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

Αυτοματοποιημένος Έλεγχος Παραγωγής και Διαχείρισης Ισχύος (AGC) σε δίκτυα Ενέργειας. Κυβερνοεπιθέσεις και τεχνικές εξάλειψής τους

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Κοκκινάκη Μαργαρίτα

Α.Μ: 03109186

Επιβλέπων : Νικόλαος Χατζηαργυρίου
Καθηγητής Ε.Μ.Π.

Αθήνα, Ιούλιος 2020

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

Αυτοματοποιημένος Έλεγχος Παραγωγής και Διαχείρισης Ισχύος (AGC) σε δίκτυα Ενέργειας. Κυβερνοεπιθέσεις και τεχνικές εξάλειψής τους

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Επιβλέπων : Νικόλαος Χατζηαργυρίου
Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 23/7/2020

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

Αθήνα, Ιούλιος 2020

.....
Κοκκινάκη Μαργαρίτα

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

Περίληψη

Η παρούσα διπλωματική εργασία παρουσιάζει τις δομές των συστημάτων Αυτοματοποιημένου Ελέγχου Παραγωγής και Διαχείρισης Ηλεκτρικής Ισχύος (Automatic Generation Control – AGC). Τα συστήματα AGC αποτελούν δομικά στοιχεία των σύγχρονων δικτύων για την παραγωγή και τη διαχείριση της ηλεκτρικής ισχύος, διασφαλίζοντας την απαιτούμενη εξισορρόπηση μεταξύ του μεταβαλλόμενου φορτίου του δικτύου και της παραγωγής. Τα συστήματα AGC, αρχικά αποτελούσαν αυτοματοποιημένα συστήματα αναλογικού τύπου, τα οποία έλεγχαν την παραγωγή της ισχύος επί των γεννητριών του δικτύου, με την εφαρμογή τεχνικών αναλογικού ελέγχου (PI ελεγκτές). Η πρόοδος της τεχνολογίας, η διαδικασία ψηφιοποίησης των δεδομένων σε συνδυασμό με τα δίκτυα υπολογιστών, συνέτειναν στη μετεξέλιξη των AGC σε αυτοματοποιημένους διαχειριστές Ενέργειας (EMS). Οι διαχειριστές Ενέργειας αποφασίζουν με τη χρήση μίας συνολικής δικτυακής υποδομής, μετρήσεων και ελέγχου, μέσω ανίχνευσης καταστάσεων (states) λειτουργίας, για τις απαιτούμενες ενέργειες που χρειάζεται να επιβληθούν στο δίκτυο για την εξασφάλιση της εξισορρόπησης. Από την άλλη πλευρά, η συνένωση των δομικών στοιχείων και ο κεντρικός έλεγχος, κατέστησε τους Διαχειριστές Ενέργειας πιο ευάλωτους σε κυβερνοεπιθέσεις. Οι κυβερνοεπιθέσεις (cyber-attacks) αποσκοπούν να πλήξουν τις δομές και τη λειτουργία του δικτύου ισχύος, με στόχο την καταστροφική κατάληξη όλου του συστήματος. Στα πλαίσια αυτά, η εργασία παρουσιάζει μεθόδους και τεχνικές για την αποφυγή και αντιμετώπιση των κυβερνοεπιθέσεων στα σύγχρονα συστήματα AGC. Πιο συγκεκριμένα:

Στο κεφάλαιο 1 παρουσιάζεται μία περιγραφή των λειτουργιών ενός AGC συστήματος (αρχική μορφή του AGC και εξέλιξή του στη σύγχρονη μορφή του σε EMS). Στο κεφάλαιο 2 παρουσιάζονται οι σημαντικότερες μετρικές που χρησιμοποιούνται για την αξιολόγηση των επιδόσεων ενός πληροφοριακού συστήματος και η διασύνδεση των AGC συστημάτων με αυτές. Στο κεφάλαιο 3 παρουσιάζονται οι τύποι όλων των μορφών επίθεσης σε ένα σύστημα AGC με βάση την ερευνητική βιβλιογραφία. Το κεφάλαιο 4 αναλύει τους αμυντικούς μηχανισμούς που μπορούν να χρησιμοποιηθούν για την αντιμετώπιση των επιθέσεων. Το κεφάλαιο 5 καταδεικνύει τα ανοικτά θέματα που σχετίζονται με τους τύπους των προηγούμενων επιθέσεων καθώς και των μεθόδων αντιμετώπισης που συστήνονται. Η εργασία ολοκληρώνεται με την παρουσίαση των συμπερασμάτων καθώς και των μελλοντικών τεχνικών και μεθοδολογιών για την αντιμετώπιση του ανοικτού ερευνητικού προβλήματος, της προστασίας των υποδομών παραγωγής και διαχείρισης ισχύος από κυβερνο-επιθέσεις.

Λέξεις κλειδιά

Συστήματα παραγωγής και Διαχείρισης Ισχύος. Διαχειριστές Ενέργειας, Λήψη Αποφάσεων, Κατάσταση Δικτύου, Έλεγχος συχνότητας λειτουργίας, γεννήτριες, κυβερνο-επιθέσεις, τύποι επιθέσεων, αμυντικοί μηχανισμοί, ευφυείς αλγόριθμοι, μαθηματικά μοντέλα περιγραφής δικτύου

Abstract

This thesis presents the structures of Automated power Generation and power management Control (Automatic Generation Control - AGC) systems. These systems are structural elements of modern power networks handling the production and management of power, ensuring balance between the dynamically changing network load and power production. AGC systems were originally automated analog-type systems, which controlled the production of power on network generators by applying analog control techniques (PI controllers). Advances in technology, the process of digitizing data in conjunction with computer networks, have contributed to the evolution of AGCs into automated Energy Management Systems (EMS). EMS decide using a comprehensive network infrastructure, measurements and control, through network state estimation, for the required actions that need to be imposed on the network to ensure load balance. On the other hand, the merging of structural elements and central control has made Energy Management more vulnerable to cyber-attacks. Cyber-attacks are intended to damage the structures and operation of the power grid, with the aim of destroying the entire system. In this context, the work presents methods and techniques for the prevention and mitigation of cyber-attacks in modern AGC systems. More specifically:

Chapter 1 describes functions of the AGC system (as evolved through time to the EMS definition). Chapter 2 presents the most important metrics used to evaluate the performance of an information system and the interconnection of AGC systems with them. Chapter 3 presents types of attack on an AGC system based on research literature. Chapter 4 analyzes the defense mechanisms used to counter attacks. Chapter 5 demonstrates the open issues related to the types of the afford-mentioned attacks in conjunction with coping methods recommended. The work concludes with the presentation of the conclusions, as well as, future techniques and methodologies for tackling the open research problem, for the protection of production infrastructure and power management from cyber-attacks.

Key words

Power Production and Management Systems. Energy Management Systems, Decision Making, Network States, Load Frequency Control, Generators, Cyber-Attacks, Types of Attacks, Defense Mechanisms, Intelligent Algorithms, Mathematical Network Description Models

Ευχαριστίες

Σε αυτό το σημείο θα ήθελα να ευχαριστήσω τον Καθηγητή μου Κο. Νικόλαο Χατζηαργυρίου τόσο για την εμπιστοσύνη που μου έδειξε αναθέτοντάς μου την διεκπεραίωση της παρούσας εργασίας, όσο και για την άριστη συνεργασία μας για την επιτυχημένη ολοκλήρωσή της.

Επίσης, θα ήθελα να ευχαριστήσω τον μεταπτυχιακό ερευνητή και υποψήφιο διδάκτορα Κο. Ανδρέα-Δωρόθεο Συρμακέση, για την άριστη συνεργασία που είχαμε κατά τη διάρκεια εκπόνησης της διπλωματικής μου εργασίας. Η συνεισφορά, καθώς και οι υποδείξεις του κατά τη διάρκεια μελέτης και συγγραφής του κειμένου συνέβαλαν σημαντικά στη διαμόρφωση της τελικής μορφής της εργασίας.

Κλείνοντας, θα ήθελα να ευχαριστήσω την οικογένειά μου και τα κοντινά μου πρόσωπα, που με την αμέριστη υποστήριξη και εμπιστοσύνη που μου έδειξαν καθ' όλη τη διάρκεια της προσπάθειάς μου συνέβαλαν αποφασιστικά στην επίτευξη αυτού του στόχου.

Πίνακας Περιεχομένων

Κατάλογος Σχημάτων

Κατάλογος Πινάκων

1 Εισαγωγή στον Αυτόματο Έλεγχο Παραγωγής και Διαχείρισης Ισχύος

1.1 Γενικά

Ο αυτόματος έλεγχος παραγωγής ηλεκτρικής ισχύος (Automatic Generation Control - AGC) είναι ένα από τα πλέον σημαντικά προβλήματα ελέγχου στο σχεδιασμό και τη λειτουργία των διασυνδεδεμένων συστημάτων παραγωγής ηλεκτρικής ισχύος **[1]**. Το συγκεκριμένο πρόβλημα γίνεται όλο και σημαντικότερο σήμερα, δεδομένου του αυξανόμενου μεγέθους των δικτύων ισχύος, των συνεχών αλλαγών της δομής αυτών με το δυναμικό χαρακτήρα των διασυνδεόμενων φορτίων τους, και τις 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).

Στις παραπάνω παραμέτρους του προβλήματος, έρχονται να προστεθούν και οι νέες αβεβαιότητες, όπως οι περιβαλλοντικοί περιορισμοί λειτουργίας των δομών παραγωγής ενέργειας και η πολυπλοκότητα των σύγχρονων συστημάτων ισχύος. 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. Η εξισορρόπηση, πέρα από τη σταθερότητα της λειτουργίας του ηλεκτρικού δικτύου, διασφαλίζει και χαμηλότερο κόστος λειτουργίας για τη διανεμόμενη ισχύ προς τους καταναλωτές.

Τα σημερινά συστήματα AGC, 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). Κατά δεύτερο λόγο, η διαφοροποίηση μπορεί να υπεισέρχεται στις στρατηγικές ελέγχου του δικτύου και τις τεχνικές ή επιλογές ανάθεσης της ζητούμενης 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 παρεχόμενες νέες τεχνολογίες κορμού για να ανταπεξέλθουν στα προηγούμενα χαρακτηριστικά. Ο πυρήνας αυτών των έξυπνων συστημάτων θα πρέπει να βασίζεται σε ευέλικτους - ευφυείς αλγορίθμους, σε εμπλουτισμένες και ακριβείς ανταλλασσόμενες πληροφορίες, καθώς και σε υποσυστήματα ταχείας επικοινωνίας. Ο αυτόματος έλεγχος παραγωγής και διαχείρισης ηλεκτρικής ισχύος, που αλληλεπιδρά με άλλες βοηθητικές υπηρεσίες (ευαίσθητες καλύψεις φορτίων π.χ. νοσοκομεία, εργαστήρια, διαχείριση κυκλοφορίας οχημάτων, κλπ), θα πρέπει να είναι σε θέση να συμβάλει στις επερχόμενες προκλήσεις για μελλοντικό έλεγχο και λειτουργία των συστημάτων **[1]**, **[2]**.

Τα υπάρχοντα συστήματα AGC, έχουν εξελιχθεί σημαντικά τις τελευταίες έξι δεκαετίες και χρησιμοποιούνται σε διασυνδεδεμένα συστήματα μικρής, μεσαίας και μεγάλης κλίμακας. Η συνεχής βελτίωση αυτών των συστημάτων αναμένεται μέσω νέων εφαρμογών, αλγορίθμων και τεχνολογιών ελέγχου διεργασιών.
Επομένως, σημαντική είναι η διασφάλιση ισορροπημένης λειτουργίας του δικτύου ισχύος (δηλ, προσφορά ισχύος σε συνάφεια με τη ζήτηση – κατανάλωση ισχύος). Σε ένα σύστημα ηλεκτρικής ενέργειας, στόχος του αυτόματου ελέγχου παραγωγής (AGC) είναι η εξασφάλιση ισορροπίας μεταξύ παραγόμενης ισχύος (από τις διαφορετικές μονάδες παραγωγής), και των καταναλισκόμενων δυναμικών φορτίων που το δίκτυο τροφοδοτεί **[1]**.

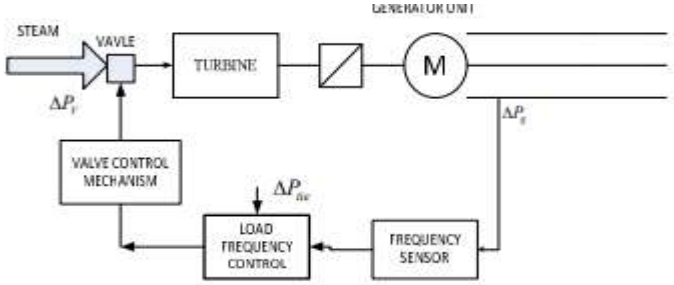
1.1.1 Η έννοια της εξισορρόπησης ισχύος στο δίκτυο

Δεδομένου ότι ένα δίκτυο ηλεκτρικής ισχύος απαιτεί την ισορροπία μεταξύ της παραγωγής και του φορτίου του σε κάθε χρονική στιγμή, αυτό απαιτεί συχνές μεταβολές του επιπέδου παραγόμενης ισχύος από τις ηλεκτρικές γεννήτριες του συστήματος. Η κατάσταση ενός δικτύου παραγωγής, και η επιτυγχανόμενη εξισορρόπηση μεταξύ παραγωγής και ζήτησης ισχύος, μπορεί να διαπιστωθεί με την εφαρμογή μετρήσεων της συχνότητας της παρεχόμενης τάσης.
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.
Επομένως, η μέτρηση της συχνότητας λειτουργίας ενός δικτύου ισχύος αποτελεί μία σημαντική βάση εκτίμησης για την εξισορροπημένη λειτουργία του δικτύου. Μικρές διακυμάνσεις από την επιθυμητή συχνότητα λειτουργίας συνεπάγονται ικανοποιητική εξισορρόπηση μεταξύ παραγόμενης και καταναλισκόμενης ισχύος στο δίκτυο. Οι μεταβολές της συχνότητας, καθώς και τα επίπεδα διακύμανσής της, είναι οι βασικοί μηχανισμοί που, μέσω των μετρήσεων, αναγκάζουν την ενεργοποίηση των υποσυστημάτων για εξισορρόπηση. Η διαδικασία της ενεργοποίησης στα παλαιότερα συστήματα AGC αφορούσε σε άμεσες δράσεις (ενέργειες) στα συστήματα ελέγχου των γεννητριών παραγωγής. Στα σύγχρονα συστήματα διαχείρισης και ελέγχου ισχύος, οι μεταβολές συχνότητας συνεπάγονται λήψη αποφάσεων, οι οποίες υλοποιούνται στα κέντρα Διαχείρισης Ενέργειας που διαχειρίζονται συνολικά τα συστήματα AGC και το δίκτυο.

1.1.2 Τα αρχικά συστήματα AGC ως βασικοί ρυθμιστές ελέγχου των ηλεκτρικών γεννητριών

Τα συστήματα AGC αποτελούν τη βάση ελέγχου για την παραγωγή και την εξισορρόπηση της ισχύος σε ένα δίκτυο. Η αρχική τους εφαρμογή εμφανιζόταν στον απευθείας έλεγχο της παραγωγής ισχύος από τις ηλεκτρογεννήτριες. Αρχικά ήταν προσαρμοσμένα ως κυκλώματα αυτομάτου ελέγχου επί των γεννητριών,

διασφαλίζοντας σε μικρή κλίμακα την ορθή λειτουργία των τοπικών συστημάτων παραγωγής. Η λειτουργία τους βασιζόταν στις αρχές ελέγχου λειτουργίας των γεννητριών με απευθείας μετρήσεις επί των εξόδων διανομής ισχύος αυτών.
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, η οποία είναι άμεσα ανάλογη με τη μείωση της συχνότητας του δικτύου **[3]**. Στο σχήμα που ακολουθεί, παρουσιάζεται μία βασική δομή ελέγχου της γεννήτριας ενός δικτύου, η οποία συνθέτει ένα βασικό σύστημα ελέγχου AGC ως ρυθμιστή για την εξισορρόπηση παραγόμενης και καταναλισκόμενης ισχύος.



Σχήμα 1: Block διάγραμμα Αυτόματου ελέγχου συχνότητας

Στο **Σχήμα 1** παρουσιάζεται ένας τέτοιος κλειστός βρόχος δράσης για τον έλεγχο μίας γεννήτριας. Ο βασικός σκοπός του ελεγκτή είναι να διατηρήσει την επιθυμητή συχνότητα του συστήματος ρυθμίζοντας τη μηχανική ισχύ εξόδου της γεννήτριας **[2]**. Οι ελεγκτές αυτού του τύπου έχουν γίνει αυτοματοποιημένοι, και σε σταθερή κατάσταση, η σχέση συχνότητας-ισχύος είναι,

$$\Delta p_m = \Delta p_{ref} - \frac{\Delta f}{R}$$

Όπου:

Δp_m αποτελεί την αλλαγή μηχανικής ισχύος στην έξοδο της τουρμπίνας – γεννήτριας

Δp_{ref} αποτελεί την αλλαγή στο δεδομένο σημείο αναφοράς ισχύος

R είναι η σταθερά κανονικοποίησης η οποία ποσοτικοποιεί την ευαισθησία της γεννήτριας ως προς την αλλαγή της συχνότητας

Δf είναι το διάστημα μεταβολής της συχνότητας

Η παραπάνω εξίσωση αποτελεί τη βάση λειτουργίας ενός ελεγκτή – πρωτογενούς συστήματος AGC σε συνδεσμολογία κλειστού βρόχου. Στόχος του ελεγκτή είναι η σταθεροποίηση της προσφερόμενης ισχύος, εξισορροπώντας τα φορτία και διατηρώντας το επίπεδο αλλαγής συχνότητας όσο το δυνατόν πιο χαμηλό.

1.1.3 Η μετεξέλιξη των αρχικών συστημάτων AGC στα σύγχρονα συστήματα ελέγχου

Τα σύγχρονα συστήματα AGC αποτελούν επεκτάσεις της παραπάνω βασικής δομής ελέγχου του επιπέδου παραγωγής ισχύος μίας γεννήτριας, με κλιμάκωση η οποία αφορά τόσο στην έκταση του δικτύου κάλυψης όσο και στο πλήθος των διασυνδεόμενων περιοχών ελέγχου (σε περιοχές οι οποίες ελέγχονται από πολλαπλά συστήματα AGC που διασυνδέονται και επικοινωνούν μεταξύ τους).
Επιπλέον, τα σύγχρονα συστήματα AGC περιλαμβάνουν υποσυστήματα διακίνησης και διαχείρισης πληροφορίας με ηλεκτρονικό τρόπο, βασίζοντας τη λήψη αποφάσεων σε πρωτόκολλα χειρισμού της ισχύος για ομαλή λειτουργία, δηλ. έχουν εξελιχθεί σημαντικά σε σχέση με τα πρωταρχικά συστήματα ελέγχου των γεννητριών που παρουσιάστηκαν και τα οποία βασίζονταν στη χρήση κλειστών κυκλωμάτων ελέγχου με αναλογικά σήματα.

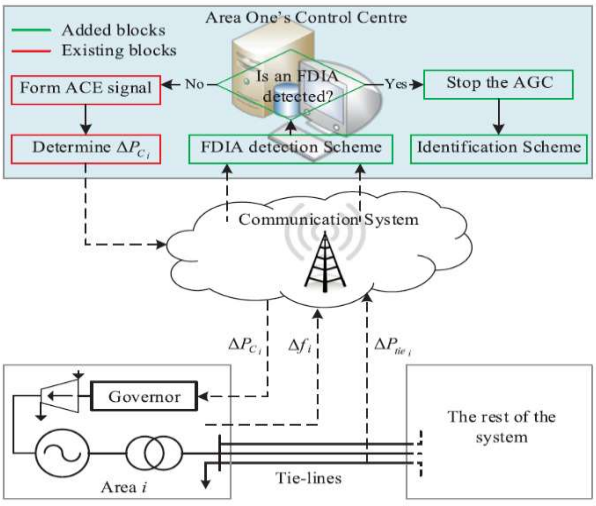
1.2 Πεδίο Εφαρμογής και Αρχιτεκτονικές διασύνδεσης των σύγχρονων AGC συστημάτων

Ο έλεγχος των διασυνδεδεμένων συστημάτων ισχύος έχει καταστεί πιο σημαντικός, καθώς το μέγεθος και η πολυπλοκότητα του συνολικού συστήματος παραγωγής ισχύος αυξάνεται για να καλύψει τη ζήτηση **[3]**, **[5]**. Ένας μεγάλος αριθμός τεχνικών ελέγχου έχει προταθεί από τους ερευνητές για το σχεδιασμό των σύγχρονων ρυθμιστικών αρχών για τα συστήματα AGC **[6]**, **[7]**.
Στις πρώτες εποχές, οι στρατηγικές AGC προτάθηκαν βάσει στρατηγικής κεντρικού ελέγχου (centralized control model). Ένας σημαντικός περιορισμός της στρατηγικής κεντρικού ελέγχου AGC, είναι ότι απαιτεί την ανταλλαγή πληροφοριών από το σταθμό λήψης αποφάσεων με τους αισθητήρες μετρήσεων, διασπείροντας 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 – φορτίου για την περιοχή την οποία χειρίζεται το υποσύστημα ελέγχου.
Οι εργασίες **[24]**, [55] (2011) πρότειναν μία μέθοδο για την ανάλυση της σταθερότητας του συστήματος ισχύος πολλαπλών περιοχών με την καταγραφή της μορφολογίας διασύνδεσης του συστήματος ισχύος σε πολλαπλές περιοχές. Σε άλλη ερευνητική εργασία [56] προτείνεται η χρήση ελεγκτή ασαφούς λογικής (fuzzy logic) για αποκεντρωμένο σύστημα διασύνδεσης δύο ζωνών, λαμβάνοντας υπόψιν τον περιορισμό του ρυθμού παραγωγής.

1.2.1 Περιοχές δράσης των συστημάτων AGC

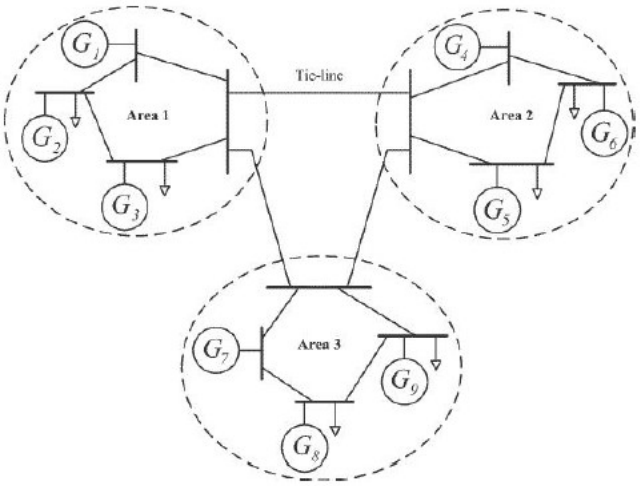
Από τα παραπάνω γίνεται εμφανές ότι οι σύγχρονες αρχιτεκτονικές χρήσης των τεχνικών AGC αφορούν τόσο σε κεντρική όσο και σε αποκεντρωμένη διασύνδεσή τους, με ανάλογα πλεονεκτήματα και μειονεκτήματα για την κάθε αρχιτεκτονική **[6]**, [7].
Η δράση του AGC μπορεί επίσης να κατηγοριοποιηθεί ανάλογα με το πλήθος των περιοχών ελέγχου , είτε σε σύστημα απλής 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 για τη διασφάλιση της ισορροπίας ισχύος στο σύνολο όλων των περιοχών ελέγχου.
Στα σχήματα που ακολουθούν δίνονται δομικά διαγράμματα (blocks) για την εφαρμογή ελέγχου απλής περιοχής/πολλαπλών περιοχών με χρήση AGC υποσυστημάτων.



Σχήμα 2: Παράδειγμα εφαρμογής υποσυστήματος ελέγχου AGC σε απλή περιοχή (single – area)

Στο Σχήμα 2 παρουσιάζεται ο χειρισμός του συστήματος AGC για μία απλή περιοχή, λαμβάνοντας υπόψιν τα ποσά ισχύος που απαιτούνται στην περιοχή, καθώς και τα φορτία της περιοχής ελέγχου. Η λήψη απόφασης γίνεται μετά τη συγκέντρωση της

πληροφορίας στο τοπικό σύστημα Διαχείρισης Ενέργειας. Στις απλές περιοχές ένα σύστημα AGC καλείται αυτόνομα να επιλύσει το πρόβλημα εξισορρόπησης ισχύος.



