην συνέχεια την ίδια απότομη αύξηση φορτίου μέσω μιας βηματικής απόκρισης 5% αμ, αυτή τη φορά στην περιοχή 2 και ελέγχουμε τα αποτελέσματα που προκύπτουν, αναμένοντας παρόμοια αποτελέσματα με της προηγούμενης ενότητας.



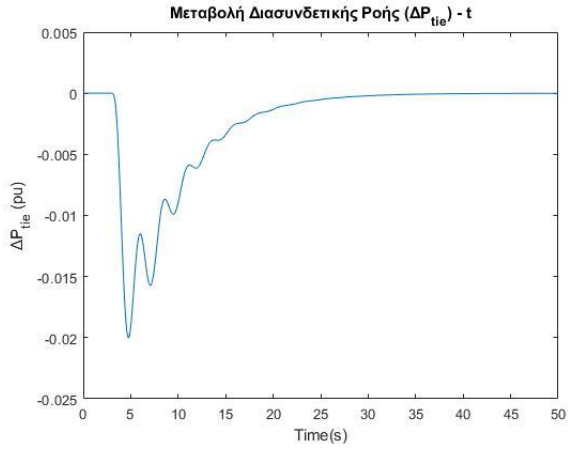
Σχήμα 5. 12 : Μεταβολή Συχνότητας Περιοχής 1 με αύξηση φορτίου 0.5 αμ στην περιοχή 2 τη χρονική στιγμή t = 3 sec



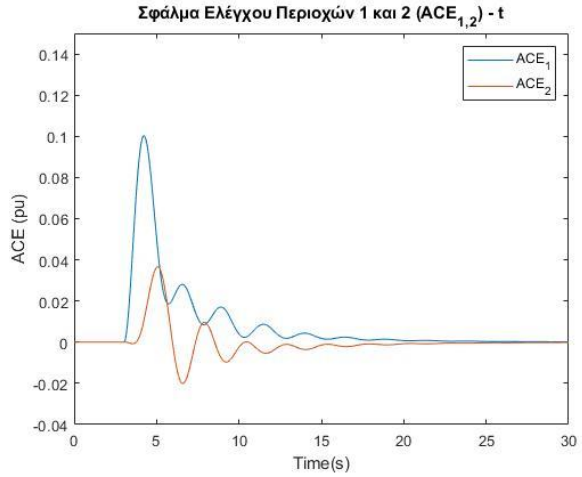
Σχήμα 5. 13 : : Μεταβολή Συχνότητας Περιοχής 2 με αύξηση φορτίου 0.5 αμ στην περιοχή 2 τη χρονική στιγμή t = 3 sec



Σχήμα 5. 14 : Μεταβολή Συχνοτήτων περιοχών 1 και 2 με αύξηση φορτίου 0.5 αμ τη χρονική στιγμή t = 3 sec στην περιοχή 2

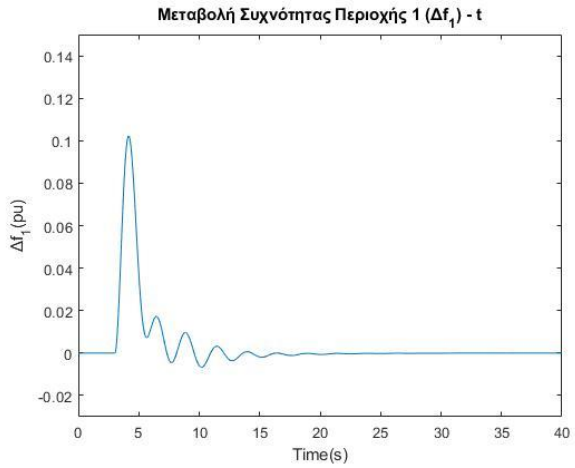


Σχήμα 5. 15 : : Μεταβολή Διασυνδετικής Ροής Περιοχής 2 με αύξηση φορτίου 0.5 αμ τη χρονική στιγμή t = 3 sec

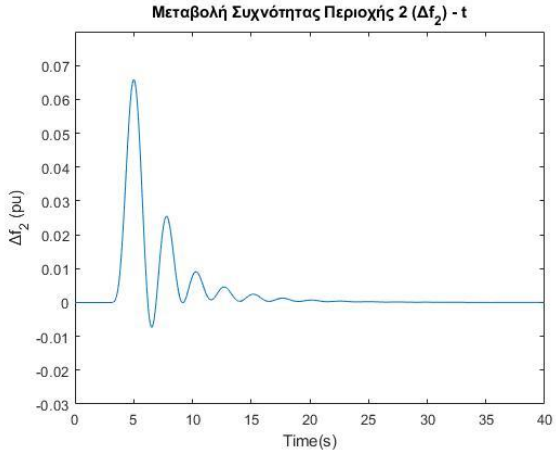


Σχήμα 5. 16 : Σφάλμα Ελέγχου Περιοχής 1 και 2 με αύξηση φορτίου 0.5 αμ τη χρονική στιγμή t = 3 sec

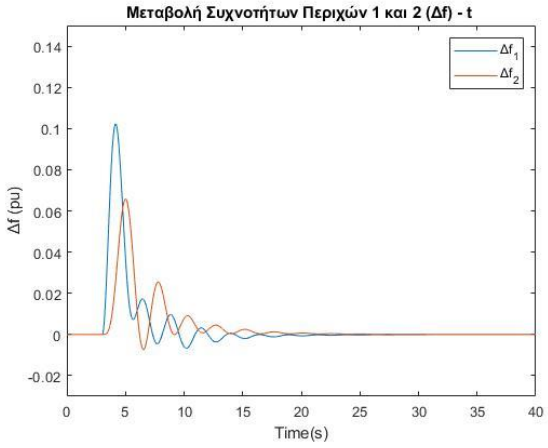
5.1.1.1. Προσομοιώσεις απότομης μείωσης φορτίου στην περιοχή 2 με χρήση βηματικής απόκρισης step (-0.05 pu) την χρονική στιγμή t = 3 sec



Σχήμα 5. 17 : Μεταβολή Συχνότητας Περιοχής 1 με μείωση φορτίου 0.5 αμ στην περιοχή 1 τη χρονική στιγμή t = 3 sec

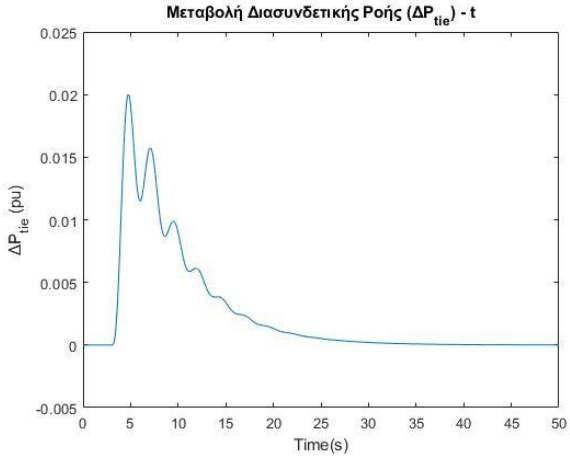


Σχήμα 5. 18 : Μεταβολή Συχνότητας Περιοχής 2 με μείωση φορτίου 0.5 αμ στην περιοχή 1 τη χρονική στιγμή t = 3 sec

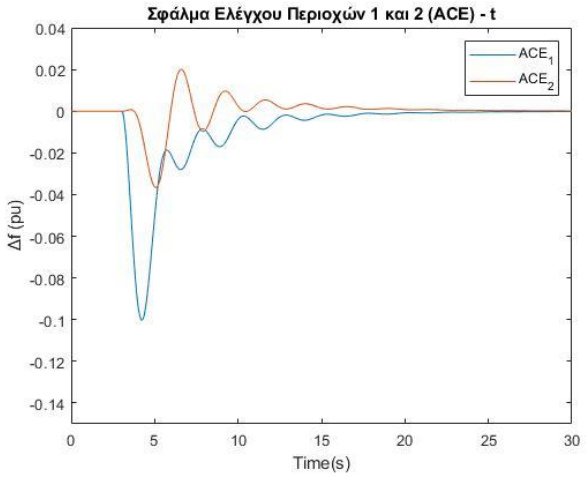


Σχήμα 5. 19 : Μεταβολή Συχνοτήτων Περιοχών 1 και 2 με μείωση φορτίου 0.5 αμ στην περιοχή 1 τη χρονική στιγμή t = 3 sec

Για μείωση φορτίου παρατηρούμε αύξηση της συχνότητας όπως αναμέναμε και για τις δύο περιοχές, καθώς η ηλεκτρική ισχύς άρα και η μηχανική είναι μεγαλύτερη από το φορτίο, γεγονός που οδηγεί μείωση της ταχύτητας του ρότορα και συνεπώς σε πτώση της συχνότητας όπως αναλύσαμε σε προηγούμενα κεφάλαια.



Σχήμα 5. 20 : Μεταβολή Διασυνδετικής Ροής Περιοχής 1 με μείωση φορτίου 0.5 αμ τη χρονική στιγμή t = 3 sec

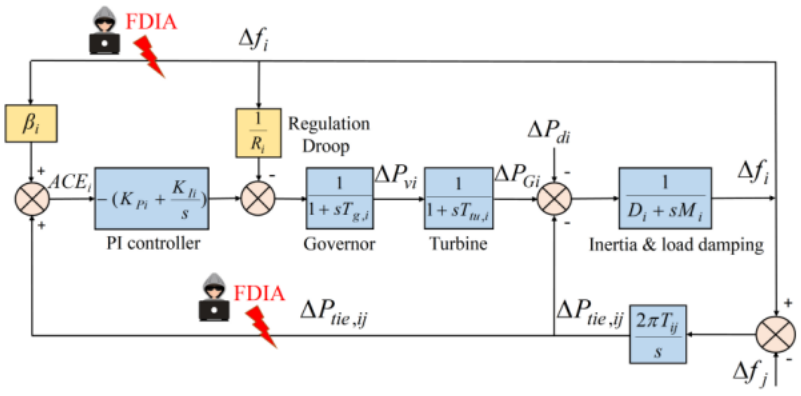


Σχήμα 5. 21 : Σφάλμα Ελέγχου Περιοχής 1 και 2 με μείωση φορτίου 0.5 αμ τη χρονική στιγμή t = 3 sec

Παρατηρούμε πως και με μείωση φορτίου, τα σφάλματα ελέγχου περιοχής συγκλίνουν ταυτόχρονα στο μηδέν (μετά το πέρας περίπου 25 sec), όπως επίσης και την διαφορετική πολικότητα που έχουν κάθε χρονική στιγμή, πράγμα που είναι φυσικό σύμφωνα με τη διαδικασία που ακολουθεί ο αλγόριθμος του ΣΕΠ.

5.2.Προσομοιώσεις και ανάλυση Επιθέσεων Έγχυσης Ψευδών Δεδομένων στο LFC

Τα ψευδή δεδομένα τω FDI επιθέσεων μπορούν να εγχυθούν στις μετρήσεις διασύνδεσης και συχνότητας είτε μέσω των δικτυακών καναλιών επικοινωνίας είτε απευθείας στους αισθητήρες ή/και στους ενεργοποιητές., δηλαδή ο επιτιθέμενος στέλνει ψευδείς πληροφορίες από αισθητήρες στο κέντρο ελέγχου ή από το κέντρο ελέγχου στις γεννήτριες που ελέγχονται από το AGC ή στα κανάλια επικοινωνίας.



Σχήμα 5. 22 : Πιθανά Σημεία FDI επιθέσεων στο σύστημα Ρύθμισης Φορτίου – Συχνότητας περιοχής i

Η εξίσωση στο χώρο κατάστασης της περιοχής ισχύος κατά τη διάρκεια επιθέσεων σύμφωνα με την (4.21) είναι :

$$\dot{x}(t) = A \cdot x(t) + B \cdot u(t) + E \cdot d(t) + F \cdot f_{FDIA}(t)$$

$$y(t) = C \cdot x(t)$$

Όπου F ο πίνακας επίθεσης και $f_{FDIA}(t)$ το σήμα της επίθεσης (σε συχνοτικές μετρήσεις και μετρήσεις διασυνδετικής ροής). Σε μαθηματική μορφή:

$$F = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \qquad \text{και} \qquad f_{FDIA}(t) = f_{FDIA,tie}(t) + \beta_i \, f_{FDIA,freq}(t)$$

Όλες οι προσομοιώσεις έχουν πραγματοποιηθεί μέσω MATLAB και Simulink.

5.2.1. Επιθέσεις σε Σύστημα Ρύθμισης Φορτίου – Συχνότητας Απομονωμένης Περιοχής

Στο πλαίσιο της παρούσας διπλωματικής γίνονται αρχικά προσομοιώσεις δύο τύπων στο Σύστημα Ρύθμισης Φορτίου Συχνότητας Μιας Περιοχής (Single Area LFC). Οι επιθέσεις είναι έγχυσης ψευδών δεδομένων στις μετρήσεις της συχνότητας της περιοχής. Τα σενάρια των επιθέσεων περιγράφονται παρακάτω.

5.2.1.1. Περίπτωση Επίθεσης 1 : Bias Injection Attack στον αισθητήρα της Συχνότητας

Σε αυτού του τύπου επίθεσης, οι εισβολείς προσθέτουν ένα διάνυσμα μεροληψίας (bias factor) στη μέτρηση συχνότητας της περιοχής. Το σήμα που προκύπτει μετά την επίθεση μπορεί να περιγραφεί ως εξής:

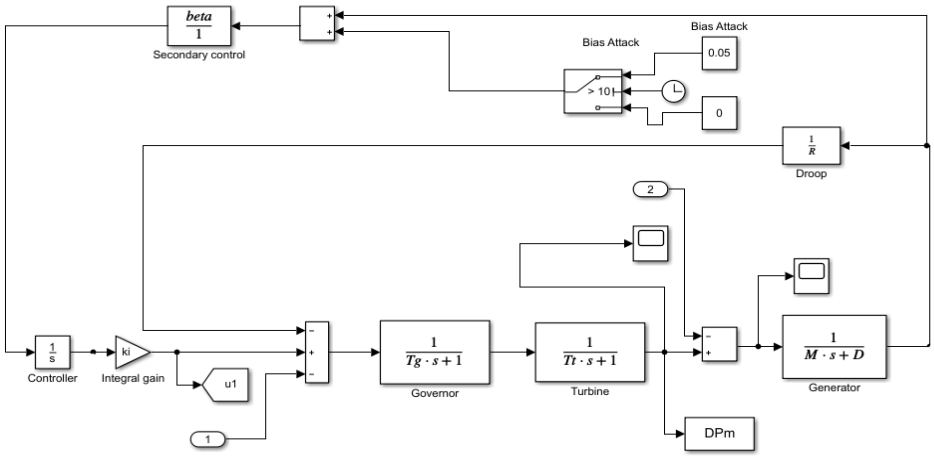
$$x_{final}(t) = x(t) + f_{bias} = x(t) + 0.05$$

ή

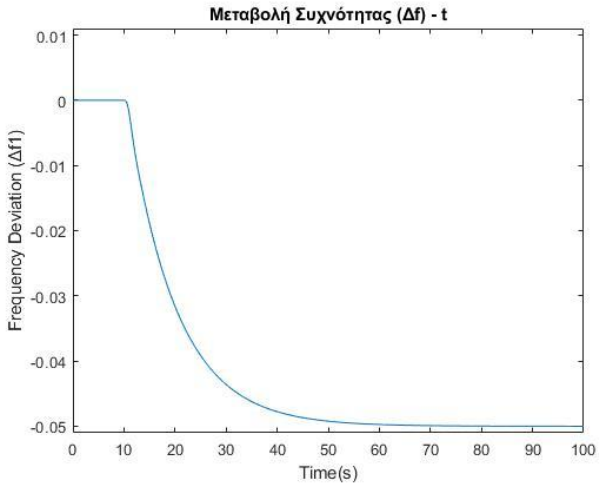
$$x_{final}(t) = x(t) + f_{bias} = x(t) - 0.05$$

με $f_{bias} = \pm 0.05$

(5.1)

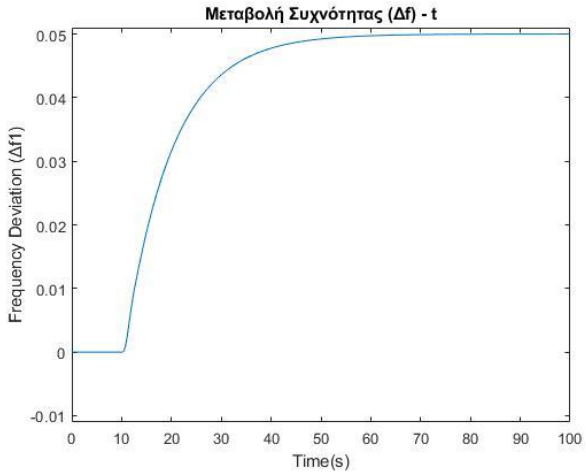


Σχήμα 5. 23 : Σύστημα Ρύθμισης Φορτίου -Συχνότητας υπό την επιβολή Bias Injection Attack στις μετρήσεις της συχνότητας



Σχήμα 5. 24 : Μεταβολή Συχνότητας υπό την επίδραση επίθεσης έγχυσης παράγοντα θετικού "Bias"

Κατά την συγκεκριμένη επίθεση, το υποσύστημα (block) "bias" χειρίζεται από τον επιτιθέμενο. Είναι προφανές ότι η απόκριση της συχνότητας πέφτει αμέσως κατά τη χρονική στιγμη της επίθεσης (t = 5 sec) και παραμένει σταθερή δημιουργώντας έτσι ένα μόνιμο σφάλμα στη συχνότητα. Ομοίως, όπως φαίνεται ακριβώς από κάτω, μια αντίστοιχη επίθεση αρνητικού παράγοντα "bias" , αφήνει το ίδιο μόνιμο σφάλμα στη συχνότητα, θετικό όμως αυτή τη φορά.



Σχήμα 5. 25 : Μεταβολή Συχνότητας υπό την επίδραση επίθεσης έγχυσης παράγοντα αρνητικού "Bias"

Η συγκεκριμένη επίθεση (Bias Injection Attack) στην πραγματικότητα παράγει μια σταθερή μεταβολή στην προγραμματισμένη συχνότητα και στην ουσία ακυρώνει τον δευτερεύοντα έλεγχο, αφήνοντας ένα μόνιμο σφάλμα στη συχνότητα.