Σχήμα 3: Παράδειγμα εφαρμογής υποσυστήματος ελέγχου AGC πολλαπλών περιοχών (multi - area)

Στις πολλαπλές περιοχές απαιτείται συναρμογή και συλλειτουργία πολλών τοπικών δομών AGC, οι οποίες είναι υπεύθυνες τόσο για την τοπική εξισορρόπηση καθώς και για τα ανταλλασσόμενα επίπεδα ισχύος μεταξύ των περιοχών. Στις εφαρμογές πολλαπλών περιοχών με χρήση AGC, διαταραχές που αφορούν στην ισχύ και τη συχνότητα λειτουργίας μίας περιοχής, διαδίδονται και αντανακλώνται και στις υπόλοιπες περιοχές λόγω της ζεύξης ισχύος και διασύνδεσης μεταξύ τους. Κατά συνέπεια, η ρύθμιση των συστημάτων AGC για χειρισμό πολλαπλών περιοχών αποτελεί ένα πιο σύνθετο πρόβλημα από το χειρισμό απλών περιοχών, παρέχοντας όμως το πλεονέκτημα της πολλαπλής όδευσης στη διανομή ισχύος από εναλλακτικούς παρόχους ισχύος προς τα φορτία. Το τελευταίο χαρακτηριστικό επιτρέπει τη δυνατότητα βελτιστοποιημένης τιμολόγησης για την επίτευξη μειωμένου κόστος στην παροχή ισχύος προς τους τελικούς καταναλωτές. Αυτό βασίζεται στο ότι ένα σύστημα πολλαπλών περιοχών μπορεί να αξιοποιεί ετερογενή συστήματα παραγωγής ισχύος, όπως Α.Π.Ε., ανεμογεννήτριες, υδροστρόβιλους, κλπ, εξισορροπώντας κατά τον οικονομικότερο τρόπο τις μεταβαλλόμενες ανάγκες ζήτησης ισχύος στο σύνολο των περιοχών που ελέγχει.
Οι απαιτήσεις ισχύος κάθε περιοχής αποτελούν εισόδους για ένα μοντέλο περιγραφής της λειτουργίας ενός δικτύου, δίνοντας σαν εξόδους τις εντολές για τα επίπεδα ισχύος που απαιτούνται για την κάλυψη των αναγκών διαχείρισης. Αυτό το μοντέλο ανταλλαγής σημάτων εισόδων/εξόδων αποτελεί και τη βάση για μία μαθηματικοποιημένη περιγραφή εξισώσεων κατάστασης, που θα δοθεί στη συνέχεια της ενότητας.
Επομένως, μία εφαρμογή σε πολλαπλή περιοχή κάλυψης από τον AGC θα πρέπει να λάβει υπόψιν της όλες τις καταστάσεις των γεννητριών – παρόχων, καθώς και τις τοπικές - γενικές μεταβολές φορτίου. Οι τελευταίες θα εισάγουν μεταβολές συχνότητας που θα ανιχνευθούν συνολικά από τις μετρητικές διατάξεις του συστήματος. Ο κεντρικός έλεγχος θα πρέπει να αναλάβει δράση με την παροχή εντολών προς τις υπομονάδες, για να ελαχιστοποιήσει τις παρατηρούμενες μεταβολές συχνότητας. Η ζεύξη ισχύος σε συστήματα πολλαπλών περιοχών αποτελεί

ένα εγγενές μειονέκτημα και ταυτόχρονα ένα σημαντικό πλεονέκτημα. Μειονέκτημα, διότι οι μεταβολές φορτίου μίας περιοχής επιδρούν στη συχνότητα λειτουργίας για τη διανεμόμενη ισχύ στις υπόλοιπες περιοχές που βρίσκονται σε ζεύξη. Πλεονέκτημα της τοπολογίας είναι η δυνατότητα κάλυψης των μεταβαλλόμενων φορτίων από πολλαπλές διαδρομές ισχύος, αξιοποιώντας την πολύπλευρη παροχή ισχύος. Ο χειρισμός για την παραγωγή ισχύος σε πολλαπλές περιοχές μπορεί να συνδυαστεί με διαφορετικά κόστη λειτουργίας και παραγωγής (ανάλογα με τον πάροχο από τον οποίο αγοράζεται η ενέργεια και την τεχνολογία παραγωγής που αυτός χρησιμοποιεί), δίνοντας έτσι ένα πρόβλημα για την οικονομική βελτιστοποίηση της παρεχόμενης ισχύος προς τους καταναλωτές. Αυτή η προσέγγιση μπορεί να αποτελέσει ένα επιπρόσθετο οικονομικό πρόβλημα βελτιστοποίησης, πλέον του αρχικού προβλήματος ελέγχου ισχύος που χειρίζονται τα συστήματα AGC.

1.3 Βασικές Λειτουργίες των αρχικών AGC συστημάτων για τον έλεγχο των γεννητριών παραγωγής

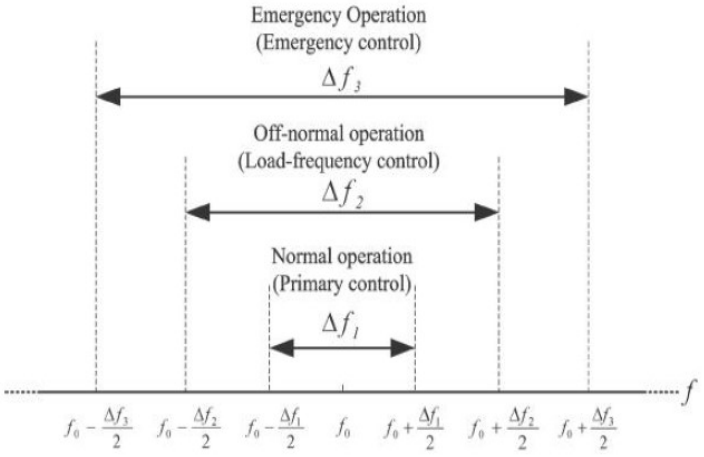
Όπως παρουσιάστηκε και στην προηγούμενη ενότητα, τα αρχικά AGC συστήματα αποτελούν ένα μέρος από τα δομικά υποσυστήματα που χρησιμοποιεί ένα σύγχρονο σύστημα Διαχείρισης Ενέργειας για τη λήψη αποφάσεων και τον συνολικό έλεγχο του δικτύου κάλυψης. Οι λειτουργίες των συστημάτων AGC, εφόσον έρχονται σε άμεση επικοινωνία με τους σταθμούς παραγωγής ισχύος – γεννήτριες του δικτύου, θα πρέπει να παρέχουν άμεσες λειτουργίες ελέγχου που βασίζονται στις δομές και τα σήματα ελέγχου των γεννητριών. Ο παραδοσιακός AGC έλεγχος **[1]** βασίζεται στη δυνατότητα και την εφαρμογή δράσεων επί των γεννητριών του συστήματος που επιτηρούν. Στη συνέχεια θα παρουσιαστούν αναλυτικά:

- Η έννοια του ελέγχου συχνότητας στα συστήματα AGC.
- Η εσωτερική δομή ενός συστήματος AGC. Το μοντέλο του υποσυστήματος μετρήσεως συχνότητας LFC.
- Τα συστήματα AGC και η απόκριση συχνότητας
- Η παράμετρος πτώσης ισχύος (droop) για τα συστήματα AGC.
- Το γραμμικοποιημένο μοντέλο απόκρισης συχνότητας του συστήματος AGC

Οι παραπάνω έννοιες αποτελούν σημαντικά χαρακτηριστικά των πρωταρχικών υποσυστημάτων AGC και άπτονται θεμελιωδών λειτουργιών των γεννητριών και της παραγωγής ισχύος **[1]**. Ο ρόλος των παραμέτρων που ορίζουν εξακολουθεί να είναι θεμελιώδης και στα σύγχρονα συστήματα Διαχείρισης Ενέργειας, δεδομένου ότι ο έλεγχος και η λήψη αποφάσεων από τα σύγχρονα ψηφιακά κέντρα ελέγχου, εξακολουθεί να λαμβάνει υπόψιν του σήματα – δράσεις που επιδρούν επί των γεννητριών παραγωγής στο δίκτυο.

1.3.1 Έλεγχος συχνότητας του συστήματος παροχής ισχύος

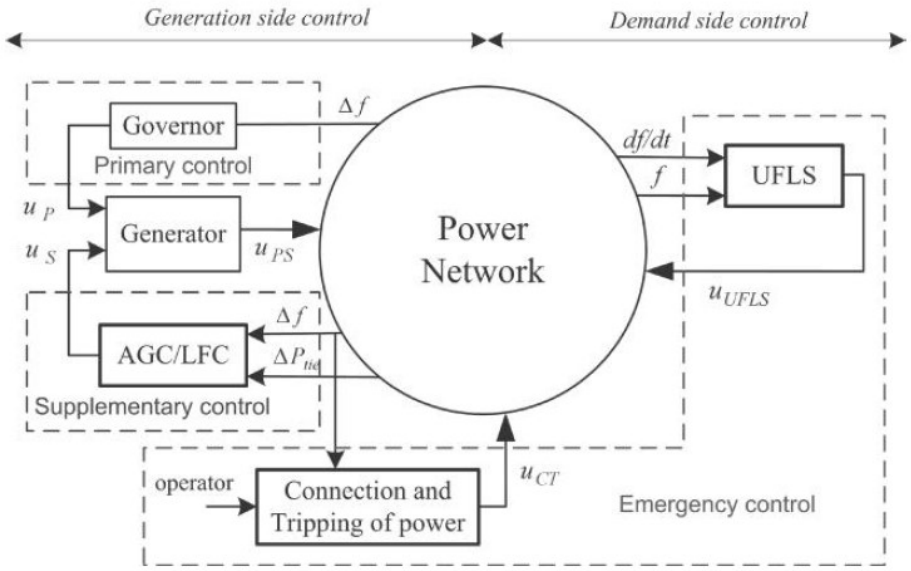
Η απόκλιση συχνότητας (frequency deviation) είναι άμεσο αποτέλεσμα της ανισορροπίας μεταξύ του ηλεκτρικού φορτίου και της παροχής ισχύος από τις συνδεδεμένες γεννήτριες στο δίκτυο και αποτελεί την πρωταρχική μετρική βάση για την ανίχνευση και τον έλεγχο της εξισορρόπησης. Έτσι, η απόκλιση συχνότητας παρέχει ένα χρήσιμο δείκτη για την ένδειξη της παραγόμενης ισχύος και της ανισορροπίας φορτίου - κατανάλωσης. Μία μόνιμη μεταβολή της κανονικής συχνότητας επηρεάζει άμεσα τη λειτουργία του συστήματος ισχύος, την ασφάλεια, την αξιοπιστία και την αποτροπή καταστροφής του διασυνδεόμενου ηλεκτρικού εξοπλισμού στο δίκτυο. Επίσης, αποτρέπει την υποβάθμιση της λειτουργίας των φορτίων, τη μείωση της απόδοσης, την υπερφόρτωση των γραμμών μεταφοράς και την ενεργοποίηση της προστασίας για τις συνδεδεμένες συσκευές στο δίκτυο.
Δεδομένου ότι η συχνότητα που παράγεται στο ηλεκτρικό δίκτυο είναι ανάλογη προς την ταχύτητα περιστροφής της γεννήτριας, το πρωταρχικό πρόβλημα του ελέγχου συχνότητας 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 (ως αίτιο παραγωγής ισχύος δηλ, diesel, ποσότητα νερού, πυρηνικό καύσιμο, κλπ) για να αλλάξει το μηχανικό επίπεδο ισχύος στην έξοδο, παρακολουθώντας ταυτόχρονα τα φορτία, επαναφέροντας έτσι τη συχνότητα στην ονομαστική τιμή λειτουργίας για το δίκτυο.
Ανάλογα με την περιοχή απόκλισης συχνότητας **[1]**, όπως φαίνεται στο σχήμα που ακολουθεί, τρεις τύποι ελέγχου αναλαμβάνουν να αποκαταστήσουν τη συχνότητα λειτουργίας. Επιπρόσθετα με τον πρωτεύοντα έλεγχο της γεννήτριας που είναι γνωστός ως ο πρωταρχικός έλεγχος (primary control), υπάρχει και συμπληρωματικός έλεγχος (AGC) γνωστός ως δευτερεύων έλεγχος (secondary control), καθώς και ο έλεγχος έκτακτης ανάγκης (emergency control). Οι παραπάνω έλεγχοι αποτελούν το σύνολο των ελεγκτικών μηχανισμών στο επίπεδο μίας γεννήτριας, που θα χρησιμοποιηθούν για να διατηρήσουν τη συχνότητα του ηλεκτρικού συστήματος.



Σχήμα 4: Μεταβολές συχνότητας και οι συσχετιζόμενοι έλεγχοι

Στο παραπάνω σχήμα, η f είναι η ονομαστική συχνότητα και οι Δf_1, Δf_2 και Δf_3 δείχνουν τα εύρη διακύμανσης συχνότητας που αντιστοιχούν στις διαφορετικές

συνθήκες λειτουργίας βάσει των αποδεκτών προτύπων λειτουργίας για τη συχνότητα του δικτύου παροχής ισχύος.
Υπό κανονική λειτουργία, οι μικρές αποκλίσεις συχνότητας μπορούν να ελαχιστοποιηθούν από τον κύριο έλεγχο. Για μεγαλύτερη απόκλιση συχνότητας (εκτός κανονικής λειτουργίας), σύμφωνα με το διαθέσιμο ποσό αποθεματικού ισχύος, ο έλεγχος AGC, που βασίζεται στη λειτουργία του υποσυστήματος LFC (Load Frequency Control) είναι υπεύθυνος για την επαναφορά της συχνότητας του συστήματος. Η λειτουργία και η δομή του LFC αποτελεί εσωτερική δομή του AGC και θα παρουσιασθεί αναλυτικά στην επόμενη παράγραφο. Ωστόσο, για μία σοβαρή ανισορροπία φορτίων που σχετίζεται με ταχείες μεταβολές συχνότητας μετά από σημαντικό σφάλμα, το σύστημα AGC ενδέχεται να μην μπορεί να αποκαταστήσει τη συχνότητα μέσω του συμπληρωματικού συστήματος ελέγχου συχνότητας.
Σε αυτή την περίπτωση, ο έλεγχος έκτακτης ανάγκης πρέπει να ενεργοποιηθεί για να μειωθεί ο κίνδυνος αλυσιδωτών βλαβών, αποτροπή ενεργειών από το δίκτυο προς τα φορτία και συμβάντα αποκοπής των φορτίων από το δίκτυο (power down).

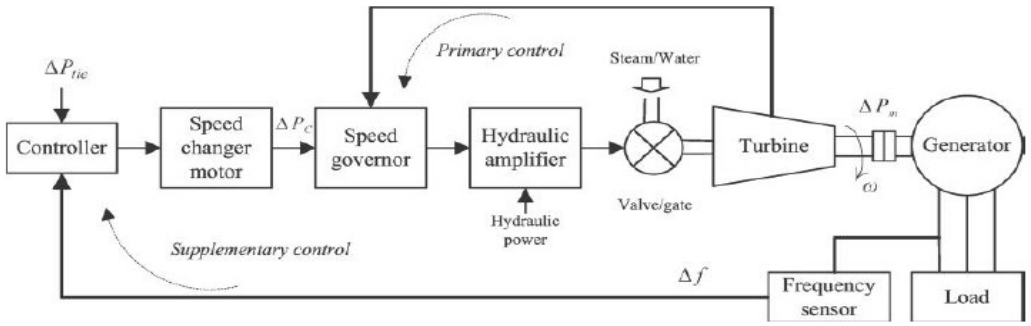


Σχήμα 5: Βρόχοι Ελέγχου της συχνότητας λειτουργίας του δικτύου

Στο Σχήμα 5 παρουσιάζονται οι τρεις τύποι ελέγχου που περιγράφηκαν, σε εφαρμογή σε ένα δίκτυο ισχύος (με περισσότερες ενδεχομένως από μία γεννήτρια).

1.3.2 Εσωτερική δομή του AGC ως σύστημα δευτερεύοντος ελέγχου. Ο έλεγχος συχνότητας LFC

Εκτός από τον πρωτεύοντα έλεγχο συχνότητας για την παραγωγή εξισορροπημένης ισχύος, όπως παρουσιάστηκε και στο προηγούμενο σχήμα, μία μεγάλη σύγχρονη γεννήτρια είναι εφοδιασμένη με συμπληρωματικό βρόχο ελέγχου συχνότητας (AGC) **[1]**. Ένα σχηματικό block διάγραμμα μίας σύγχρονης γεννήτριας εξοπλισμένης με πρωτεύοντα και συμπληρωματικό βρόχο ελέγχου συχνότητας, σε μορφή block διαγραμμάτων παρουσιάζεται στο ακόλουθο σχήμα:



Σχήμα 6: Δυετερεύων Βρόχος Ελέγχου της συχνότητας του δικτύου μέσω AGC

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 ΔP_c) 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 ΔP_m) για να αποδώσει τη ζητούμενη ισχύ στο φορτίο και να επαναφέρει τη συχνότητα του συστήματος.

Ορισμός: Ο συμπληρωματικός έλεγχος συχνότητας, είναι γνωστός ως έλεγχος συχνότητας φορτίου (Load Frequency Control - **LFC**), και αποτελεί βασική λειτουργία των συστημάτων AGC.

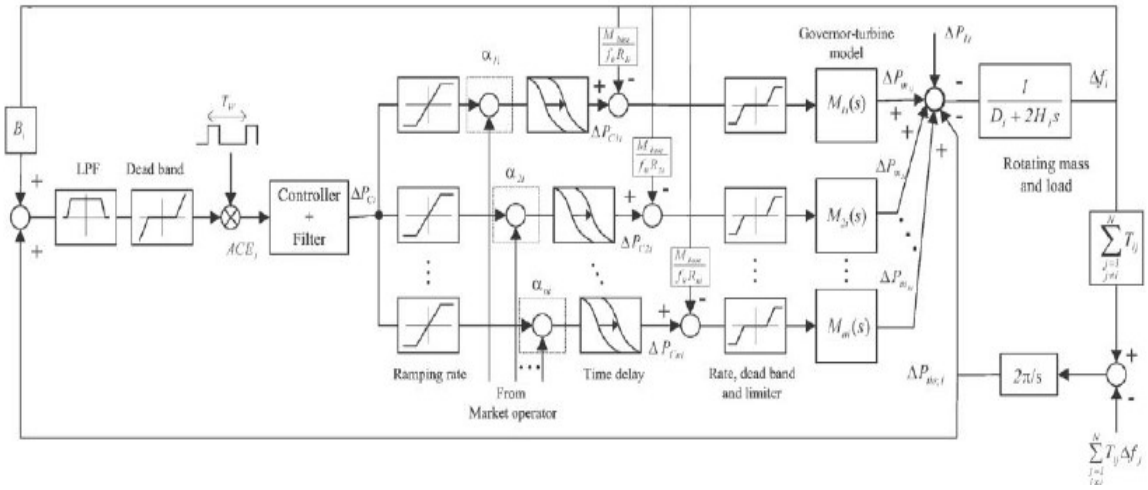
Όπως αναφέρθηκε, η απόδοση του AGC εξαρτάται σε μεγάλο βαθμό από τον τρόπο με τον οποίο οι κύριες μονάδες παραγωγής ισχύος θα ανταποκριθούν στα σήματα της δράσης ελέγχου.
Κατά τη διάρκεια μίας ξαφνικής αύξησης του φορτίου περιοχής, η συχνότητα της περιοχής παρουσιάζει μία παροδική πτώση. Η πτώση αυτή μπορεί να διαδοθεί και στις υπόλοιπες περιοχές χειρισμού, εφόσον πρόκειται για ένα σύστημα ελέγχου πολλαπλών περιοχών με κεντρικό έλεγχο. Στη μεταβατική κατάσταση, προορίζονται ροές ισχύος από άλλες περιοχές για την κάλυψη του υπερβολικού φορτίου που ανέκυψε 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 συμφωνεί στενά με τα φορτία ζήτησης, προκαλώντας σχεδόν μηδενικές αποκλίσεις ισχύος και συχνότητας **[6]**.

1.3.3 Χαρακτηριστικά του ελέγχου AGC και μοντέλο απόκρισης συχνότητας

Σε ένα διασυνδεδεμένο σύστημα ισχύος πρέπει να χρησιμοποιηθεί η έννοια της περιοχής ελέγχου για λόγους σύνθεσης και ανάλυσης του συστήματος AGC.

Ορισμός: Η **περιοχή ελέγχου** είναι μία συνεκτική περιοχή που αποτελείται από μία ομάδα γεννητριών και φορτίων, όπου όλες οι γεννήτριες απαντούν σε αλλαγές στα φορτία ή τις ρυθμίσεις αλλαγής ταχύτητας περιστροφής, από κοινού.

Η συχνότητα λειτουργίας θεωρείται ότι είναι η ίδια σε όλα τα σημεία μίας περιοχής ελέγχου. Ένα σύστημα πολλαπλών περιοχών περιλαμβάνει περιοχές που διασυνδέονται συνήθως με γραμμές μεταφοράς ή γραμμές σύνδεσης υψηλής τάσης. Το σύστημα AGC είναι ένα διασυνδεδεμένο σύστημα ισχύος το οποίο θα πρέπει να ελέγχει τη συχνότητα περιοχής, καθώς και την ανταλλαγή ισχύος με τις άλλες περιοχές ελέγχου.
Ένα μοντέλο απόκρισης συχνότητας για μία περιοχή ελέγχου i για ένα σύστημα ελέγχου πολλαπλών περιοχών (multi - area) σε μορφή block διαγραμμάτων παρουσιάζεται στο ακόλουθο σχήμα **[1]**, **[5]**:



Σχήμα 7: Ένα μοντέλο απόκρισης συχνότητας για ανάλυση επιδόσεων σε πολλαπλές περιοχές

Σε μία πρακτική εφαρμογή του AGC, για να καθορισθούν οι γρήγορες μεταβολές συχνότητας και πιθανόν προστιθέμενοι θόρυβοι και η σταδιακή υποβάθμιση συχνότητας του συστήματος, απαιτείται τα σήματα **ACE** που διαδίδονται να φιλτραριστούν πριν να χρησιμοποιηθούν από το σύστημα ελέγχου **[4]**.

Ορισμός: Οι αντικειμενικοί στόχοι του AGC θέτουν ως βάση μία παράμετρο επιπέδου ισχύος B για μία περιοχή. Είναι επιθυμητό το AGC σε κάθε περιοχή ελέγχου να παρέχει σήματα ελέγχου που διασφαλίζουν ένα επίπεδο ισχύος, η οποία κατά γενικό κανόνα να αποτελεί το άθροισμα του φορτίου και των απωλειών της συγκεκριμένης περιοχής. Η διαφορά παραγόμενης ισχύος, καταναλισκόμενης ισχύος από τα φορτία και ενός κατωφλίου ισχύος (threshold) καλείται Σφάλμα Ελέγχου Περιοχής (Area Control Error – **ACE**).

Ο ελεγκτής που βασίζει τη λειτουργία του στο σήμα ACE μπορεί να ενεργοποιηθεί για να στείλει υψηλούς/χαμηλότερους παλμούς σήματος στις συμμετέχουσες γεννήτριες εφόσον το σήμα εισόδου του ACE υπερβαίνει ένα τυποποιημένο όριο - κατώφλι. Οι καθυστερήσεις (delays), ο ρυθμός αύξησης (ramping rate) και τα όρια

εύρους ενεργοποίησης (range limits) 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).
Όσον αφορά το όριο παραγωγής, τη νεκρή ζώνη για τη λήψη απόφασης (dead band) και τις χρονικές καθυστερήσεις, το μοντέλο AGC που είναι εξαρτώμενο από τις παραπάνω παραμέτρους γίνεται ισχυρά μη γραμμικό ως προς αυτές **[1]**. Ως εκ τούτου, θα είναι δύσκολο να χρησιμοποιηθεί σε συνδυασμό με τις συμβατικές γραμμικές τεχνικές βελτιστοποίησης και ελέγχου απόδοσης. Επομένως, στόχος είναι ο καθορισμός των παραπάνω παραμέτρων σε τοπικό επίπεδο, διατηρώντας μία γραμμικοποιημένη λειτουργία του συστήματος AGC από το αρχικό μη γραμμικό μοντέλο περιγραφής.
Σε καμία περίπτωση δεν είναι επιθυμητό, ακόμη και αν αυτό είναι δυνατό, να προσπαθήσουμε να μηδενίσουμε την παράμετρο μόνιμα. Ο λόγος είναι ότι αυτό θα απαιτούσε πολύ γρήγορες μεταβολές για τις μονάδες παραγωγής ισχύος μέσω των διαδιδόμενων σημάτων ελέγχου. Ο καθορισμός της τιμής του παραπάνω ορίου ως ένα κατώφλι (κατώφλι δράσης), αποτελεί ένα ανοικτό ερευνητικό θέμα για τα υποσυστήματα ελέγχου AGC.

1.3.4 Η παράμετρος Πτώσης Ισχύος (droop)

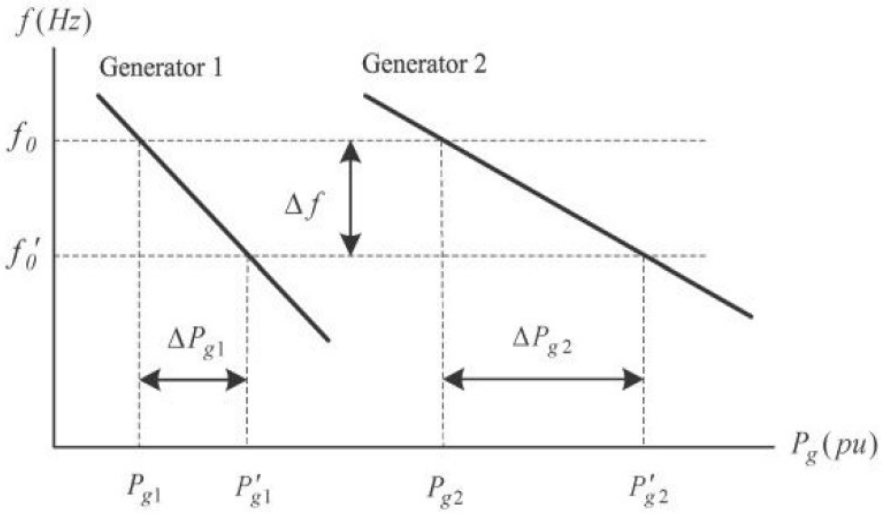
Όπως αναφέρθηκε και στην προηγούμενη ενότητα, η αλλαγή συχνότητας που διαπιστώνεται στο δίκτυο έχει άμεση επίδραση στην απαιτούμενη μεταβολή ισχύος στο επίπεδο της εξόδου ισχύος μίας γεννήτριας. Η παράμετρος αυτή είναι διαφορετική από γεννήτρια σε γεννήτρια ενός συστήματος παραγωγής και καλείται παράμετρος πτώσης ισχύος (droop).