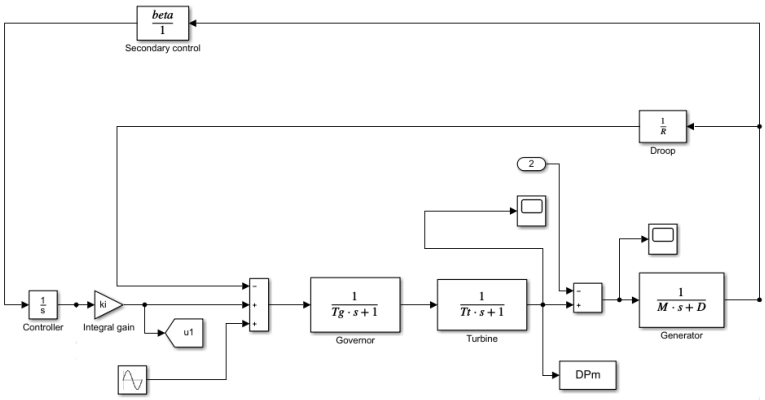
5.2.1.2.Περίπτωση Επίθεσης 2 : Additive Harmonic Attack στον ενεργοποιητή

Στο συγκεκριμένο σενάριο επίθεσης, στα πειράματά μας χρησιμοποιούμε ως προσθετικό σήμα μια αρμονική (ημιτονική) συνάρτηση :

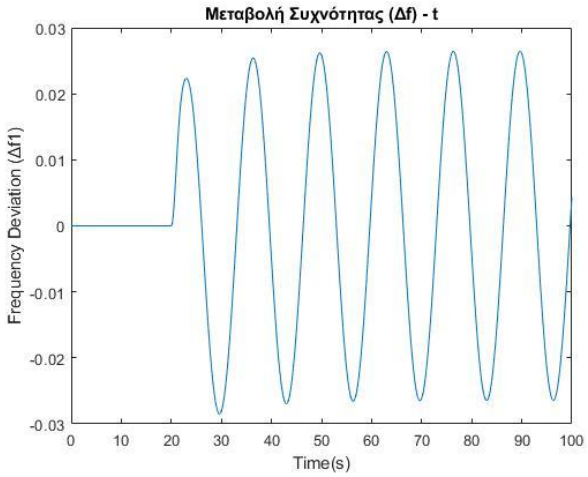
$$x_{final}(t) = x(t) + f_{ad\_attack}(t)$$

Χρησιμοποιούμε μια ημιτονική συνάρτηση πλάτους $A_f = 0.15$, $w = 0.15 \cdot \pi$ rad/sec, $\varphi = 0$ rad/sec. Η εξίσωση είναι η εξής :

$$x_{final}(t) = x(t) + A_f \sin(wt + \varphi) \qquad (5.2)$$



Σχήμα 5. 26 : Σύστημα Ρύθμισης Φορτίου -Συχνότητας υπό την επιβολή Προσθετικής Αρμονικής Επίθεσης στο κανάλι επικοινωνίας κέντρου ελέγχου και ρυθμιστή στροφών



Σχήμα 5. 27 : Μεταβολή Συχνότητας υπό την επίδραση προσθετικής αρμονικής επίθεσης στο κανάλι επικοινωνίας κέντρου ελέγχου και ρυθμιστή στροφών

Σε μια αρμονική προσθετική επίθεση, δίνεται μια συνεχής ημιτονική είσοδος στον ενεργοποιητή (actuator), δηλαδή στις εντολές που στέλνει το κέντρο ελέγχου, που διαταράσσει εντελώς την απόκριση όπως φαίνεται στο παραπάνω σχήμα. Εδώ, το πλάτος της ημιτονικής εισόδου είναι 0.15. Όσο μεγαλύτερο είναι το πλάτος, τόσο μεγαλύτερες είναι οι ταλαντώσεις και τόσο πιο ασταθές γίνεται το σύστημα.

5.2.2. Επιθέσεις σε Σύστημα Ρύθμισης Φορτίου – Συχνότητας Δύο Περιοχών

Στη συνέχεια πραγματοποιούνται επιθέσεις τεσσάρων τύπων, καθώς στα διασυνδεδεμένα συστήματα ο κίνδυνος κυβερνοεπιθέσεων είναι αισθητά μεγαλύτερος όπως έχουμε ήδη αναφέρει, αφού ως στόχοι επίθεσης, εκτός από τους αισθητήρες μετρήσεων της συχνότητας, προστίθενται οι αισθητήρες μέτρησης διασυνδετικής ροής και τα κανάλια επικοινωνίας των δύο περιοχών.

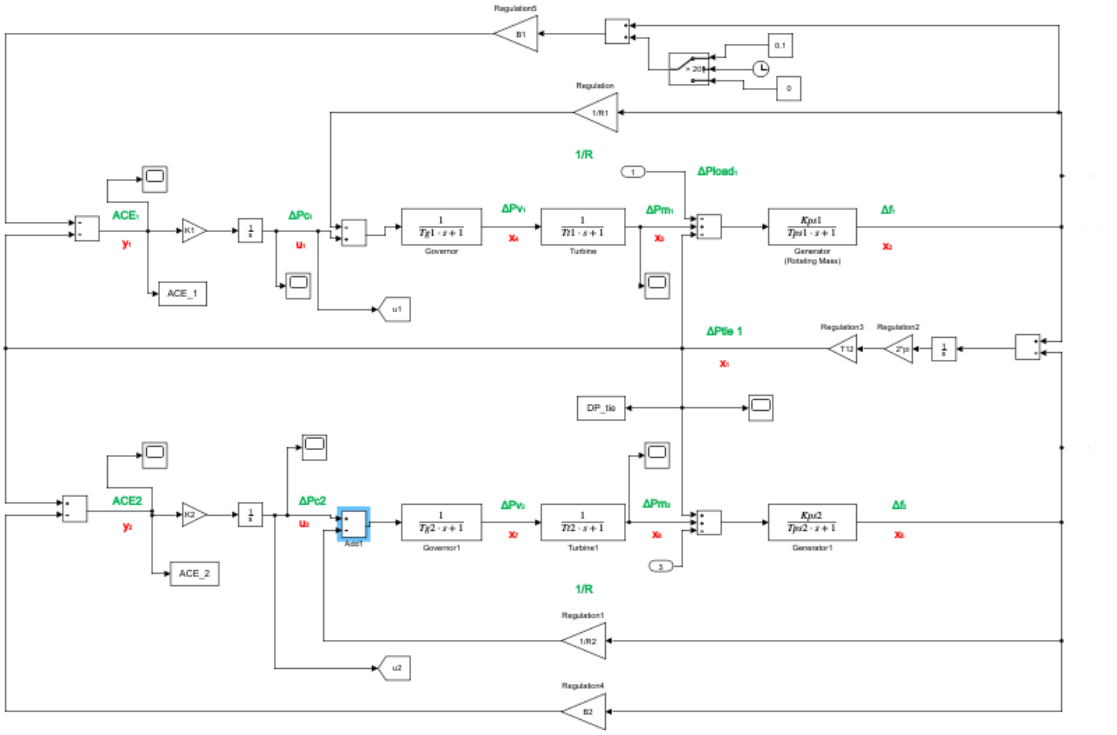
5.2.2.1.Περίπτωση Επίθεσης 1 : Bias Injection Attack στο κανάλι του αισθητήρα της Συχνότητας

Σε αυτού του τύπου επίθεση, οι εισβολείς προσθέτουν ένα διάνυσμα μεροληψίας (bias factor) στη μέτρηση συχνότητας της περιοχής i. Το σήμα που προκύπτει μετά την επίθεση μπορεί να περιγραφεί ως εξής:

$$x_{final}(t) = x(t) + f_{bias} = x(t) + 0.1$$

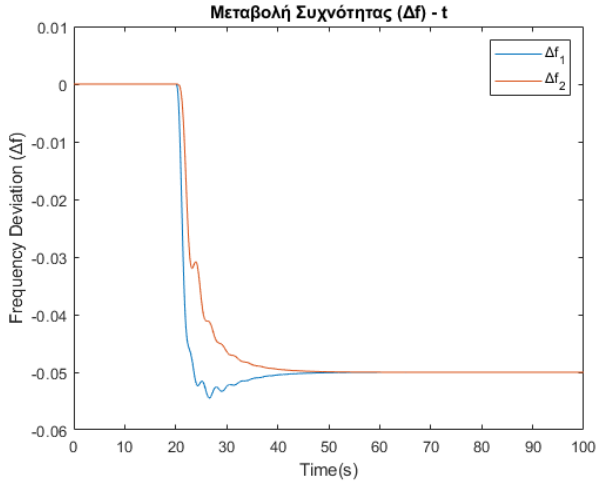
με f_{bias} = 0.1 (5.3)

Στο πλαίσιο των πειραμάτων μας προσομοιώνουμε την επίθεση στον αισθητήρα συχνότητας της περιοχής 1, τη χρονική στιγμή t = 20sec, όπως απεικονίζεται στο παρακάτω σχήμα:



Σχήμα 5. 28 : Σύστημα Ρύθμισης Φορτίου -Συχνότητας υπό την επιβολή Επίθεσης έγχυσης παράγοντα "bias" στις μετρήσεις της συχνότητας της περιοχής 1

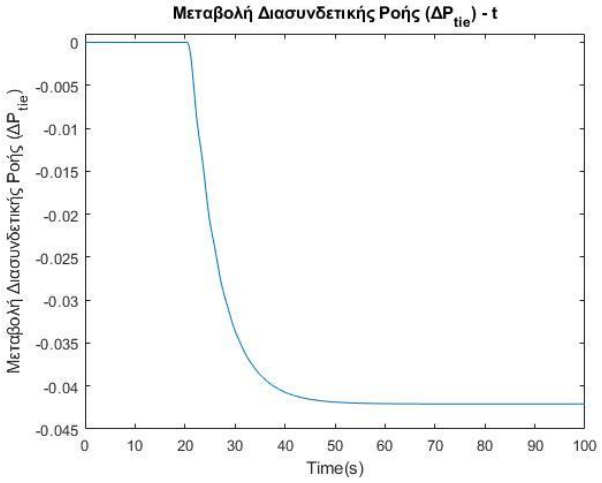
Οι χαρακτηριστικές μεταβολής συχνότητας (Δf_1, Δf_2) των δύο περιοχών, του σφάλματος ελέγχου περιοχής 1 και 2 (ACE_1, ACE_2), καθώς και της διασυνδετικής ροής (ΔP_{tie}) που προκύπτουν είναι οι παρακάτω :



Σχήμα 5. 29 : Μεταβολες Συχνοτήτων Περιοχών 1 και 2 υπό την επίθεση παράγοντα έχγυσης "bias", με b =0.1

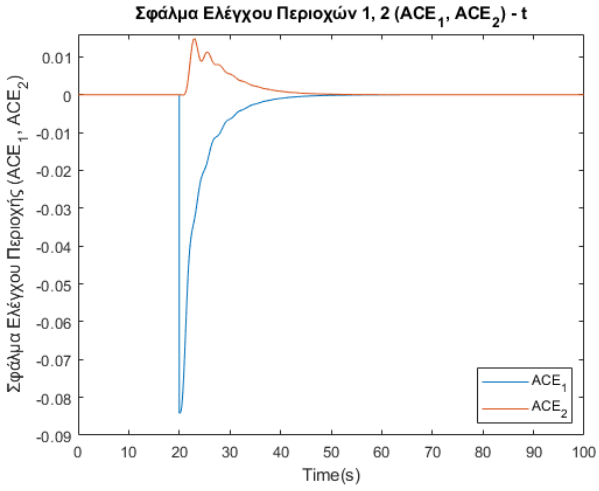
Στη μεταβολή των συχνοτήτων παρατηρούμε ότι η συγκεκριμένη επίθεση (Bias Injection Attack) αφήνει όπως και στο σύστημα ρύθμισης Φορτίου – Συχνότητας της

μιας περιοχής, ένα μόνιμο σφάλμα. Από την μια παραμένει ευσταθές το σύστημα, από την άλλη όμως ακυρώνεται στην ουσία ο δευτερεύοντας έλεγχος.



Σχήμα 5. 30 : Μεταβολή Διασυνδετική Ροής υπό την επίδραση επίθεση παράγοντα έχγυσης "bias", με b =0.1

Η διασυνδετική ροή ακολουθεί τη γραφική της μεταβολής της συχνότητας, κάτι το οποίο αναμένουμε εξετάζοντας τον μαθηματικό τύπο της, όπως αναλύσαμε σε προηγούμενα κεφάλαια.



Σχήμα 5. 31 : Μεταβολή Σφάλματος Ελέγχου Περιοχής 1 και 2 υπό επίθεση παράγοντα έχγυσης "bias", με b =0.1

Όσον αφορά το σφάλμα ελέγχου περιοχής παρατηρούμε ότι η μεταβολή είναι μεγαλύτερη στην περιοχή 1, λόγω του ότι η επίθεση πραγματοποιείται στη συγκεκριμένη περιοχή και αντίθετη από τη μεταβολή του σφάλματος της περιοχής 2, όπως είναι λογικό λόγω της αντίθετης πορείας της ίσχυος (η μία περιοχή «ζητά», η άλλη «προσφέρει»). Παρατηρούμε επίσης ότι απολύτως λογικά η μεταβολή του σφάλματος της περιοχής 2 ξεκινά λίγο μετά από αυτήν της 1ης, ενώ τέλος παρατηρούμε

ότι μετά τα 40 sec οι μεταβολές συγκλίνουν στο μηδέν, αφού το σύστημά μας έχει έρθει σε ισορροπία, ανεξάρτητα από το γεγονός της ύπαρξης μόνιμου σφάλματος.

5.2.2.2.Περίπτωση Επίθεσης 2 : Additive Harmonic Attack στο κανάλι του αισθητήρα μετρήσεων της Διασυνδετικής Ροής

Στο συγκεκριμένο σενάριο επίθεσης, στα πειράματά μας χρησιμοποιούμε ως προσθετικό σήμα μια αρμονική (ημιτονική) συνάρτηση.

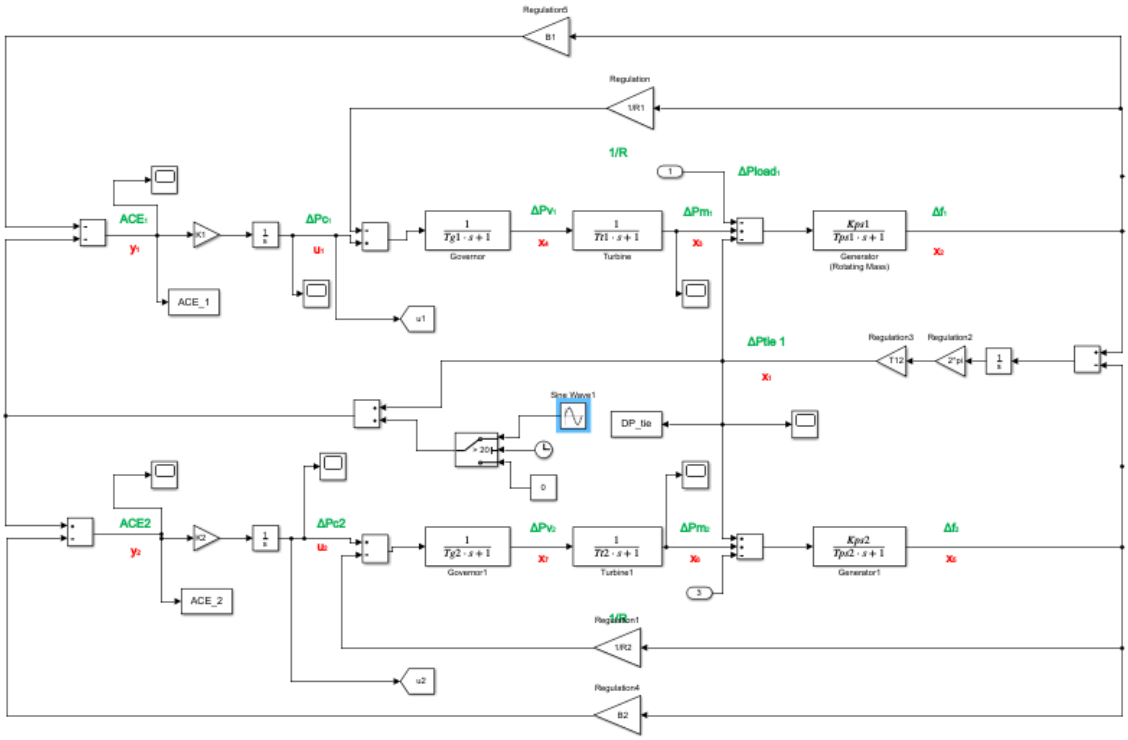
$$x_{final}(t) = x(t) + f_{ad\_attack}(t)$$

Χρησιμοποιούμε μια ημιτονική συνάρτηση πλάτους $A_f = 0.15$, $w = 0.15 \cdot \pi$ rad/sec, $\varphi = 0$ rad/sec. Η εξίσωση είναι η εξής :

$$x_{final}(t) = x(t) + A_f \sin(wt + \varphi)$$

ή

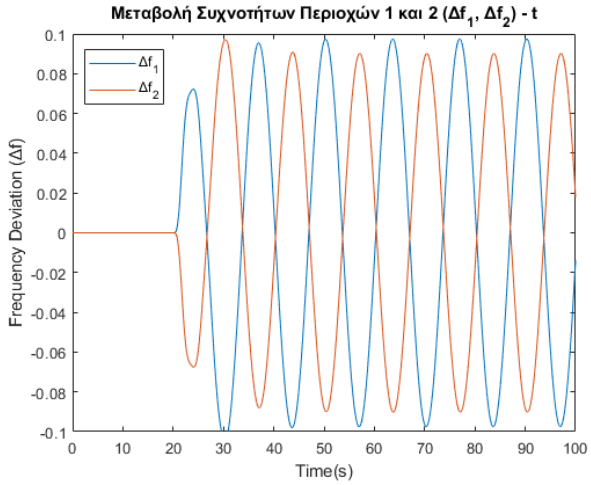
$$x_{final}(t) = x(t) + 0.15 \sin(0.15\pi t) \qquad (5.4)$$



Σχήμα 5. 32 : Σύστημα Ρύθμισης Φορτίου -Συχνότητας υπό την επιβολή Προσθετικής Αρμονικής Επίθεσης έγχυσης στο κανάλι μετρήσεων της διασυνδετικής ροής

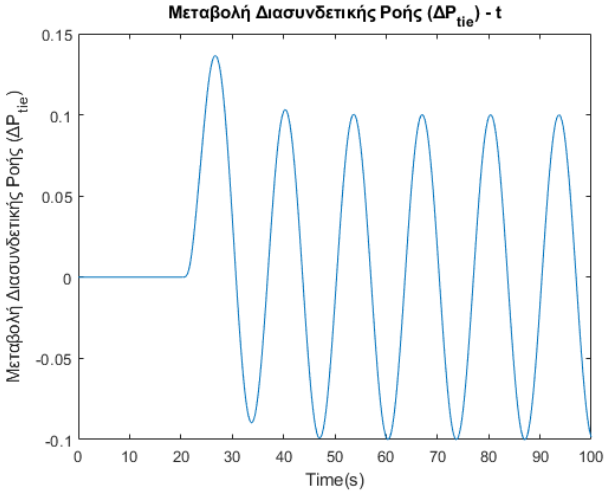
Οι χαρακτηριστικές μεταβολής συχνότητας (Δf_1, Δf_2) των δύο περιοχών, του σφάλματος ελέγχου περιοχής 1 και 2 (ACE_1, ACE_2), καθώς και της διασυνδετικής ροής

(ΔP_{tie}) που προκύπτουν μετά την επίθεση τη χρονική στιγμή t = 20 sec είναι οι παρακάτω :

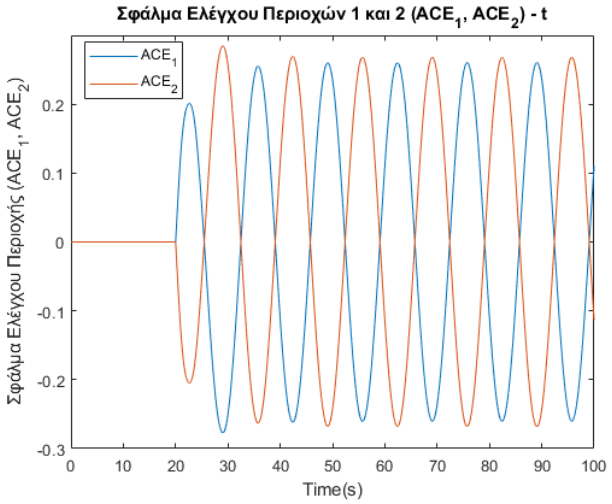


Σχήμα 5. 33: Μεταβολές Συχνοτήτων Περιοχών 1 και 2 υπό προσθετική αρμονική επίθεση πλάτους 0.15 αμ |

Στη συγκεκριμένη προσθετική επίθεση, δίνεται μια συνεχής ημιτονική είσοδος στο κανάλι της διασυνδετικής ροής, δηλαδή στις μετρήσεις που προκύπτουν στον αισθητήρα της διασυνδετικής ροής. Η απόκριση αυτή διαταράσσει εντελώς το σύστημα όπως φαίνεται στο παραπάνω σχήμα. Εδώ, το πλάτος της ημιτονικής εισόδου είναι 0.15 αμ. Όσο μεγαλύτερο είναι το πλάτος, τόσο μεγαλύτερες είναι οι ταλαντώσεις και τόσο πιο ασταθές γίνεται το σύστημα. Προφανώς το σύστημα μας είναι ασταθές και οι συχνότητες δεν συγκλίνουν ποτέ.



Σχήμα 5. 34 : : Μεταβολή Διασυνδετική Ροής υπό την επίδραση προσθετικής αρμονικής επίθεσης πλάτους 0.15 αμ



Σχήμα 5. 35 : : Μεταβολή Σφάλματος Ελέγχου Περιοχής 1 και 2 υπό επίδραση προσθετικής αρμονικής επίθεσης πλάτους 0.15 αμ

Το σφάλματα ελέγχου περιοχής ACE είναι αντίθετα κάθε χρονική στιγμή όπως αναμένουμε και δε συγκλίνουν ποτέ όπως οι συχνότητες των συστημάτων τους.

Η συγκεκριμένη επίθεση αντιλαμβανόμαστε ότι είναι πολύ «βαριά» για το σύστημά μας και ο επιτιθέμενος καταφέρνει να το βγάζει εκτός μέσω της επιβολής του ημιτονικού σήματος.

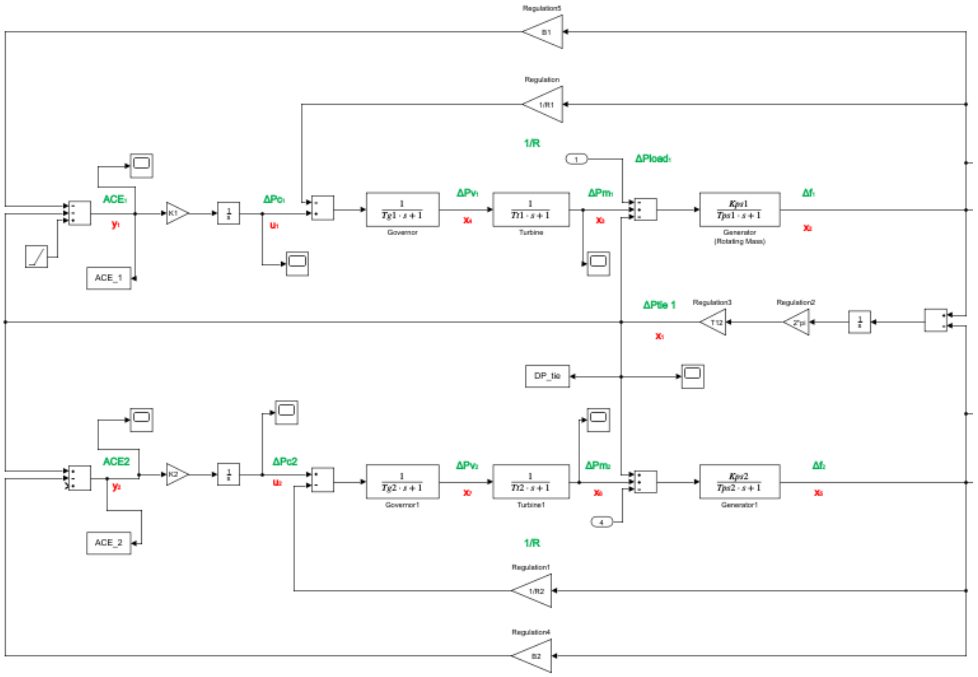
5.2.2.3.Περίπτωση Επίθεσης 3 : Ramp Attack στο σήμα ACE της περιοχής 1 στο κανάλι του Ενεργοποιητή

Στη συγκεκριμένη επίθεση, οι πραγματικές μετρήσεις τροποποιούνται σταδιακά με την προσθήκη μίας συνάρτησης ράμπας (ramp function) που σταδιακά αυξάνεται/μειώνεται με το χρόνο. Η εξίσωση που περιγράφει την συγκεκριμένη επίθεση είναι η εξής :

$$x_{final}(t) = x(t) + \lambda_A \cdot t$$

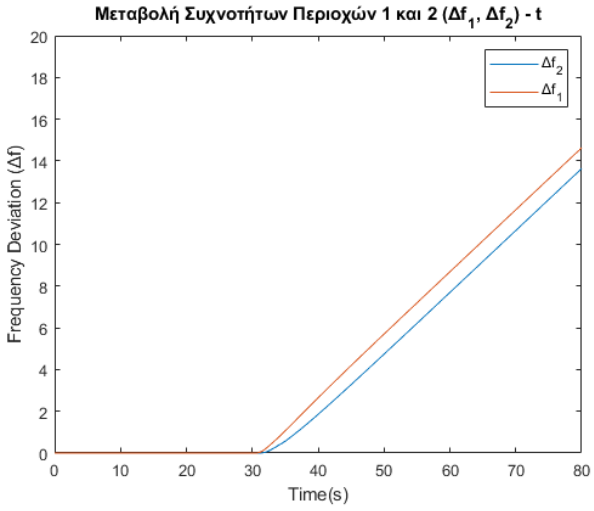
Όπου στα πειράματά μας λ_A = 0.5 (5.5)

Στο πλαίσιο των πειραμάτων μας πραγματοποιούμε την επίθεση στο κανάλι επικοινωνίας του σφάλματος ελέγχου της περιοχής 1, τη χρονική στιγμή t = 30sec, όπως απεικονίζεται στο παρακάτω σχήμα:



Σχήμα 5. 36 : Σύστημα Ρύθμισης Φορτίου -Συχνότητας υπό την επιβολή Επίθεσης Ράμπας στο κανάλι επικοινωνίας του κέντρου ελέγχου

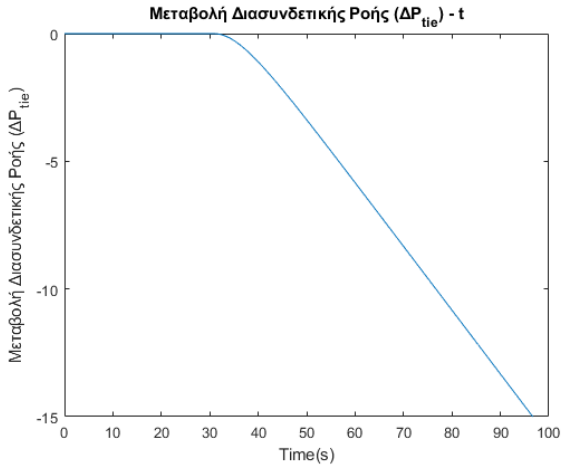
Οι χαρακτηριστικές μεταβολής συχνότητας (Δf_1, Δf_2) των δύο περιοχών, του σφάλματος ελέγχου περιοχής 1 και 2 (ACE_1, ACE_2), καθώς και της διασυνδετικής ροής (ΔP_{tie}) που προκύπτουν είναι οι παρακάτω :



Σχήμα 5. 37 : : Μεταβολές Συχνοτήτων Περιοχών 1 και 2 υπό επίθεση ράμπας με $\lambda_A = 0.5$

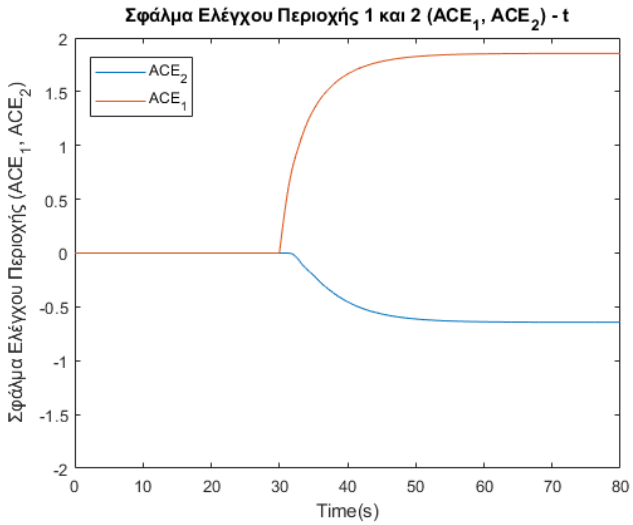
Μια επίθεση ράμπας εκτελείται όταν προσθέσουμε στο συνεχώς μεταβαλλόμενο ACE μια σταθερά. Κάτω από αυτήν την επίθεση, η απόκριση συχνότητας αυξάνεται κατά

0.5 με αυτή τη σταθερή κλίση και δεν μηδενίζεται ποτέ, καθιστώντας έτσι το σύστημα ασταθές όπως είδαμε, για $\lambda_A = 0.5$. Αντίστοιχη είναι η κατάσταση και στο σήμα μεταβολής της διασυνδετικής ροής του συστήματος, όπως φαίνεται παρακάτω.



Σχήμα 5. 38 : Μεταβολή Διασυνδετική Ροής υπό την επίδραση επίθεσης ράμπας στο κανάλι επικοινωνίας του κέντρου ελέγχου

Το σφάλμα ελέγχου περιοχής, όπως παρατηρούμε με βάση το παρακάτω σχήμα, δεν μηδενίζεται, πράγμα απολύτως λογικό δεδομένου ότι η συχνότητες των δύο συστημάτων συνεχώς αυξάνεται. Παρόλα αυτά σταθεροποιείται σε συγκεκριμένες τιμές, αφού η διαφορά των μεταβολών ($\Delta f_1 - \Delta f_2$) είναι σταθερή.



Σχήμα 5. 39 : Σφάλματα Ελέγχου Περιοχής 1 και 2 υπό επίδραση επίθεσης ράμπας κλίσης 0.5

5.2.2.4.Περίπτωση Επίθεσης 4 : Scaling Attack στο σήμα ACE της περιοχής 1

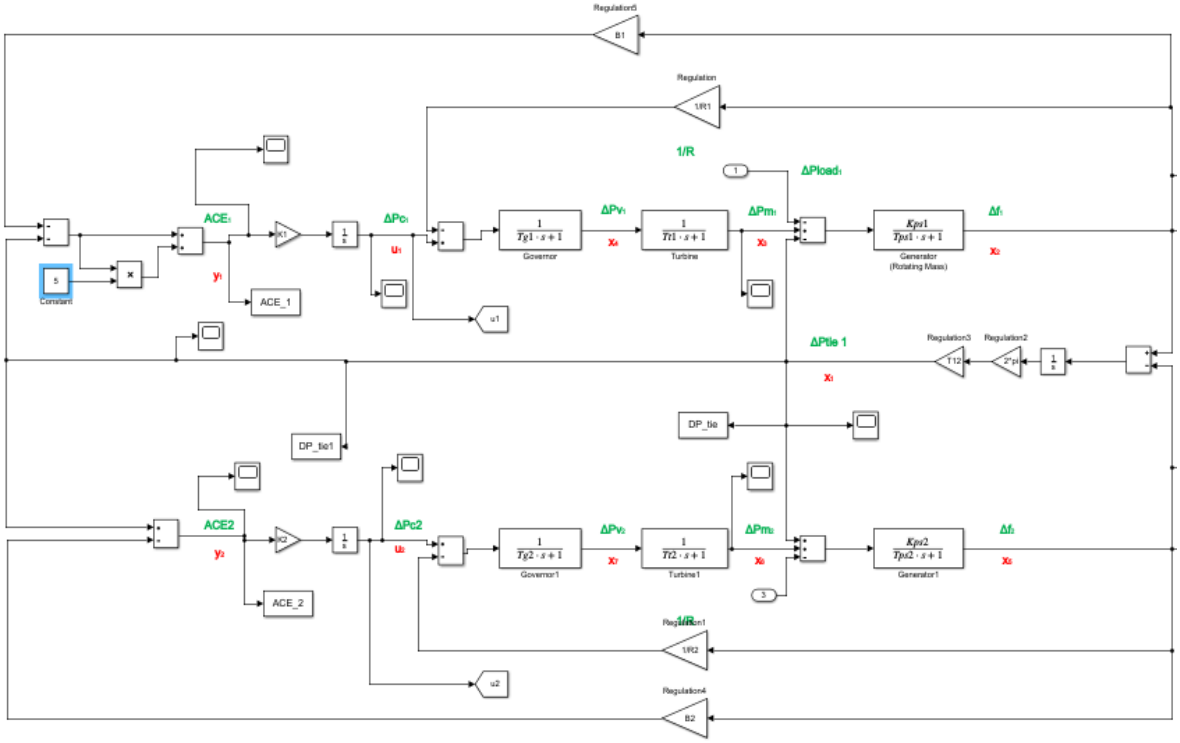
Στη συγκεκριμένη επίθεση οι πραγματικές μετρήσεις τροποποιούνται σε υψηλότερες ή χαμηλότερες τιμές, ανάλογα με την παράμετρο της επίθεσης. Η συνάρτηση της επίθεσης είναι :

$$x_{final}(t) = (1 + \lambda_A)\, x(t)$$

με $\lambda_A = 5$

(5.6)

Στο πλαίσιο των προσομοιώσεών μας πραγματοποιούμε την επίθεση σήμα του σφάλματος ελέγχου της περιοχής 1, τη χρονική στιγμή t = 30sec, όπως απεικονίζεται στο παρακάτω σχήμα:



Σχήμα 5. 40 : Σύστημα Ρύθμισης Φορτίου -Συχνότητας υπό την επιβολή Κλιμακούμενης Επίθεσης στο κανάλι επικοινωνίας του κέντρου ελέγχου της 1ης περιοχής

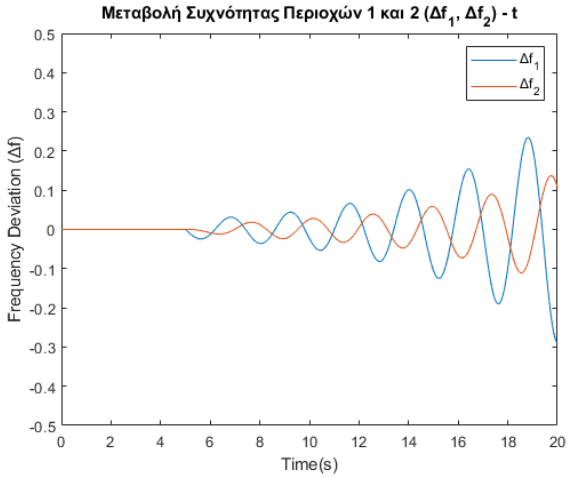
Στα πλαίσια των πειραμάτων μας λαμβάνουμε τις χαρακτηριστικές των σημάτων συχνότητας και ACE των δύο περιοχών, καθώς και της διασυνδετικής ροής του 2 φορές.

Αρχικά για το χρονικό διάστημα t = 0 – 20 sec κι εν συνεχεία στο χρονικό διάστημα t = 0 - 50 sec. Αυτό γιατί όπως θα δούμε στη συνέχεια η συγκεκριμένη επίθεση κλιμακώνεται συνεχώς όπως δηλώνει το όνομα της και η τάξη μεγέθους στην οποία

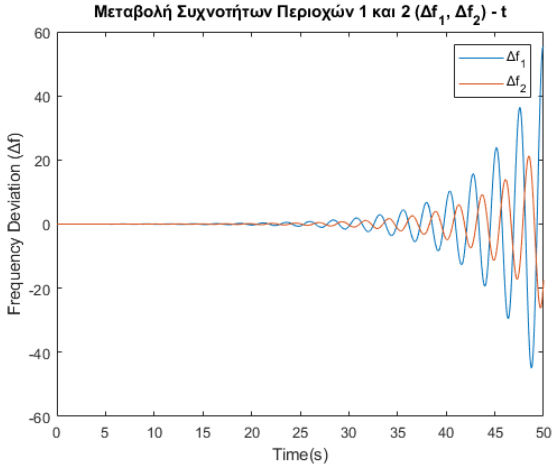
φτάνει μετά το πέρας 50 sec, δεν μας επιτρέπει να δούμε την αισθητή μεταβολή που ήδη υπάρχει μέχρι την t = 20 sec.

Έτσι για τη μελέτη της επίθεσης αυτής, προκαλούμε μια μεταβολή φορτίου στην περιοχή 1 και αμέσως μεταβάλουμε τις μετρήσεις του σήματος ACE που προκύπτουν μέσω του παράγοντα κλιμάκωσης $\lambda_A = 5$.

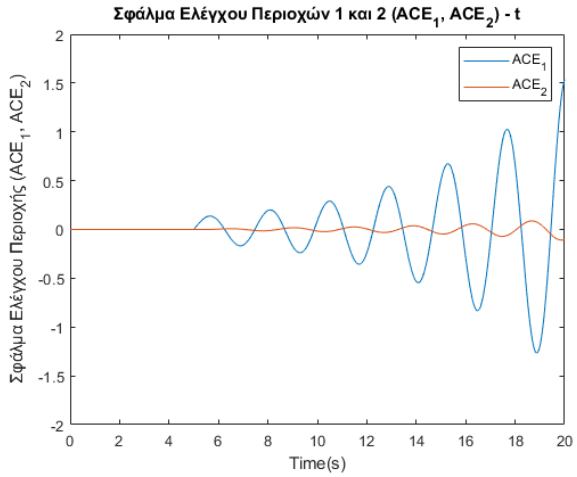
Οι χαρακτηριστικές μεταβολής συχνότητας (Δf_1, Δf_2) των δύο περιοχών, του σφάλματος ελέγχου περιοχής 1 και 2 (ACE_1, ACE_2), καθώς και της διασυνδετικής ροής (ΔP_{tie}) που προκύπτουν μετά την επίθεση, είναι οι παρακάτω :



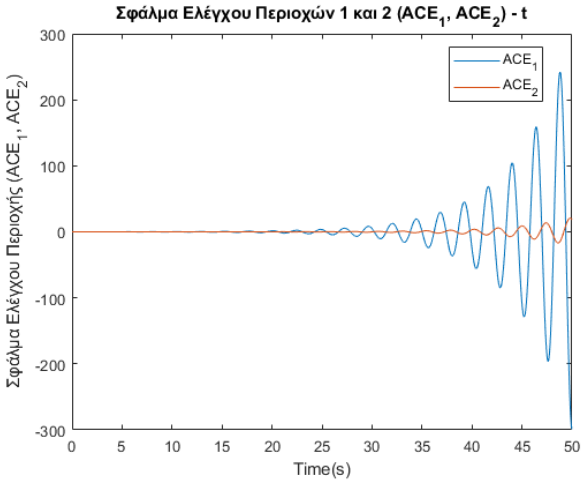
Σχήμα 5. 41: Μεταβολή Συχνοτήτων περιοχών 1 και 2 υπό την επίθεση κλιμακούμενης επίθεσης με $\lambda_A = 0.5$ για t = 0 - 20 sec



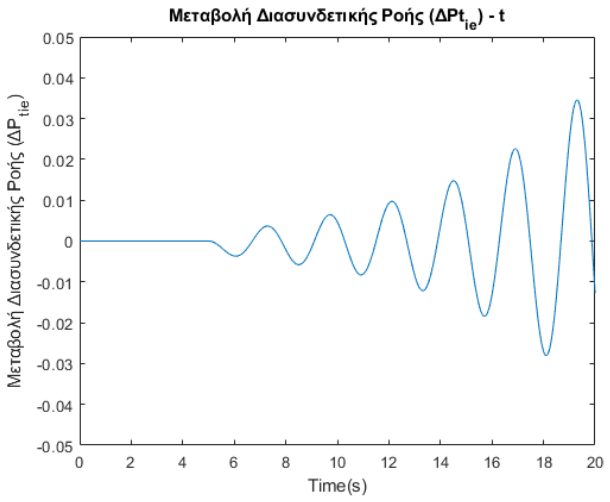
Σχήμα 5. 42 : Μεταβολή Συχνοτήτων περιοχών 1 και 2 υπό την επίθεση κλιμακούμενης επίθεσης με $\lambda_A = 0.5$ για t = 0 - 50 sec



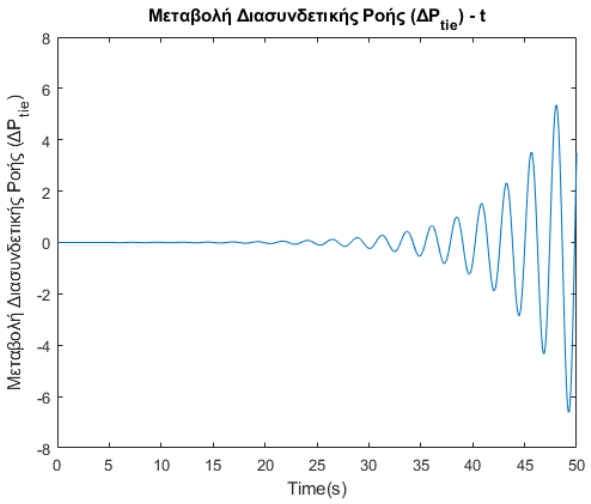
Σχήμα 5. 43: Σφάλμα Ελέγχου Περιοχών 1 και 2 υπό την επίθεση κλιμακούμενης επίθεσης με $\lambda_A = 0.5$ για t = 0 - 20 sec



Σχήμα 5. 44 : Σφάλμα Ελέγχου Περιοχών 1 και 2 υπό την επίθεση κλιμακούμενης επίθεσης με $\lambda_A = 0.5$ για t = 0 - 50 sec



Σχήμα 5. 45 : Μεταβολή Διασυνδετικής Ροής υπό την επίθεση κλιμακούμενης επίθεσης με $\lambda_A = 0.5$ για t = 0 - 20 sec



Σχήμα 5. 46: Μεταβολή Διασυνδετικής Ροής υπό την επίθεση κλιμακούμενης επίθεσης με $\lambda_A = 0.5$ για t = 0 - 50 sec

Παρατηρούμε σε όλα τα παραπάνω ότι μια κλιμάκωση του σήματος ACE στην περιοχή προκαλεί σχεδόν αμέσως ταλαντώσεις σε όλα τα σήματα, των οποίων τα πλάτη όλο και αυξάνουν. Το σύστημα προφανώς πηγαίνει σε αστάθεια και καταλαβαίνουμε πόσο επιδραστική είναι αυτού του τύπου η επίθεση για το σύστημα Ρύθμισης φορτίου – συχνότητας.