Ορισμός: Ο λόγος της αλλαγής συχνότητας (Δf) προς την αλλαγή στην παραγόμενη ισχύ εξόδου μιας γεννήτριας (ΔP_g) είναι γνωστός ως **ρύθμιση πτώσης ισχύος** (**droop**) και μπορεί να εκφραστεί ως

$$R\left({}^{Hz}/_{pu.MW}\right) = \frac{\Delta f}{\Delta P_g}$$

Για παράδειγμα, μία πτώση 5% σημαίνει ότι υπάρχει απόκλιση 5% στην ονομαστική συχνότητα λειτουργίας του δικτύου (από 50 έως 52.5 Hz ή από 47.5 έως 50 Hz) και αυτό προκαλεί 100% αλλαγή στην ισχύ εξόδου. Στο **Σχήμα 7**, τα χαρακτηριστικά πτώσης για τις μονάδες παραγωγής (R_{ki}) εμφανίζονται ως παράμετροι του μοντέλου στους κύριους βρόχους ελέγχου συχνότητας.
Οι διασυνδεδεμένες μονάδες παραγωγής με διαφορετικά χαρακτηριστικά πτώσης (droop) μπορούν να παρακολουθήσουν από κοινού την αλλαγή φορτίου για να επαναφέρουν την ονομαστική συχνότητα λειτουργίας του συστήματος.
Αυτό απεικονίζεται στο σχήμα που ακολουθεί, για δύο διαφορετικές μονάδες παραγωγής ισχύος με διαφορετικό χαρακτηριστικό πτώσης, οι οποίες τροφοδοτούν ένα κοινό φορτίο. Δύο μονάδες παραγωγής λειτουργούν σε μία μοναδική

ονομαστική συχνότητα προσφέροντας διαφορετικές ισχύες εξόδου, εξαιτίας του διαφορετικού συντελεστή πτώσης που αυτές εμφανίζουν.



Σχήμα 8: Παρακολούθηση φορτίου από δύο γεννήτριες με διαφορετικά χαρακτηριστικά πτώσης ισχύος

Η αλλαγή στο φορτίο δικτύου αναγκάζει τις μονάδες να μειώσουν την ταχύτητα περιστροφής τους και οι ρυθμιστές να αυξήσουν τις εξόδους τους μέχρι να φτάσουν σε μία νέα κοινή συχνότητα λειτουργίας. Όπως εκφράζεται στην παρακάτω εξίσωση, η ποσότητα παραγόμενης ισχύος για κάθε μονάδα παραγωγής για να ανταπεξέλθει στην αλλαγή του φορτίου, εξαρτάται από το χαρακτηριστικό droop κάθε μονάδας **[7],[8]**.

$$\Delta P_{gi} = \frac{\Delta f}{R_i}$$

Έτσι ώστε:

$$\frac{\Delta P_{g1}}{\Delta P_{g2}} = \frac{R_2}{R_1}$$

Άρα, για την επίτευξη και αποκατάσταση της ονομαστικής συχνότητας λειτουργίας στο κοινό φορτίο οι γεννήτριες είναι υποχρεωμένες να μεταβάλλουν με διαφορετικό τρόπο τα παραγόμενα ποσά ισχύος τους.

1.3.5 Το γραμμικοποιημένο μοντέλο παραγωγής ισχύος - φορτίου

Για τους σκοπούς της σύνθεσης και ανάλυσης των υποσυστημάτων AGC παρουσία διαταραχών φορτίου, χρησιμοποιείται συνήθως ένα απλό, χαμηλής τάξης, γραμμικοποιημένο μοντέλο, με βάση το μη γραμμικό σύστημα που παρουσιάστηκε στο **Σχήμα 7**. Η συνολική δυναμική σχέση φορτίου γεννήτριας μεταξύ της

στοιχειώδους μεταβολής του επιπέδου ισχύος (ΔP_m - ΔP_L) και την απόκλιση συχνότητας (Δf) μπορεί να εκφραστεί ως **[9]**:

$$\Delta P_m(t) - \Delta P_L(t) = 2H\frac{d\Delta f(t)}{dt} + D\Delta f(t)$$

όπου ΔP_m είναι η μηχανική αλλαγή ισχύος, ΔP_L είναι η αλλαγή του επιπέδου ισχύος του φορτίου, H είναι η σταθερά αδράνειας του συστήματος, και D είναι ο παράγοντας απόσβεσης (damping) του φορτίου.
Κάνοντας χρήση μετασχηματισμού Laplace, η παραπάνω εξίσωση ισοδύναμα έρχεται στη μορφή:

$$\Delta P_m(s) - \Delta P_L(s) = 2Hs\Delta f(s) + D\Delta f(s)$$

η οποία αποτελεί και την εξίσωση της δυναμικής συμπεριφοράς για το συνολικό μοντέλο που καλύπτει το block διάγραμμα περιγραφής που παρουσιάστηκε στο **Σχήμα 7**.
Ο λόγος για τη διαδικασία γραμμικοποίησης του μοντέλου του υποσυστήματος AGC είναι η απλούστευση της μαθηματικής περιγραφής του υποσυστήματος, με αποτέλεσμα να μπορεί να χρησιμοποιηθεί κατά την εφαρμογή και ανάπτυξη γραμμικών τεχνικών βελτιστοποίησης. Επομένως, η γραμμικοποίηση προσφέρει μία επαρκή μαθηματική βάση για τη μετατροπή ενός σύνθετου μη-γραμμικού προβλήματος στη γενικότητά του, σε ένα ισοδύναμο γραμμικοποιημένο μοντέλο, διευκολύνοντας την εφαρμογή γραμμικών περιγραφών στη συνολική διαδικασία μοντελοποίησης και προσομοίωσης αυτών των συστημάτων.

1.4 Μαθηματικά μοντέλα καταστάσεων περιγραφής της λειτουργίας των υποσυστημάτων AGC

Το AGC τείνει να συμπεριλάβει όλα τα δομικά στοιχεία (γεννήτριες – ζυγοί διανομείς ισχύος – συστήματα παρακολούθησης λειτουργίας – αισθητήρες – καταγραφείς – ενεργοποιητές - actuators), τα οποία συνδυάζονται σε καθορισμένες αρχιτεκτονικές, με στόχο την απρόσκοπτη παροχή και παρακολούθηση ισχύος στα τελικά φορτία καταναλωτών **[1]**. Η εφαρμογή και χρήση των συστημάτων AGC αναφέρεται τόσο σε μικρής όσο και σε μεγαλύτερης κλίμακας συστήματα παραγωγής και διανομής ηλεκτρικής ισχύος, που μπορεί να κυμαίνονται μέχρι και σε αρκετές δεκάδες πλήθους ζυγών φορτίων. Ένα από τα σημαντικά χαρακτηριστικά των συστημάτων AGC είναι η διασυνεχής παρακολούθηση της λειτουργίας του δικτύου παροχής, καθώς και του επιπέδου ποιότητας της παρεχόμενης ισχύος στους τελικούς καταναλωτές (επίπεδα τάσεως, επίπεδα ισχύος για την κάλυψη των ενεργειακών αναγκών, έλεγχος συχνότητας και φάσεων διανομής, αρμονικές παρεχόμενης ισχύος, κλπ). Το σύστημα που υλοποιεί την τεχνολογία AGC συμπεριλαμβάνει τόσο τις δράσεις όσο και τις αντιδράσεις (δυναμικές συμπεριφορές) για τη διόρθωση των αναπτυσσόμενων σφαλμάτων κατά τη λειτουργία εκτός των καθορισμένων ορίων και προδιαγραφών για τα δίκτυα ηλεκτρικής ισχύος.

Αρχιτεκτονικά τα συστήματα AGC μπορούν να κατηγοριοποιηθούν σε δύο κατευθύνσεις:

Στην απλούστερη υλοποίησή τους συνίστανται από τους αισθητήρες ελέγχου και μετρήσεων, οι οποίοι επιστρέφουν τις καταγραφόμενες μετρήσεις με καθορισμένο ρυθμό (rate) από το δίκτυο, οπότε η λήψη αποφάσεων αυτοματοποιείται με βάση τις συγκεκριμένες μετρήσεις και τα καθορισμένα όρια λειτουργίας κατά τον έλεγχο ποιότητας. Οι αντιδράσεις είναι άμεσες ενέργειες και περιλαμβάνουν ενεργοποίηση – απενεργοποίηση τμημάτων – υποδικτύων με στόχο την αποκατάσταση της ομαλής λειτουργίας.
Τα σήματα μετρήσεων που παράγονται, αποτελούν συνεχή σήματα που καταγράφονται στις μετρητικές διατάξεις, και τα οποία στη συνέχεια διακριτοποιούνται από αναλογικά σε ψηφιακά (με χρήση μετατροπέων A/D Converters) για να μεταδοθούν πλέον ως ψηφιακά δεδομένα (πακέτα δεδομένων) προς το κέντρο λήψης απόφασης. Για τη μετάδοση των δεδομένων μπορεί να γίνει χρήση νέων τεχνολογιών ενθυλάκωσης σε δομές πακέτου IP (packet encapsulation) ή άλλες ισοδύναμες δομές πρωτοκόλλων (Industrial protocols) ανάλογα με τον τύπο, την ασφάλεια του δικτύου, των πρωτοκόλλων χρήσεως, κλπ. Με τη λήψη των πληροφοριών ελέγχου στο διαχειριστή ενέργειας EMS (μέρος του οποίου είναι ο έλεγχος AGC), λαμβάνονται οι αποφάσεις οι οποίες θα δώσουν και τις εντολές εκτέλεσης προς τα δομικά υποσυστήματα παραγωγής ισχύος στο δίκτυο (γεννήτριες, φορτία, μετασχηματιστές, κλπ).

Σήματα ανταλλαγής της δομής ελέγχου: Τα μεταδιδόμενα σήματα αφορούν εκτιμήσεις των επιπέδων ισχύος από τους παρόχους ($P_{sources}$), εκτιμήσεις κατανάλωσης από τα φορτία (P_{Loads}), καθώς και μετρήσεις συχνότητας (f) στις περιοχές του δικτύου κάλυψης.

Στην πιο σύνθετη μορφή τους υλοποιούνται από κεντρικά καταγραφικά συστήματα που βασίζουν τη λήψη αποφάσεων σε κεντρικό έλεγχο αναγνωρίζοντας καταστάσεις (states) για κάθε χρονική στιγμή λειτουργίας του συνολικού δικτύου.
Τα μαθηματικά μοντέλα που παρουσιάζονται στη συνέχεια καλύπτουν τη δράση συστημάτων πολλαπλών περιοχών (ενσωματώνοντας έτσι και το απλούστερο πρόβλημα της μιας περιοχής), δίνοντας τη βάση για την ανάπτυξη αλγορίθμων λειτουργίας μέσω προσομοιώσεων. Όπως θα παρουσιαστεί και παρακάτω, η μαθηματικοποίηση των περιγραφών αποτελεί τη βάση για την εφαρμογή προσομοιώσεων με χρήση ΗΥ για τον έλεγχο και την πιστοποίηση της λειτουργίας των δικτύων ισχύος μεγάλης κλίμακας. Επιπρόσθετα, τα μαθηματικά μοντέλα δίνουν τη δυνατότητα εφαρμογής προσομοιώσεων ειδικού τύπου (σενάρια προσομοίωσης). 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. Τα μαθηματικά μοντέλα αποτελούν επίσης χρήσιμα εργαλεία για την ανάλυση λειτουργίας των δικτύων ισχύος σε φάσεις επιθέσεων, όπως θα παρουσιασθεί και στις επόμενες ενότητες της εργασίας. Τα παραγόμενα μοντέλα περιγραφής μπορούν να ενσωματωθούν στους σύγχρονους

Διαχειριστές Ενέργειας, διευκολύνοντας την αναγνώριση συνθηκών – καταστάσεων, καθώς και τη Λήψη Αποφάσεων σε ένα κεντρικό σχήμα.
Στη συνέχεια παρουσιάζεται μία μαθηματικοποιημένη περιγραφή λειτουργίας ενός μοντέλου πολλαπλών περιοχών (με έμφαση στα σήματα λειτουργίας), με χρήση και χωρίς χρήση AGC.

1.4.1 Το μοντέλο ενός συστήματος πολλαπλών περιοχών (multi – area) χωρίς τη χρήση AGC

Η μαθηματικοποίηση αφορά κυρίως σε μία γραμμικοποιημένη περιγραφή του συστήματος, δίνοντας την ανταλλασσόμενη πληροφορία εντός δικτύου, ως διάνυσμα κατάστασης, τις εισόδους – παροχές ισχύος, καθώς και τις εξόδους, που αφορούν στη διαδικασία λήψης των μετρήσεων από τον έλεγχο των περιοχών.
Η δυναμική ενός συστήματος ηλεκτρικής ενέργειας πολλαπλών περιοχών για ένα καθορισμένο σημείο λειτουργίας, μπορεί να περιγραφεί ικανοποιητικά, με ένα συνεχές μοντέλο εξισώσεων κατάστασης **[10]**:

$$\dot{x}(t) = Ax(t) + Bu(t) + \gamma'(t),$$
$$y(t) = Cx(t) + n'(t),$$

όπου $x(t) \in R^{n'+1}$, $u(t) \in R^{d+1}$ και $y(t) \in R^{m+1}$, ως διάνυσμα κατάστασης, διάνυσμα εισόδων και μετρήσεις εξόδου για τη χρονική στιγμή t αντίστοιχα. Οι πίνακες A, B και C αποτελούν μήτρες κατάλληλων διαστάσεων για την περιγραφή του συστήματος. Οι παράμετροι $\gamma'(t)$ και $n'(t)$ αποτελούν θορυβικές διαδικασίες, ασυσχέτιστες μεταξύ τους, και ακολουθούν κανονικές κατανομές για το σύστημα και τη μέτρηση αντίστοιχα.

$$\gamma'(t) \sim N(0, Q')$$
$$n'(t) \sim N(0, R')$$

Οι έξοδοι του συστήματος περιγράφονται από το διάνυσμα

$$y(t) = [y_1(t)^T \quad y_2(t)^T \quad \dots \quad y_i(t)^T \quad \dots \quad y_r(t)^T]$$

όπου το στοιχείο $y_i(t)$ αποτελείται από

$$y_i(t) = [p_{ti}(t)^T \quad \omega_i(t)]^T$$

με $p_{ti}(t)$ το επίπεδο μεταβαλλόμενης ισχύος και $\omega_i(t)$ η μεταβολή της συχνότητας για την περιοχή i.

Ενώ το διάνυσμα εισόδου για την περιγραφή $u(t)$ δίνεται στη μορφή:

$$u(t) = [u_1(t)^T \quad u_2(t)^T \quad \dots \quad u_i(t)^T \quad \dots \quad u_r(t)^T] \quad \text{με}$$

$$u_i(t) = [p_{si}(t)^T \quad u_{loadi}(t)^T]^T$$

όπου:

$u_{loadi}(t) = [p_{loadi}(t)^T \quad q_{loadi}(t)^T]^T$

με p_{si} να συμβολίζεται η προσφερόμενη ισχύς προς την περιοχή i, και με p_{loadi} και q_{loadi} η ενεργός και άεργη τιμή της ισχύος του φορτίου, αντίστοιχα.

1.4.2 Το μοντέλο ενός συστήματος πολλαπλών περιοχών (multi – area) με τη χρήση AGC

Από θεωρητική πλευρά, ένα σύστημα με AGC, μπορεί να θεωρηθεί ως ένας βρόχος ανατροφοδότησης πολλαπλών μεταβλητών που προστίθεται στο προηγούμενο μοντέλο περιγραφής. Προκειμένου να επιτευχθεί ανεξάρτητη ρύθμιση για κάθε ροή ισχύος και τη συχνότητα των τοπικών περιοχών, η προσπάθεια εξισορρόπησης σε μία περιοχή ενεργοποιεί μόνο τους τοπικούς παρόχους ισχύος που συμμετέχουν στον AGC χωρίς παρεμβολές από γεννήτριες σε άλλες περιοχές **[10**].
Ως εκ τούτου, η πολυεπίπεδη πολιτική ελέγχου μπορεί να αποκεντρωθεί ανά περιοχή ως:

$u[t] = f(y^t) = [\, f_1({y_1}^t)^T \, f_2({y_2}^t)^T \quad \dots \quad f_i({y_i}^t)^T \quad \dots \quad f_r({y_r}^t)^T]^T$

όπου ${y_i}^t$ είναι η απομακρυσμένα μετρούμενη τιμή για την έξοδο του συστήματος μέχρι τη χρονική στιγμή t. Για να επεξεργαστούμε την πολιτική ελέγχου, υποθέτουμε ότι υπάρχουν ψ τοπικές μονάδες παραγωγής στον AGC και φ μετρήσεις στην περιοχή i, και τότε η πολιτική ελέγχου συνιστά μία συνάρτηση της μορφής:

$f_i(\cdot) : R^{\varphi} \rightarrow R^{\psi}$

η οποία συνίσταται από τις ακόλουθες διεργασίες για το χρονικό διάστημα:

- Σφάλμα Ελέγχου Περιοχής (ACE) το οποίο υπολογίζεται από τις απομακρυσμένα μετρούμενες ροές ισχύος σε ένα καθορισμένο χρονικό διάστημα στη μορφή:

$$ACE_i = \sum_{s=1}^{\varphi} p_{ti,s} + \beta_i \omega_i$$

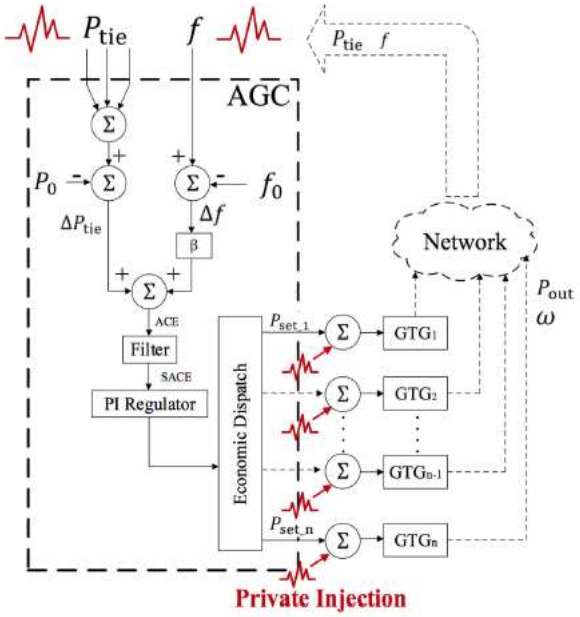
  όπου οι καθορισμένες παράμετροι β_i αποτελούν παραμέτρους πόλωσης - κατώφλια ισχύος (bias).
- Το ACE εξομαλύνεται περνώντας το μέσα από ένα φίλτρο χαμηλής τάξης για να μετριάσει την κόπωση των διατάξεων ελέγχου, π.χ. βαλβίδες στροβίλου και τον έλεγχο μοτέρ **[9**] από γρήγορες λήψεις αποφάσεων.
- Το κέντρο ελέγχου, υπολογίζει μία εντολή ελέγχου από το ACE σύμφωνα με την πολιτική ελέγχου που αναφέρεται στο **[11**], και εκτελείται σε καθορισμένο χρονικό διάστημα.

- Η εντολή ελέγχου που υπολογίζεται από τον AGC αποστέλλεται στις ψ τοπικές μονάδες παραγωγής. Το απαιτούμενο επίπεδο ισχύος για κάθε γεννήτρια είναι ανάλογο προς το συντελεστή ζεύξης ισχύος.

Η παραπάνω διαδικασία, η οποία συνοψίζεται και στο σχήμα που ακολουθεί, βασίζεται στο γεγονός ότι μόνο οι μετρήσεις από τα επιλεγμένα δείγματα συνεισφέρουν στη σύνθεση των εντολών ελέγχου που αποστέλλονται από τον AGC προς την περιοχή i. Η παραπάνω πολιτική ελέγχου θέτει τα σημεία λειτουργίας για την παραγωγή ισχύος $p_{si}(t)$, έτσι ώστε:

$p_{si}(t) = f_i(y_i{}^t) \quad \forall i \in \{1, 2, \cdots, r\}$.

Η παραπάνω εξίσωση συνδέει τη φυσική υποδομή (μονάδες γεννητριών) με τα κέντρα ελέγχου, συνιστώντας έτσι ένα υβριδικό σχήμα για τον έλεγχο πολλών περιοχών από τον AGC.



Σχήμα 9: Αλγόριθμος ελέγχου από τον AGC προς τις πολλαπλές περιοχές ελέγχου

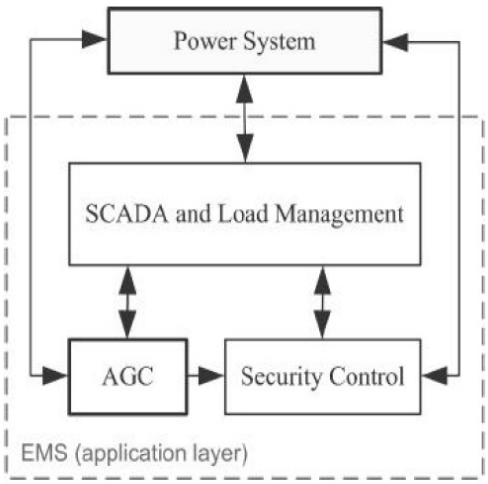
1.5 Δομή συστημάτων AGC και επικοινωνία με τον Διαχειριστή Ενέργειας (Energy Management System – EMS)

Τα υποσυστήματα ελέγχου AGC παρέχουν έναν αποτελεσματικό μηχανισμό ρύθμισης της παραγωγής για την ελαχιστοποίηση απόκλισης συχνοτήτων, ρυθμίζοντας τη ροή ισχύος στις περιοχές ελέγχου μέσω των γεννητριών. Τα συστήματα AGC πραγματοποιούν αλλαγές επιπέδου λειτουργίας των σταθμών παραγωγής, στέλνοντας μηνύματα στις υπό-έλεγχο μονάδες. Η απόδοση του AGC εξαρτάται σε μεγάλο βαθμό από το πώς αυτές οι μονάδες παραγωγής ανταποκρίνονται στις εντολές **[4]**. Η απόκριση της μονάδας παραγωγής, εξαρτάται από πολλούς παράγοντες, όπως ο τύπος μονάδας, το καύσιμο, η στρατηγική ελέγχου,

καθώς και το σημείο λειτουργίας αυτής. Η ενσωμάτωση των AGC συστημάτων και η διακίνηση των δεδομένων που απαιτούνται για τη λήψη αποφάσεων συνθέτουν έναν Διαχειριστή Ενέργειας.

Ορισμός: Ως Διαχειριστής Ενέργειας (Energy Management System – **EMS**), καλείται η συνολική δομή που υλοποιεί το κέντρο έκδοσης αποφάσεων και εντολών με στόχο την κάλυψη των φορτίων και τη βέλτιστη λειτουργία ενός συστήματος παραγωγής ισχύος, βασισμένο στους υπάρχοντες πόρους.

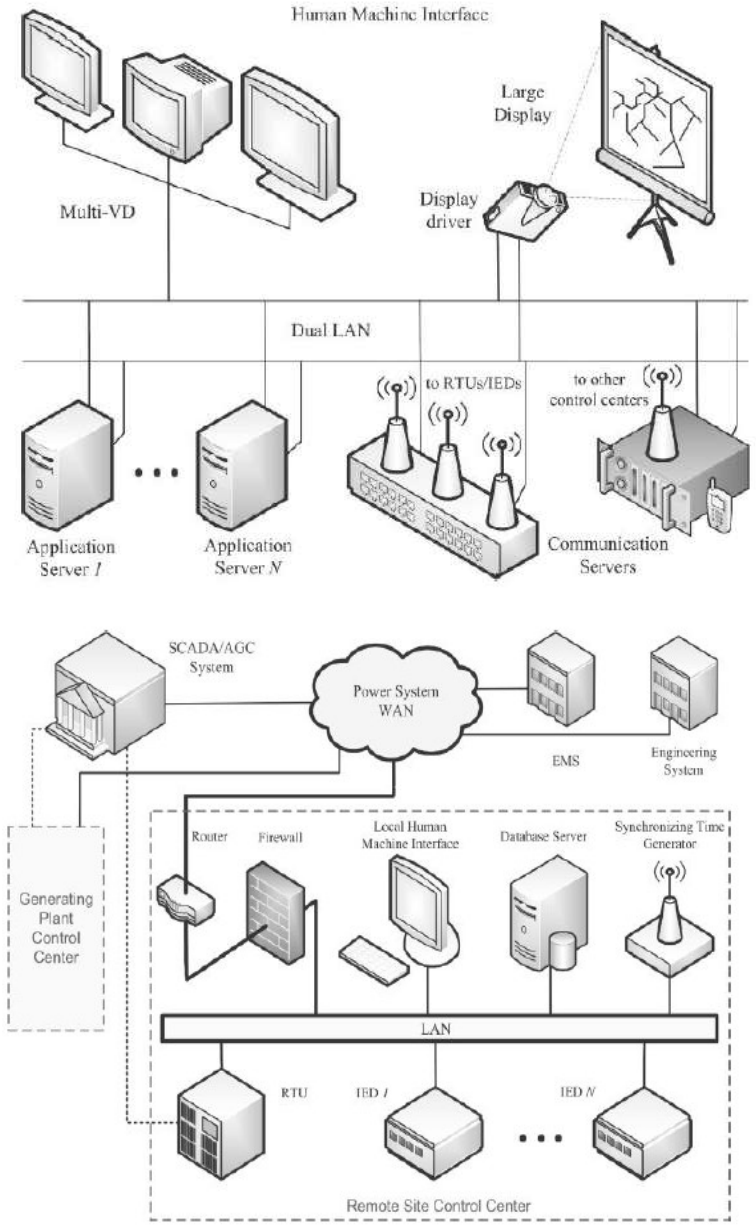
Στο σχήμα που ακολουθεί παρουσιάζεται η δομική οντότητα του Διαχειριστή Ενέργειας (EMS) και οι διεπαφές που απαιτούνται για την υλοποίηση των λειτουργιών του.



Σχήμα 10: Δομή επικοινωνίας του συστήματος AGC με τον Διαχειριστή Ενέργειας – EMS

Τα συστήματα AGC, ο έλεγχος ασφαλείας, ο εποπτικός έλεγχος, η απόκτηση δεδομένων (Supervisory Control and Data Acquisition - **SCADA**) και η διαχείριση φορτίου, είναι οι κύριες μονάδες στο επίπεδο εφαρμογής ενός σύγχρονου συστήματος διαχείρισης ενέργειας (EMS) **[5]**. 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.
Το σύστημα AGC επικοινωνεί μέσω SCADA, με τη μονάδα διαχείρισης φορτίου, τη μονάδα ασφαλείας και μέσω του κέντρου ελέγχου με το Διαχειριστή Ενέργειας (Energy Management System – EMS), όπως φαίνεται στο προηγούμενο σχήμα.
Το σύστημα διαύλων SCADA αποτελείται από έναν κύριο σταθμό, για επικοινωνία με απομακρυσμένες τερματικές μονάδες (Remote Terminal Units - RTU), και έξυπνες ηλεκτρονικές συσκευές (Intelligent Electronic Devices - IEDs), για ένα ευρύ φάσμα διαδικασιών παρακολούθησης και ελέγχου. 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. Μία τέτοια δομή επικοινωνίας SCADA εμφανίζεται στο σχήμα που ακολουθεί. Παρά το γεγονός ότι

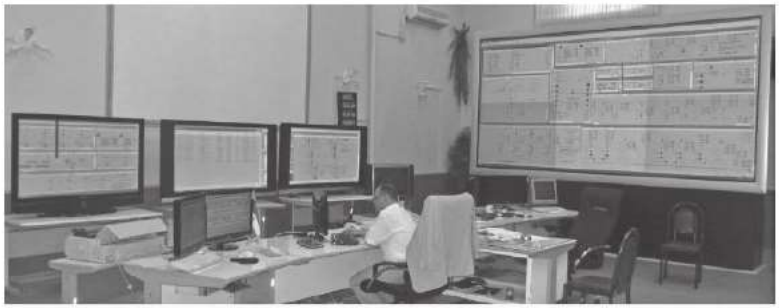
σήμερα πολλές λειτουργίες επεξεργασίας και ελέγχου δεδομένων μεταφέρονται στα IEDs, τα συστήματα ισχύος χρειάζονται ακόμη έναν κύριο σταθμό ή κέντρο ελέγχου για την οργάνωση και το συντονισμό των διαφόρων εφαρμογών **[1]**, **[12]**.



Σχήμα 11: Τυπική Δομή ενός κέντρου συγκέντρωσης και διαχείρισης δεδομένων – και οι διεπαφές SCADA

Και στις δύο παραπάνω μορφές, η επικοινωνία και η ανταλλαγή μετρητικών σημάτων μπορεί να κάνει χρήση διαύλων (busses), οι οποίοι είναι είτε βιομηχανικών προδιαγραφών (π.χ. SCADA), είτε με χρήση τεχνικών διασύνδεσης HY (servers) που βασίζονται σε υποδομές διασύνδεσης διαδικτύου. Τα επίπεδα ασφαλείας για την επικοινωνία είναι ελεγχόμενα (π.χ. συγκρότηση VPNs για την απομόνωση των δομών επικοινωνίας από τον κορμό του διαδικτύου, TLS/SSL πρωτόκολλα, κλπ.). Στις ενότητες που ακολουθούν θα αναλυθούν περαιτέρω οι δομές επικοινωνίας, καθώς και οι τεχνολογίες και τα πρωτόκολλα διασύνδεσης δικτύου – Διαχειριστή Ενέργειας. Ο λόγος είναι ότι η συνολική υποδομή αυτού του σύγχρονου επιπέδου

ελέγχου ενός συστήματος ισχύος αποτελεί και τη βάση μέσω των δομικών του στοιχείων, για την ανάπτυξη επιθετικών ενεργειών προσβολής της λειτουργίας του.
Ο AGC εκτελεί μία συνεχή λειτουργία σε πραγματικό χρόνο για να ρυθμίσει την παραγωγή ηλεκτρικής ισχύος του συνολικού συστήματος - δικτύου, παρακολουθώντας τις αλλαγές στα φορτία. Ο έλεγχος της συχνότητας, το οικονομικό κόστος για την παροχή ισχύος, το αποθεματικό ισχύος, η παρακολούθηση και η σχετική καταγραφή δεδομένων, αποτελούν τις κύριες λειτουργίες ενός AGC συστήματος. Ο έλεγχος συχνότητας είναι το πιο σημαντικό ζήτημα της λειτουργίας του AGC.



Σχήμα 12: Σύγχρονο κέντρο Διαχείρισης Λειτουργίας και Λήψης Αποφάσεων παραγωγής και ελέγχου ισχύος

Επομένως, τα υποσυστήματα AGC που αρχικά αφορούσαν στον αναλογικό τύπο ελέγχου των γεννητριών έχουν εξελιχθεί στα σύγχρονα ψηφιακά συστήματα Διαχείρισης Ενέργειας (EMS). Έτσι, τα αρχικά αναλογικά συστήματα AGC μέσω της εξέλιξης σε ψηφιακούς Διαχειριστές Ενέργειας κάνοντας χρήση των νέων τεχνολογιών, αποτελούν κεντρικούς σταθμούς λήψης και εφαρμογής αποφάσεων – πολιτικών διαχείρισης ισχύος **[1]**.
Στη βιβλιογραφία παραμένει η υιοθέτηση του όρου «σύστημα AGC», εννοώντας όμως τη σύγχρονη μετεξέλιξή του σε «Διαχειριστή Ενέργειας EMS». Επομένως, οι όροι στη συνέχεια χρησιμοποιούνται ισοδύναμα και ταυτόσημα **[1]**, **[13]**, **[14]**, δηλ. με τον όρο AGC θεωρούμε τον ισοδύναμο όρο της Διαχείρισης Ενέργειας, όπως παρέχεται ολοκληρωμένα από τα σύγχρονα ψηφιακά συστήματα.

2 Τα AGC ως πληροφοριακά συστήματα

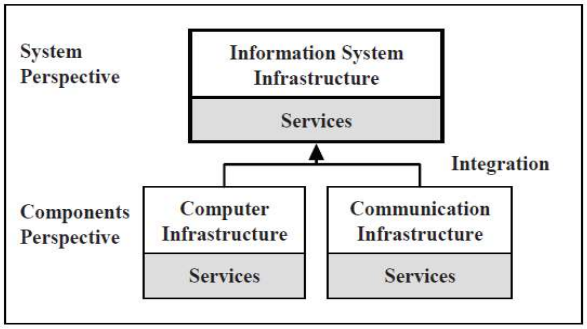
2.1 Γενικά χαρακτηριστικά των πληροφοριακών συστημάτων

Τα πληροφοριακά συστήματα (Information Systems – IS) αποτελούν έναν συνδυασμό τεχνολογιών υλικού πλατφόρμας (hardware) και λογισμικού (software) που στοχεύουν στην αποθήκευση, ανάκτηση και διαχείριση ψηφιακών πληροφοριών. Σκοπός των πληροφοριακών συστημάτων είναι η εκτέλεση λειτουργιών – εφαρμογών που βασίζονται στις πληροφορίες που διαχειρίζεται το πληροφοριακό σύστημα. Οι εφαρμογές που βασίζονται σε ψηφιακά συστήματα δεδομένων, αναφέρονται σε ένα ετερογενές και ευρύτατο πεδίο όπως, η ηλεκτρονική διαχείριση και μεταφορά δεδομένων, οι εμπορικές πωλήσεις – αγορές αγαθών (ηλεκτρονικό εμπόριο), οι τραπεζικές συναλλαγές, φτάνοντας μέχρι την αυτοματοποιημένη διαχείριση διεργασιών (συστήματα αυτοματισμών και αυτόματου ελέγχου για εφαρμογές όλων των τύπων και τεχνολογιών). Τα AGC συστήματα δεδομένου ότι διαχειρίζονται δομές πληροφορίας, άλλες σταθερές και άλλες μεταβαλλόμενες στο χρόνο, μπορούν να ιδωθούν κατά ένα μέρος υπό το πρίσμα της ανάλυσης πληροφοριακών συστημάτων.

Οι μετρικές ποιότητας που χαρακτηρίζουν τις επιδόσεις ενός πληροφοριακού συστήματος (ως ποσοτικοποιήσιμες και σαφώς ορισμένες συναρτήσεις), αποτελούν επίσης σημαντικές βάσεις για την ανάλυση ποιότητας και επίδοσης και των AGC συστημάτων. Για το λόγο αυτό, στη συνέχεια της ενότητας θα παρουσιαστούν οι σημαντικότερες έννοιες των πληροφοριακών συστημάτων, καθώς αυτά σχετίζονται άμεσα με την ανταλλαγή και διαχείριση πληροφορίας, άρα και με τα AGC συστήματα.

Ένα πληροφοριακό σύστημα υλοποιείται από τη διασύνδεση των δομικών του στοιχείων (structural elements - components) με στόχο την παροχή των υπηρεσιών εντός των προδιαγραφών λειτουργίας και σχεδιασμού του. Η συναρμογή ετερογενών πεδίων τεχνολογίας και η διαδικασία της επικοινωνίας αυτών των δομικών στοιχείων χαρακτηρίζει άμεσα τα επίπεδα επίδοσης και λειτουργίας του πληροφοριακού συστήματος.

Η υλοποίηση ενός σύγχρονου συστήματος διαχείρισης πληροφορίας σε αφαιρετικό επίπεδο, μπορεί να αποδομηθεί στις δομικές οντότητες που παρουσιάζονται στο σχήμα που ακολουθεί:



Σχήμα 13: Αφαιρετική αποδόμηση (abstract structural decomposition) των στοιχείων ενός πληροφοριακού συστήματος

Στα πλαίσια μίας αφαιρετικής αποδόμησης ενός πληροφοριακού συστήματος, από πλευράς συστήματος και στοιχείων που το συνθέτουν, αυτό μπορεί να θεωρηθεί ότι συνίσταται από υπηρεσίες (services) και υπολογιστικές δομές (Computer Infrastructure). Στις υπολογιστικές δομές βασίζεται η επικοινωνία και η ανταλλαγή της πληροφορίας στους κόμβους του συστήματος, υλοποιώντας παράλληλα ως υπηρεσίες τον εμπλουτισμό της ανταλλασσόμενης πληροφορίας στα παρεχόμενα επεξεργαστικά συστήματα. Και από τις δύο πλευρές (συστήματος και στοιχείων που το συνθέτουν), η αποδόμηση διατηρεί ένα κοινό επίπεδο υλοποίησης. Η ολοκλήρωση **-** διαδικασία σύνθεσης του συνολικού συστήματος (integration)**,** συντελείται μέσω της επικοινωνίας των τμημάτων του.

Η αποδόμηση ενός πληροφοριακού συστήματος, δίνοντας έμφαση στις ιδιότητες που απορρέουν και τα χαρακτηριστικά του, μπορεί να αποτελέσει αντικείμενο ανάλυσης μέσω τριών τεχνικών. Οι τεχνικές αυτές διακρίνουν την οργάνωσή του (i) από πλευράς του επιπέδου των στοιχείων σύνθεσής του (component level perspective), (ii) από πλευράς της συνολικής δομής διασύνδεσης (Infrastructure perspective) και (iii) από πλευράς των παρεχόμενων υπηρεσιών του (service perspective). Όπως θα παρουσιαστεί και στη συνέχεια, πολλά από τα χαρακτηριστικά και τις εγγενείς ιδιότητες ενός πληροφοριακού συστήματος επηρεάζονται από την τεχνική οργάνωσής του.

Η προσέγγιση του 'component level' έχει καθαρά τη βάση της στις τεχνικές σχεδίασης μηχανικών συστημάτων (engineering concept). Η προσέγγιση αυτή διευκολύνει, ως βάση αποδόμησης, το σχεδιασμό, τόσο μικρής όσο και πολύ μεγάλης κλίμακας συστημάτων. Το κύριο χαρακτηριστικό αυτής της βάσης αποδόμησης είναι η ικανότητα ελέγχου που δίνεται στο σχεδιαστή - μηχανικό στη δομή και τη λειτουργία του συστήματος, ασχέτως του συνολικού μεγέθους του. Σε αυτή την τεχνική σχεδιασμού, πολλές οντότητες μικρότερης κλίμακας συνδυάζονται για την υλοποίηση μεγαλύτερης κλίμακας συστημάτων που είναι ικανά να εκτελούν πολύπλοκες διεργασίες.

Η προσέγγιση του 'Infrastructure perspective' για την ανάλυση ενός συστήματος προκύπτει από την ικανότητα διασύνδεσης που εμφανίζουν τα υπολογιστικά συστήματα, καθώς δίνεται σε αυτά η ικανότητα μεταφοράς και ανταλλαγής πληροφορίας μέσω δικτύων διασύνδεσης. Επομένως, η εντοπισμένη έννοια της πληροφορίας επεκτείνεται σε πληροφοριακή υποδομή (information infrastructure), εφόσον οι πληροφορίες διασπείρονται και γίνονται αντικείμενο επεξεργασίας της συνολικής δικτυακής υποδομής. Παρά το γεγονός ότι συνήθως τα πληροφοριακά συστήματα συνεπάγονται συναρμογή των υπολογιστών με τις δομές επικοινωνίας (topology), τη θέση (location) και τα στοιχεία που τα συνθέτουν (components), η επέκταση της έννοιας της πληροφοριακής υποδομής συνθέτει μία συλλογή από πληροφοριακά συστήματα. Τα συστήματα αυτά έχουν τη δυνατότητα διασύνδεσης ή μη με τους υπόλοιπους κόμβους της συνολικής υποδομής. Σε αντίθεση με τα συστήματα τα οποία βασίζουν το σχεδιασμό τους σε στοιχεία (component level perspective), οι πληροφοριακές υποδομές, όπως είναι το Internet, επεκτείνονται δυναμικά και με μη προβλεπόμενο τρόπο στο χρόνο.

Η προσέγγιση από πλευράς υπηρεσιών (service perspective), βασίζεται στο γεγονός ότι η διασύνδεση είτε σε επίπεδο στοιχείων (components level) είτε σε επίπεδο υποδομής (Infrastructure), συντείνει στη δημιουργία και παροχή εφαρμογών και υπηρεσιών για τον τελικό χρήστη. Η επίδοση αυτών των συστημάτων αποτελεί

επίσης αντικείμενο του σχεδιασμού και της ανάλυσης. Αν και οι χρήστες των συστημάτων αναμένουν ένα ικανοποιητικό επίπεδο επιδόσεων από αυτήν την προσέγγιση, οι απαιτήσεις τους μπορεί να γίνουν άμεσα ποσοτικοποιήσιμες ως δείκτες για την ανάλυση των επιδόσεων.

2.2 Τα ιδιαίτερα χαρακτηριστικά των πληροφοριακών συστημάτων

Τα προβλήματα στην υλοποίηση ενός πληροφοριακού συστήματος εμφανίζονται κατά τη διαδικασία διασύνδεσης των υποδομών του (infrastructures). Για την υλοποίησή τους είναι αναγκαίο να συνδυάζουν στοιχεία (components) που έχουν αναπτυχθεί, βασισμένα σε διαφορετικές αρχές σχεδιασμού. Η ολοκλήρωση συστημάτων που βασίζονται σε τέτοιες ετερογένειες, συμπεριλαμβάνοντας και τον ανθρώπινο παράγοντα, έχει δημιουργήσει αρκετές δυσκολίες στην ανάπτυξη ευέλικτων μηχανισμών για την ανάλυση και την ικανότητα βελτίωσης των υποδομών των συστημάτων αυτών. Ένα από τα προβλήματα βελτίωσης, που ήδη έχει αναφερθεί, οφείλεται στην ετερογένεια των τεχνολογιών που χρησιμοποιούνται για την ανάπτυξη της συνολικής λειτουργικότητας του συστήματος.

Επιπλέον έχει διαπιστωθεί **[16]**, ότι και οι χρήστες αλλά και οι σχεδιαστές αυτών των συστημάτων, έρχονται αντιμέτωποι με όρους οι οποίοι μπορεί να είναι συνώνυμοι ή συμπληρωματικοί ως προς τις περιγραφές των χαρακτηριστικών και των ιδιοτήτων τους. Επομένως, υπάρχει άμεσα η ανάγκη για τη διατύπωση μίας κοινής βάσης για την επίδοση του ακριβούς νοήματος στους όρους περιγραφής των ικανοτήτων – ιδιοτήτων ενός συστήματος, χωρίς να γίνεται σύνδεσή τους με τεχνολογίες ή αρχές σχεδιασμού. Επιπλέον της ασάφειας καθορισμού, παρουσιάζεται η ανάγκη για την εισαγωγή νέων όρων που προορίζονται για να περιγράψουν ιδιαίτερα χαρακτηριστικά – ιδιότητες των συστημάτων. Όταν οι όροι είναι νέοι και εισάγονται για την κάλυψη περιγραφής κάποιων χαρακτηριστικών, αυτό θα πρέπει να γίνει με σαφή και καθορισμένο τρόπο για να αποφευχθεί η σύγχυση με άλλες παρεμφερείς περιγραφές. Επιπρόσθετα, χρειάζεται ιδιαίτερη προσοχή όταν για την περιγραφή των χαρακτηριστικών ενός συστήματος χρησιμοποιούνται όροι που έχουν εισαχθεί χρονολογικά παλαιότερα, και μετεξελίσσονται για την πρόσθετη κάλυψη αυτών των νέων ιδιοτήτων. Το τελευταίο μπορεί να δημιουργήσει σύγχυση ή ασάφεια, η οποία βασίζεται στα προηγούμενα χαρακτηριστικά που αφορούσαν στη χρήση αυτών των όρων (legacy).

Η χρήση συγκεκριμένων όρων για την περιγραφή των ειδικών χαρακτηριστικών των πληροφοριακών συστημάτων παρουσιάζονται στις παραγράφους που ακολουθούν. Στη συνέχεια, η παρουσίαση θα επικεντρωθεί στην περιγραφή των μαθηματικοποιήσιμων – ποσοτικοποιήσιμων χαρακτηριστικών των πληροφοριακών συστημάτων, καθώς αυτά σχετίζονται με τα AGC συστήματα. Έμφαση δίνεται στα ιδιαίτερα χαρακτηριστικά των πληροφοριακών συστημάτων που σχετίζονται με τα AGC συστήματα, καθώς και την ικανότητα/αδυναμία που αυτά εμφανίζουν στην εκδήλωση κυβερνο-επιθέσεων. Επομένως, τα ιδιαίτερα χαρακτηριστικά, παρά το γεγονός ότι μπορούν να αποτελέσουν γενικά βάσεις για την ανάπτυξη μετρικών ποιότητας, παρουσιάζονται ως χαρακτηριστικά ελέγχου των επιδόσεων των AGC συστημάτων και της ικανότητας – ανεκτικότητας που αυτά εμφανίζουν στην εκδήλωση, την αποτροπή και το μετριασμό κυβερνο-επιθέσεων.

2.2.1 Αξιοπιστία (Reliability)

Η έννοια της Αξιοπιστίας (Reliability) μπορεί να χρησιμοποιηθεί ως μία καλά ορισμένη μαθηματική συνάρτηση με βάση τον ακόλουθο ορισμό:

Ορισμός#1: Ως **Αξιοπιστία** ορίζεται η ικανότητα ενός συστήματος/υποσυστήματος να λειτουργεί υπό τις προδιαγραφές σχεδιασμού του, κάτω από δεδομένες συνθήκες λειτουργίας, για ένα καθορισμένο χρονικό διάστημα.

Ένας εναλλακτικός ορισμός της Αξιοπιστίας κάνει χρήση των μαθηματικών όρων πιθανότητας υπό συνθήκη, σύμφωνα με τον ακόλουθο ορισμό:

Ορισμός#2: Ως **Αξιοπιστία** ορίζεται η υπό συνθήκη πιθανότητα για τη λειτουργία ενός συστήματος, κάτω από συγκεκριμένες προδιαγραφές, χωρίς την εμφάνιση αποτυχίας λειτουργίας για τη χρονική στιγμή t, δεδομένου ότι κατά την αρχική χρονική στιγμή t=0 το σύστημα ήταν πλήρως λειτουργικό.

Εναλλακτικά, η βιβλιογραφία περιγραφής ιδιοτήτων συστημάτων ορίζει το χαρακτηριστικό της Αξιοπιστίας ως μία μετρική της συνεχόμενης σωστής λειτουργίας για ένα σύστημα. Κατά τον ορισμό του συγκεκριμένου χαρακτηριστικού, μία σχετιζόμενη αντίληψη που θα πρέπει να ληφθεί υπόψιν στο σημείο αυτό, είναι η έννοια της **διαθεσιμότητας** (availability). Η παραπάνω έννοια σχετίζεται άμεσα με το χαρακτηριστικό της αξιοπιστίας και ορίζεται ως η ικανότητα ενός συστήματος να βρίσκεται σε κατάσταση παροχής μίας συγκεκριμένης λειτουργίας σε μία δεδομένη χρονική στιγμή ή σε οποιαδήποτε χρονική στιγμή ορίζεται μέσα σε ένα χρονικό διάστημα.
Για να εντοπιστεί η διαφορά των όρων της αξιοπιστίας και της διαθεσιμότητας, είναι σημαντικό να γίνει εμφανές ότι το χαρακτηριστικό της αξιοπιστίας αναφέρεται σε λειτουργία χωρίς αποτυχία λειτουργίας (failure – free) για ένα χρονικό διάστημα, ενώ το χαρακτηριστικό της διαθεσιμότητας αναφέρεται σε λειτουργία χωρίς αποτυχία σε μία δεδομένη χρονική στιγμή. Κατά συνέπεια, στο σημείο αυτό μπορεί να θεωρηθεί ότι η έννοια της διαθεσιμότητας είναι ταυτόσημη με την έννοια της αξιοπιστίας όταν αυτά τα χαρακτηριστικά εξομοιώνονται για την ίδια χρονική στιγμή.
Η έννοια της αξιοπιστίας συνδέει την ικανότητα λειτουργίας του συστήματος με την παρεχόμενη αξιοπιστία του μέσα στο χρόνο. Η έννοια είναι σημαντική, διότι διασφαλίζει ένα χρονικό διάστημα λειτουργικότητας για ένα σύστημα, πέρα από την ικανοποίηση των προδιαγραφών λειτουργίας του.
Για την επίτευξη ενός συστήματος με αυξημένη αξιοπιστία, αυτό το χαρακτηριστικό θα πρέπει να ενσωματωθεί σε κάθε στοιχείο/υποσύστημα του συνολικού συστήματος. Επομένως, η διαδικασία σχεδιασμού του συστήματος θα πρέπει να συμπεριλάβει το χαρακτηριστικό ήδη από τα αρχικά βήματα σχεδιασμού της αρχιτεκτονικής και της λειτουργικότητάς του. Τέσσερις (4) σημαντικές ιδιότητες θα πρέπει να ληφθούν υπόψιν ως βάσεις σχεδιασμού για την επίτευξη της αξιοπιστίας και της διαθεσιμότητας σε ένα σύστημα. Οι ιδιότητες αυτές είναι η αποφυγή σφάλματος (fault – avoidance), η ανοχή σε λειτουργία σφάλματος (fault – tolerant), η ανίχνευση σφάλματος (fault – detection), και η αποκατάσταση σφάλματος (fault – restoration).

2.2.2 Ανοχή σε λειτουργία σφάλματος (Fault – Tolerance)

Η έννοια της Ανοχής σε λειτουργία σφάλματος (Fault – tolerance), εισήχθη από τη σχεδίαση πολύπλοκων αλγορίθμων που υλοποιούνται σε λογισμικό (software) καθώς τα συστήματα αυτά εξελίσσονται με την προσθήκη νέων συνθηκών λειτουργικότητας.

Ορισμός: Ως **Ανοχή σε λειτουργία σφάλματος** ορίζεται η ικανότητα ενός συστήματος ή στοιχείου συστήματος (component) να λειτουργεί ακόμη και με χρήση εσφαλμένων δεδομένων (διεγέρσεων ή καταστάσεων), χωρίς να διακόπτεται η διασυνεχής λειτουργία του. Αυτό μπορεί να οφείλεται σε λανθασμένη ή κακή λειτουργία των υποσυστημάτων του (software/hardware).

Προφανώς, οι έννοιες της αξιοπιστίας και της ανοχής σε λειτουργία σφάλματος, αν και παρουσιάζονται ως ταυτόσημες, είναι εντελώς διαφορετικές, δεδομένου ότι η έννοια της αξιοπιστίας σχετίζεται κυρίως με τη λειτουργικότητα του υλικού (hardware), ενώ η έννοια της ανοχής σε λειτουργία σφάλματος αναφέρεται κυρίως στη διασυνεχή λειτουργικότητα του λογισμικού ενός συστήματος (software).
Ένα σύστημα που διαθέτει το χαρακτηριστικό της ανοχής σε λειτουργία σφάλματος, έχει την ικανότητα να συνεχίζει να λειτουργεί σωστά (ως προς την εκτέλεση και τις διεγέρσεις/αποκρίσεις του), ακόμη και όταν εμφανίζονται σφάλματα. Το χαρακτηριστικό αυτό στοχεύει στη σωστή παροχή υπηρεσιών από πλευράς συστήματος προς το χρήστη ακόμη και παρουσία σφαλμάτων, ή τουλάχιστον αφήνει το σύστημα λειτουργικό ακόμη και στην παρουσία σφαλμάτων.
Τρεις (3) είναι οι βασικές αρχές που πρέπει να συμπεριληφθούν στη διασφάλιση της ανοχής σε λειτουργία σφάλματος. Οι αρχές αυτές αφορούν στους όρους σφάλμα (fault), λάθος εισόδου/εξόδου (error), αποτυχία (failure), καθώς και στη σχέση/εξάρτηση που αυτές οι αρχές δημιουργούν μεταξύ τους. Για να μπορεί να προκύψει ένα σύστημα με ικανότητα να ανταπεξέρχεται σε σφάλματα (fault – tolerant system), θα πρέπει οι παραπάνω έννοιες να έχουν συμπεριληφθεί ως τμήματα της βάσης σχεδιασμού των στοιχείων του συστήματος. Οι όροι fault-tolerance και error – tolerance πολλές φορές χρησιμοποιούνται για να δηλώσουν ταυτόσημα το ίδιο χαρακτηριστικό.
Υπάρχουν πολλές και διαφορετικές τεχνικές για την επίτευξη του χαρακτηριστικού της ανοχής σε λειτουργία σφάλματος (fault – tolerance). Γενικά, οι τεχνικές αυτές βασίζονται στην ανίχνευση σφαλμάτων, η οποία συνεπάγεται συγκεκριμένες δράσεις για την επίτευξη της αποκατάστασης λειτουργίας του συστήματος (system recovery). Μία άλλη τεχνική είναι η εφαρμογή «μασκαρίσματος» στα σφάλματα (fault masking), στοχεύοντας στη μη επίδρασή τους σε ένα σύστημα, και κατά συνέπεια στην αποφυγή της εσφαλμένης λειτουργίας του (system crash). Άλλες τεχνικές χρησιμοποιούν την ανίχνευση (detecting), τον εντοπισμό (locating), τη διάγνωση (diagnosing) και τον περιορισμό των σφαλμάτων (confining), καθώς επαναπρογραμματίζουν το σύστημα με στόχο την απομάκρυνση του τμήματος (component) που σχετίζεται με το σφάλμα. Ο επαναπρογραμματισμός (reconfiguration) είναι η διαδικασία της εξάλειψης μίας εσφαλμένης εισόδου από ένα σύστημα και στη συνέχεια η αποκατάσταση της λειτουργίας του συνολικού συστήματος με χρήση μίας προηγούμενης κατάστασής του, στην οποία δεν είχε υπεισέλθει ακόμη το σφάλμα (previous normal state of operation). Όταν

χρησιμοποιούνται οι τεχνικές του επαναπρογραμματισμού, ο σχεδιαστής ενός συστήματος θα πρέπει να έχει ήδη συμπεριλάβει τους μηχανισμούς της ανίχνευσης σφαλμάτων (fault detection), του εντοπισμού σφαλμάτων (fault location), του περιορισμού της δράσης των σφαλμάτων (fault confinement) και της αποκατάστασης των σφαλμάτων (fault recovery).
Η σύγχυση που δημιουργείται από τους παραπάνω όρους οδήγησε στην εισαγωγή του όρου της **εξαρτησιμότητας** (dependability) ως έναν όρο, ο οποίος καλείται να συμπεριλάβει την αξιοπιστία της λειτουργίας αντικαθιστώντας με τη χρήση του, τους δύο προηγούμενους όρους (δηλ, της αξιοπιστίας και της ανοχής σε λειτουργία σφάλματος).