5.3. Προσομοιώσεις Ανίχνευσης Επιθέσεων Έγχυσης Ψευδών Δεδομένων στο σύστημα ρύθμισης Φορτίου – Συχνότητας

Η ανίχνευση των επιθέσεων έχει σκοπό την αντιμετώπισή με κατάλληλο τρόπο των επιθέσεων και βασίζεται στην παρατήρηση και η πρόβλεψη των δεδομένων. Στο κέντρο ελέγχου όπου εκτελείται η λειτουργία LFC, είναι διαθέσιμος ένας όγκος πληροφοριών και δεδομένων σε πραγματικό χρόνο από τα διάφορα είδη δεδομένων μέτρησης. Όταν το LFC υφίσταται επιθέσεις και δεν μπορεί να λάβει τα δεδομένα μέτρησης (για παράδειγμα, σε περίπτωση επίθεσης με χρονική καθυστέρηση), το κέντρο ελέγχου εκτελεί αμέσως τον αλγόριθμο εκτίμησης δεδομένων για να προβλέψει τα καθυστερημένα ή χαμένα δεδομένα προκειμένου να τα διαβιβάσει στο κέντρο ελέγχου.

Η επίθεση με ψευδείς εισαγωγές δεδομένων (FDIA), τις οποίες και μελετάμε στην παρούσα εργασία, είναι ένας από τους πιο σοβαρούς τύπους επιθέσεων στον κυβερνοχώρο, κατά τις οποίες ένας κακόβουλος εισβολέας μπορεί να θέσει σε κίνδυνο τα δίκτυα επικοινωνίας και να εισάγει ψευδή δεδομένα στο σύστημα LFC, κάτι το οποίο μπορεί να προκαλέσει τεράστια ζημιά στο σύστημα ισχύος []. Ως εκ τούτου, είναι πολύ σημαντικό να ανιχνευθούν και να εκτιμηθούν οι FDIAs που ενδέχεται να εμφανιστούν στο σύστημα LFC.

Έχουν υπάρξει αρκετές τεχνικές ανίχνευσης για FDIA σε συστήματα LFC, όπως έχουμε αναφέρει στο κεφάλαιο 4. Στην παρούσα διπλωματική εργασία, επιχειρούμε να **ανιχνεύσουμε** μια πιθανή κυβερνοεπίθεση στο LFC χρησιμοποιώντας έναν παρατηρητή Luenberger μέσω του οποίου εκτιμούμε κάθε στιγμή τα δεδομένα που θέλουμε. Στην ουσία εκτιμούμε το σφάλμα εξόδου που προκύπτει ανάμεσα στην πραγματική τιμή εξόδου του συστήματος και την «παρατηρούμενη». Οι εξισώσεις του παρατηρητή:

$$\dot{\hat{x}}(t) = A\hat{x}(t) + Bu(t) + F\,\hat{f}_{FDI}(t) + L(y(t) - \hat{y}(t))$$

$$\hat{y}(t) = C\,\hat{x}(t)$$

όπου $\hat{x}(t)$ και $\hat{f}_{FDI}$ είναι τα διανύσματα εκτίμησης κατάστασης και επίθεσης και L ο πίνακας κέρδους του παρατηρητή.

Το σφάλμα εκτίμησης εξόδου $e_y(t)$:

$$e_y(t) = y(t) - \hat{y}(t)$$

5.3.1. Ανάλυση Πειραματικής Μεθόδου

Στα πλαίσια της διπλωματικής μας, οι επιθέσεις που δοκιμάζουμε να ανιχνεύσουμε, είναι Έγχυσης Ψευδών Δεδομένων (FDIAs) και συγκεκριμένα είναι οι τέσσερις των οποίων μελετήσαμε την επίδραση στη Ρύθμιση Φορτίου – Συχνότητας σε προηγούμενο κεφάλαιο (Bias Injection Attack, Additive Harmonic Attack, Ramp Attack, Scaling Attack). Για κάθε μία από αυτές τις επιθέσεις θα μελετήσουμε αν ο παρατηρητής μας πετυχαίνει ανίχνευση και κάτω από ποιες συνθήκες αυτό πραγματοποιείται.

Για την ανίχνευση λοιπόν, ελέγχουμε κάθε φορά τη χαρακτηριστική του σφάλματος εκτίμησης εξόδου που προκύπτει από το σύστημά μας και από τον εκτιμητή μας.

$$e_y(t) = y(t) - \hat{y}(t)$$

με $y = \Delta f_1$ $και$ $\hat{y} = \widehat{\Delta f_1}$.

Ο άξονας στον οποίο κινούνται οι προσομοιώσεις μας έχει ως εξής:

1) Αρχικά μελετάμε στο σύστημα ρύθμισης φορτίου συχνότητας μιας περιοχής (**Single Area LFC**) δύο τύπων επιθέσεις:

   A. Έγχυσης ενός παράγοντα (Bias) στις συχνοτικές μετρήσεις και
   B. Επίθεση Ράμπας (Ramp Attack) στο κανάλι επικοινωνίας του ενεργοποιητή.

Για κάθε τύπο από τους παραπάνω, μελετάμε το σφάλμα εξόδου σε δύο κύριους άξονες. Αρχικά ελέγχουμε αν ο παρατηρητής μας αντιλαμβάνεται μέσω του σφάλματος τη μεταβολή που συμβαίνει (είτε είναι απλή διαταραχή φορτίου ΔP_L, είτε επίθεση) και

εν συνεχεία ελέγχουμε εάν μπορεί ο παρατηρητής μας να ξεχωρίσει το είδος της μεταβολής σε επίθεση ή σε απλή διαταραχή φορτίου.

2) Ακολουθούμε την ίδια διαδικασία για το σύστημα Ρύθμισης Φορτίου – Συχνότητας Δύο περιοχών (**Two Area LFC**). Εδώ οι επιθέσεις που ελέγχουμε είναι τεσσάρων τύπων
    A. Έγχυσης ενός παράγοντα (Bias) στις συχνοτικές μετρήσεις όπως στη μία περιοχή.
    B. Προσθετικές αρμονικές επιθέσεις (Additive Harmonic Attack) στις μετρήσεις της διασυνδετικής ροής.
    C. Επίθεση ράμπας (Ramp Attack) στο κανάλι επικοινωνίας του κέντρου ελέγχου της 1ης περιοχής.
    D. Κλιμακωτή Επίθεση (Scaling Attack) στο κανάλι επικοινωνίας του κέντρου ελέγχου της 1ης περιοχής

Για κάθε τύπο επίθεσης από τους παραπάνω, μελετάμε όπως και για τη μία περιοχή, το σφάλμα εξόδου της συχνότητας της πρώτης περιοχής σε δύο κύριους άξονες ακριβώς όπως κάνουμε και στη μελέτη ρύθμισης φορτίου συχνότητας στη μια περιοχή. Σκοπός μας σε όλα τα πειράματα που διενεργούμε είναι να παρατηρήσουμε τη χρονική στιγμή των μεταβολών, την απότομη μεταβατική μεταβολή του σφάλματος εξόδου και να εξάγουμε τα ανάλογα συμπεράσματα σχετικά με το είδος της μεταβολής και το την επιτυχή ή όχι λειτουργία αναγνώρισης κυβερνοεπίθεσης του παρατηρητή Luenberger.

5.3.2. Μελέτη Ανίχνευσης (Detection) σε Απομονωμένο Σύστημα Ρύθμισης Φορτίου – Συχνότητας

5.3.2.1. Μελέτη Ανίχνευσης (Detection) υπό την επιβολή επίθεσης έγχυσης παραγοντικού (Bias) όρου στις μετρήσεις της συχνότητας

Όπως αναφέραμε προηγουμένως, μελετάμε την περίπτωση που στο σύστημά μας μπορεί να πραγματοποιηθεί τόσο επίθεση όσο και μεταβολή φορτίου κανονικά και ελέγχουμε αν ο παρατηρητής μας μέσω του κριτηρίου που θέτουμε στην χαρακτηριστική του σφάλματος εξόδου, μπορεί να κάνει αναγνώριση της επίθεσης έναντι της διαταραχής του φορτίου.

Για την πραγματοποίηση των πειραμάτων αυτής της ενότητας έχουμε τις εξής παραδοχές:

- Οι μεταβολές φορτίου που μπορούν να πραγματοποιηθούν είναι:

$$\mathbf{\Delta P_L \leq 0.05 \ \alpha\mu \ (5\%)}$$

- Ο παράγοντας (bias) που εγχέουμε στις μετρήσεις τις συχνότητας είναι:

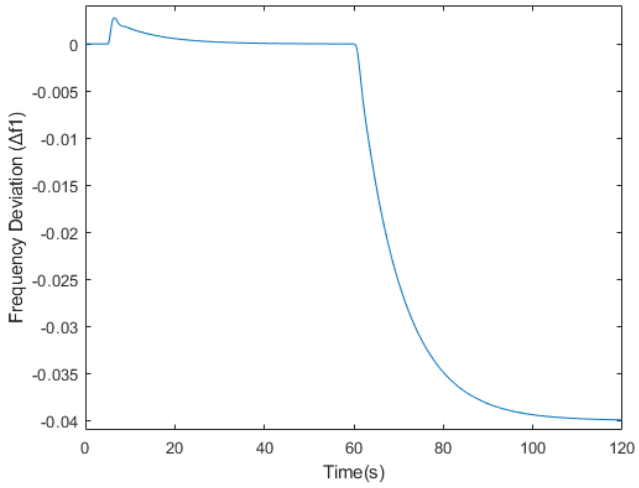
$$\mathbf{b \geq 0.05}$$

- Το όριο της ακαριαίας απότομης μεταβολής του σφάλματος, πάνω από το οποίο γίνεται αναγνώριση (detection) της επίθεσης είναι:

$$\|\boldsymbol{T_h}\| \geq \mathbf{0.85 \cdot 10^{-6}}$$

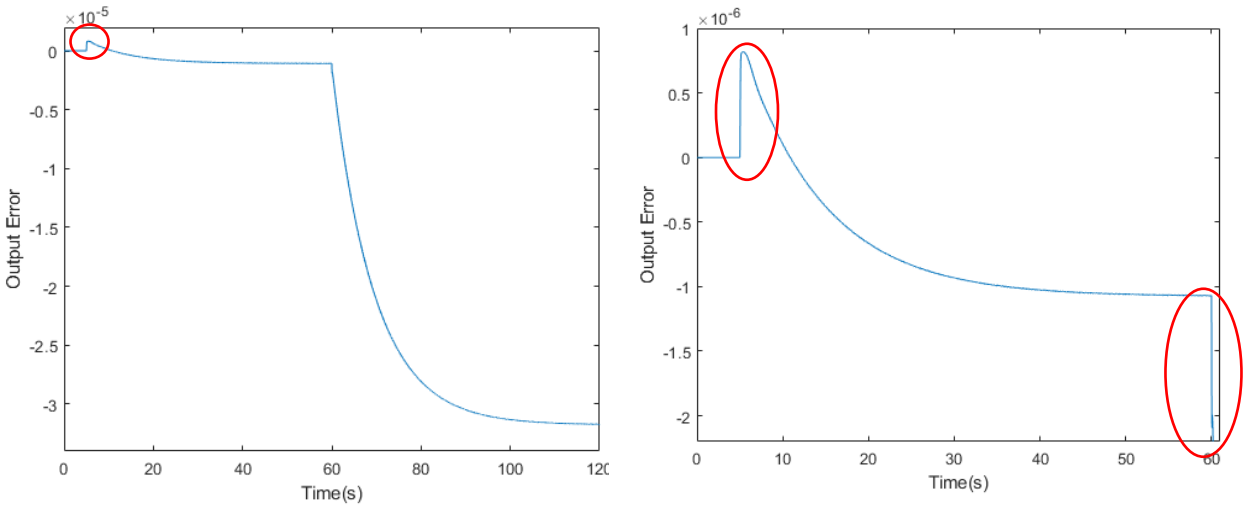
Τα όρια τόσο στη συγκεκριμένη περίπτωση, όσο και στις επόμενες προσομοιώσεις επιθέσεων, επιλέγονται έτσι καθώς για τη μεταβολή φορτίου θεωρούμε πως οι απότομες μεταβολές άνω του 5% είναι περισσότερο σπάνιες στα συστήματα ηλεκτρικής ενέργειας, ενώ για τον όρο "Bias", θεωρούμε πως σκοπός του επιτιθέμενου είναι να θέσει το σύστημα εντελώς εκτός λειτουργίας και όχι να του αφήσει κάποιο μόνιμο σφάλμα ή να το κάνει να υπολειτουργει / υπερλειτουργει. Το κατώφλι προκύπτει από πειραματική ανάλυση, παίρνοντας τις ακραίες τιμές των παραπάνω ορίων με σκοπό την αναγνώριση των επιθέσεων σε σχέση με τις απότομες διαταραχές

Τη χρονική στιγμή t = 5 sec πραγματοποιείται μια μεταβολή φορτίου στο σύστημά μας ΔP_L = 0.05 αμ, δηλαδή η ανώτερη τιμή της, ενώ τη χρονική στιγμή t = 60 sec πραγματοποιούμε την επίθεση μας στα δεδομένα της συχνότητας, μέσω του παράγοντα b = 0.05 και παρατηρούμε τις χαρακτηριστικές που προκύπτουν.



Σχήμα 5. 47 : Μεταβολή συχνότητας περιοχής 1 έπειτα από μεταβολή φορτίου ΔP_L = 0.1 αμ την t = 5 sec και επίθεση έγχυσης ψευδών δεδομένων παράγοντα b>0.05 την t = 60 sec

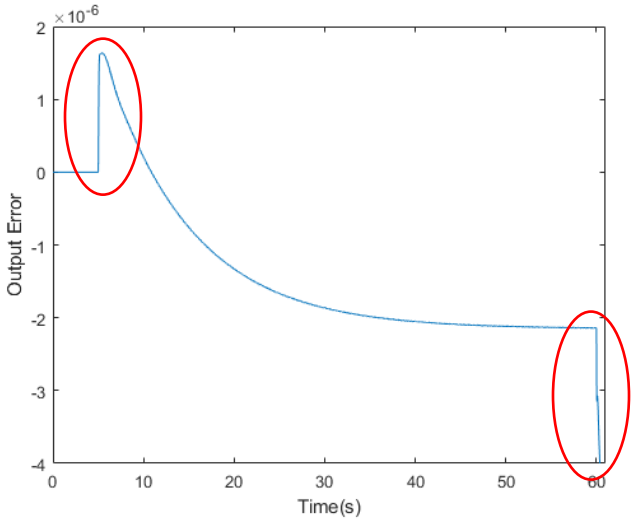
Από το παραπάνω διάγραμμα της συχνότητας, παρατηρούμε ότι ο δευτερεύοντας έλεγχος μετά τη μεταβολή του φορτίου, επαναφέρει επιτυχώς τη συχνότητα στην ονομαστική της τιμή, όπως περιμένουμε και έχουμε αναλύσει εκτενώς στα προηγούμενα κεφάλαια. Το ίδιο όμως δε συμβαίνει και μετά την έγχυση ψευδών δεδομένων, καθώς όπως παρατηρούμε παραμένει ένα μόνιμο σφάλμα μεγέθους 0.05 αμ, όσο και ο παράγοντας b.



Σχήμα 5. 48 : Χαρακτηριστική Σφάλματος Εξόδου Παρατηρητή έπειτα από μεταβολή φορτίου $\Delta P_L = 0.05$ αμ την $t = 5$ sec και επίθεση έγχυσης ψευδών δεδομένων παράγοντα $b = 0.05$ την $t = 60$ sec

Από τις παραπάνω γραφικές του σφάλματος εξόδου, παρατηρούμε ότι ακαριαία ξεπερνιέται το όριο του σφάλματος που έχουμε θέσει μόνο κατά την επίθεση. Επομένως η επίθεση αναγνωρίζεται αμέσως και ενεργοποιούνται οι απαραίτητοι συναγερμοί ανίχνευσης.

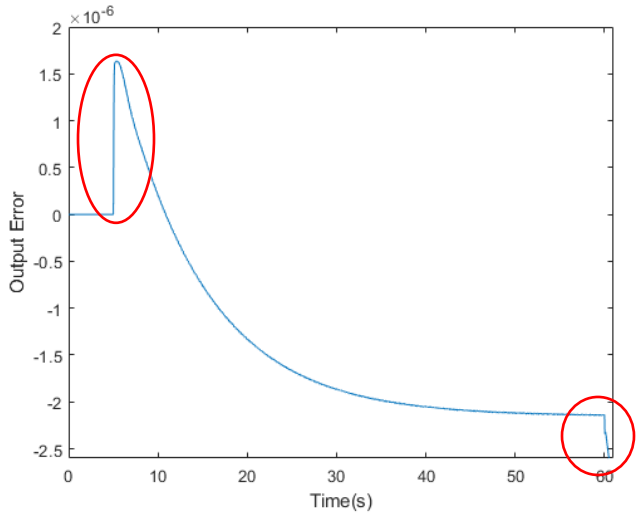
Η υπόθεση που κάνουμε σχετικά με τη μέγιστη αποδεκτή μεταβολή φορτίου για το σύστημα μας, καθορίζει και τα όριο (Threshold) πάνω από το οποίο ενεργοποιούνται οι συναγερμοί. Αν θεωρήσουμε μέγιστο αποδεκτό όριο της μεταβολής του φορτίου το 10 %, τότε το όριο $\|T_h\|$ μεγαλώνει, $\|\boldsymbol{T_h}\| \geq \mathbf{1.7 \cdot 10^{-6}}$, και όπως θα δούμε ακριβώς από κάτω, με $\mathbf{b \geq 0.05}$, πάλι το όριο αυτό ξεπερνιέται και η επίθεση αναγνωρίζεται.



Σχήμα 5. 49 : Χαρακτηριστική Σφάλματος Εξόδου Παρατηρητή έπειτα από μεταβολή φορτίου $\Delta P_L = 0.1$ αμ την $t = 5$ sec και επίθεση έγχυσης ψευδών δεδομένων παράγοντα $b>0.05$ την $t = 60$ sec

- Το πρόβλημα της αναγνώρισης υπάρχει όμως για $\mathbf{b \leq 0.05}$, όπου η επίθεση δεν αναγνωρίζεται ακαριαία, αφού σε αυτήν την περίπτωση η απότομη μεταβολή της διαταραχής είναι μεγαλύτερη από αυτήν της επίθεσης και δεν μπορούμε να

ξέρουμε αν η μεταβολή που αντιλαμβάνεται ο παρατηρητής μας είναι μια επίθεση ή μια απλή διαταραχή φορτίου.



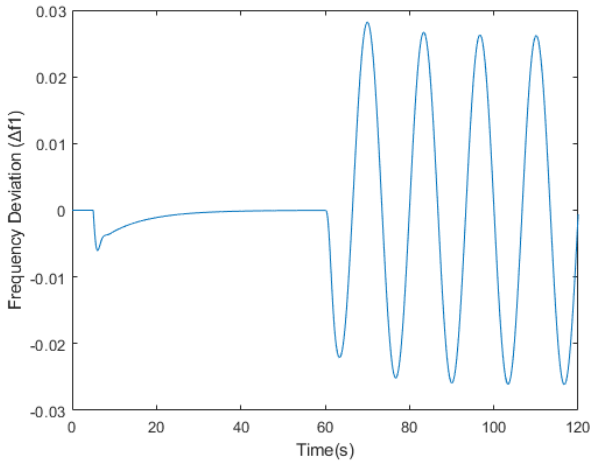
Σχήμα 5. 50 : Χαρακτηριστική Σφάλματος Εξόδου Παρατηρητή έπειτα από μεταβολή φορτίου ΔP_L = 0.1 αμ την t = 5 sec και επίθεση έγχυσης ψευδών δεδομένων παράγοντα b<0.05 την t = 60 sec

- Επομένως ο παρατηρητής Luenberger αναγνωρίζει τις επιθέσεις αυτού του τύπου (Bias Injection Attacks) σε σχέση με μια απλή μεταβολή στο φορτίο για **b ≥ 0.05.**

5.3.2.2. Μελέτη Ανίχνευσης υπό την επιβολή προσθετικής αρμονικής επίθεσης (Additive Harmonic Attack) στο κέντρο ελέγχου της περιοχής

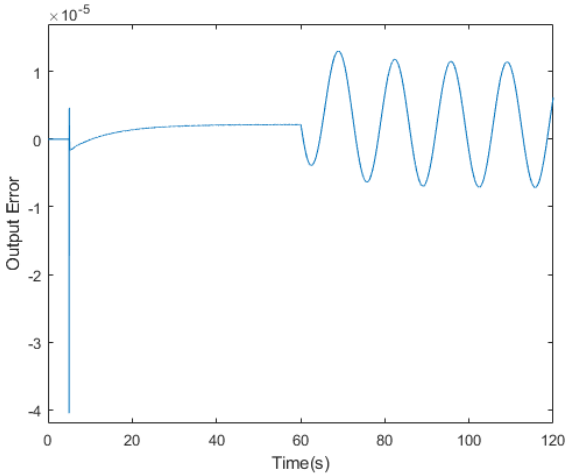
Σε αυτήν την ενότητα μελετάμε την περίπτωση προσθετικής ημιτονικής επίθεσης στο κανάλι επικοινωνίας του κέντρου ελέγχου και του συστήματος. Θεωρούμε ότι μπορεί να πραγματοποιηθεί τόσο επίθεση όσο και μεταβολή φορτίου κανονικά και ελέγχουμε αν ο παρατηρητής μας μέσω του κριτηρίου που θέτουμε στην χαρακτηριστική του σφάλματος εξόδου, μπορεί να κάνει αναγνώριση της επίθεσης έναντι της διαταραχής του φορτίου.

Για την πραγματοποίηση των προσομοιώσεων αυτής της ενότητας εξετάζουμε την περίπτωση κατά την οποία έχουμε μεταβολή φορτίου ΔP_L = 0.1 αμ. τη χρονική στιγμή t = 5 sec. και επιβολή ημιτονικής αρμονικής επίθεσης τη χρονική στιγμή t = 60 sec. Με τα δεδομένα αυτά λαμβάνουμε τις εξής χαρατκηριστικές:



Σχήμα 5. 51 : Μεταβολή Συχνότητας Περιοχής 1, έπειτα από μεταβολή φορτίου ΔP_L = 0.1 αμ. τη χρονική στιγμή t = 5 sec. και επιβολή ημιτονικής αρμονικής επίθεσης τη χρονική στιγμή t = 60 sec

Από την παραπάνω χαρακτηριστική της συχνότητας της περιοχής, παρατηρούμε αρχικά πως με την διαταραχή του φορτίου τη χρονική στιγμή t = 5 sec, η συχνότητα επανέρχεται στην ονομαστική της τιμή γρήγορα και χωρίς κάποια ακραία μεταβολή στη μεταβατική συχνότητα. Αντίθετα με την επιβολή της ημιτονικής επίθεσης παρατηρούμε ότι η συχνότητα του συστήματός μας ταλαντώνεται αενάως, με αποτέλεσμα να οδηγείται σε αστάθεια. Όπως ήδη αναφέραμε στο προηγούμενο κεφάλαιο που μελετήσαμε τις επιθέσεις αναλυτικά αυτή η διαταραχή, ανεξαρτήτως του πλάτους της, θα οδηγήσει το σύστημα μας σε αστάθεια καθώς δεν είναι δυνατό να αντέξει τις συνεχείς ταλαντώσεις στις οποίες θα επιβάλλεται συνεχώς.



Σχήμα 5. 52: Χαρακτηριστική Σφάλματος Εξόδου Παρατηρητή έπειτα από μεταβολή φορτίου ΔP_L = 0.1 αμ. τη χρονική στιγμή t = 5 sec. και επιβολή ημιτονικής αρμονικής επίθεσης τη χρονική στιγμή t = 60 sec

Μελετώντας την χαρακτηριστική του σφάλματος εξόδου ακριβώς από πάνω θα εξάγουμε συμπεράσματα σχετικά με την ανίχνευση της παραπάνω ανίχνευσης.

Η μέθοδος ανίχνευσής μας στηρίζεται στο μέγεθος της απότομης μεταβολής του σφάλματος εξόδου του παρατηρητή Luenberger. Η φύση της συγκεκριμένης επίθεσης δεν είναι δυνατόν να ανιχνευθεί από τον παρατηρητή μας επειδή το σφάλμα μεταβάλλεται αρμονικά ακολουθώντας την ημιτονική μορφή της επίθεσης με w = 0.15 · π rad/sec, και δεν κάνει κάποια ακαριαία μετβαολή στο σφάλμα.

Επιπλέον παρατηρούμε ότι για $\Delta P_L = 0.1$, και A = 0.1, η απότομή μεταβολή του σφάλματος της διαταραχής φορτίου είναι πολύ μεγαλύτερη από αυτήν της επίθεσης και μία επίθεση με πολύ μεγαλύτερο πλάτος δε θα είχε νόημα, καθώς επιτυγχάνει το σκοπό της με πολύ μικρότερο.

5.3.3. Μελέτη Ανίχνευσης (Detection) Κυβερνοεπιθέσεων σε Σύστημα Ρύθμισης Φορτίου – Συχνότητας Δύο Περιοχών (Two Area LFC)

5.3.3.1. Μελέτη Ανίχνευσης (Detection) υπό την επιβολή επίθεσης έγχυσης παραγοντικού (Bias) όρου στις μετρήσεις της συχνότητας

Σε αυτήν την ομάδα προσομοιώσεων μελετάμε την περίπτωση που στο σύστημά μας μπορεί να πραγματοποιηθεί τόσο επίθεση όσο και μεταβολή φορτίου κανονικά και ελέγχουμε αν ο παρατηρητής μας μέσω κριτηρίων που θέτουμε στην χαρακτηριστική του σφάλματος εξόδου, μπορεί να κάνει αναγνώριση της επίθεσης έναντι της διαταραχής του φορτίου.

Για την πραγματοποίηση των προσομοιώσεων αυτής της ενότητας έχουμε τις εξής παραδοχές:

- Οι μεταβολές φορτίου που μπορούν να πραγματοποιηθούν είναι:

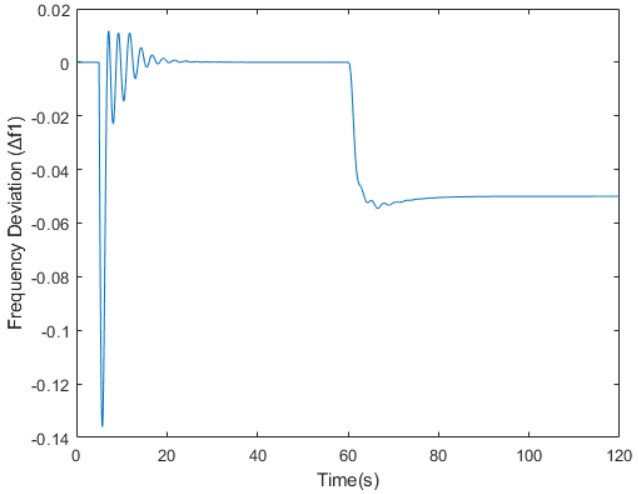
$$\mathbf{\Delta P_L \leq 0.05 \text{ αμ } (5\%)}$$

- Το όριο της ακαριαίας απότομης μεταβολής του σφάλματος, πάνω από το οποίο θα πρέπει να γίνεται αναγνώριση (detection) της επίθεσης για το παραπάνω ΔP_L είναι:

$$\mathbf{\|T_h\| \geq 14 \cdot 10^{-4}}$$

Με τα παραπάνω δεδομένα εξετάζουμε την περίπτωση κατά την οποία η έγχυση ψευδών δεδομένων παράγοντα b, αφήνουν μόνιμο σφάλμα στη συχνότητα που δεν βγάζει το σύστημα εκτός (δηλαδή $\pm$ 2.5 %). Αυτό συμβαίνει για **b = 0.1.**

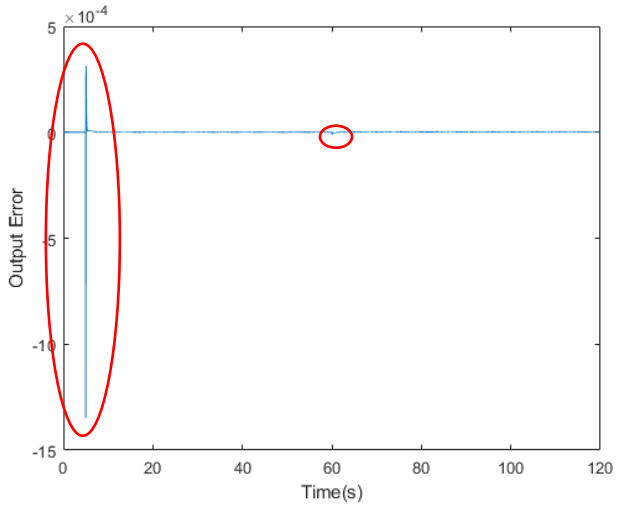
Τη χρονική στιγμή t = 5 sec πραγματοποιείται μια μεταβολή φορτίου στο σύστημά μας $\Delta P_L = 0.05$ αμ, δηλαδή η ανώτερη τιμή της, ενώ τη χρονική στιγμή t = 60 sec πραγματοποιούμε την επίθεση μας στα δεδομένα της συχνότητας, μέσω του παράγοντα b = 0.1 και παρατηρούμε τις χαρακτηριστικές που προκύπτουν.



Σχήμα 5. 53 : Μεταβολή συχνότητας περιοχής 1 έπειτα από μεταβολή φορτίου $\Delta P_L = 0.05$ αμ την t = 5 sec και επίθεση έγχυσης ψευδών δεδομένων παράγοντα b>0.05 την t = 60 sec

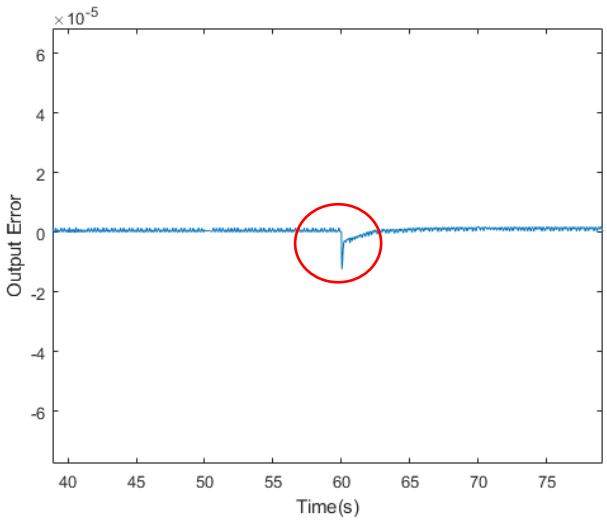
Παρατηρούμε το μόνιμο σφάλμα που αφήνει η επίθεση για b = 0.1. Όπως αναφέραμε εκτενώς και στο κεφάλαιο προσομοιώσεων επιθέσεων η συγκεκριμένη επίθεση ακυρώνει τον δευτερεύοντα έλεγχο μεν αλλά δεν θέτει το σύστημα εκτός για το συγκεκριμένο b.

Ελέγχουμε τώρα το σφάλμα εξόδου του παρατηρητή μας



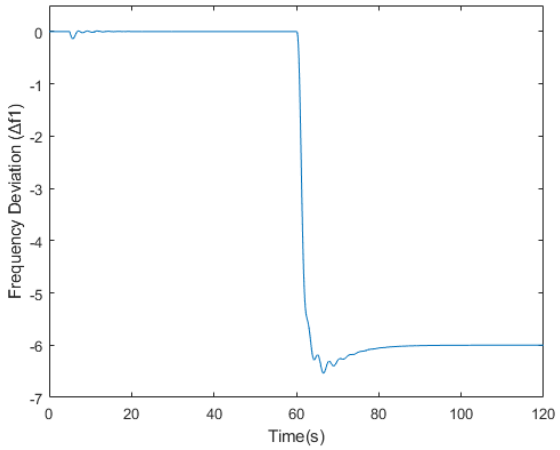
Σχήμα 5. 54 : Χαρακτηριστική Σφάλματος Εξόδου Παρατηρητή έπειτα από μεταβολή φορτίου $\Delta P_L = 0.05$ αμ. τη χρονική στιγμή t = 5 sec. και επιβολή επίθεσης έγχυσης ψευδών δεδομένων παράγοντα b = 0.1 τη χρονική στιγμή t = 60 sec

Εδώ παρατηρούμε ότι για τόσο μικρό b, ο παρατηρητής μας δεν μπορεί να ανιχνεύσει την επίθεση σε σχέση με την απλή διαταραχή του φορτίου. Παρόλα αυτά αν εστιάσουμε στη χρονική στιγμή t = 60 sec, θα δούμε πως αντιλαμβάνεται κάποια διαταραχή, χωρίς όμως να χρησιμοποιήσουμε το δεδομένο αυτό για να αποφανθούμε αν είναι επίθεση αυτή η διαταραχή.



Σχήμα 5. 55 : Χαρακτηριστική Σφάλματος Εξόδου Παρατηρητή έπειτα μόνο από επιβολή επίθεσης έγχυσης ψευδών δεδομένων παράγοντα b = 0.1 τη χρονική στιγμή t = 60 sec

Η ανίχνευση για $\mathbf{\Delta P_L \leq 0.05}$ **αμ,** θεωρείται επιτυχημένη μόνο όταν $\mathbf{b \geq 12}$.



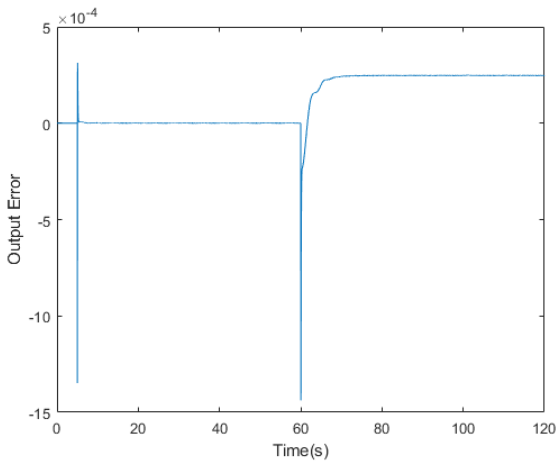
Σχήμα 5. 56 : Μεταβολή συχνότητας περιοχής 1 έπειτα από μεταβολή φορτίου ΔP_L = 0.05 αμ. τη χρονική στιγμή t = 5 sec. και επιβολή επίθεσης έγχυσης ψευδών δεδομένων παράγοντα b = 0.1 τη χρονική στιγμή t = 60 sec

Καταλαβαίνουμε ότι το σύστημα πηγαίνει σε αστάθεια και για πολύ μικρότερο b από αυτό που έχουμε, άρα και ότι ο επιτιθέμενος μπορεί να καταφέρει να πετύχει την επίθεση του και με πολύ μικρότερο παράγοντα.

Όμως για b ≥ 12 ο παρατηρητής μας μπορεί να αναγνωρίσει ότι πραγματοποιείται επίθεση και όχι κάποια μεταβολή (δεδομένου $\Delta P_L \leq 0.05$ αμ (5%)) όπως θα δούμε ακριβώς από κάτω, θεωρώντας το όριο της ακαριαίας απότομης μεταβολής του σφάλματος, πάνω από το οποίο γίνεται αναγνώριση (detection) της επίθεσης ως:

$$\|\boldsymbol{T_h}\| \geq \mathbf{14 \cdot 10^{-4}}$$

Γίνεται κατανοητό πως αν θεωρήσουμε ακόμα μεγαλύτερο ΔP_L, τότε για να ανιχνευθεί η επίθεση θα πρέπει ο παράγοντας b να είναι ακόμη μεγαλύτερος.



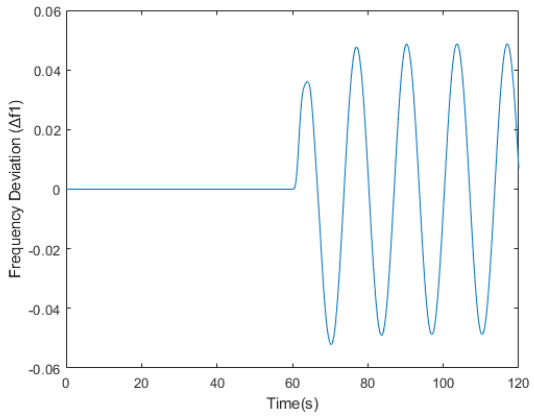
Σχήμα 5. 57: Χαρακτηριστική Σφάλματος Εξόδου Παρατηρητή έπειτα από μεταβολή φορτίου $\Delta P_L = 0.05$ αμ. τη χρονική στιγμή $t = 5$ sec. και επιβολή επίθεσης έγχυσης ψευδών δεδομένων παράγοντα $b = 12$ τη χρονική στιγμή $t = 60$ sec

5.3.3.2. Μελέτη Ανίχνευσης υπό την επιβολή προσθετικής αρμονικής επίθεσης (Additive Harmonic Attack) στις μετρήσεις της διασυνδετικής ροής ΔP_{tie}.

Θεωρούμε και πάλι ότι $\Delta P_L \leq 0.05$ αμ (5%) και ελέγχουμε την απόκριση του συστήματος για μία ημιτονική επίθεση $x_{final}(t) = x(t) + A_f \sin(wt + \varphi)$.

Όπως έχουμε ήδη αναφέρει όσο μεγαλύτερο το πλάτος του σήματος επίθεσης, τόσο μεγαλύτερες οι ταλαντώσεις και άρα τόσο πιο ασταθές το σύστημα.