2.2.3 Ασφάλεια (Security)

Αρχικά η ασφάλεια (security) ήταν ταυτόσημη έννοια με το φυσικό επίπεδο προστασίας για ένα σύστημα. Με τη διαρκώς επεκτεινόμενη εισαγωγή και χρήση των σύγχρονων συστημάτων επικοινωνίας και των δικτύων υπολογιστών, η έννοια της ασφάλειας έχει αρχίσει να μετατοπίζεται προς την έννοια της ασφάλειας της πληροφορίας (information security). Η έννοια της ασφάλειας δεν επιδέχεται έναν επακριβή ορισμό. Εάν γινόταν μία απόπειρα να οριστεί, η έννοια θα περιλάμβανε το παρακάτω:

Ορισμός: Ως **Ασφάλεια** ορίζονται οι μηχανισμοί για τη φύλαξη και προστασία από ανεπιθύμητες ενέργειες ή/και δράσεις σε ένα σύστημα.

Το χαρακτηριστικό της ασφάλειας συνδέεται στενά με την έννοια της εμπιστευτικότητας (confidentiality), της ακεραιότητας της πληροφορίας (integrity) και της διαθεσιμότητας των πόρων/στοιχείων λειτουργίας ενός συστήματος (availability of assets). Σύμφωνα με τον von Neumann η έννοια της ασφάλειας θα πρέπει να συμπεριλάβει την εξαρτημένη προστασία έναντι όλων των σχετιζόμενων μεγεθών. Στα σχετιζόμενα μεγέθη συμπεριλαμβάνονται η εμπιστευτικότητα της πληροφορίας (confidentiality), η ακεραιότητα της πληροφορίας (integrity) και η διαθεσιμότητα της πληροφορίας σταθμιζόμενη ως προς τους κινδύνους ασφαλείας που αυτή εισάγει. Τα παραπάνω στοχεύουν στην πρόληψη καταστάσεων αποτροπής λειτουργίας (denial of service). Επιπλέον, θα πρέπει να προβλέπει και να ανιχνεύει την κακή χρήση της πληροφορίας, καθιστώντας το σύστημα μη αποκρινόμενο με δεδομένα εξόδου σε καταστάσεις απειλής, μειώνοντας τις συνέπειες από απειλές οι οποίες μπορεί να μην είναι δυνατόν να προβλεφθούν ή να εντοπιστούν εκ των προτέρων.
Για τους παραπάνω λόγους, η έννοια της ασφάλειας ενσωματώνει την προστασία των συστημάτων, των δικτύων και των υποσυστημάτων τους από διάφορες και μη κατάλληλες δράσεις, καθώς επίσης θα πρέπει να προστατεύει την πληροφορία την οποία το σύστημα διαχειρίζεται. Η ασφάλεια, επίσης, επιβάλλει την πρόβλεψη επιθετικών ενεργειών συμπεριλαμβάνοντας και τις εσωτερικές απειλές που προκύπτουν από αυτούς που χειρίζονται το σύστημα, αλλά και από εξωτερικές δράσεις. Κατά συνέπεια, η έννοια της ασφάλειας επεκτείνεται σε κάτι μεγαλύτερο από την προστασία απορρήτου των δεδομένων ενός συστήματος, την ακεραιότητά

τους και τη διαθεσιμότητά τους για τους σκοπούς λειτουργίας. Εναλλακτικά, αυτό μπορεί να εκφραστεί ως **ανεκτικότητα** (resilience) ενός συστήματος σε κάθε μορφή κακόβουλης επίθεσης.
Αξίζει να σημειωθεί ότι πολλές παραδοσιακές τεχνικές για την επίτευξη της ασφάλειας, βασίζουν τους σχεδιασμούς ασφαλείας για τη λειτουργία των συστημάτων τους, σε επιπρόσθετα δομικά στοιχεία της αρχιτεκτονικής τους (add-ons), καθώς δεν επιθυμούν να τα ενσωματώσουν εσωτερικά μέσα στο ίδιο το σύστημα. Κατά συνέπεια, η ασφάλεια και οι πολιτικές ασφαλείας (security policies), σε αυτή τη βάση, υλοποιούνται με μη αποδοτικό τρόπο.

2.2.4 Εξαρτησιμότητα (Dependability)

Δεν υπάρχει μοναδικός ορισμός για την έννοια της Εξαρτησιμότητας (Dependability). Η έννοια εξελίχθηκε από τους όρους της Αξιοπιστίας και της Διαθεσιμότητας.

Ορισμός#1: Ως **Εξαρτησιμότητα** ορίζεται η ικανότητα ενός συστήματος για παροχή συγκεκριμένων υπηρεσιών, οι οποίες είναι δικαιολογημένα εμπιστεύσιμες κατά τη χρονική στιγμή παροχής τους.

Εναλλακτικά προτείνεται και ο ακόλουθος ορισμός:
Ορισμός#2: Ως **Εξαρτησιμότητα** ορίζεται η ικανότητα ενός συστήματος για την αποφυγή αποτυχημένης λειτουργίας, η οποία είναι πιο συχνή ή πιο σοβαρή από τα επίπεδα που είναι αποδεκτά για τους χρήστες του συστήματος.

Η εξαρτησιμότητα αποτιμά τον βαθμό κατά τον οποίο ένα σύστημα είναι λειτουργικό σε μία τυχαία χρονική στιγμή, για ένα δεδομένο πλάνο χρήσης του, δεδομένου ότι τα λειτουργικά χαρακτηριστικά του συστήματος είναι διαθέσιμα από την αρχική χρονική στιγμή του πλάνου χρήσης. Μερικές από τις απαιτήσεις για να διασφαλιστεί η έννοια της εξαρτησιμότητας είναι το σύστημα να μην εμφανίζει ένα καθοριστικό σημείο αποτυχίας λειτουργίας (no single point of failure), και να μπορεί να ανταπεξέλθει στα επαγόμενα σφάλματα λειτουργίας. Κατά την εμφάνιση των σφαλμάτων λειτουργίας, το σύστημα θα πρέπει να μειώνει την επίδρασή τους σε αποδεκτά επίπεδα, επιτυγχάνοντας αυτό με χρήση ειδικών μηχανισμών χειρισμού των συνθηκών σφάλματος. Τα παραπάνω χαρακτηριστικά σηματοδοτούν ένα σημαντικό βαθμό δυσκολίας για την υλοποίηση ενός συστήματος το οποίο θα είναι ικανό να χειρισθεί όλους τους τύπους των παρουσιαζόμενων σφαλμάτων. Η έννοια της εξαρτησιμότητας μπορεί να διασφαλιστεί με ενσωμάτωση και χρήση τεσσάρων μηχανισμών, όπως η πρόβλεψη εσφαλμένης λειτουργίας (fault – forecasting), η αποτροπή εσφαλμένης λειτουργίας (fault – prevention), η απομάκρυνση των αιτιών σφάλματος (fault removal) και η ανοχή σε εσφαλμένες συνθήκες λειτουργίας (fault – tolerance).

2.2.5 Επιβιωσιμότητα (Survivability)

Η έννοια της Επιβιωσιμότητας (Survivability) έχει τις ρίζες της σε καθαρά στρατιωτικής φύσεως συστήματα. Ένας ορισμός της έννοιας του Survivability είναι ο ακόλουθος:

Ορισμός#1: Ως **Επιβιωσιμότητα** ορίζεται η ικανότητα ενός συστήματος, υποσυστήματος, εξοπλισμού, διεργασίας ή διαδικασίας, για την παροχή ενός σταθμισμένου βαθμού διασφάλισης (assurance) ότι θα συνεχίσει να λειτουργεί και να παρέχει υπηρεσίες κατά τη διάρκεια, αλλά και μετά από μία φυσική ή ανθρώπινης προέλευσης εξωτερική διαταραχή.

Εναλλακτικές προσεγγίσεις ορισμού έχουν εισαχθεί στην παραπάνω προσέγγιση, με σκοπό να συμπεριλάβουν προσδοκίες για την επίδοση των υπηρεσιών που παρέχονται από τα πληροφοριακά συστήματα, λαμβάνοντας υπόψιν τον παράγοντα του χρόνου. Με βάση αυτήν την προσέγγιση δίνεται ο ακόλουθος ορισμός.

Ορισμός#2: Ως **Επιβιωσιμότητα** ορίζεται η ικανότητα ενός συστήματος να υλοποιήσει την αποστολή (mission) για την οποία προορίζεται στο χρόνο, παρουσία και επιβολή επιθέσεων, αποτυχιών δράσης, ή/και ατυχημάτων.

Αυτός ο ορισμός έχει έναν εγγενή κρίσιμο σκοπό, να ικανοποιήσει την έννοια της αποστολής μέσα στο χρόνο. Κάποιοι εναλλακτικοί ορισμοί της έννοιας της Επιβιωσιμότητας απαιτούν την ικανότητα αποκατάστασης των υπηρεσιών ενός συστήματος (service recovery), ενώ άλλοι ορισμοί στέκονται κυρίως στην έννοια της ικανότητας εκπλήρωσης της αποστολής (mission).
Σε αυτούς τους ορισμούς αξίζει να σημειωθεί ότι δεν προσδιορίζονται σαφείς συσχετισμοί ανάμεσα στους όρους λειτουργίας, αποστολής και υπηρεσίας για ένα σύστημα. Υπό το πρίσμα της έννοιας της επιβιωσιμότητας, οι παρεχόμενες υπηρεσίες από ένα σύστημα θα πρέπει να έχουν την ικανότητα να αναγνωρίζουν και να αντιστέκονται σε επιθέσεις, να αναρρώνουν και να αποκαθιστούν τη λειτουργία τους μετά από αυτές, και να αναπροσαρμόζουν τη λειτουργία τους κατά τη δράση των επιθέσεων, έτσι ώστε να μειώνουν τις επιδράσεις τους σε φάσεις εξέλιξης μελλοντικών άλλων επιθέσεων. Για να μπορέσουμε να χαρακτηρίσουμε ένα σύστημα ως επιβιώσιμο (survivable), είναι πρωτίστως αναγκαίο οι υπηρεσίες που παρέχονται από το σύστημα σε ένα εχθρικό περιβάλλον, να κατηγοριοποιηθούν ως σημαντικές (essential) και μη σημαντικές (non-essential). Περαιτέρω, οι υπηρεσίες που αναμένονται από ένα σύστημα παρουσία επιθέσεων, θα πρέπει να τεθούν σε λειτουργικά επίπεδα προτεραιότητας (service priorities). Οι εργασίες **[16**], [57] περιγράφουν μία στρατηγική επιβίωσης (survivability strategy) η οποία μπορεί να υλοποιηθεί με χρήση τριών βημάτων. Οι βασικές της αρχές είναι η προστασία (protection), η ανίχνευση (detection) και η ικανότητα αποκρίσεως (response) του συστήματος κατά την αποκατάσταση της λειτουργίας του (recovery). Οι ερευνητές θέτουν πέντε προϋποθέσεις οι οποίες σχετίζονται με την έννοια της επιβιωσιμότητας για τα συστήματα. Οι προϋποθέσεις αυτές αφορούν την ικανότητα επιβίωσης του συστήματος (system/survivability), τη χρήση κατά τη φάση επίθεσης (use/intrusion), τις απαιτήσεις για την ανάπτυξή του (development requirements),

τις λειτουργικές του απαιτήσεις (operational requirements), καθώς και τις απαιτήσεις εξέλιξης και αναβάθμισής του (evolution requirements).
Η έννοια της επιβιωσιμότητας εφαρμόζεται καθολικά σε ένα σύστημα το οποίο παρέχει υπηρεσίες, και όχι σε τμήματα ή υποσυστήματά του. Ο πρωταρχικός σκοπός της έννοιας είναι η ικανότητα εκπλήρωσης της έννοιας της αποστολής (mission). Αυτό συνεπάγεται κυρίως την επιβίωση των βασικών του υπηρεσιών, παρά την ικανότητά του για πλήρη αποκατάσταση της λειτουργικότητάς του μετά από την εκδήλωση μίας επίθεσης. Ένα σύστημα με ικανότητα επιβίωσης θα πρέπει πρωτίστως να αντιδρά και να προσπαθεί να αποφύγει μία καταστροφική επίδραση στα υποσυστήματά του πριν καταλήξει σε ολοκληρωτική καταστροφή από την επίθεση. Επομένως, κατά τη λειτουργία ενός συστήματος κάτω από εχθρικές συνθήκες δράσης, ένα σύστημα με ικανότητα επιβίωσης μπορεί είτε να συνεχίζει να λειτουργεί με μειωμένες δυνατότητες ή τουλάχιστον να μπορεί να συνεχίσει τη λειτουργία του κατά τρόπο που να μπορεί να ικανοποιήσει τις προσφερόμενες υπηρεσίες του πριν την ολική του καταστροφή.

2.3 Οι μετρικές ποιότητας που εισάγονται στη λειτουργία των συστημάτων με βάση τα ιδιαίτερα χαρακτηριστικά τους

Τα ιδιαίτερα χαρακτηριστικά των πληροφοριακών συστημάτων, ορίστηκαν και αποσαφηνίστηκαν στις προηγούμενες ενότητες. Στη συνέχεια παρουσιάζεται μία αναφορά των βασικών εργαλείων που χρησιμοποιούνται στην αξιολόγηση για τα πέντε ιδιαίτερα χαρακτηριστικά, χωρίς όμως να γίνεται αναφορά σε εφαρμογές συγκεκριμένου τύπου και ειδικά περιβάλλοντα. Στην πράξη, οι μετρικές επίδοσης και αξιολόγησης, σχετίζονται με συγκεκριμένες εφαρμογές και λειτουργικά περιβάλλοντα. Στόχος είναι η παροχή γενικών δεικτών (Indicators) που σχετίζονται με τις προσεγγίσεις που αφορούν σε κάθε ιδιαίτερο χαρακτηριστικό.
Δεδομένου ότι αυτές οι προσεγγίσεις αξιολόγησης έχουν εξελιχθεί παράλληλα με την τεχνολογία και την πάροδο του χρόνου, μία καλή απόπειρα προσέγγισης στο συγκεκριμένο θέμα, είναι η παρακολούθηση της χρονικής εξέλιξης αυτών των μετρικών. Η έννοια της αξιοπιστίας είναι και η πρώτη χρονικά έννοια που αξιολογείται ιστορικά κατά την ανάπτυξη των συστημάτων. Στη συνέχεια ακολουθούν οι έννοιες της ανοχής σε λειτουργία σφάλματος, της ασφάλειας, της εξαρτησιμότητας και, τέλος, η έννοια της επιβιωσιμότητας. Η εξέλιξη των μέτρων επίδοσης και ποιότητας προσθέτει ή/και αλλάζει τους δείκτες, από ένα ιδιαίτερο χαρακτηριστικό σε άλλο ιδιαίτερο χαρακτηριστικό.

Ορισμός: Ως **μετρική επίδοσης** ενός χαρακτηριστικού καλείται μία μαθηματική συνάρτηση εκτίμησης (με βαθμό πιθανότητας ή ντετερμινιστική), η οποία προσδίδει ποσοτικοποιήσιμα μία τιμή αποτίμησης του χαρακτηριστικού.

Στόχος των μετρικών επίδοσης είναι η υλοποίηση σαφώς καθορισμένων μαθηματικών συναρτήσεων, οι οποίες αποδίδουν στο πεδίο τιμών τους μία εκτίμηση του επιπέδου του κάθε χαρακτηριστικού για τη λειτουργία ενός συστήματος. Η βιβλιογραφία, για την κατασκευή κάθε συνάρτησης μετρικής επίδοσης χρησιμοποιεί διάφορα χαρακτηριστικά, όπως η αξιοπιστία, η διαθεσιμότητα, Μέσος Χρόνος

Μεταξύ Αποτυχημένων Λειτουργιών, Μέσος Χρόνος Αποκατάστασης, κλπ. Η χρήση αυτών των παραμέτρων για την εκτίμηση των μετρικών ποιότητας διαφέρει από ιδιαίτερο χαρακτηριστικό σε άλλο (δηλ, κάθε ιδιαίτερο χαρακτηριστικό δίνει έμφαση σε αυτές τις παραμέτρους που ρυθμίζουν σημαντικότερα την εκτίμησή του).

2.4 Τα πληροφοριακά συστήματα ως υποσυστήματα του ελέγχου AGC

Οι εφαρμογές που αφορούν στη Διαχείριση της Παραγωγής και τον Έλεγχο της διανεμόμενης ηλεκτρικής ισχύος (συστήματα AGC), αποτελούν επίσης πεδίο διαλειτουργικότητας και ανταλλαγής πληροφορίας που κάνει χρήση τεχνολογιών πληροφοριακών συστημάτων.

Τα συστήματα AGC, όπως θα καταδειχθεί αναλυτικότερα και στις επόμενες ενότητες της εργασίας, απαιτούν χρήση μηχανισμών ταυτοποίησης και επιπέδου πρόσβασης στα ψηφιακά περιβάλλοντα – εφαρμογές διαχείρισής τους. Τα συστήματα AGC βασίζονται σε μηχανισμούς απόφασης και αποστολής εντολών σε αναλογικά – ψηφιακά κυκλώματα που υλοποιούν τους αισθητήρες (sensors) και ενεργοποιητές (actuators) του συστήματος ισχύος. Η διασύνδεση των συστημάτων AGC και η επικοινωνία τους με τον Διαχειριστή Ενέργειας (EMS), απαιτεί επίσης χρήση τεχνολογιών δικτύων κορμού και κάνει χρήση όλων των τεχνολογιών για την ασφάλεια των επικοινωνιών (κρυπτογράφηση, αποκρυπτογράφηση) για να διασφαλίσει το αναλλοίωτο τόσο των παρεχόμενων μετρήσεων όσο και τη διανομή των ενεργειών απόφασης.

Τα πληροφοριακά συστήματα που απαιτούνται για τη λειτουργία των AGC συστημάτων, δεν αφορούν μόνο στα δεδομένα των χρηστών που κάνουν τη διαχείριση και τον έλεγχο των δικτύων παραγωγής και διανομής ισχύος, αλλά και στα ευαίσθητα πληροφοριακά στοιχεία που αναφέρονται στα χαρακτηριστικά των μηχανισμών παραγωγής και διανομής (τύποι των γεννητριών παραγωγής, διασυνδεόμενα φορτία, χαρακτηριστικά και επιδόσεις των δικτύων, ηλεκτρικά χαρακτηριστικά, ευαισθησίες, αδράνειες, γραμμές μεταφοράς, μέγιστα όρια λειτουργίας, κλπ).

Επομένως, τα προβλήματα που αναλύθηκαν σχετικά με την ασάφεια και τον καθορισμό των πέντε ειδικών χαρακτηριστικών, αποτελούν ένα επίσης ανοικτό θέμα και για το πρόβλημα της Διαχείρισης και Παραγωγής Ηλεκτρικής Ισχύος. Τα χαρακτηριστικά της Αξιοπιστίας, της Ανοχής σε λειτουργία σφάλματος, της Ασφάλειας, της Εξαρτησιμότητας και της Επιβιωσιμότητας, αποτελούν επίσης ανοικτά πεδία που χρειάζονται έναν επακριβή ορισμό τόσο για τη διασφάλιση της παρεχόμενης λειτουργίας του συστήματος AGC, καθώς και ποσοτικοποίηση η οποία θα διευκολύνει τη δυνατότητα Λήψης Αποφάσεων μέσω του κέντρου Διαχείρισης (EMS).

Η έννοια της Αξιοπιστίας για τα συστήματα AGC, αναφέρεται τόσο στο επίπεδο των στοιχείων που συνθέτουν την υποδομή του δικτύου παραγωγής και διανομής ηλεκτρικής ισχύος, όσο και γενικότερα στην ικανότητα απρόσκοπτης παροχής ισχύος σε όλο το δίκτυο με την προσέγγιση της έννοιας της συνεχούς προσφερόμενης υπηρεσίας (continuous service). Η ποσοτικοποίηση του χαρακτηριστικού μπορεί να κάνει χρήση των ανάλογων μετρικών αποτιμώντας (i) τα επίπεδα βλαβών του

δικτύου, (ii) την ικανότητα μετρήσεων των συστημάτων των αισθητήρων, (iii) την ορθή μεταβίβαση των εντολών από τον EMS προς το δίκτυο, (iv) τη λειτουργία των ενεργοποιητών (actuators) για την υλοποίηση των εντολών, καθώς και (v) των παραμέτρων MTBF (Mean Time Between Failure), MTTR (Mean Time To Repair).
Το χαρακτηριστικό της Ανοχής σε λειτουργία σφάλματος συμπεριλαμβάνεται ήδη στις εφαρμοζόμενες πολιτικές διαχείρισης ισχύος από τα κέντρα λήψης αποφάσεων, μέσω των αργών μεταβολών των χαρακτηριστικών παραγωγής (αδράνεια) για την αποφυγή άμεσων εντολών δράσης **[1]**, αλλά και μέσω της χρήσης επιλεγμένων σταθμών για τη ρύθμιση των επιπέδων διακύμανσης ισχύος σε ένα δίκτυο πολλαπλών περιοχών.
Η ασφάλεια (security) αποτελεί επίσης ένα σημαντικό χαρακτηριστικό λειτουργίας για τα συστήματα AGC. Οι μηχανισμοί της ασφάλειας διασφαλίζονται με τη χρήση πρωτοκόλλων κρυπτογράφησης στην επικοινωνία των σταθμών μέτρησης με τα κέντρα λήψης απόφασης. Επιπλέον, η διαχείριση των συστημάτων Λήψης Απόφασης του EMS αποτελεί αντικείμενο διασυνεχούς παρακολούθησης μέσω των διαδικασιών καταγραφής και παρακολούθησης της δράσης των χρηστών (administrators) στο σύστημα (monitoring process). Εντούτοις, και για τα συστήματα AGC η έννοια της ασφάλειας δεν είναι εύκολο να ποσοτικοποιηθεί.
Οι έννοιες της εξαρτησιμότητας και της επιβιωσιμότητας είναι δύσκολο να ποσοτικοποιηθούν επίσης, για τα συστήματα AGC. Επιπλέον, η έννοια της επιβιωσιμότητας εμπλέκεται άμεσα με το χειρισμό διαταραχών μέσω επιθέσεων, οι οποίες μπορεί να είναι τυχαίες ή/και σκόπιμες προς ένα σύστημα παραγωγής ισχύος.
Στα συστήματα AGC η μερική λειτουργία συστημάτων, καθώς και ο μερικός έλεγχος του δικτύου παραγωγής δεν αποτελούν εφαρμόσιμες εναλλακτικές, δεδομένου ότι το σύστημα παροχής ισχύος πρέπει να βρίσκεται διαρκώς σε πλήρη λειτουργική κατάσταση.
Τα φορτία που χειρίζεται ένα σύστημα AGC μπορούν όμως να κατηγοριοποιηθούν σε σημαντικά (essential) και μη σημαντικά (non-essential) ως προς τα θέματα διαρκούς κάλυψης, δίνοντας έτσι τη δυνατότητα στον EMS να λειτουργήσει με χρήση προτεραιοτήτων σε περίπτωση έλλειψης επαρκούς ισχύος για τη συνολική κάλυψη των απαιτήσεων του δικτύου.
Εντούτοις, μία ενδεχόμενη προσπάθεια ποσοτικοποίησης τόσο της έννοιας της εξαρτησιμότητας όσο και της έννοιας της επιβιωσιμότητας για ένα σύστημα AGC, μπορεί να αναδείξει τα κρίσιμα στοιχεία του δικτύου.
Στη συνέχεια θα παρουσιαστούν οι επιδράσεις υπό τη μορφή επιθέσεων που ένα σύστημα AGC μπορεί να δεχθεί, καθώς και οι μηχανισμοί αντίδρασης για την αποφυγή καταστροφικών συνεπειών για τη λειτουργία του.