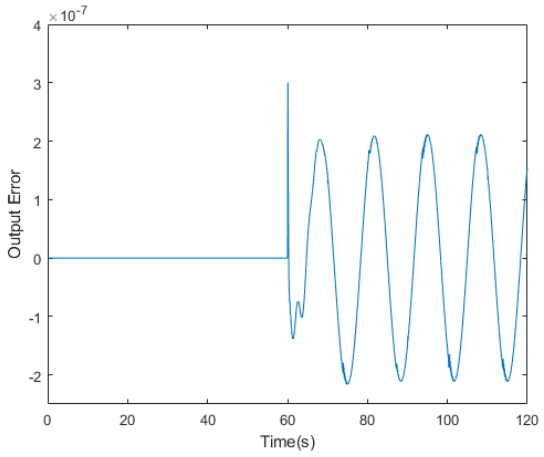
Ελέγχουμε την απόκριση του συστήματος μας για A = 0.15 την χρονική στιγμή t = 60 sec., ελέγχουμε την έξοδο του παρατηρητή και στη συνέχεια προσθέτουμε μια διαταραχή φορτίου ΔP_L τη χρονική στιγμή t = 5 sec. και παρατηρούμε τη χαρακτηριστική του σφάλματος εξόδου.



Σχήμα 5. 58: Μεταβολή συχνότητας περιοχής 1 έπειτα μόνο από επιβολή επίθεσης προσθετικής αρμονικής επίθεσης πλάτους $A = 0.15$ τη χρονική στιγμή $t = 60$ sec

Με A = 0.15 παρατηρούμε πως η συχνότητα δεν βγαίνει εκτός των ορίων (±2,5%), κάνει όμως ταλαντώσεις, γεγονός μη επιθυμητό για το σύστημά μας.

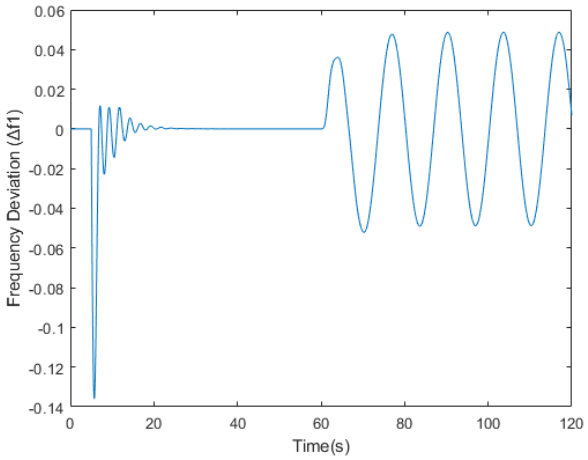
Η χαρακτηριστική του σφάλματος εξόδου :



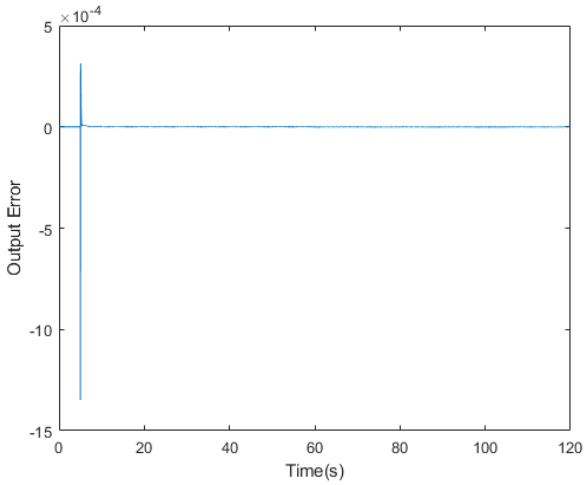
Σχήμα 5. 59 Χαρακτηριστική Σφάλματος Εξόδου Παρατηρητή έπειτα μόνο από επιβολή προσθετικής αρμονικής πλάτους A = 0.15 τη χρονική στιγμή t = 60 sec

Παρατηρούμε ότι χωρίς τη μεταβολή φορτίου και εστιάζοντας μόνο στην επίθεση, από το σφάλμα εξόδου, ορίζοντας ένα όριο ακαριαίας μεταβολής $\|\boldsymbol{T_h}\| \geq \mathbf{3 \cdot 10^{-7}}$ **,** μπορούμε να ανιχνεύσουμε ότι πραγματοποιείται μια επίθεση.

Προσθέτουμε τώρα μία διαταραχή φορτίου $\Delta P_L = 0.05$ και ελέγχουμε αν μπορεί να ανιχνεύσει ο παρατηρητής μας την επίθεση έναντι της απλής διαταραχής. Η τάξη μεγέθους του ορίου (Threshold) που λάβαμε πριν, μας προϊδεάζει ότι κάτι τέτοιο δεν είναι εφικτό, μένει όμως να το επιβεβαιώσουμε.



Σχήμα 5. 60: Μεταβολή συχνότητας περιοχής 1 έπειτα από μεταβολή φορτίου $\Delta P_L = 0.05$ αμ. τη χρονική στιγμή t = 5 sec. και επιβολή προσθετικής ημιτονικής επίθεσης πλάτους A = 0.15 τη χρονική στιγμή t = 60 sec

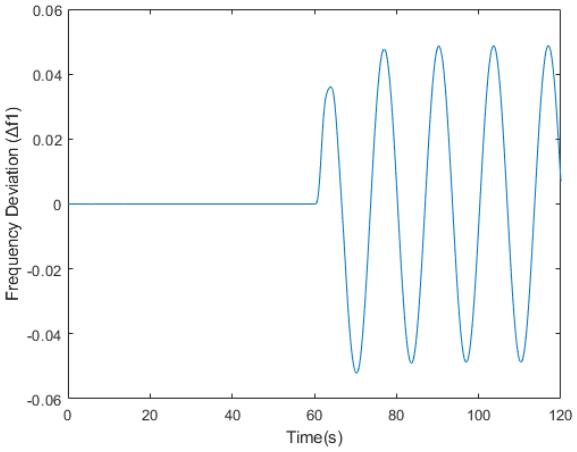


Σχήμα 5. 61 : Χαρακτηριστική Σφάλματος Παρατηρητή έπειτα από μεταβολή φορτίου $\Delta P_L = 0.05$ αμ. τη χρονική στιγμή $t = 5$ sec. και επιβολή προσθετικής αρμονικής επίθεσης πλάτους $A = 0.15$ τη χρονική στιγμή $t = 60$ sec

Πράγματι σε σχέση με τη μεταβολή φορτίου, για τη συγκεκριμένη επίθεση και μέσω του παρατηρητή Luenberger δεν γίνεται να ανιχνεύσουμε την επίθεση.

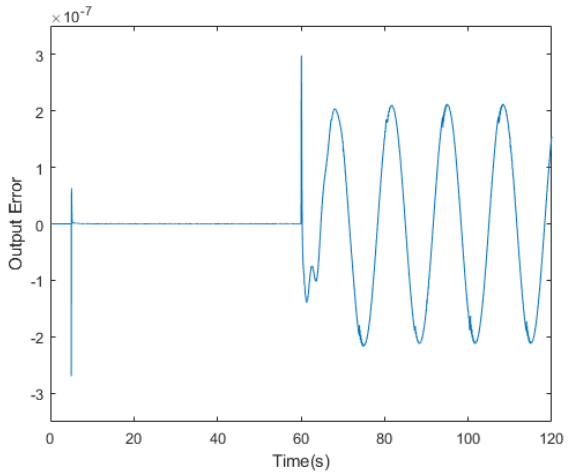
Κάτι τέτοιο θα ήταν εφικτό, μόνο σε δύο ακραία σενάρια.

Α) Αν θεωρούσαμε $\Delta P_L \leq 0.00001$ αμ :



Σχήμα 5. 62: Μεταβολή συχνότητας περιοχής 1 έπειτα από μεταβολή φορτίου $\Delta P_L = 0.00001$ αμ. τη χρονική στιγμή $t = 5$ sec. και επιβολή προσθετικής ημιτονικής επίθεσης πλάτους $A = 0.15$ τη χρονική στιγμή $t = 60$ sec

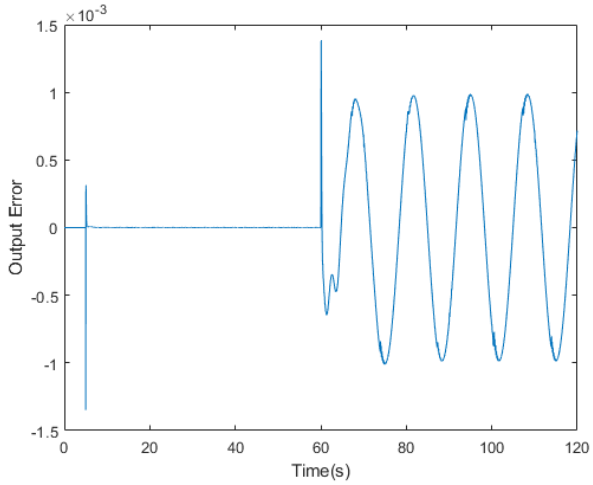
Παρατηρούμε ότι η μεταβολή φορτίου είναι τόσο μικρή που δεν αναγνωρίζεται καν ως διαταραχή για το σύστημα. Παρόλα αυτά για αυτήν την υπόθεση και μόνο και θεωρώντας $\|\boldsymbol{T_h}\| \geq \mathbf{28 \cdot 10^{-6}}$ γίνεται επιτυχώς η αναγνώριση όπως βλέπουμε στο σχήμα ακριβώς από κάτω.



Σχήμα 5. 63: Χαρακτηριστική Σφάλματος Εξόδου Παρατηρητή έπειτα από μεταβολή φορτίου ΔP_L = 0.00001 αμ. τη χρονική στιγμή t = 5 sec. και επιβολή προσθετικής αρμονικής επίθεσης πλάτους A = 0.15 τη χρονική στιγμή t = 60 sec

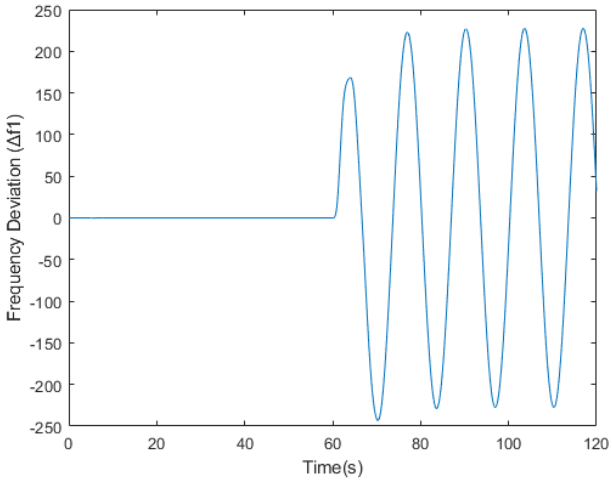
Β) Αν θεωρούσαμε Α ≥ 700 :

Με την υπόθεση ότι $\Delta P_L \leq 0.5$ αμ και πλάτος επίθεσης A = 700, παίρνουμε την εξής χαρακτηριστική σφάλματος εξόδου:



Σχήμα 5. 64: Χαρακτηριστική Σφάλματος Εξόδου Παρατηρητή έπειτα από μεταβολή φορτίου ΔP_L = 0.05 αμ. τη χρονική στιγμή t = 5 sec. και επιβολή προσθετικής αρμονικής επίθεσης πλάτους A = 700 τη χρονική στιγμή t = 60 sec

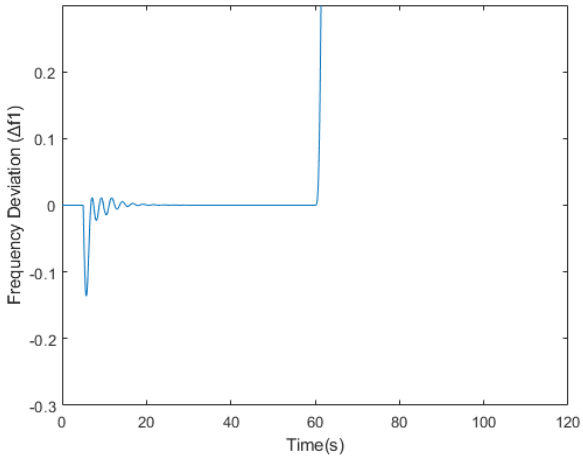
Επομένως για αυτήν την περίπτωση, με $\|\boldsymbol{T_h}\| \geq \mathbf{1{,}3 \cdot 10^{-3}}$ γίνεται αναγνώριση της επίθεσης. Όμως όπως θα δούμε και ακριβώς από κάτω ένα τέτοιο σενάριο είναι μη ρεαλιστικό καθώς ο επιτιθέμενος δεν έχει κανέναν λόγο να στείλει σήμα με τόσο μεγάλο πλάτος τη στιγμή που μπορεί να πετύχει το σκοπό του με πολύ μικρότερο.



Σχήμα 5. 65: Μεταβολή συχνότητας περιοχής 1 έπειτα από μεταβολή φορτίου ΔP_L = 0.05 αμ. τη χρονική στιγμή t = 5 sec. και επιβολή προσθετικής ημιτονικής επίθεσης πλάτους A = 700 τη χρονική στιγμή t = 60 sec

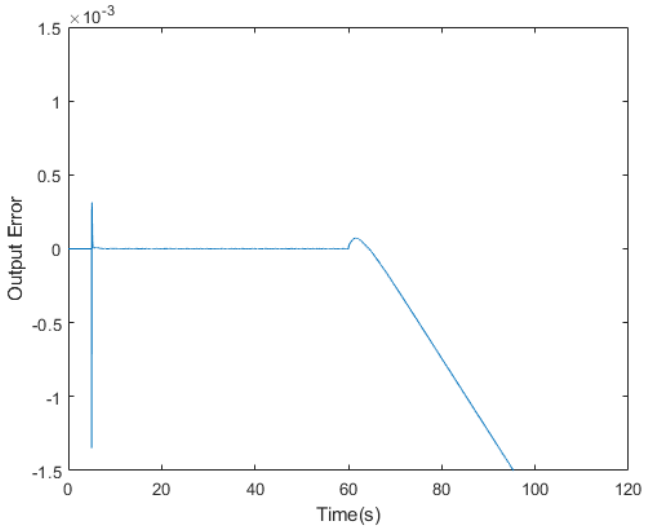
5.3.3.3. Μελέτη Ανίχνευσης υπό την επιβολή επίθεσης ράμπας (Ramp Attack) στο κανάλι επικοινωνίας του κέντρου ελέγχου της 1ης περιοχής.

Σε αυτήν την ομάδα προσομοιώσεων θεωρούμε με $\Delta P_L \leq 0.5$ αμ, κλίση (slope) s = 2 και πραγματοποιούμε τη χρονική στιγμή t = 5 sec και t = 60 sec μεταβολή φορτίου ΔP_L και επίθεση ράμπας (Ramp Attack) αντίστοιχα. Το διάγραμμα συχνότητας που προκύπτει είναι το εξής :



Σχήμα 5. 66: Μεταβολή συχνότητας περιοχής 1 έπειτα από μεταβολή φορτίου ΔP_L = 0.05 αμ. τη χρονική στιγμή t = 5 sec. και επιβολή επίθεσης ράμπας κλίσης (slope) s = 2, τη χρονική στιγμή t = 60 sec

Παρατηρούμε ότι σχεδόν ακαριαία το σύστημα βγαίνει εκτός. Επομένως είναι αναγκαίο να γίνεται η ανίχνευση ακαριαία. Γι' αυτό ελέγχουμε την χαρακτηριστική του σφάλματος εξόδου και βγάζουμε τα ανάλογα συμπεράσματα.



Σχήμα 5. 67: Χαρακτηριστική Σφάλματος Εξόδου Παρατηρητή έπειτα από μεταβολή φορτίου ΔP_L = 0.05 αμ. τη χρονική στιγμή t = 5 sec. και επιβολή επίθεσης ράμπας, κλίσης (slope) s = 2 τη χρονική στιγμή t = 60 sec

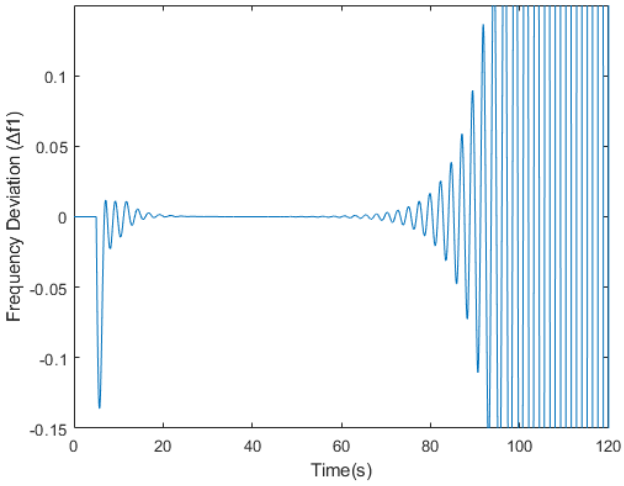
Παρατηρούμε ότι η ακαριαία μεταβολή του σφάλματος της επίθεσης (που έχει ήδη αρκετά μεγάλη κλίση και δεν έχει νόημα να θεωρήσουμε ακόμη μεγαλύτερη) είναι μικρότερη από την ακαριαία μεταβολή του σφάλματος εξόδου για την μεταβολή φορτίου ΔP_L.

Επομένως για τον συγκεκριμένο τύπο επίθεσης δεν είναι επιτυχημένη η χρήση του παρατηρητή Luenberger, καθώς ανίχνευση μπορεί να γίνει μόνο αν θεωρήσουμε ΔP_L πάρα πολύ μικρό (πράγμα αδύνατο) ή κλίση (Slope) παρα πολύ μεγαλύτερη που πάλι δεν έχει νόημα για τον επιτιθέμενο.

5.3.3.4. Μελέτη Ανίχνευσης υπό την επιβολή κλιμακούμενης επίθεσης (Scaling Attack) στο κανάλι επικοινωνίας του κέντρου ελέγχου της 1ης περιοχής.

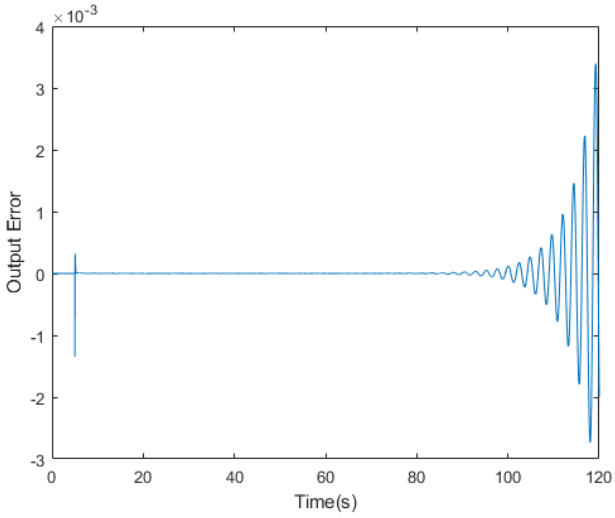
Σε αυτό το κεφάλαιο μελετάμε τη δυνατότητα ανίχνευσης της κλιμακούμενης επίθεσης (Scaling Attack) μέσω του παρατηρητή Luenberger. Για τις προσομοιώσεις μας θεωρούμε $\Delta P_L \leq 0.5$ αμ.

Τη χρονική στιγμή t = 5 sec πραγματοποιείται μια μεταβολή φορτίου στο σύστημά μας ΔP_L = 0.05 αμ, δηλαδή η ανώτερη τιμή της, ενώ τη χρονική στιγμή t = 40 sec πραγματοποιούμε την κλιμακούμενη επίθεση στο κανάλι επικοινωνίας του κέντρου ελέγχου, με παράγοντα scaling λ = 5 και ελέγχουμε τη συχνότητα.



Σχήμα 5. 68: Μεταβολή συχνότητας περιοχής 1 έπειτα από μεταβολή φορτίου ΔP_L = 0.05 αμ. τη χρονική στιγμή t = 5 sec. και επιβολή κλιμακούμενης επίθεσης κλίσης λ = 5, τη χρονική στιγμή t = 40 sec

Η επίθεση ξεκινά στα 40 sec, όμως γίνεται εμφανής η επίδρασή της μετά τα 70 sec. Θα πρέπει λοιπόν ο παρατηρητής να μας δείχνει ότι συμβαίνει επίθεση μέχρι εκείνη τη χρονική στιγμή ώστε να θεωρείται χρήσιμος.



Σχήμα 5. 69: Χαρακτηριστική Σφάλματος Εξόδου Παρατηρητή έπειτα από μεταβολή φορτίου ΔP_L = 0.05 αμ. τη χρονική στιγμή t = 5 sec. και επιβολή κλιμακούμενης επίθεσης κλίσης λ = 5 τη χρονική στιγμή t = 40 sec

Κάτι τέτοιο δε φαίνεται να ισχύει καθώς από την χαρακτηριστική του σφάλματος εξόδου, βλέπουμε πως η επίθεση καθυστερεί πολύ να γίνει αντιληπτή.

Επιθέσεις με λ < 5 δεν γίνονται αντιληπτές εντός των 120 sec που εμείς μελετάμε, ενώ όσο μεγαλύτερο γίνεται το λ, τόσο πιο γρήγορα γίνεται το σύστημα ασταθές.

6. Γενικά συμπεράσματα και προτάσεις για περαιτέρω έρευνα

6.1.Γενικά Συμπεράσματα

Στην παρούσα εργασία μελετήσαμε τη ρύθμιση φορτίου - συχνότητας ενός συστήματος παραγωγής μίας (Single Area LFC) και δύο (Two Area LFC) περιοχών και τον αντίκτυπο πιθανών κακόβουλων επιθέσεων έγχυσης ψευδών δεδομένων που μπορούν να πραγματοποιηθούν σε αυτά. Στη συνέχεια χρησιμοποιήσαμε έναν απλό παρατηρητή Luenberger με σκοπό την ανίχνευση των επιθέσεων αυτών και καταλήξαμε στα ακόλουθα συμπεράσματα :

- Η δομή των συστημάτων Ρύθμισης Φορτίου – Συχνότητας αποτελείται από πολλά κανάλια επικοινωνίας, τα οποία μεταφέρουν πολύ σημαντικές πληροφορίες για το ίδιο το σύστημα, όπως οι μετρήσεις της συχνότητας και της ισχύος του συστήματος, οι μετρήσεις της διασυνδετικής ροής εφόσον αναφερόμαστε σε συστήματα δύο ή περισσοτέρων περιοχών, αλλά και οι εντολές που εξέρχονται του κέντρου ελέγχου με κατεύθυνση το φυσικό σύστημα. Όπως επιβεβαιώσαμε πειραματικά, οι επιθέσεων Έγχυσης Ψευδών δεδομένων, σε αυτά τα κανάλια μπορούν να αποβούν μοιραία για το σύστημα μάς, το οποίο είτε μπορεί να υπολειτουργεί/υπερλειτουργεί σε λάθος συχνότητες λειτουργίας, είτε να καταρρεύσει (Black Out), είτε ακόμη και να καταστραφεί. Επομένως κατανοήσαμε τη σημαντικότητα της έγκαιρης και έγκυρης ανίχνευσης των επιθέσεων αυτών και για τον λόγο αυτόν μελετήσαμε την επίδραση ενός παρατηρητή Luenberger στην προσπάθεια ανίχνευσης των συγκεκριμένων κυβερνοεπιθέσεων.

- Ο παρατηρητής Luenberger είναι ένας αρκετά εύκολα υλοποιήσιμος και οικονομικός σε υλοποίηση παρατηρητής, καθώς η μέθοδος που ακολουθείται για την κατασκευή του είναι παρόμοια με τη μέθοδο ελέγχου μέσω τοποθέτησης πόλων. Απαιτείται η εύρεση ενός πίνακα κερδών L όπως ακριβώς

στον έλεγχο μέσω τοποθέτησης πόλων η εύρεση του πίνακα κερδών K. Τα κέρδη αυτά του παρατηρητή είναι μικρότερα σε μέγεθος και ποσότητα, γεγονός που τον καθιστά ελκυστικό παρατηρητή για μελέτη.

- Από τις προσομοιώσεις μας με τον συγκεκριμένο παρατηρητή, διαπιστώσαμε πως στο σύστημα ρύθμισης φορτίου – συχνότητας της μίας περιοχής, ο παρατηρητής μας μπορεί επιτυχημένα να ανιχνεύσει ακαριαία την παρουσία επίθεσης σε σχέση με την απλή διαταραχή φορτίου, γεγονός που τον καθιστά ιδιαίτερα χρήσιμο σε απλά συστήματα.

- Αντίθετα, στο σύστημα δύο περιοχών, ναι μεν ανιχνεύει ότι κάτι συμβαίνει, δεν μπορεί όμως να ξεχωρίσει αν αυτή η απότομη μεταβολή κατάστασης είναι επίθεση ώστε να ενεργοποιήσει τους συναγερμούς ή μια απλή διαταραχή φορτίου. Πιο συγκεκριμένα για τις κλιμακούμενες, τις αρμονικές και τις επιθέσεις ράμπας, που η μεταβολή δεν γίνεται απότομα όπως με την έγχυση ενός παράγοντα (Bias) στις μετρήσεις, ο παρατηρητής δεν μπορεί να μας δώσει μέσω του σφάλματος εξόδου συμπέρασμά για το αν πραγματοποιείται επίθεση καθώς η ακαριαία μεταβολή του σφάλματος που μελετάμε είναι αρκετά μικρότερη από την ακαριαία μεταβολή του σφάλματος κατά την επίδραση μιας απλής διαταραχής φορτίου.

- Παρατηρούμε επίσης πως ο έλεγχος ανίχνευσης μέσω ενός απλού παρατηρητή Luenberger είναι επιτυχής για της επιθέσεις έγχυσης ενός παράγοντα (bias) στις μετρήσεις, ακόμη και σε πιο πολύπλοκα συστήματα όπως των δύο περιοχών. Δεν είναι όμως για τις υπόλοιπες επιθέσεις που μελετήσαμε. Μόνο εάν θέσουμε κάποια πολύ αυστηρά κριτήρια που ξεπερνούν τα όρια του ρεαλισμού και της λογικής τόσο των επιτιθέμενων όσο και της ίδιας της δομής και λειτουργίας του συστήματος μας, μπορεί ο παρατηρητής μας να ανιχνεύσει τις συγκεκριμένου τύπου επιθέσεις. (π.χ. τεράστιο πλάτος ημιτονικού σήματος, τεράστια κλίση κλιμακούμενων επίθέσεω, αποδοχή πως το σύστημα μπορεί να δεχτεί πολύ μικρές μεταβολές φορτίου κλπ).

6.2.Προτάσεις για περαιτέρω έρευνα

- Αρχικά όσον αφορά το σύστημα της ρύθμισης φορτίου – συχνότητας, έχουμε θεωρήσει γραμμικά συστήματα δίχως αβεβαιότητες και άγνωστες διαταραχές, όπως επίσης και συστήματα μιας και δύο περιοχών. Επομένως είναι λογικό να προτείνουμε για επόμενη μελέτη πιο αναλυτικά συστήματα που περιλαμβάνουν τις παραπάνω παραμέτρους ή ακόμη και να αποτελούνται από περισσότερες περιοχές. Επίσης ενδιαφέρον θα παρουσίαζε και η μελέτη των επιθέσεων σε Α.Π.Ε.

- Όσον αφορά τον έλεγχο, θα μπορούσε σε μελλοντική εργασία να χρησιμοποιηθεί μια πιο σύγχρονη βέλτιστη μέθοδος που θα είναι οικονομικότερη και αποτελεσματικότερη από τη δική μας που έγινε με ολοκληρωτή και τοποθέτηση πόλων.

- Όσον αφορά την ανίχνευση των επιθέσεων, μπορεί αρχικά να βελτιωθεί ακόμη περισσότερο ο παρατηρητής μέσω των κερδών του και να ελεγχθεί κατά πόσο αυτό συμβάλει στην ανίχνευση. Επιπλέον μπορεί να βελτιωθεί η μέθοδος μέσω παρατηρητή Luenberger με την προσθήκη νευρωνικών δικτύων, όπως αναφέραμε στο κεφάλαιο 4, καθώς ήδη έχουν υπάρξει μελέτες πάνω σε αυτό.

- Τέλος σε μελλοντικές μελέτες μπορεί να ελεγχθεί πειραματικά η χρήση και άλλων πιο προηγμένων και σύνθετων παρατηρητών όπως οι παρατηρητές άγνωστης εισόδου (Unknown Input Observers) και οι παρατηρητές ολισθαίνουσας κατάστασης (Sliding Mode Observers), για να εξετάσουμε αν μπορούν να αναγνωρίσουν επιθέσεις σε πιο σύνθετα συστήματα και αν μπορούν να τις ξεχωρίσουν από άλλες διαταραχές.

Βιβλιογραφία

[1] 2003 Blackout in the United States Final Report on the August 14, Canada: Causes, and Recommendations. Energy policy highlights. U.S. - Canada Power System Outage Task Force, page 30, 2004

[2] Ali, R.; Mohamed, T.H.; Qudaih, Y.S.; Mitani, Y. A new load frequency control approach in an isolated small power systems using coefficient diagram method. Int. J. Electr. Power Energy Syst. 2014, 56, 110–116.

[3] S. Duman and Y. Nuran, "Automatic generation control of the two area non-reheat thermal power system using gravitational search algorithm ," Przeglad Elektrotechniczny (Electrical Review), vol. 88, no lOa, pp. 254-259,2012.

[4] R. J. Abraham, D. Das and A. Patra, "Automatic generation control of an interconnected hydrothermal power system considering superconductive magnetic energy storage," International Journal of Electrical Power and Energy Systems, vol. 29, pp. 571-579, Oct. 2007.

[5] Α. Β. Μαχιας, Κ. Δ. Βουρνας, "Ευσταθεια Συστηματων Ηλεκτρικης Ενεργειας", ΕΜΠ, Αθηνα 1990.

[6] Β. Κ. Παπαδιας, "Αναλυση Συστημ ατος Ηλεκτρικης Ενεργειας", Τομοι I, II, ΕΜΠ, Αθηνα 1985.

[7] T. Van Cutsem, C. D. Vournas, "Voltage Stability of Electric Power Systems", Kluwer Academic Publishers, 1998.

[8] Δρ. Τσικαλακης Αντωνιος, "Προσθετες σημειωσεις για τα Κεντρα Ελεγχου Ενεργειας"

[9] Energy Management Systems, "https://www.brainkart.com/article/Energy-Management-System-(EMS)_12473/"

[10] Energy Management Systems, "https://www.genextpowersolutions.com/services/ems

[11] Αλαφοδημος Κωνσταντινος, "Ελεγχος Παραγωγικων Διεργασιων, Ενοτητα: Συστηματα Εποπτικου Ελεγχου και Συλλογης Πληροφοριων (S C A D A)"

[12] "Power System Analysis and Design J. Duncan Glover", Mulucutla S. Sarma, Thomas J. Overbye, Cambridge, © 2012.

[13] Nizamuddin Hakimuddin, Anita Khosla, Jitendra Kumar Garg, "Centralized and decentralized AGC schemes in 2-area interconnected power system considering multi source power plants in each area", © 2018

[14] "Market operations in Electric Power Systems: Forecasting, Scheduling, and Risk Management", M. Shahidehpour, H. Yamin, Z. Li, New York: John Wiley & Sons, © 2002.

[15] "Power generation, operation and control", A. J. Wood, B. F. Wollenberg, New York: John Wiley & Sons, © 1996.

[16] "Power System Stability and Control", Kundur, Prabha S., OP Malik, ©2022

[17] "Bevrani H. Robust Power System Frequency Control. New York: Springer; 2009. pp. 15-61

[18] D. P. Kothari and I. J. Nagrath, Modern Power System Analysis, 4th ed. McGraw Hill, 2011.

[19] "State Space Based Load Frequency Control Of Multi-Area Power Systems", Krishna Pal Singh Parmar, 2013

[20] "Παραγωγη Ηλεκτρικης Ενεργειας Έλεγχος και Ευσταθεια Συστηματος", Κ. Βουρνας, Β. Κ. Παπαδιας, Κ. Ντελκης, © 2011

[21] "Cyber Physical Systems Security: A Brief Survey", Qaisar Shafi, © 2012

[22] Chatterjee, K.; Padmini, V.; Khaparde, S.A. Review of cyber-attacks on power system operations. In Proceedings of the 2017 IEEE Region 10 Symposium (TENSYMP), Cochin, India, 14–16 July 2017; pp. 1–6.

[23] Smith, E.; Corzine, S.; Racey, D.; Dunne, P.; Hassett, C.; Weiss, J. Going beyond cybersecurity compliance: What power and utility companies really need to consider. IEEE Power Energy Mag. 2016, 14, 48–56

[24] Case, D.U. Analysis of the cyber-attack on the Ukrainian power grid. Electr. Inf. Shar. Anal. Cent. (E-ISAC) 2016, 21, 388.

[25] "Cyber Attack-resilient Control for Smart Grid, Siddharth Sridhar", Adam Hahn, Manimaran Govindarasu, © 2011

[26] "Cyber–Physical System Security for the Electric Power Grid", Siddharth Sridhar, Adam Hahn, Manimaran Govindarasu, © 2012

[27] Load Frequency Control in Two Area Power System", Siddhahast Mohapatra

[28] "power-system-analysis-hadi-saadat-ElCoM.pdf."

[29] S. Sivanagaraju, G Sreenivasan, "Power System Operation and Control", Pearson India

[30] Nilaykumar N. Shah, Chetan D. Kotwal, "The State Space Modeling of Single, Two and Three ALFC of Power System Using Integral Control and

OPTIMAL LQR CONTROL METHOD", IOSR JOURNAL OF ENGINEERING MAR. 2012, VOL. 2(3) PP: 501-510

[31] I. J NAGRATH AND D. P KOTHARI MODERN POWER SYSTEM ANALYSIS - TMH 1993

[32] A COMPREHENSIVE REVIEW OF THE CYBER-ATTACKS AND CYBER-SECURITY ON LOAD FREQUENCY CONTROL OF POWER SYSTEMS, ATHIRA M. MOHAN, NADER MESKIN AND HASAN MEHRJERDI, 2020

[33] "MODEL-BASED SECURE LOAD FREQUENCY CONTROL OF SMART GRIDS AGAINST DATA INTEGRITY ATTACK", HUI YANG, SHICHAO LIU, CHAO FANG, 2020

[34] IOSR JOURNAL OF ENGINEERING, THE STATE SPACE MODELING OF SINGLE, TWO AND THREE ALFC OF POWER SYSTEM USING INTEGRAL CONTROL AND OPTIMAL LQR CONTROL METHOD (NILAYKUMAR N. SHAH, CHETAN D. KOTWAL)

[35] INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN ELECTRICAL, ELECTRONICS AND INSTRUMENTATION ENGINEERING (IJAREEI), L-Q-R BASED LOAD FREQUENCY CONTROLLER FOR TWO AREA POWER SYSTEM BY K.VASU AND P.BHAVANA V.GANESH.

[36] INTERNATIONAL JOURNAL OF CURRENT ENGINEERING AND SCIENTIFIC RESEARCH (IJCESR), AUTOMATIC LOAD FREQUENCY CONTROL OF TWO AREA SYSTEM USING L-Q-R METHOD BY NILAYKUMAR N. SHAH, ANAMIKA R. PANDIT, MANSI T. SHAH, . SHERIN CHERIN, SHEETAL G. VSAVA,

[37] BEHERA, NIRANJAN (2013), LOAD FREQUENCY CONTROL OF POWER SYSTEM. MTECH THESIS

[38] REVIEW OF VARIOUS LOAD FREQUENCY CONTROLLERS, ALOK KUMAR, MOHAMMED ASIM, MIRZA MOHD. SHADAB & IRAM AKHTAR, PP 275–283, 2012

[39] AHMED, SERIEN HASHIM ALI (2017), LOAD FREQUENCY CONTROL FOR A TWO AREA POWER SYSTEM"

[40] J. C. BASILIO AND S. R. MATOS, "DESIGN OF PI AND PID CONTROLLERS WITH TRANSIENT PERFORMANCE SPECIFICATION - EDUCATION, IEEE TRANSACTIONS ON - IEEE-EDU2002.PDF," VOL. 45, NO. 4, PP. 364–370, 2002.

[41] T. POWER, M. J. CHANDRASHEKAR, AND R. JAYAPAL, "PERFORMANCE ANALYSIS OF FL , PI AND PID CONTROLLER FOR," VOL. 5, NO. 1, PP. 1–7, 2015.

[42] W. JOURNAL, "OPTIMAL TUNING OF PID CONTROLLER FOR LFC OF TWO AREA POWER SYSTEM (PV DIESEL) USING BIO- INSPIRED OPTIMIZATION ALGORITHMS *," VOL. 12, NO. JANUARY, PP. 112–124, 2016.

[43] B. PORTER AND J. J. D"AZZO, "CLOSED-LOOP EIGEN STRUCTURE ASSIGNMENT BY STATE FEEDBACK IN MULTIVARIABLE LINEAR SYSTEMS," JNT. J. CONTR., VOL. 27, PP. 487-492, 1978.

[44] B. P. Molinari, "The state regulator problem and its inverse," IEEE Trans. Automat. Contr., vol. AC-18, pp. 454-459, Oct. 1973

[45] Eigenstructure Assignment for Control System Design, G. P. Liu and R. J. Patton, Wiley, Chichester, UK, 1998

[46] Μαριλενα Χ. Διδασκαλου, "Επανατοποθετηση πολων στον χωρο των καταστασεων", 2015

[47] Ali M. Yousef, Optimal Shifting of Eigenvalues for Load Frequency Control Systems, Article 9, Volume 41, No 5, September and October 2013, Page 1857-1876

[48] Shen Y., Fei M., Du D., Cyber security study for power systems under denial-of-service attacks

[49] Chatterjee, K.; Padmini, V.; Khaparde, S.A. Review of cyber attacks on power system operations. In Proceedings of the 2017 IEEE Region 10 Symposium (TENSYMP), Cochin, India, 14–16 July 2017; pp. 1–6

[50] Cybersecurity Analysis of Load Frequency Control in Power Systems: A Survey by Sahaj Saxena, Sajal Bhatia and Rahul Gupta, 2021

[51] Li, Y.; Zhang, P.; Ma, L. Denial of service attack and defense method on load frequency control system. J. Frankl. Inst. 2019, 356, 8625–8645.

[52] Chen, C.; Cui, M.; Wang, X.; Zhang, K.; Yin, S. An investigation of coordinated attack on load frequency control. IEEE Access 2018, 6, 30414–30423

[53] Wu, Y.; Wei, Z.; Weng, J.; Li, X.; Deng, R.H. Resonance attacks on load frequency control of smart grids. IEEE Trans. Smart Grid 2017, 9, 4490–4502.

[54] Alhelou, H.H.; Hamedani-Golshan, M.E.; Zamani, R.; Heydarian-Forushani, E.; Siano, P. Challenges and opportunities of load frequency control in conventional, modern and future smart power systems: A comprehensive review. Energies 2018, 11, 2497

[55] Alrifai, M.T.; Hassan, M.F.; Zribi, M. Decentralized load frequency controller for a multi-area interconnected power system. Int. J. Electr. Power Energy Syst. 2011, 33, 198–209.

[56] Ding, D., Han, Q.L., Xiang, Y., Ge, X., Zhang, X.M., A survey on security control and attack detection for industrial cyber-physical systems. Neurocomputing 2018, 275, 1674–1683.

[57] Wang, Q.; Tai, W.; Tang, Y.; Zhu, H.; Zhang, M.; Zhou, D. Coordinated Defense of Distributed Denial of Service Attacks against the Multi-Area Load Frequency Control Services. Energies 2019, 12, 2493.

[58] Mahmoud, M.S.; Hamdan, M.M.; Baroudi, U.A. Modeling and control of Cyber-Physical Systems subject to cyber-attacks: A survey of recent advances and challenges. Neurocomputing 2019, 338, 101–115

[59] Roy, S.D.; Debbarma, S. Detection and Mitigation of Cyber-Attacks on AGC Systems of Low Inertia Power Grid. IEEE Syst. J. 2019, 14, 2023–2031.

[60] Liu, X.; Li, Z. False data attack models, impact analyses and defense strategies in the electricity grid. Electr. J. 2017, 30, 35–42.