3 Τύποι Επιθέσεων σε δομές AGC

3.1 Σκοπός και στόχοι μίας επίθεσης σε ένα σύστημα AGC

Όπως ήδη έχει παρουσιαστεί και στο Κεφάλαιο 1 της εργασίας, ένα σύστημα AGC είναι υπεύθυνο για τη διασφάλιση της ομαλής λειτουργίας του δικτύου παραγωγής και διαχείρισης της ηλεκτρικής ισχύος. Επομένως, ο ρόλος του AGC είναι εξαιρετικά σημαντικός για την επίτευξη της ευσταθούς λειτουργίας στην παραγωγή και παροχή ισχύος προς τα φορτία-καταναλωτές. Κατά συνέπεια, οποιασδήποτε μορφής προσβολή του συστήματος AGC, στοχεύει στη δημιουργία ανωμαλίας στην παροχή ισχύος, η οποία κλιμακούμενα μπορεί να αποσκοπεί στα ακόλουθα **[10]**, **[18]**, **[19]**, **[20]**, **[21]**, **[24]**, **[25]**, **[26]**:

- **Πρόκληση δυσλειτουργίας στο δίκτυο** με στόχο την απώλεια ισχύος στα διανεμόμενα φορτία (blackout).
- **Καταστροφή δομικών συστημάτων παραγωγής και διαχείρισης ισχύος**.
- **Καταστροφή φορτίων και συσκευών** διασυνδεόμενων στο δίκτυο ισχύος.
- **Πρόκληση οικονομικής επιβάρυνσης** (ζημίας) στη λειτουργία του δικτύου.
- **Πρόκληση εκτεταμένης απώλειας ισχύος σε γεωγραφικές περιοχές** με ταυτόχρονη κοινωνική και λειτουργική αστάθεια - αναταραχή (τρομοκρατικές ενέργειες, διακοπή δημοσίων συγκοινωνιών).
- **Πρόκληση επιθετικών ενεργειών στρατιωτικής κλίμακας [28]**.

Η κλιμάκωση των αποτελεσμάτων μίας επίθεσης στα συστήματα ελέγχου AGC, αναφέρεται άμεσα στο μέγεθος και το επίπεδο ισχύος που διαχειρίζεται το συνολικό σύστημα παραγωγής και διανομής ισχύος. Δίκτυα διαχείρισης ισχύος μεγάλης κλίμακας συνεπάγεται ότι όταν βρεθούν σε κατάσταση προβληματικής λειτουργίας λόγω επίθεσης, έχουν σαφώς μεγαλύτερο αντίκτυπο στη συνολική λειτουργία των δικτύων υποδομής, σε σχέση με δίκτυα μικρότερης κλίμακας.
Η κλιμάκωση των επιθέσεων μπορεί να προκαλέσει οικονομικές καταστροφές, από τη δυσλειτουργία και υποβάθμιση του υλικού, μέχρι και την απώλεια ανθρώπινων ζωών, ειδικότερα στην περίπτωση που τα συστήματα παροχής ισχύος καλύπτουν ευαίσθητους τομείς των ανθρωπίνων δραστηριοτήτων (κίνηση, κυκλοφορία, αεροδρόμια, περίθαλψη, αποθήκευση τροφίμων, ύδρευση, κλπ).
Κατά συνέπεια οι επιθέσεις αυτού του τύπου μπορούν να θεωρηθούν ως «ασύμμετρες απειλές» **[28]** με την πλήρη έννοια του όρου, δεδομένου ότι η πρόσβαση και η αλλοίωση των δεδομένων λειτουργίας ενός δικτύου παραγωγής και παροχής ισχύος, παράγει υπέρμετρα αρνητικά αποτελέσματα στην υποδομή ισχύος.
Οι επιθέσεις αυτού του τύπου έχουν αναβαθμιστεί στο επίπεδο της έννοιας μίας κυβερνο-επίθεσης (cyber-attack) με την αυστηρή έννοια του όρου, εφόσον τα δεδομένα είναι ανταλλάξιμα και διαχειρίσιμα μέσω υποδομών δικτύων δεδομένων και ηλεκτρονικών υπολογιστών **[18]**. Η εξαπλωμένη διασύνδεση μέσω των ηλεκτρονικών υπολογιστών (internet) καθιστά ευκολότερη την πρόσβαση μεγαλύτερου αριθμού από χρήστες σε αυτά τα ευαίσθητα δεδομένα, χωρίς την απαίτηση φυσικής παρουσίας στους χώρους λειτουργίας και παραγωγής ισχύος.

Επομένως, η εξέλιξη της τεχνολογίας και η καθολική ηλεκτρονική διασύνδεση εισάγει νέο κίνδυνο στη λειτουργία των δικτύων υποδομής. Οι χρήστες που μπορεί να αποκτήσουν πρόσβαση στη διαχείριση αυτού του τύπου των δεδομένων, μπορεί να είναι κακόβουλοι ή απλά μη εξουσιοδοτημένοι. Κατά συνέπεια, οι απειλές που αφορούν στον έλεγχο των υπολογιστικών συστημάτων (hacking, cracking, DoS attacks, κλπ), αποτελούν απειλές που ενσωματώνονται στα δίκτυα παραγωγής και διαχείρισης ισχύος.
Πέρα λοιπόν από τις οικονομικές απώλειες, όπου οι επιθέσεις του παραπάνω τύπου επιφέρουν στα δίκτυα ισχύος, δημιουργούν δυσλειτουργίες μεγάλης έκτασης. Για το λόγο αυτό τα προβλήματα του εντοπισμού, απομόνωσης και αντίκρουσης των παραπάνω επιθέσεων, καθίστανται ιδιαιτέρως σημαντικά για το δίκτυο παροχής ισχύος. Η ψηφιακή τεχνολογία, καθώς και η γρήγορη μετάδοση και επεξεργασία των δεδομένων, αποτελούν χαρακτηριστικά που μπορούν να διευκολύνουν και τις δύο πλευρές: και του επιτιθέμενου στο δίκτυο, αλλά και των αμυντικών μηχανισμών που αναπτύσσει το συνολικό σύστημα διαχείρισης ισχύος. Οι επιθετικές και αμυντικές ενέργειες για τον έλεγχο του δικτύου γίνονται μέσω της υλοποίησης αλγορίθμων προς εφαρμογή στα συστήματα παραγωγής και διαχείρισης ισχύος. Δηλαδή, τα παραπάνω προβλήματα διαμορφώνουν την ανάγκη δημιουργίας και εξέλιξης ευφυών αλγορίθμων (ελέγχου και άμυνας). Οι αλγόριθμοι αυτοί εκτελούνται σε υπολογιστικά συστήματα, που υποστηρίζουν τη διαδικασία λήψης αποφάσεων στον Διαχειριστή EMS. Τα αποτελέσματα εκτέλεσης των αλγορίθμων εκτείνονται μέχρι τα όρια των έξυπνων συσκευών μέτρησης – καταγραφής και μετάδοσης δεδομένων από τους αισθητήρες.
Στη συνέχεια, παρουσιάζονται τα ιδιαίτερα χαρακτηριστικά των τύπων των επιθέσεων, ξεκινώντας από το υψηλό αλγοριθμικό επίπεδο μέχρι το χαμηλότερο επίπεδο, που αναφέρεται στη μορφή των παραγόμενων σημάτων που ανταλλάσσονται μέσα στο δίκτυο από και προς τους αισθητήρες και τους ενεργοποιητές.

3.2 Τύποι και πρότυπα επίθεσης

Η λειτουργία του AGC συνεπάγεται στενή αλληλεπίδραση μεταξύ του κυβερνοχώρου και των φυσικών τμημάτων του συστήματος παραγωγής και διαχείρισης ισχύος. Παρακολουθώντας την απόκλιση από το Σφάλμα Ελέγχου Περιοχής (ACE) που συλλέγεται από τους κατανεμημένους αισθητήρες, οι έξοδοι ισχύος των γεννητριών τροποποιούνται κατάλληλα μέσω του AGC, για να εξισορροπηθεί η τυχαία διακύμανση φορτίων στο σύστημα. Έτσι, η συχνότητα του ηλεκτρικού δικτύου διατηρείται κοντά στην ονομαστική τιμή της (50/60 Hz ανάλογα με τη γεωγραφική περιοχή και το σύστημα κάλυψης). Οι κυβερνο-επιθέσεις, που ακολουθούν προκαθορισμένες στρατηγικές επίθεσης, εντοπίζονται ελέγχοντας τον στατιστικό και χρονικό χαρακτήρα των σφαλμάτων ελέγχου περιοχής (ACE).
Η ανίχνευση και ο καθορισμός μιας επίθεσης στα δίκτυα ισχύος αποτελεί ένα σημαντικό θέμα. Ένα σύστημα AGC μπορεί να ανιχνεύσει τη διαδικασία μιας επίθεσης μέσω της αλλαγής του επιπέδου των μετρήσεων που δέχεται από τους αισθητήρες. Όταν αυτές αποκλίνουν σημαντικά από τις προβλεπόμενες, ενεργοποιούνται συναγερμοί για τη λειτουργία του δικτύου (alarms), θεωρώντας ότι

το δίκτυο σε συνδυασμό με το σύστημα ελέγχου AGC δέχεται επίθεση. Τα τυπικά πρότυπα επίθεσης είναι **[10]**, **[20]**:

- **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.
- **Επιθέσεις εισαγωγής θορύβου (Noise-Injection Attack):** Σε αυτό το μοντέλο επίθεσης, οι αισθητήρες υπό τον έλεγχο του επιτιθέμενου, προσθέτουν μία οριακή τυχαία τιμή στην πραγματική μέτρηση και στη συνέχεια οι σκόπιμα λανθασμένες μετρήσεις προωθούνται προς το κέντρο ελέγχου.
- **Επίθεση αποσταθεροποίησης (Destabilization Attack):** Σε μία επίθεση αποσταθεροποίησης, οι αισθητήρες του AGC στην περιοχή i που βρίσκονται υπό τον έλεγχο του επιτιθέμενου, αναφέρουν μία ψευδή ακολουθία μετρήσεων. Η ακολουθία αυτή είναι μία φιλτραρισμένη έκδοση της πραγματικής ακολουθίας των μετρήσεων. Εάν M είναι ένα τέτοιο φίλτρο, η επίθεση συνίσταται στην εισαγωγή του φίλτρου M στο μοντέλο του συστήματος, με το M (ως παράμετρος) να επιλέγεται από τον επιτιθέμενο έτσι ώστε το αρχικό σύστημα να είναι ασταθές. Η ακολουθία εξόδου ενός κακόβουλου φίλτρου M μπορεί να ληφθεί ακόμη και χωρίς πληροφορίες για το μοντέλο του συστήματος.
- **Επιθέσεις ακεραιότητας (Integrity Attacks):** Σε αυτού του τύπου τις επιθέσεις, 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 άρνησης εξυπηρέτησης (Denial of Service – DoS Attacks):** Σε αυτούς τους τύπους των επιθέσεων, ο επιτιθέμενος εμποδίζει τις πληροφορίες που αποστέλλουν οι αισθητήρες να φθάσουν στο διαχειριστή δικτύου. Εναλλακτικά, εμποδίζει τους ενεργοποιητές να λαμβάνουν σήματα ελέγχου από τον διαχειριστή. Κατά συνέπεια, το σύστημα διαχείρισης δεν μπορεί να λάβει αποφάσεις για τη σωστή εφαρμογή ελέγχου.
- **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.

- **Άμεσες επιθέσεις:** Πραγματοποιούνται στο φυσικό σύστημα ή στον ελεγκτή (π.χ. καταστροφή/απώλεια μετρητικού δικτύου αισθητήρων–ενεργοποιητών).

Οι επιθέσεις DoS ή TD ενδέχεται να προκληθούν από εμπλοκή των διαύλων επικοινωνίας, την υπονόμευση των συσκευών και την αποτροπή τους από το να στέλνουν δεδομένα, καθώς και από επιτιθέμενα πρωτόκολλα δρομολόγησης ή λόγω 'πλημμύρας' (flooding) του δικτύου. Στην τελευταία περίπτωση, η συμφόρηση (congestion) ενός ψηφιακού δικτύου πρωτοκόλλων για τη μετάδοση δεδομένων, έχει ως άμεσο αποτέλεσμα την απώλεια πακέτων. Η συμφόρηση σε συνδυασμό με τα πρωτόκολλα μπορεί να επιβάλει την αποστολή πακέτων με τα ίδια δεδομένα (επανάληψη λόγω απώλειας). Η επεξεργασία των δεδομένων καθίσταται δυσχερής, δημιουργώντας μεγάλα χρονικά κενά, τα οποία δημιουργούν επισφάλειες στη διασυνεχή παρακολούθηση της λειτουργίας του δικτύου ισχύος.

Γενικότερα, λοιπόν, στόχος όλων των μορφών επίθεσης είναι η προσβολή και η λανθασμένη λήψη αποφάσεων από το Διαχειριστή Ενέργειας EMS. Η προσβολή του EMS και η λανθασμένη λήψη αποφάσεων αποτελούν το χειρότερο δυνατό αποτέλεσμα, το οποίο συνιστά τη μέγιστη επιτυχία μίας κακόβουλης επίθεσης, διότι θα καταλήξουν σε καταστροφή του συστήματος παραγωγής και διαχείρισης ισχύος, υπό το πρίσμα εντολών που θεωρούνται ορθές και απορρέουν από τα κέντρα λήψης αποφάσεων (ενώ στην πραγματικότητα είναι λανθασμένες). Επομένως, οι παραγόμενες εντολές υπό αυτό το καθεστώς είναι λανθασμένες, αλλά είναι αδύνατο να διαχωρισθούν από υγιείς – σωστές εντολές που χωρίς την προσβολή θα δίνονταν προς το δίκτυο. Οι άμεσες επιθέσεις που προσβάλουν τους αισθητήρες και ενεργοποιητές μπορούν, σε πολλές περιπτώσεις, να είναι γρήγορα εντοπίσιμες και πιο εύκολα ελέγξιμες σε σχέση με τις επιθέσεις της προηγούμενης περίπτωσης. Στόχος των μεθόδων εντοπισμού των επιθέσεων όλων των τύπων είναι, αφενός η ανίχνευση της κατάστασης επίθεσης στο δίκτυο, και αφετέρου η λήψη των σωστών αποφάσεων – εντολών για την ορθή διαχείριση του δικτύου, απομονώνοντας κέντρα και σημεία που είναι υπό τον έλεγχο του επιτιθέμενου.

3.2.1 Τεχνικές επίθεσης και απόκτηση δεδομένων δικτύου ισχύος

Οι επιτιθέμενοι δεν είναι υποχρεωμένοι να ακολουθήσουν τα προδιαγεγραμμένα πρότυπα επιθέσεων που περιγράφηκαν παραπάνω, για να προκαλέσουν σημαντικές επιπτώσεις στο δίκτυο ισχύος. Παρόλο που ο μηχανισμός ανίχνευσης ανωμαλιών είναι σε θέση να προσδιορίσει τα προκαθορισμένα πρότυπα επίθεσης, η ευρύτητα των επιθέσεων και η διαφορετικότητα των τύπων τους δεν επιτρέπει την ανάπτυξη ενός γενικού αλγορίθμου που να είναι ικανός να εντοπίσει και να αναγνωρίσει αυθαίρετες κυβερνο-επιθέσεις. Εκτεταμένες πληροφορίες σχετικά με το μοντέλο του συστήματος ενδέχεται να εκτεθούν και να είναι σε γνώση του επιτιθέμενου. Υπάρχουν δύο τρόποι με τους οποίους ένας κακόβουλος αντίπαλος μπορεί να αποκτήσει πληροφορίες σχετικά με το μοντέλο του δικτύου παραγωγής και παροχής ισχύος **[10**]:

- Το λεπτομερές φυσικό μοντέλο μπορεί να διαρρεύσει απευθείας στον επιτιθέμενο μέσω δυσαρεστημένων υπαλλήλων ή κακόβουλων εσωτερικών

παραγόντων ή λόγω έλλειψης διεργασιών ασφαλείας, η οποία δίνει άμεση πρόσβαση στην πληροφορία χωρίς ταυτοποίηση.

- Το στατιστικό μοντέλο του συστήματος ισχύος μπορεί να διδαχθεί χρησιμοποιώντας μαθηματικά εργαλεία που βασίζονται στα δεδομένα λειτουργίας του συστήματος που έχουν διαρρεύσει.

Οι επιτιθέμενοι στην πρώτη περίπτωση μπορούν να παρακάμψουν τον αλγόριθμο ανίχνευσης ανωμαλιών που βασίζεται στην εκτίμηση κατάστασης, διεξάγοντας "μη παρατηρήσιμες επιθέσεις". Οι επιτιθέμενοι στη δεύτερη περίπτωση μπορούν να παραβιάσουν τις μετρήσεις χωρίς να ενεργοποιήσουν κανένα συναγερμό ελέγχου, αντικαθιστώντας την πραγματική αλληλουχία μετρήσεων με μία διαφορετική ακολουθία που εξακολουθεί να συμμορφώνεται με το μαθηματικό στατιστικό μοντέλο λειτουργίας του δικτύου. Επομένως, οι κακόβουλες παρεχόμενες μετρήσεις δε φαίνεται να διαφέρουν σημαντικά από ενδεχόμενες ορθές μετρήσεις. Μία μικρή, αλλά κακόβουλη παραμόρφωση των μετρήσεων συχνότητας με βάση το φυσικό/στατιστικό μοντέλο του συστήματος ισχύος, δεν είναι πιθανό να ανιχνευθεί από τον αλγόριθμο ελέγχου ανωμαλιών για το δίκτυο.

3.3 Ειδικοί Τύποι Επίθεσης: Έγχυση λανθασμένων δεδομένων

Η Έγχυση λανθασμένων δεδομένων (False Data Injection Attacks) **[19]** είναι μία σημαντική κατηγορία επιθέσεων κατά του AGC. 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).

3.4 Ειδικοί Τύποι Επίθεσης: Επίδραση των μεθόδων επικοινωνίας σε επιθέσεις με χρονικές καθυστερήσεις (time delays)

Ο κύριος παράγοντας που κάνει τη διαφορά ανάμεσα στο παραδοσιακό και το έξυπνο δίκτυο είναι η αμφίδρομη επικοινωνία μεταξύ των μονάδων του. Η επικοινωνία παρέχει αυτοματοποίηση καθώς και πληροφορίες για ψηφιακή επεξεργασία, που αποτελούν τα κύρια χαρακτηριστικά του έξυπνου δικτύου. Μερικές από τις παραμέτρους που επιδρούν σημαντικά στην επικοινωνία είναι η καθυστέρηση, καθώς και η απώλεια πακέτων δεδομένων που βιώνει το δίκτυο μετάδοσης δεδομένων.

Η ρύθμιση της συχνότητας μπορεί να επιτευχθεί με την εξισορρόπηση της πραγματικής παραγωγής ισχύος και των ηλεκτρικών φορτίων σε ένα σύστημα ισχύος. Όταν η ζήτηση είναι υψηλότερη από την παραγωγή, η συχνότητα θα μειωθεί από την ονομαστική συχνότητα του συστήματος. Από την άλλη, όταν η παραγωγή είναι υψηλότερη από τη ζήτηση, η συχνότητα θα είναι υψηλότερη από την ονομαστική της τιμή. Στα σημερινά διασυνδεδεμένα συστήματα ισχύος,

διαφορετικές περιοχές παραγωγής ισχύος συνδέονται μέσω γραμμών μεταφοράς, οπότε μια αλλαγή φορτίου σε μια περιοχή μπορεί να επηρεάσει τη συχνότητα σε ολόκληρο το σύστημα. Η ροή ισχύος των γραμμών σύνδεσης πρέπει να πληροί ένα χρονοδιάγραμμα, με αποτέλεσμα να παρουσιάζει ένα επιπλέον ενδιαφέρον πρόβλημα πρόσθετα από τον έλεγχο συχνότητας, όπως η ελαχιστοποίηση των αποκλίσεων ροής ισχύος των γραμμών διασύνδεσης (δεδομένων διαφορετικών τιμολογιακών πολιτικών στην παραγωγή της ισχύος).
Για τη λήψη μετρήσεων από το δίκτυο, χρησιμοποιούνται ηλεκτρονικές συσκευές που μετρούν διαφορές φάσης και συχνότητας στο δίκτυο, καλούμενες ως Phasor Measurement Units – PMUs.

Οι **καθυστερήσεις στην επικοινωνία [20]** σε ένα σύστημα που βασίζεται στις συσκευές PMUs μπορεί να **οφείλονται** στις ακόλουθες αιτίες:

- Καθυστερήσεις του μετατροπέα (Transducer delays). Αυτές οφείλονται στο χρόνο που απαιτείται για τη μετατροπή ενός αναλογικού σήματος σε ψηφιακό και την αποθήκευσή του σε μία φυσική μνήμη για τη μορφοποίηση και την αποστολή του πακέτου μετρήσεων προς το διαχειριστή.
- Μέγεθος παραθύρου για τον αριθμητικό υπολογισμό του DFT (πλήθος δειγμάτων) για τον έλεγχο αρμονικών. Η αύξηση του πλήθους δειγμάτων που χρησιμοποιούνται για τον υπολογισμό στην ανάλυση Fourier είναι ένα μη γραμμικό πρόβλημα που ακόμη και με χρήση ταχέων αλγορίθμων δίνει πολυπλοκότητα $N \times log_2 N$. Επομένως, η αύξηση του πλήθους δεδομένων ενώ συνεπάγεται καλύτερη εκτίμηση της κατάστασης συνιστά ένα χρονικό παράγοντα καθυστέρησης για την εξαγωγή της επεξεργασίας ακόμη και με ταχείς μορφές του αλγορίθμου (FFT – Fast Fourier Transform).
- Χρόνος επεξεργασίας (Processing time). Είναι ο απαιτούμενος χρόνος που οι αλγόριθμοι γενικά χρειάζονται για να επεξεργασθούν τα δεδομένα.
- Μέγεθος του πακέτου δεδομένων της PMU (Data size of the PMU output). Η αύξηση του μεγέθους ενός πακέτου προς αποστολή συνιστά έναν επιπλέον παράγοντα καθυστέρησης μέχρι τη συγκέντρωση των δεδομένων για την ολοκλήρωση (γέμισμα του πακέτου πριν την αποστολή).
- Πολύπλεξη και μεταβάσεις στη διάδοση των δεδομένων (Multiplexing and Node transitions). Οι καθυστερήσεις οφείλονται στη διέλευση των πακέτων δεδομένων μέσα από τους διαδοχικούς κόμβους της διάταξης. Κάθε κόμβος φορτώνει προσωρινά το λαμβανόμενο πακέτο κατά τη λήψη σε φυσική μνήμη και στη συνέχεια το επαναπροωθεί. Μεγάλο πλήθος κόμβων συνεπάγεται μεγάλες καθυστερήσεις διάδοσης των πακέτων προς τον τελικό αποδέκτη.
- Συγκεντρωτές δεδομένων (Data concentrators)
- Εμπλεκόμενη επικοινωνιακή σύνδεση (Communication link involved). Ο τύπος του δικτύου επικοινωνίας επιδρά τόσο στο ρυθμό μετάδοσης όσο και στην ανάπτυξη λαθών στη μετάδοση (π.χ. οπτικό μέσο, καλώδιο χαλκού, διαμορφώσεις μετάδοσης, κλπ).

Ενδεικτικά, ο πίνακας που ακολουθεί δίνει τις τυπικές καθυστερήσεις μετάδοσης, ανάλογα με την τεχνολογία και τον τύπο του δικτύου διασύνδεσης των υποσυστημάτων του δικτύου AGC:

Communication link	Associated Delay (milliseconds)
Fiber-optic cables	100-150
Digital microwave links	100-150
Power line (PLC)	150-350
Telephone lines	200-300
Satellite link	500-700

Πίνακας 1: Τυπικές χρονικές καθυστερήσεις μετάδοσης με βάση την τεχνολογία και τον τύπο δικτύου [20]

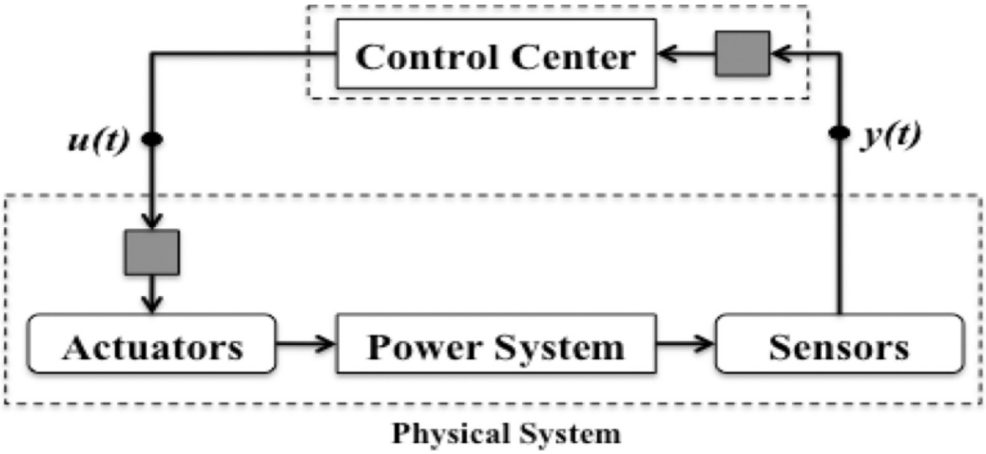
Η σχετική καθυστέρηση για μία συγκεκριμένη σύνδεση επικοινωνίας μπορεί να είναι από 100 έως 700 *msec* (χιλιοστά του δευτερολέπτου). Ωστόσο, η συνολική καθυστέρηση με την εξέταση άλλων αιτιών θα είναι μεγαλύτερη από το προβλεπόμενο εύρος.

3.5 Ειδικοί Τύποι Επίθεσης: Επιθέσεις με χρήση μοντέλων

Πρόσφατες περιπτώσεις επιθέσεων έδειξαν ότι οι κυβερνο-επιθέσεις συντάσσονται ειδικά για τα Βιομηχανικά Συστήματα Ελέγχου (ICS - Industrial Control Systems) και μάλιστα στοχεύουν σε συγκεκριμένες εφαρμογές κρίσιμου ελέγχου μέσα στο περιβάλλον του συστήματος ελέγχου. Συνεπώς, οι εξελιγμένοι επιτιθέμενοι έχουν πλήρη γνώση, όχι μόνο των υπολογιστικών συστημάτων ελέγχου και αυτοματισμού για την εκδήλωση των ευπαθειών τους, αλλά γνωρίζουν επίσης και τη δυναμική του φυσικού συστήματος για να εξασφαλίσουν τον μέγιστο δυνατό αντίκτυπο.
Η αύξηση των επιθέσεων οφείλεται στην αυξημένη συνδεσιμότητα των συστημάτων ICS, (π.χ. SCADA), με το ευρύτερο δίκτυο μετάδοσης δεδομένων, επιφέροντας σημαντικές φυσικές, οικονομικές και λειτουργικές επιπτώσεις στο σύστημα ελέγχου.

3.5.1 Πρότυπα επίθεσης με βάση τη μορφή των σημάτων αλλοίωσης

Ο Αυτόματος έλεγχος παραγωγής (AGC), όπως έχει ήδη καταδειχθεί από τις προηγούμενες ενότητες, είναι μία εφαρμογή ελέγχου συχνότητας ευρείας περιοχής που λαμβάνει μετρήσεις ροής ισχύος και συχνότητας από απομακρυσμένους αισθητήρες. Ο επιτυχής έλεγχος εξασφαλίζει ότι η συχνότητα του συστήματος διανομής ισχύος διατηρείται κοντά στην ονομαστική τιμή της, και οι ανταλλαγές ισχύος μεταξύ παρακείμενων περιοχών ελέγχου περιορίζονται στις προγραμματισμένες τιμές τους. Μία σχηματική παρουσίαση του συνολικού συστήματος διαχείρισης και παραγωγής ισχύος με το σύστημα ελέγχου σε μορφή block διαγράμματος, παρουσιάζεται στο σχήμα που ακολουθεί [21]:



Σχήμα 14: Μοντέλο του δικτύου ισχύος και συστήματος ελέγχου

Στα αυτοματοποιημένα συστήματα ελέγχου, το κέντρο ελέγχου δέχεται μετρήσεις ως είσοδο και τις επεξεργάζεται για να αποκτήσει το σήμα ελέγχου εξόδου. Ένας έξυπνος επιτιθέμενος μπορεί να χειριστεί τις μετρήσεις έτσι ώστε οποιαδήποτε επιχειρησιακή απόφαση που λήφθηκε με βάση αυτές τις μετρήσεις να μπορούσε να προκαλέσει ενέργειες ελέγχου που είναι αδικαιολόγητες για την πραγματική κατάσταση του δικτύου. Αυτό θα μπορούσε με τη σειρά του να πυροδοτήσει αστάθειες στο υποκείμενο φυσικό σύστημα ή να αναγκάσει το σύστημα να λειτουργήσει σε μη οικονομικές συνθήκες λειτουργίας, λόγω μη βέλτιστων ενεργειών ελέγχου. Συνεπώς, υπάρχει ανάγκη για ανθεκτικά συστήματα ελέγχου επίθεσης, που είναι σε θέση να ανιχνεύουν την παρουσία κακόβουλων δεδομένων.

Τα Πρότυπα επίθεσης σημάτων αναφέρονται στην αλλοίωση των λαμβανόμενων μετρήσεων από τους αισθητήρες μέτρησης του δικτύου. Οι αλλοιώσεις αυτές μπορούν να λάβουν τις ακόλουθες μορφές [21]:

- **Scaling Attack:** οι πραγματικές μετρήσεις τροποποιούνται σε υψηλότερες ή χαμηλότερες τιμές, ανάλογα με την παράμετρο της επίθεσης scaling attack.
- **Ramp Attack:** οι πραγματικές μετρήσεις τροποποιούνται σταδιακά με την προσθήκη μίας συνάρτησης κλίμακας (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.

Τα πρότυπα επίθεσης στα παραγόμενα σήματα από τους αισθητήρες, αποτελούν χαμηλότερου επιπέδου επιθέσεις, οι οποίες πηγάζουν από τους αισθητήρες προς το κέντρο λήψης απόφασης. Στην περίπτωση αυτή, η λήψη των αποφάσεων από το

κέντρο ελέγχου θα βασιστεί σε λανθασμένες τιμές, και κατά συνέπεια η λήψη των αποφάσεων θα είναι εξίσου λανθασμένη. Οι επιθέσεις αυτού του επιπέδου είναι χαμηλότερης κλιμάκωσης σε σχέση με τις εξελιγμένες επιθέσεις που προσβάλλουν απευθείας τα κέντρα λήψης αποφάσεων και διαχείρισης (EMS), εντούτοις όμως μπορεί να έχουν ανάλογα καταστροφικά αποτελέσματα όπως και οι προηγούμενες. Στην περίπτωση αυτή, στόχος του συστήματος ανίχνευσης επίθεσης και προστασίας, είναι ο εντοπισμός των αισθητήρων που βρίσκονται υπό τον έλεγχο του επιτιθέμενου και ο ενδεχόμενος αποκλεισμός τους από τη λήψη αποφάσεων. Σε αυτό μπορεί να συμβάλλει και η ύπαρξη επιπρόσθετων μετρητικών διατάξεων (redundant networks), οι οποίες παράλληλα με τις εγκατεστημένες, επιτηρούν εναλλακτικά τις περιοχές ελέγχου.

3.5.2 Σφάλμα Ελέγχου Περιοχής και χρονικά όρια αντίδρασης

Για να επιτευχθεί η λειτουργία του AGC, οι αλγόριθμοι που χρησιμοποιούνται για τη λήψη αποφάσεων στη λειτουργία του δικτύου υπολογίζουν τις διορθώσεις ισχύος των γεννητριών του συστήματος με βάση τις μετρήσεις συχνότητας και των ροών ισχύος των γραμμών διασύνδεσης που λαμβάνονται από τους απομακρυσμένους αισθητήρες μέσω του ICCP (Inter-Control Communication Protocol). Αυτές οι διορθώσεις γεννήτριας βασίζονται στο **Σφάλμα Ελέγχου Περιοχής (Area Control Error)** και εκδίδονται μία φορά κάθε 5 sec (δευτερόλεπτα) με βάση τα πρότυπα ελέγχου. Τα πρότυπα επίθεσης που είδαμε προηγουμένως περιλαμβάνουν την έγχυση κατασκευασμένων μετρήσεων της ροής ισχύος των γραμμών διασύνδεσης και της συχνότητας του συστήματος με σκοπό τον λανθασμένο υπολογισμό του ACE για το δίκτυο ισχύος.

Δεδομένου ότι ο έλεγχος AGC απαιτείται να εκδίδει εντολές ελέγχου μία φορά κάθε 5 δευτερόλεπτα [21], δεν είναι σε θέση να επωφεληθεί από τις υπάρχουσες τεχνικές επαλήθευσης μετρήσεων, όπως η εκτίμηση κατάστασης, η οποία συνήθως εκτελείται μία φορά κάθε 5 min (λεπτά) [21] με βάση τα πρότυπα λειτουργίας. Το τελευταίο καθιστά τον AGC ευάλωτο σε επιθέσεις που περιλαμβάνουν αλλοιωμένες μετρήσεις. Οι τύποι των επιθέσεων και οι χρονικοί περιορισμοί για τη λήψη αποφάσεων από τα AGC συστήματα δίνουν μία άλλη χροιά στο πρόβλημα ανίχνευσης των επιθέσεων. Τα συστήματα ανίχνευσης θα πρέπει, πέραν των δυσκολιών και των προβλημάτων που αντιμετωπίζουν, να συμπεριλάβουν και τη χρονική παράμετρο για την ταχύτητα αντιδράσεώς τους. Πολλές φορές, ακόμη και όταν μία εκδήλωση επίθεσης έχει εντοπιστεί, η μη γρήγορη αντίδραση ενός συστήματος ελέγχου, μπορεί να οδηγήσει σε καταστροφικά αποτελέσματα για τη λειτουργία.

Συνοψίζοντας, λοιπόν, οι ευφυείς αλγόριθμοι για τον εντοπισμό και τη διόρθωση των επιθετικών ενεργειών θα πρέπει εκτός από την πολυπλοκότητα για το χειρισμό καταστάσεων, να παρέχουν γρήγορες χρονικές αποκρίσεις, και επομένως να υποστηρίζονται από αποδοτικά υπολογιστικά συστήματα εκτέλεσής τους.

4 Επιθέσεις AGC και Αμυντικοί Μηχανισμοί

4.1 Το Φυσικό Επίπεδο Προστασίας και τα συστήματα AGC

Στο Κεφάλαιο 3 της εργασίας παρουσιάστηκαν όλες οι μορφές επιθέσεων και των επισφαλειών που επιφέρουν στη λειτουργία ενός κατανεμημένου ή συγκεντρωμένου συστήματος AGC (μίας ή πολλών περιοχών). Στα δομικά στοιχεία του συστήματος AGC, συγκαταλέγονται οι μετρητικές διατάξεις, οι συγκεντρωτές της πληροφορίας και τα υπολογιστικά συστήματα, που επιτελούν τον έλεγχο των αισθητήρων – ενεργοποιητών και την εκτέλεση των αλγορίθμων για τη λήψη αποφάσεων (κέντρο Διαχείρισης - EMS). Κατά συνέπεια, η συνολική υποδομή ενός συστήματος AGC δε διαφέρει σημαντικά από οποιοδήποτε άλλο ηλεκτρονικό – πληροφορικό σύστημα ελέγχου που διαχειρίζεται διεργασίες (παραγωγής – ελέγχου – ασφάλειας, κλπ).
Για την προστασία ενός κατανεμημένου συστήματος AGC, που χρησιμοποιεί διατάξεις και συσκευές οι οποίες είναι γεωγραφικά αποκεντρωμένες, πρώτιστο και σημαντικότερο μέλημα για τη διασφάλιση ορθής λειτουργίας είναι ο έλεγχος φυσικής πρόσβασης σε αυτές τις συσκευές και διατάξεις.

Ορισμός: Ως **φυσική προστασία** ορίζουμε όλο το σύνολο των τεχνικών, ενεργειών και μεθόδων που αποσκοπούν στην ελεγχόμενη φυσική πρόσβαση θέσης ενός συστήματος από μη εξουσιοδοτημένα φυσικά πρόσωπα [52].

Κατά συνέπεια, η φυσική προστασία διασφαλίζει με χρήση ασφαλών χώρων, την ελεγχόμενη πρόσβαση εξουσιοδοτημένου και μόνο προσωπικού για τη λειτουργία και συντήρηση ενός συστήματος **[52**]. Η διαδικασία της φυσικής ή ακόμη και της απομακρυσμένης πρόσβασης (remote control and supervision), βασίζεται στους γενικότερους μηχανισμούς των διαδικασιών της Ταυτοποίησης (Authentication) **[22**] και του Επιπέδου Πρόσβασης (Authorization) [23].

Ορισμός: Με τον όρο **Ταυτοποίηση** (Authentication) [22] εννοούμε όλες τις διεργασίες που απορρέουν από τη χρήση υλικού (hardware), λογισμικού (software), κλειδιών ελέγχου για είσοδο/πρόσβαση στους μηχανισμούς λειτουργίας ενός συστήματος (λογαριασμοί εισόδου – accounts και χρήση passwords, μαγνητικές κάρτες, οπτικά συστήματα αναγνώρισης, ηχητικά συστήματα φωνητικής αναγνώρισης, κλπ).

Οι μηχανισμοί ταυτοποίησης κάνουν χρήση εξειδικευμένου υλικού, όπως μαγνητικές κλειδαριές και κάρτες ελέγχου πρόσβασης για τον έλεγχο προσβασιμότητας, χρήση κλειστών κυκλωμάτων κάμερας (CCTV – Analog or Digital Video) και ήχου, αισθητήρες ασφαλείας για αποφυγή παραβιάσεων χώρων (alarms), κλπ. Επιπρόσθετα, εντός των πλαισίων των προηγούμενων διεργασιών είναι και οι διαδικασίες καταγραφής των εισόδων – εξόδων του προσωπικού (καταγραφή ημερομηνίας – ώρας και φυσικού προσώπου που εισήλθε/εξήλθε από το χώρο των συστημάτων) [52]. Οι διαδικασίες ταυτοποίησης έχουν ως άμεσο στόχο την αποφυγή της προσβασιμότητας σε φυσικό επίπεδο, ατόμων – ομάδων που δεν είναι εξουσιοδοτημένοι για αυτή την πρόσβαση. Η ταυτοποίηση εξακολουθεί να

παραμένει μία σημαντική διεργασία του γενικότερου συστήματος ασφαλείας, ακόμη και όταν οι μηχανισμοί πρόσβασης είναι απομακρυσμένοι (δηλ, δίνουν τη δυνατότητα απομακρυσμένης πρόσβασης με χρήση ηλεκτρονικών υπολογιστών και δικτύων). Η σύγχρονη τεχνολογία επιτρέπει έλεγχο και πρόσβαση σε συστήματα με απομακρυσμένη διαχείριση. Στην περίπτωση αυτή, η φυσική παρουσία προσωπικού μπορεί και να μην απαιτείται για τον έλεγχο και τη λειτουργία ενός συστήματος, δεδομένης της ικανότητας λειτουργίας του συστήματος με απομακρυσμένη διαχείριση. Ακόμη, όμως, και στην περίπτωση αυτού του τύπου ελέγχου, η φυσική προστασία των συστημάτων σε συνδυασμό με τους μηχανισμούς ταυτοποίησης, οι οποίοι τώρα αναπτύσσονται και εκτελούνται σε ηλεκτρονικό επίπεδο, θα πρέπει να διασφαλίζουν την πρόσβαση μόνο σε εξουσιοδοτημένο προσωπικό.

Γενικότερα, λοιπόν, η ταυτοποίηση αποτελεί το πρώτο επίπεδο φυσικής προστασίας ενός συστήματος, είτε αυτό απαιτεί για τη λειτουργία του φυσική παρουσία είτε επιτρέπει απομακρυσμένο έλεγχο και διαχείριση.

Ορισμός: Το **επίπεδο πρόσβασης** (Authorization) [23] διασφαλίζει τη διαβάθμιση στη διαχείριση της πληροφορίας και του ελέγχου ενός συστήματος – διεργασίας , με βάση το επίπεδο ευθύνης χειρισμού στο οποίο ανήκει ο χρήστης που αιτείται την πρόσβαση στο σύστημα.

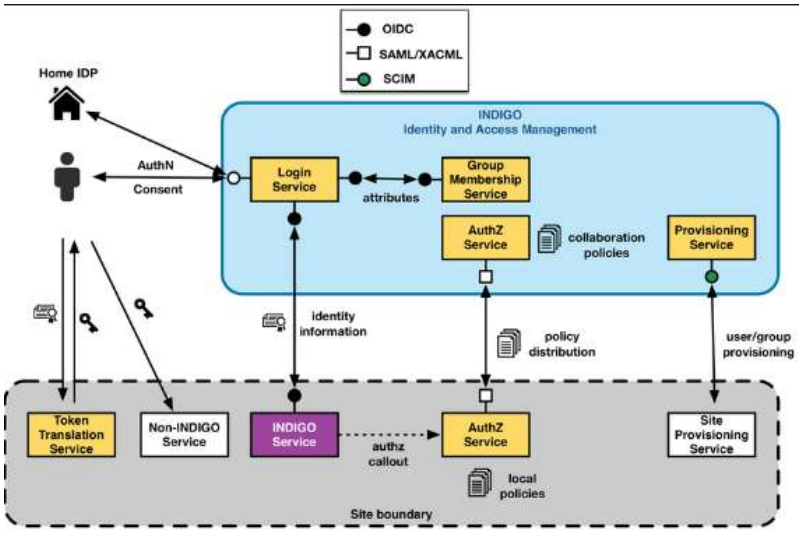
Το Επίπεδο πρόσβασης διακρίνει ιεραρχικά τρεις κατηγορίες χρηστών – χειριστών συστημάτων:

- Επίπεδο πρόσβασης χαμηλής ιεραρχίας
- Επίπεδο πρόσβασης μεσαίας ιεραρχίας
- Επίπεδο πρόσβασης υψηλής ιεραρχίας

Ανάλογα με την κλιμάκωση του επιπέδου ιεραρχίας στο οποίο συγκαταλέγεται ο χρήστης – χειριστής ενός συστήματος – διεργασίας, το σύστημα επιτρέπει κλιμακούμενο επίπεδο δράσεων – ενεργειών. Ένας χρήστης χαμηλής ιεραρχίας μπορεί να εκτελέσει – εκκινήσει μόνο περιορισμένο πλήθος ενεργειών ελέγχου – χειρισμού, ενώ καθώς το επίπεδο αυξάνεται, ο χρήστης – χειριστής του συστήματος μπορεί να εκτελέσει απόλυτες ενέργειες λειτουργίας για το σύστημα – διεργασία (π.χ. Διαχειριστής Ενέργειας – EMS ο οποίος μπορεί να θέσει εκτός λειτουργίας ολόκληρες περιοχές και φορτία ισχύος). Κατά συνέπεια, η κλιμάκωση του επιπέδου πρόσβασης αποτρέπει την εφαρμογή ανεπιθύμητων ενεργειών σε ένα σύστημα, εφόσον ο χειριστής που εκτελεί τη διαχείρισή του δεν έχει το κατάλληλο επίπεδο πρόσβασης. Οι μηχανισμοί για τη διαπίστωση του επιπέδου πρόσβασης σε ένα σύστημα, διαμορφώνονται από το υλικό – λογισμικό που διακρίνει τα επίπεδα των χρηστών κατά την εισαγωγή τους για χειρισμό σε ένα σύστημα (διαδικασίες login). Η διαμόρφωση των επιπέδων πρόσβασης ορίζεται από τον διαχειριστή απόλυτου ελέγχου του συστήματος (administrator), ο οποίος κατατάσσει σε ιεραρχικές κλάσεις τους χρήστες – χειριστές, ορίζοντας τα επίπεδα πρόσβασης και ελέγχου για το σύστημα ξεχωριστά για κάθε έναν από αυτούς.

Επιπλέον από τους μηχανισμούς που διασφαλίζουν τα επίπεδα πρόσβασης, τα συστήματα ελέγχου συμπεριλαμβάνουν εσωτερικά και μηχανισμούς καταγραφής (recording), οι οποίοι επιτρέπουν στον administrator του συστήματος, την

εξακρίβωση των χρονικών ενεργειών – εντολών που εισήχθησαν και εφαρμόστηκαν σε ένα σύστημα. Η διεργασία παρακολούθησης του συστήματος καταγράφει και εντοπίζει τις ενέργειες των χρηστών του, συσχετίζοντάς τες ως προς το χρόνο (log recording and analysis process). Με τη χρήση αυτών των μηχανισμών διασφαλίζεται τόσο η καταγραφή των χρηστών που χειρίζονται ένα σύστημα καθώς και οι επιβαλλόμενες ενέργειες που επιβλήθηκαν στο σύστημα κατά τη χρονική διάρκεια ελέγχου από τους συγκεκριμένους χειριστές. Η μέθοδος αυτή επιτρέπει την πλήρη ανασύσταση στο χρόνο των επιβαλλόμενων ενεργειών προς το σύστημα – διεργασία. Στόχος της διεργασίας παρακολούθησης είναι η εξακρίβωση δυσλειτουργιών, επιτυχών – ανεπιτυχών χειρισμών, καθώς και ο εντοπισμός και η ταυτοποίηση των χρηστών που διαχειρίστηκαν το σύστημα στο χρόνο.
Για την υλοποίηση των μηχανισμών Ταυτοποίησης και Επιπέδου Πρόσβασης, το σύστημα κάνει χρήση τόσο υλικού – λογισμικού καθώς και πρωτοκόλλων επικοινωνίας και μηχανισμών κρυπτογράφησης – αποκρυπτογράφησης των δεδομένων για τους χρήστες του, διασφαλίζοντας ότι η κρίσιμη πληροφορία των δεδομένων ιεραρχικού χρήστη δε θα περιέλθει σε άλλα μη εξουσιοδοτημένα φυσικά πρόσωπα [53], [54].
Στο σχήμα που ακολουθεί παρουσιάζονται σε αφαιρετικό επίπεδο (abstract layer) οι εσωτερικές διεργασίες ενός συστήματος Ταυτοποίησης και Επιπέδου Πρόσβασης χρηστών.



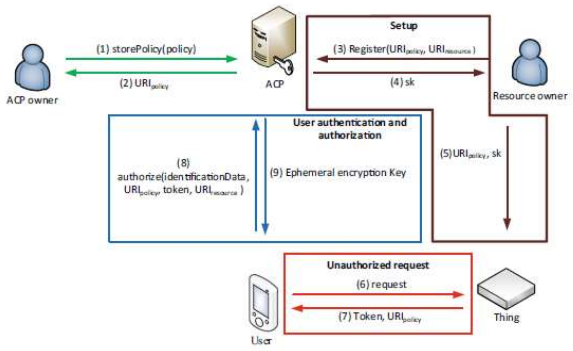
Σχήμα 15: Μοντέλο Διεργασιών Authentication - Authorization

Τα επίπεδα προστασίας, όμως, σε καμία περίπτωση δεν μπορούν να διασφαλίσουν εξ ολοκλήρου και απόλυτα την ασφαλή λειτουργία ενός συστήματος AGC, δεδομένου ότι στην προσπάθεια επιβολής κακόβουλων ενεργειών σε ένα σύστημα διαχείρισης και διανομής ισχύος υπεισέρχονται παράμετροι, όπως:

- Π1. Πρόσβαση των κακόβουλων ομάδων – ατόμων στα πληροφοριακά στοιχεία των χρηστών ενός συστήματος διαχείρισης ενέργειας
- Π2. Συμμετοχή μέρους του προσωπικού στις κακόβουλες ομάδες (πρώην δυσαρεστημένοι υπάλληλοι, ανταγωνιστές, κλπ)

- Π3. Χρήση απομακρυσμένης πρόσβασης στα δομικά υποσυστήματα του Δικτύου Διαχείρισης και Διανομής Ενέργειας
- Π4. Χρήση διαδικτυακών υπολογιστικών συστημάτων με επικοινωνία σε ευρύτερες τοπολογίες δικτύων

Η πρόσβαση των κακόβουλων ομάδων στα πληροφοριακά στοιχεία των χρηστών ενός συστήματος AGC συνεπάγεται την πρόσβασή τους σε πληροφορία πρόσβασης και λογαριασμών (Login passwords) [27].



Σχήμα 16: Παράδειγμα Τυπικής Διαδικασίας Εισόδου και Ταυτοποίησης χρήστη βάσει μηχανισμών με πρωτόκολλα επικοινωνίας

Η συμμετοχή μέρους του προσωπικού που είναι εξουσιοδοτημένο για τη λειτουργία του Διαχειριστή Ενέργειας, ως μέλη κακόβουλων ομάδων, συνιστά έναν εξαιρετικά σημαντικό κίνδυνο. Ο λόγος είναι ότι οι επιθέσεις που πρόκειται να εκδηλωθούν στο σύστημα AGC προέρχονται από το εσωτερικό των δομών ασφαλείας και κατά συνέπεια είναι υψηλού ιεραρχικού επιπέδου με σχεδόν απόλυτη πρόσβαση στο σύστημα. Κατά συνέπεια, οι κακόβουλες ομάδες μπορεί να γνωρίζουν εκ των έσω, και εφόσον έχουν την απαιτούμενη ιεραρχική πρόσβαση, να απενεργοποιούν τόσο μηχανισμούς καταγραφής ενεργειών, όσο και μηχανισμούς για την επιβολή ακραίων ενεργειών.
Η διασυνεχής παρακολούθηση των δομών του συστήματος σε συνδυασμό με την ιεραρχική πρόσβαση και τα αυτοματοποιημένα συστήματα λήψης αποφάσεων, αντιμετωπίζουν ένα σημαντικό μέρος του παραπάνω κινδύνου.
Η απομακρυσμένη πρόσβαση στα δομικά υποσυστήματα ενός δικτύου διαχείρισης και διανομής ενέργειας AGC, συνιστά ίσως τον μεγαλύτερο από τους κινδύνους για τη δημιουργία επισφαλειών λειτουργίας. Στην περίπτωση αυτή, οι κακόβουλες ομάδες φυσικών προσώπων είναι απομακρυσμένες και αποκτούν πρόσβαση στα στοιχεία και τον έλεγχο από απομακρυσμένες γεωγραφικές περιοχές σε σχέση με τη φυσική θέση του συστήματος AGC. Ο εντοπισμός τους μπορεί να είναι δύσκολος ή ακόμη και αδύνατος στην περίπτωση όπου κάνουν χρήση τεχνολογιών απομακρυσμένης πρόσβασης μέσω τοπικών και κρυπτογραφημένων VPNs [30] που συνδέονται με χρήση διανεμητών (proxies), οι οποίοι αποκρύπτουν τη διεύθυνση σύνδεσής τους (IP washers). Η πρόσβασή τους στο σύστημα δεν απαιτεί φυσική παρουσία και κατά συνέπεια μπορεί να ενταθεί σε χρονικές περιόδους όπου η διαχείριση και ο έλεγχος δεν υπόκεινται άμεσα σε έλεγχο και φυσική παρουσία του απόλυτου διαχειριστή και του προσωπικού (π.χ. νυκτερινές ώρες, αργίες, κλπ).