[61] Tan, R.; Nguyen, H.H.; Foo, E.Y.S.; Dong, X.; Yau, D.K.Y.; Kalbarczyk, Z.; Iyer, R.K.; Gooi, H.B. Optimal false data injection attack against automatic generation control in power grids. In Proceedings of the 2016 ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS), Vienna, Austria, 11–14 April 2016; pp. 1–10.

[62] Abbaspour, A.; Sargolzaei, A.; Yen, K. Detection of false data injection attack on load frequency control in distributed power systems. In Proceedings of the 2017 North American Power Symposium (NAPS), Morgantown, WV, USA, 17–19 September 2017; pp. 1–6.

[63] Abbaspour, A.; Sargolzaei, A.; Forouzannezhad, P.; Yen, K.K.; Sarwat, A.I. Resilient Control Design for Load Frequency Control System under False Data Injection Attacks. IEEE Trans. Ind. Electron. 2019, 67, 7951–7962.

[64] Teixeira, A.; Pérez, D.; Sandberg, H.; Johansson, K.H. Attack models and scenarios for networked control systems. In Proceedings of the 1st International Conference on High Confidence Networked Systems; ACM: New York, NY, USA, 2012; pp. 55–64.

[65] Hoehn, A.; Zhang, P. Detection of covert attacks and zero dynamics attacks in cyber-physical systems. In Proceedings of the 2016 American Control Conference (ACC), Boston, MA, USA, 6–8 July 2016; pp. 302–307.

[66] Li, W.; Xie, L.; Wang, Z. A novel covert agent for stealthy attacks on industrial control systems using least squares support vector regression. J. Electr. Comput. Eng. 2018, 2018, 1–14.

[67] Sargolzaei, A.; Yen, K.K.; Abdelghani, M.N. Preventing time-delay switch attack on load frequency control in distributed power systems. IEEE Trans. Smart Grid 2015, 7, 1176–1185.

[68] Model-Based Attack Detection and Mitigation for Automatic Generation Control, Siddharth Sridhar, Manimaran Govindarasu

[69] Chen, C.; Zhang, K.; Yuan, K.; Zhu, L.; Qian, M. Novel detection scheme design considering cyber-attacks on load frequency control. IEEE Trans. Ind. Informat. 2017, 14, 1932–1941.

[70] KONTOURAS, E.; TZES, A.; DRITSAS, L. CYBER-ATTACK ON A POWER PLANT USING BIAS INJECTED MEASUREMENTS. IN PROCEEDINGS OF THE 2017 AMERICAN CONTROL CONFERENCE (ACC), SEATTLE, WA, USA, 24–26 MAY 2017; PP. 5507–5512.

[71] VULNERABILITY ASSESSMENT OF LOAD FREQUENCY CONTROL CONSIDERING CYBER SECURITY, BY CHUNYU CHEN, YANG CHEN, KAIFENG ZHANG, WENJUN BI, MENG TIAN

[72] ESTIMATION OF FALSE DATA INJECTION ATTACKS FOR LOAD FREQUENCY CONTROL SYSTEMS, JUN YE, 2021

[73] ACTIVE FAULT-TOLERANT CONTROL FOR LOAD FREQUENCY CONTROL IN MULTI-AREA POWER SYSTEMS WITH PHYSICAL FAULTS AND CYBER-ATTACKS, YAJIAN ZHANG, TING YANG, ZIHUI TANG, 2020

[74] DATA INTEGRITY ATTACKS AND THEIR IMPACTS ON SCADA CONTROL SYSTEM, SIDDHARTH SRIDHAR, AND G. MANIMARAN

[75] "CHAPTER 2", CE 295 — ENERGY SYSTEMS AND CONTROL PROFESSOR SCOTT MOURA — UNIVERSITY OF CALIFORNIA, BERKELEY

[76] ΕΙΣΑΓΩΓΗ ΣΤΟΝ ΑΥΤΟΜΑΤΟ ΈΛΕΓΧΟ (8090) ΣΗΜΕΙΩΣΕΙΣ ΜΑΘΗΜΑΤΟΣ 2020-2021 ΜΕΡΟΣ 2Ο: ΜΟΝΤΕΡΝΟΣ ΈΛΕΓΧΟΣ, 2021

[77] "STATE ESTIMATORS" , SYSTEM AND CONTROL THEORY. PROF. ROBERTO ZANASI MODENA, A.A. 2016–2017

[78] LECTURE NOTES PREPARED BY DR. GREGORY L. PLETT. COPYRIGHT " © 2015, 2011, 2009, 2007, 2005, 2003, 2001, 2000, GREGORY L. PLETT

[79] A DECENTRALIZED FUNCTIONAL OBSERVER BASED OPTIMAL LFC CONSIDERING UNKNOWN INPUTS, UNCERTAINTIES AND CYBER-ATTACKS, HASSAN HAES ALHELOU, MOHAMAD ESMAIL HAMEDANI GOLSHAN, NIKOS D. HATZIARGYRIOU, 2019

[80] VASEGHI, S. V. (2000). ADVANCED DIGITAL SIGNAL PROCESSING AND NOISE REDUCTION (SECOND ED.). JOHN WILEY & SONS LTD.

[81] GREWAL, M. S., & ANDREWS, A. P. (2014). KALMAN FILTERING: THEORY AND PRACTICE WITH MATLAB. JOHN WILEY & SONS.

[82] CATLIN, D. E. (2012). ESTIMATION, CONTROL, AND THE DISCRETE KALMAN FILTER. SPRINGER SCIENCE & BUSINESS MEDIA.

[83] ZARCHAN, P., & MUSOFF, H. (2009). FUNDAMENTALS OF KALMAN FILTERING: A PRACTICAL APPROACH. AIAA.

[84] BASILE, G., & MARRO, G. (1969). ON THE OBSERVABILITY OF LINEAR, TIME-INVARIANT SYSTEMS WITH UNKNOWN INPUTS. JOURNAL OF OPTIMIZATION THEORY AND APPLICATIONS, 3, 410–415.

[85] GUIDORZI, R., & MARRO, G. (1971). ON WONHAM STABILIZABILITY CONDITION IN THE SYNTHESIS OF OBSERVERS FOR UNKNOWN-INPUT SYSTEMS. IEEE TRANSACTIONS ON

AUTOMATIC CONTROL, 16, 499–500.

[86] BHATTACHARYYA, S. P. (1978). OBSERVER DESIGN FOR LINEAR SYSTEMS WITH UNKNOWN INPUTS. IEEE TRANSACTIONS ON AUTOMATIC CONTROL, 23, 483–484.

[87] HAUTUS, M. L. J. (1983). STRONG DETECTABILITY AND OBSERVERS. LINEAR ALGEBRA AND ITS APPLICATIONS, 50, 353–368.

[88] DAROUACH, M., ZASADZINSKI, M., & XU, S. J. (1994). FULL-ORDER OBSERVERS FOR LINEAR SYSTEMS WITH UNKNOWN INPUTS. IEEE TRANSACTIONS ON AUTOMATIC CONTROL, 39, 606–609.

[89] HOU, M., & MULLER, P. C. (1992). DESIGN OF OBSERVERS FOR LINEAR SYSTEMS WITH UNKNOWN INPUTS. IEEE TRANSACTIONS ON AUTOMATIC CONTROL, 37, 871–875.

[90] WATANABE, K., & HIMMELBLAU, D. M. (1982). INSTRUMENT FAULT DETECTION IN SYSTEMS WITH UNCERTAINTIES. INTERNATIONAL JOURNAL OF SYSTEMS SCIENCE, 13, 137–158.

[91] PATTON, R. J., & CHEN, J. (1993). OPTIMAL SELECTION OF UNKNOWN INPUT DISTRIBUTION MATRIX IN THE DESIGN OF ROBUST OBSERVERS FOR FAULT DIAGNOSIS. AUTOMATICA, 29, 837–841.

[92] WUNNENBERG, J., & FRANK, P. M. (1982). SENSOR FAULT USING DETECTION VIA ROBUST OBSERVER. INTERNATIONAL JOURNAL OF SYSTEMS SCIENCE, 13, 137–158.

[93] LUENBERGER, D. G. (1964). OBSERVING THE STATE OF A LINEAR SYSTEM. IEEE TRANSACTIONS ON MILITARY ELECTRONICS

[94] LUENBERGER, D. G. (1971). AN INTRODUCTION TO OBSERVERS. IEEE TRANSACTIONS ON AUTOMATIC CONTROL.

[95] LUENBERGER, D. G. (1979). INTRODUCTION TO DYNAMIC SYSTEMS: THEORY, MODELS, AND APPLICATIONS. JOHN WILEY & SONS, INC.

[96] R. CLARK R. PATTON, P. FRANK, FAULT DIAGNOSIS IN DYNAMIC SYSTEMS: THEORY AND APPLICATIONS, PRENTICE HALL, NEW YORK, 1989.

[97] THORALF A. SCHWARZ, UNCERTAINTY ANALYSIS OF A FAULT DETECTION AND ISOLATION SCHEME FOR MULTI-AGENT SYSTEMS, MASTER'S THESIS, KTH, SWEDEN, 2012.

[98] H. H. ALHELOU, M. H. GOLSHAN, AND J. ASKARI-MARNANI, "ROBUST SENSOR FAULT DETECTION AND ISOLATION SCHEME FOR INTERCONNECTED SMART POWER SYSTEMS IN PRESENCE OF RER AND EVS USING UNKNOWN INPUT OBSERVER," INTERNATIONAL JOURNAL OF ELECTRICAL POWER & ENERGY SYSTEMS, VOL. 99, PP. 682–694, 2018.

[99] J. CHEN AND R. J. PATTON, ROBUST MODEL-BASED FAULT DIAGNOSIS FOR DYNAMIC SYSTEMS. SPRINGER SCIENCE & BUSINESS MEDIA, 2012, VOL. 3.

[100] T. A. SCHWARZ, "UNCERTAINTY ANALYSIS OF A FAULT DETECTION AND ISOLATION SCHEME FOR MULTI-AGENT SYSTEMS," 2012

[101] J. LIU, Y. GAO, X. SU, M. WACK, AND L. WU, "DISTURBANCE-OBSERVERBASED CONTROL FOR AIR MANAGEMENT OF PEM FUEL CELL SYSTEMS VIA SLIDING MODE TECHNIQUE," IEEE TRANSACTIONS ON CONTROL SYSTEMS TECHNOLOGY, NO. 99, PP. 1–10, 2018.

[102] SLIDING MODE OBSERVERS FOR DISTRIBUTED PARAMETER SYSTEMS: THEORY AND APPLICATIONS, NILOOFAR NASIRI KAMRAN, 2016

[103] NESRINE MONTACER, SAMAH BEN ATIA, KHADIJA DEHRI, AND RIDHA BEN ABDENNOUR, SLIDING MODE OBSERVER SYNTHESIS FOR MULTIVARIABLE SYSTEMS: AN LMI APPROACH, DE GRUYTER OLDENBOURG, ASSD – ADVANCES IN SYSTEMS, SIGNALS AND DEVICES, VOLUME 9, 2019, PP. 303–320.

[104] ABUR, A., EXPOSITO, A. : "POWER SYSTEM STATE ESTIMATION: THEORY AND IMPLEMENTATION" (CRC PRESS, MARCEL DEKKER, INC. NEW YORK, USA., 2004)

[105] TALEBI, M., LI, C., QU, Z.: 'ENHANCED PROTECTION AGAINST FALSE DATA INJECTION BYDYNAMICALLY CHANGING INFORMATION STRUCTURE OF MICROGRIDS'. PROC. IEEESEVENTH SENSOR ARRAY MULTICHANNEL SIGNAL PROCESS. WORKSHOP (SAM),HOBOKEN, NJ, USA., 2012, PP. 393– 96

[106] KOSUT, O., JIA, L., THOMAS, R.J., ET AL.: 'LIMITING FALSE DATA ATTACKS ON POWERSYSTEM STATE ESTIMATION'. 2010 44TH ANNUAL CONF. INFORMATION SCIENCES ANDSYSTEMS (CISS), PRINCETON, NJ, 2010, PP. 1–6

[107] CHEN, C.; ZHANG, K.; YUAN, K.; ZHU, L.; QIAN, M. NOVEL DETECTION SCHEME DESIGN CONSIDERING CYBER-ATTACKS ON LOAD FREQUENCY CONTROL. IEEE TRANS. IND. INFORMAT. 2017, 14, 1932–1941.

[108] "CHAPTER 2", CE 295 — ENERGY SYSTEMS AND CONTROL PROFESSOR SCOTT MOURA — UNIVERSITY OF CALIFORNIA, BERKELEY

[109] BEFEKADU, G.K.; GUPTA, V.; ANTSAKLIS, P.J. RISK-SENSITIVE CONTROL UNDER MARKOV MODULATED DENIAL-OF-SERVICE (DOS) ATTACK STRATEGIES. IEEE TRANS.

[110] AUTOM. CONTROL 2015, 60, 3299–3304ZHANG, H.; QI, Y.; ZHOU, H.; ZHANG, J.; SUN, J. TESTING AND DEFENDING METHODS AGAINST DOS ATTACK IN STATE ESTIMATION. ASIAN J. CONTROL 2017, 19, 1295–1305.

[111] ASHOK, A., GOVINDARASU, M., AJJARAPU, V.: 'ONLINE DETECTION OF STEALTHY FALSEDATA INJECTION ATTACKS IN POWER SYSTEM STATE ESTIMATION', IEEE TRANS. SMARTGRID, 2018, 9, (3), PP. 1636–1646

[112] [8] BERTHIER, R., SANDERS, W., KHURANA, H.: 'INTRUSION DETECTION FOR ADVANCEDMETERING INFRASTRUCTURES: REQUIREMENTS AND ARCHITECTURAL DIRECTIONS'. IEEE INT.CONF. SMART GRID COMMUNICATIONS (SMARTGRIDCOMM),

GAITHERSBURG, MD,USA., OCTOBER 2010, PP. 350–355

[113] S. SRIDHAR AND M. GOVINDARASU, "MODEL-BASED ATTACK DETECTION AND MITIGATION FOR AUTOMATIC GENERATION CONTROL," IEEE TRANS. SMART GRID, VOL. 5, NO. 2, PP. 580–591, MAR. 2014.

[114] HOU, Y.; ZHU, F.; ZHAO, X.; GUO, S. OBSERVER DESIGN AND UNKNOWN INPUT RECONSTRUCTION FOR A CLASS OF SWITCHED DESCRIPTOR SYSTEMS. IEEE TRANS. SYST. MAN CYBERN. SYST. 2017, 48, 1411–1419.

[115] LUO, X.; WANG, X.; ZHANG, M.; GUAN, X. DISTRIBUTED DETECTION AND ISOLATION OF BIAS INJECTION ATTACK IN SMART ENERGY GRID VIA INTERVAL OBSERVER. APPL. ENERGY 2019, 256, 113703.

[116] NIU, H.; BHOWMICK, C.; JAGANNATHAN, S. ATTACK DETECTION AND APPROXIMATION IN NONLINEAR NETWORKED CONTROL SYSTEMS USING NEURAL NETWORKS. IEEE TRANS. NEURAL NETW. LEARN. SYST. 2019, 31, 235–245.

[117] LIAO, K.; XU, Y. A ROBUST LOAD FREQUENCY CONTROL SCHEME FOR POWER SYSTEMS BASED ON SECOND-ORDER SLIDING MODE AND EXTENDED DISTURBANCE OBSERVER. IEEE TRANS. IND. INFORM. 2017, 14, 3076–3086.

[118] SU, X.; LIU, X.; SONG, Y.D. FAULT-TOLERANT CONTROL OF MULTIAREA POWER SYSTEMS VIA A SLIDING-MODE OBSERVER TECHNIQUE. IEEE/ASME TRANS. MECHATRONICS 2017, 23, 38–47.

[119] MODEL-BASED ATTACK DETECTION AND MITIGATION FOR AUTOMATIC GENERATION CONTROL, SIDDHARTH SRIDHAR, MANIMARAN GOVINDARASU

[120] AYAD, A.; KHALAF, M.; EL-SAADANY, E. DETECTION OF FALSE DATA INJECTION ATTACKS IN AUTOMATIC GENERATION CONTROL SYSTEMS CONSIDERING SYSTEM NONLINEARITIES. IN PROCEEDINGS OF THE 2018 IEEE ELECTRICAL POWER AND ENERGY CONFERENCE (EPEC), TORONTO, ON, CANADA, 10–11 OCTOBER 2018; PP. 1–6.

[121] JEVTIC, A.; ZHANG, F.; LI, Q.; ILIC, M. PHYSICS-AND LEARNING-BASED DETECTION AND LOCALIZATION OF FALSE DATA INJECTIONS IN AUTOMATIC GENERATION CONTROL. IFAC-PAPERSONLINE 2018, 51, 702–707.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.

[122] A. J. GALLO, M. S. TURAN, P. NAHATA, F. BOEM, T. PARISINI, AND G. FERRARITRECATE, "DISTRIBUTED CYBER-ATTACK DETECTION IN THE SECONDARY CONTROL OF DC MICROGRIDS," IN PROC. EUR. CONTROL CONF., 2018, PP. 344–349.

[123] Y. SHOUKRY AND P. TABUADA, "EVENT-TRIGGERED STATE OBSERVERS FOR SPARSE SENSOR NOISE/ATTACKS," IEEE TRANS. AUTOM. CONTROL, VOL. 61, NO. 8, PP. 2079–2091, AUG. 2015.

[124] W. AO, Y. SONG, AND C. WEN, "ADAPTIVE CYBER-PHYSICAL SYSTEM ATTACK DETECTION AND RECONSTRUCTION WITH APPLICATION TO POWER SYSTEMS," IET CONTROL THEORY APPL., VOL. 10, NO. 12, PP. 1458–1468, 2016

[125] A. A. CARDENAS, S. AMIN, AND S. SASTRY, "SECURE CONTROL: TOWARDS SURVIVABLE CYBER-PHYSICAL SYSTEMS," IN PROC. 28TH INT. CONF. DISTRIB. COMPUT. SYST. WORKSHOPS, 2008, PP. 495–500

[126] ALHELOU, H.H.; GOLSHAN, M.E.H.; HATZIARGYRIOU, N.D. A DECENTRALIZED FUNCTIONAL OBSERVER BASED OPTIMAL LFC CONSIDERING UNKNOWN INPUTS, UNCERTAINTIES, AND CYBER-ATTACKS. IEEE TRANS. POWER SYST. 2019, 34, 4408–4417.

[127] 40. HUANG, T.; SATCHIDANANDAN, B.; KUMAR, P.; XIE, L. AN ONLINE DETECTION FRAMEWORK FOR CYBER ATTACKS ON AUTOMATIC GENERATION CONTROL. IEEE TRANS. POWER SYST. 2018, 33, 6816–6827.

[128] 41. MO, Y.; CHABUKSWAR, R.; SINOPOLI, B. DETECTING INTEGRITY ATTACKS ON SCADA SYSTEMS. IEEE TRANS. CONTROL. SYST. TECHNOL. 2013, 22, 1396–1407.

[129] 51. BI, W.; ZHANG, K.; LI, Y.; YUAN, K.; WANG, Y. DETECTION SCHEME AGAINST CYBER-PHYSICAL ATTACKS ON LOAD FREQUENCY CONTROL BASED ON DYNAMIC CHARACTERISTICS ANALYSIS. IEEE SYST. J. 2019, 13, 2859–2868.

[130] 54. KONTOURAS, E.; ANTHONY, T.; DRITSAS, L. SET-THEORETIC DETECTION OF DATA CORRUPTION ATTACKS ON CYBER PHYSICAL POWER SYSTEMS. J. MOD. POWER SYST. CLEAN ENERGY 2018, 6, 872–886.

[131] WENJUN BI, KAIFENG ZHANG AND CHUNYU CHEN, CYBER ATTACK DETECTION SCHEME FOR A LOAD FREQUENCY CONTROL SYSTEM BASED ON DUAL-SOURCE DATA OF COMPROMISED VARIABLES