Ο συνδυασμός επιθέσεων με χρήση υπολογιστικών συστημάτων κάνει ακόμη πιο δυσχερή τον εντοπισμό και την ανίχνευση των κακόβουλων ομάδων, δεδομένου ότι τα υπολογιστικά συστήματα που βρίσκονται υπό τον έλεγχό τους, σε συνδυασμό με τις τεχνολογίες διαδικτύου, μπορούν να εκδηλώνουν τις επιθέσεις απομακρυσμένα, χρονικά ετεροχρονισμένα και αυτοματοποιημένα.
Κατά συνέπεια, για την αντιμετώπιση των δύο τελευταίων τύπων επίθεσης, ένας σημαντικός τρόπος άμυνας του συστήματος, είναι η χρήση εσωτερικών υπολογιστικών συστημάτων, τα οποία διασυνεχώς παρακολουθούν την εξέλιξη της λειτουργίας και την επιβολή ενεργειών επί του δικτύου ισχύος.
Οι μορφές επίθεσης που περιγράφηκαν παραπάνω αποτελούν τη βασική τεχνική εκδήλωσης κυβερνοεπιθέσεων (cyberattacks) στα συστήματα AGC. Οι τεχνολογίες που χρησιμοποιούνται για την εκδήλωση αυτών των επιθέσεων δυσχεραίνουν τον εντοπισμό και την ανάσχεση τους.
Για την προφύλαξη της ορθής λειτουργίας του AGC, απαιτείται η ανάπτυξη ειδικών αλγορίθμων, οι οποίοι εκτελούνται σε παράλληλα υπολογιστικά συστήματα. Οι αλγόριθμοι αναλύουν τα παρεχόμενα δεδομένα από τους αισθητήρες του συστήματος και ελέγχουν διαρκώς τις επιβαλλόμενες ενέργειες που το δίκτυο υφίσταται με στόχο: (i) να εντοπίσουν την κατάσταση του δικτύου AGC, (ii) να ελέγξουν τις εφαρμοζόμενες εντολές προς και από το δίκτυο, (iii) να αναλύσουν τα παρεχόμενα δεδομένα με στόχο να εντοπίσουν την έγχυση ψευδών – σκόπιμα λανθασμένων δεδομένων μετρήσεων.
Οι αλγόριθμοι αυτοί πρέπει να είναι υβριδικοί προς τη φύση τους, συνδυάζοντας μεγάλη πληθώρα τεχνολογιών και τεχνικών (αναλυτικοί, ευριστικοί, υπολογιστικοί, ασαφούς λογικής, κλπ) [2] προσπαθώντας να εξακριβώσουν την ορθότητα και το βαθμό επιμόλυνσης που τα δεδομένα των αισθητήρων ενός δικτύου AGC έχουν υποστεί. Στα πλαίσια αυτού του τύπου των κυβερνοεπιθέσεων, το σύστημα ελέγχου θα πρέπει να μπορεί να διαγνώσει τύπους επιθέσεων όπως:

- Επιθέσεις με Αλλοιωμένα σήματα αισθητήρων με βάση σήματα αλλοίωσης ειδικού ή τυχαίου τύπου
- Επιθέσεις με Έγχυση Λανθασμένων Δεδομένων (FDIA)
- Επιθέσεις με Έγχυση Χρονικά Καθυστερημένων Δεδομένων (TDA)
- Επιθέσεις με χρήση μοντέλων (Model Based Attacks – MBA)

Προφανώς με βάση την ετερογένεια των μορφών επίθεσης, είναι λογικό ότι ένα ενιαίο σύστημα αντιμετώπισης των επιθέσεων στη μορφή ενός αλγορίθμου, δεν μπορεί να ανταποκριθεί απόλυτα. Η ερευνητική βιβλιογραφία [10] – [21] στους χώρους αυτούς αφορά κυρίως στην ανάπτυξη αλγορίθμων ειδικού τύπου οι οποίοι είναι κατάλληλοι για την αντιμετώπιση αποκλειστικά και μόνο ενός είδους από τις παραπάνω επιθέσεις. Η υπάρχουσα τεχνολογία και οι ερευνητικές εργασίες δεν μπορούν να δημιουργήσουν έναν καθολικό αλγόριθμο, ικανό τόσο για τον εντοπισμό, όσο και την αντιμετώπιση των παραπάνω επιθέσεων. Κατά συνέπεια, η προτεινόμενη λύση για την αντιμετώπιση της ευρύτητας των κυβερνο-επιθέσεων βασίζεται στην παράλληλη ανάπτυξη και εκτέλεση δέσμης αλγορίθμων, στα υπολογιστικά συστήματα του κέντρου διαχείρισης και διανομής, με στόχο την ανίχνευση και τη δημιουργία σημάτων συναγερμού (alerts), που θα επικεντρωθούν στη χρονική στιγμή και τον τύπο επίθεσης.

4.2 Η έννοια της εισβολής του επιτιθέμενου στα δίκτυα AGC. Τεχνικές Ανίχνευσής της

Η ανίχνευση μίας εισβολής στο δίκτυο ελέγχου παραγωγής και διαχείρισης ισχύος, αποτελεί τη σημαντικότερη αλγοριθμική διεργασία για την προστασία μίας υποδομής ισχύος και των διασυνδεόμενων φορτίων. Επειδή το πλήθος των τύπων των επιθέσεων ποικίλει και διαφοροποιείται ανάλογα με τον επιτιθέμενο και την υποδομή ενός δικτύου, έχει αναπτυχθεί μία ομάδα αλγορίθμων, για τη διαδικασία ανίχνευσης εισβολών και επιθέσεων.

Αναλυτικότερα οι τεχνικές που χρησιμοποιούνται είναι [21]:

- **Signature-based detection:** Οι τεχνικές αυτές αναζητούν γνωστά πρότυπα κακόβουλων δραστηριοτήτων. Η βάση δεδομένων των συστημάτων IDS ενημερώνεται συνεχώς με νέες 'υπογραφές' επίθεσης (Intrusion signatures), καθώς και όποτε αυτές ανακαλύπτονται. Τα περισσότερα συστήματα IDS ανήκουν σε αυτήν την κατηγορία. Ωστόσο, μία περιορισμένη βάση δεδομένων από 'υπογραφές' επίθεσης, θα μπορούσε να καταστήσει το IDS ευάλωτο σε ορισμένες μη εντοπίσιμες επιθέσεις, καθιστώντας το σύστημα αναποτελεσματικό. Η αρχιτεκτονική λειτουργίας αυτών των συστημάτων μοιάζει σημαντικά με τις αρχιτεκτονικές που χρησιμοποιούνται στο λογισμικό (software) για την ανίχνευση κακόβουλων προγραμμάτων (ιών - viruses) σε επεξεργαστικά περιβάλλοντα ΗΥ.
- **Anomaly-based detection:** Οι τεχνικές αυτές δεν αναζητούν την αναγνώριση της πραγματικής ακολουθίας εισβολής, αλλά αναζητούν αποκλίσεις στα παρατηρούμενα δεδομένα. Αυτές οι τεχνικές συνιστούν δυναμικά συστήματα IDS τα οποία έχουν τη δυνατότητα να μαθαίνουν την κανονική συμπεριφορά του συστήματος ισχύος με βάση τα στατιστικά χαρακτηριστικά που έχουν οι μετρήσεις του. Κατά τη λειτουργία σε πραγματικό χρόνο, οι παρατηρήσεις συγκρίνονται με την κανονική συμπεριφορά του συστήματος και τα επίπεδα ζήτησης ισχύος που έχουν καταγραφεί οπότε κάθε απόκλιση χαρακτηρίζεται ως ανωμαλία. Τα συστήματα αυτά προφανώς είναι ευφυέστερα των προηγουμένων, αλλά απαιτούν αρκετή υπολογιστική ισχύ για την επίτευξη της επεξεργασίας σε πραγματικό χρόνο. Εμφανίζουν το χαρακτηριστικό της δυναμικής συμπεριφοράς, η οποία τα καθιστά άμεσα προσαρμόσιμα στις δυναμικές συνθήκες λειτουργίας του δικτύου ισχύος.

4.3 Αντιμετώπιση Επιθέσεων με Αλλοιωμένα Σήματα Αισθητήρων

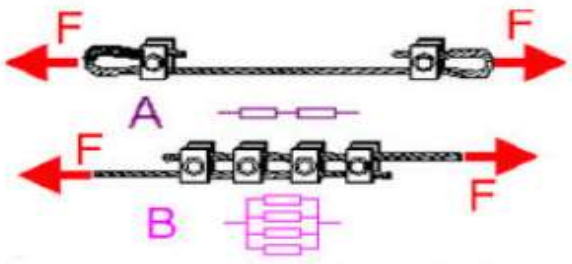
Οι επιθέσεις με αλλοιωμένα σήματα από τους αισθητήρες του συστήματος AGC, παρουσιάστηκαν στο Κεφάλαιο 3 της εργασίας. Η μορφή που έχουν τα σήματα αλλοίωσης περιγράφει και κατηγοριοποιεί και τον τύπο της αντίστοιχης επίθεσης (scaling, ramp, pulse, random attacks). Η αλλοίωση των σημάτων που προέρχονται από τους αισθητήρες ενός δικτύου AGC, συνιστά έναν τύπο επίθεσης όπου οι επιτιθέμενοι έχουν αναλάβει τον έλεγχο και τη λειτουργία μέρους από το σύνολο των αισθητήρων του δικτύου. Για την ανίχνευση και τον εντοπισμό τους, απαιτούνται ενέργειες όπως [1], [10], [21], [24]:

- Έλεγχος και ανάλυση των παραγόμενων σημάτων από τους αισθητήρες για τον εντοπισμό αλλοιώσεων που παράγονται με προκαθορισμένο πρότυπο.
- Ανάλυση των συνθηκών λειτουργίας του δικτύου και σύγκριση με τα παρεχόμενα επίπεδα σημάτων.

Οι παραπάνω ενέργειες από τους αλγορίθμους ανίχνευσης ψευδών – αλλοιωμένων σημάτων, θα δώσουν μία ένδειξη με πιθανότητα σταθμισμένου σφάλματος για τον εντοπισμό και την εκδήλωση πιθανής επίθεσης μέσω των απομακρυσμένων αισθητήρων καταγραφής της λειτουργίας του δικτύου. Στη διαδικασία ανίχνευσης και εντοπισμού αυτών των επιθέσεων βοηθά σημαντικά:

- Η ύπαρξη δευτερευόντων δικτύων αισθητήρων (redundant sensors network)
- Η άμεση προσβασιμότητα στους χώρους και τα κέντρα λειτουργίας των αισθητήρων
- Η προστασία των παραγόμενων μετρήσεων από τους αισθητήρες με χρήση κωδικοποιήσεων ή προτύπων ασφαλείας
- Η δυνατότητα μετάδοσης εντολών προς/από τους αισθητήρες

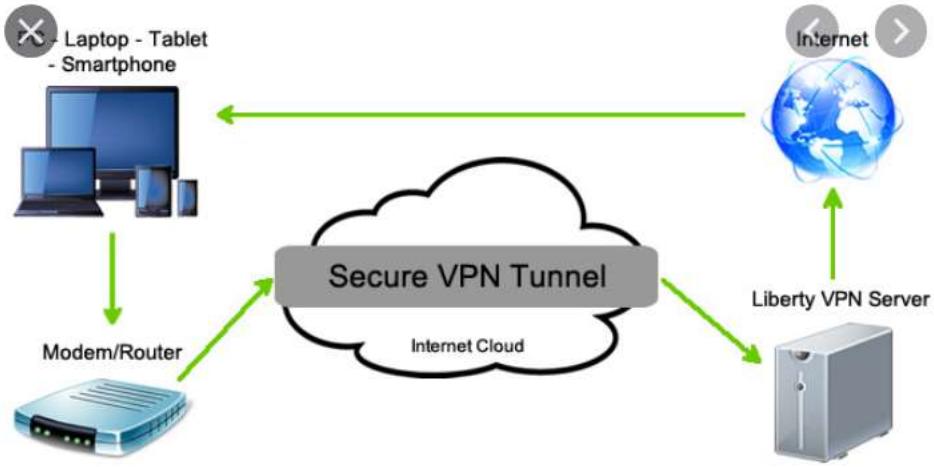
Η ύπαρξη δευτερευόντων δικτύων αισθητήρων αποτελεί ένα σημαντικό παράγοντα ασφαλείας, δεδομένου ότι η ύπαρξη του συγκεκριμένου δικτύου είναι σε γνώση ιεραρχικά διαπιστευμένου προσωπικού. Η ύπαρξη του δευτερεύοντος δικτύου επιτρέπει την παράλληλη αξιολόγηση των παρεχόμενων μετρήσεων από τα υπάρχοντα υφιστάμενα δίκτυα των αισθητήρων και μπορεί να εντοπίσει κατά πόσο τα παρεχόμενα δεδομένα από το δίκτυο έχουν αλλοιωθεί ή όχι. Το επαγόμενο κόστος από τη λειτουργία και την ύπαρξη δευτερευόντων – παράλληλων μετρητικών δικτύων αντισταθμίζεται από την αμεσότητα στον εντοπισμό και την ανίχνευση της κακόβουλης επίθεσης, δίνοντας τη δυνατότητα της ορθής λειτουργίας ακόμη και όταν το σύστημα διαχείρισης και ελέγχου είναι επιμολυσμένο από λανθασμένα δεδομένα.



Σχήμα 17: Πλεονάζον δευτερεύον κύκλωμα αισθητήρων παράλληλης λειτουργίας μετρήσεων

Η άμεση προσβασιμότητα στους χώρους εγκατάστασης και λειτουργίας των αισθητήρων από διαπιστευμένο προσωπικό (φυσική προστασία) παρέχει έναν μηχανισμό άμεσου ελέγχου για το δίκτυο αισθητήρων στην περίπτωση όπου διαπιστωθεί αλλοίωση των παραγόμενων δεδομένων. Οι διαδικασίες αλλοίωσης των δεδομένων όταν δεν προέρχονται από τη χρήση υπολογιστικών συστημάτων (ψηφιακά δεδομένα), συνήθως συντελείται με τη διασύνδεση ειδικού εξοπλισμού επί

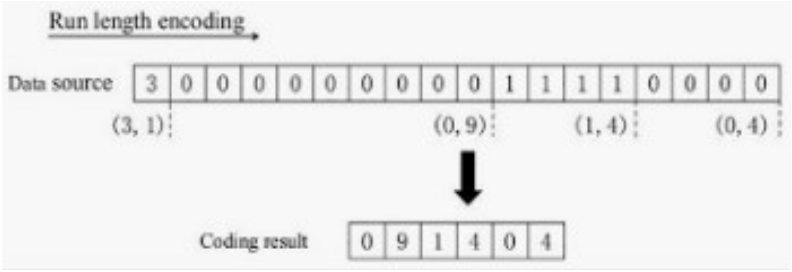
των κυκλωμάτων των αισθητήρων. Κατά την άμεση πρόσβαση στους χώρους λειτουργίας των αισθητήρων, η εποπτεία και ο έλεγχος του υλικού μπορεί να ανιχνεύσει την παρουσία και την επίδραση εξωτερικών κυκλωμάτων ελέγχου. Όταν η επιμόλυνση των δεδομένων προέρχεται από τη χρήση υπολογιστικών συστημάτων, αυτό συνεπάγεται ότι ενδεχόμενα οι αισθητήρες του δικτύου μπορεί να μετρούν με ορθό τρόπο τις συνθήκες λειτουργίας του δικτύου, ενώ η αλλοίωση συντελείται από λογισμικό που εκτελείται στο κακόβουλο υπολογιστικό κέντρο. Η αποστολή των πακέτων δεδομένων προς τον Διαχειριστή Ενέργειας συντελείται συνήθως με τους μηχανισμούς μετάδοσης των τεχνολογιών κορμού, όπως αναφέρθηκε και προηγουμένως (VLANs, Proxies, IP washers, κλπ) [30].



Σχήμα 18: Χρήση VPNs για την απόκρυψη IP συνδεόμενου χρήστη

Η χρήση κωδικοποιήσεων και κρυπτογραφίας κατά τη δημιουργία και μετάδοση των πακέτων δεδομένων από τους αισθητήρες, προστατεύει σε σημαντικό βαθμό την μεταδιδόμενη πληροφορία. Τα παρεχόμενα κλειδιά για την κωδικοποίηση και αποκωδικοποίηση πρέπει να είναι ισχυρά, έτσι ώστε να ελαχιστοποιούν την εφαρμογή μεθόδων άμεσου hacking – cracking [27]. Ένα εγγενές μειονέκτημα σε αυτή τη βάση προστασίας προκύπτει από την εσωτερική λειτουργία του ίδιου του αισθητήρα, ο οποίος κωδικοποιεί και μπορεί να προστατεύει τα αλλοιωμένα δεδομένα που ο ίδιος παράγει. Επιπρόσθετα, η χρήση προτύπων – υπογραφών (signature patterns) εντός των ψηφιακών πεδίων που παράγονται με καθορισμένο τρόπο από τη συνεργασία υλικού – λογισμικού του αισθητήρα, συντελεί επιπλέον στην προστασία των αποστελλόμενων δεδομένων.
Βοηθητικά στην αντιμετώπιση των επιθέσεων με αλλοιωμένα σήματα από τους αισθητήρες μπορεί να λειτουργήσει και η συνολική ανάλυση από το Διαχειριστή Ενέργειας του δικτύου AGC. Τα απαιτούμενα επίπεδα ισχύος και οι ανάγκες διανομής για τη δεδομένη χρονική στιγμή από και προς το σύστημα, εφόσον διατίθενται ισχυρά υπολογιστικά συστήματα, μπορούν να αναλύονται. Τα παρεχόμενα δεδομένα από τους αισθητήρες αποτελούν αντικείμενο σύγκρισης με ανάλογες καταστάσεις στο δίκτυο από παρελθοντικές χρονικές περιόδους. Η λειτουργία και οι αντιδράσεις των αισθητήρων στην περίπτωση αυτή μπορεί να αναλυθεί και να συγκριθεί με τις μετρήσεις και τις αντιδράσεις σε ανάλογες συνθήκες κατά το παρελθόν. Με τον τρόπο αυτό μπορούν να εντοπισθούν με κάποια

πιθανότητα σφάλματος, τυχόν αλλοιώσεις στα σήματα που προορίζονται προς το κέντρο διαχείρισης [1].



Σχήμα 19: Παράδειγμα Προσθήκης επιπλέον πεδίων κωδικοποίησης σε ένα πακέτο δεδομένων

4.4 Αντιμετώπιση Επιθέσεων Με Έγχυση Λανθασμένων Δεδομένων (False Data Injection Attacks)

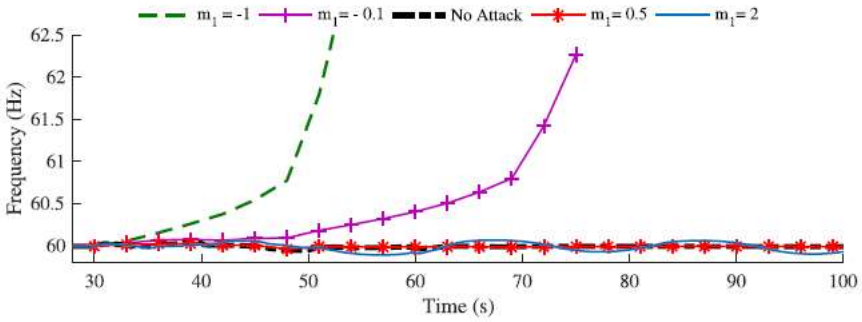
Στις επιθέσεις Έγχυσης Λανθασμένων Δεδομένων (False Data Injection Attacks – FDIA), ο επιτιθέμενος αποστέλλει λανθασμένα δεδομένα προς τα κέντρα διαχείρισης και λήψης αποφάσεων του συστήματος AGC. Στις επιθέσεις αυτού του τύπου δεν είναι απαραίτητο ότι η έγχυση των ψευδών δεδομένων προέρχεται από τα μετρητικά συστήματα (αισθητήρες), καθώς ο επιτιθέμενος έχει πρόσβαση στη δομή της πληροφορίας των ψηφιακών δεδομένων (πακέτων) που αποστέλλονται από/προς το δίκτυο Διαχείρισης και Λήψης Αποφάσεων (EMS**) [19].** Συνήθως αυτού του τύπου οι επιθέσεις είναι πιο δύσκολο να εντοπιστούν, να αντιμετωπιστούν και κατά συνέπεια είναι πιο καταστροφικές από άλλου τύπου επιθέσεις για τη λειτουργία του δικτύου AGC.

Η εξάρτηση του AGC συστήματος από την ανταλλαγή δεδομένων και την επικοινωνία με τους αισθητήρες, καθιστά το υποσύστημα ελέγχου συχνότητας LFC περισσότερο εκτεθειμένο στις κυβερνο-επιθέσεις. Ειδικότερα οι δικτυακές δομές ηλεκτρονικών υπολογιστών οι οποίες χρησιμοποιούνται για τη συλλογή, προώθηση και επεξεργασία των δειγμάτων, επιφέρουν όλα τα χαρακτηριστικά των διαδικτυακών επιθέσεων στα συστήματα AGC. Αρκετές τεχνικές από την ερευνητική βιβλιογραφία έχουν προταθεί για την αντιμετώπιση των επιθέσεων FDIAs:

- Χρήση συναρτήσεων δυναμικού για την περιγραφή του AGC καθώς και ανάλυση ευαισθησιών των παραμέτρων του δικτύου για τη στάθμιση των αποτελεσμάτων των επιθέσεων [31], [32].
- Ανάλυση των επιθέσεων FDIAs για την αναζήτηση της βέλτιστης πολιτικής του επιτιθέμενου [33].
- Μελέτη της επίδρασης των FDIAs με ανάλυση του δικτύου AGC για την αναζήτηση των επιδράσεων [34].
- Πειραματικές μέθοδοι για την αναζήτηση των επιδράσεων των FDIAs σε πραγματικά συστήματα AGC [35], [24].
- Αντιμετώπιση των FDIAs με χρήση προβλέψεων για τα απαιτούμενα επίπεδα ισχύος κατά τη λειτουργία του δικτύου [25].

- Χρήση παρατηρητών κατάστασης με άγνωστες τις εισόδους του συστήματος (Unknown Input Observers – UIOs), για την ανίχνευση των επιθέσεων στο AGC σύστημα, χωρίς να απαιτείται γνώση για τα επίπεδα ισχύος στα τροφοδοτούμενα δίκτυα (είσοδοι μοντέλου καταστάσεων) [19].
- Χρήση παρατηρητών κατάστασης κυλιόμενου παραθύρου (Sliding Mode Observers – SMOs) για τη δυναμική εκτίμηση των καταστάσεων ενός γραμμικοποιημένου συστήματος περιγραφής χωρίς γνώση των εισόδων του συστήματος [29].

Για την αντιμετώπιση αυτών των κυβερνο-επιθέσεων είναι υποχρεωτική η δημιουργία αλγορίθμων, οι οποίοι ανιχνεύουν την κατάσταση στην οποία βρίσκεται το σύστημα LFC (υποσύστημα το οποίο είναι υπεύθυνο για τη μέτρηση της τρέχουσας συχνότητας λειτουργίας του δικτύου και την παραγωγή των σημάτων ελέγχου για τη μεταβολή της ισχύος). Αυτό βασίζεται στη σύγκριση του επιπέδου κατάστασης της συχνότητας από τη διαδικασία εκτίμησης, με μία υπολειπόμενη συνάρτηση (residual function). Η υπολειπόμενη συνάρτηση κάνει χρήση ενός καθορισμένου κατωφλίου εκτίμησης (threshold) εξετάζοντας κατά πόσον η μέτρηση είναι εντός των αποδεκτών ορίων λειτουργίας.
Για την εκτίμηση των καταστάσεων του συστήματος ελέγχου LFC, προτείνεται η χρήση των μεθόδων SMO/UIO, οι οποίες εμφανίζουν το πλεονέκτημα ότι δεν χρειάζονται γνώση όλων των εισόδων του συστήματος (προσφερόμενη ισχύς από τους κόμβους παραγωγής του συστήματος). Αυτή η τεχνική της ανεξαρτησίας της μεθόδου από τις εισόδους, χρησιμοποιείται για την ανίχνευση των FDIAs.



Σχήμα 20: Μεταβολή της συχνότητας λειτουργίας του AGC κατά την επιβολή επιθέσεων over/under/negative τύπων

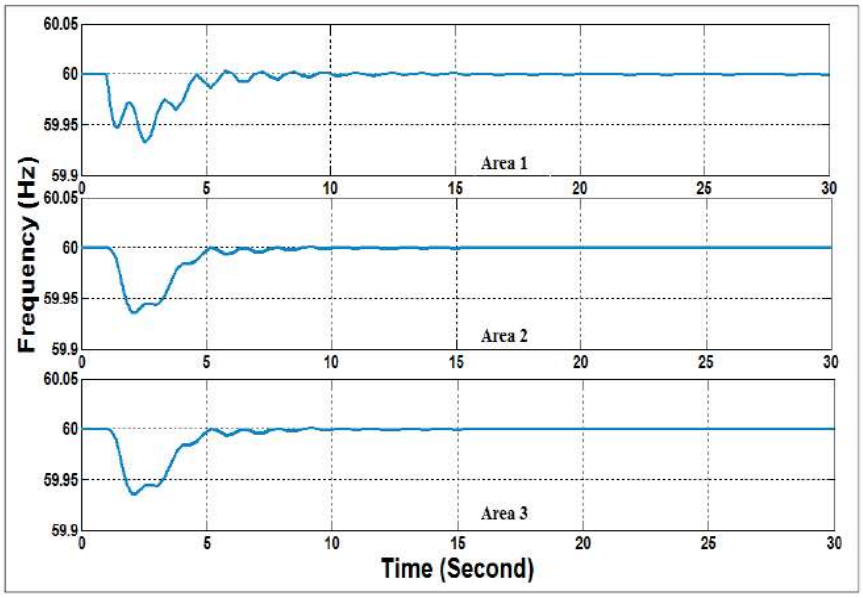
Στο παραπάνω σχήμα παρουσιάζονται διακυμάνσεις της συχνότητας από το σύστημα LFC, οι οποίες θα πρέπει να συσχετισθούν με τις μεταβολές εκτίμησης κατάστασης από τους αλγορίθμους που υλοποιούν τις μεθόδους των παρατηρητών. Για το σχεδιασμό των παρατηρητών UIOs πρώτα καθορίζονται τα επίπεδα δυναμικού των επιθέσεων. Στη συνέχεια κάθε UIO σχετιζόμενος με την επίθεση σχεδιάζεται βασιζόμενος στο επίπεδο των καταστάσεων του LFC, χρησιμοποιώντας όλα τα επίπεδα δυναμικών επίθεσης στις εισόδους, εκτός από μία είσοδο που θεωρεί άγνωστη προς το επίπεδο επίθεσης. Κατά συνέπεια, το υπόλοιπο της UIO συνάρτησης αυξάνει καθώς εκδηλώνεται επίθεση από τις εισόδους που δεν γνωρίζει. Μία διαφορά μεταξύ των εκτιμήσεων των UIOs και της κατάστασης του LFC

σηματοδοτεί μία επίθεση. Από τις διαφορετικές εκτιμήσεις των UIOs μπορεί να εκτιμηθεί ο τύπος της επίθεσης, δηλ. ποια παράμετρος λειτουργίας του δικτύου ισχύος βρίσκεται υπό την εξέλιξη επίθεσης [19].
Τα αποτελέσματα από την προσομοίωση των αλγορίθμων δείχνουν ότι κάθε μέθοδος είναι ικανή να ανιχνεύσει τις επιθέσεις στο AGC σύστημα, τους τύπους των επιθέσεων καθώς ενδεχόμενα και τις χρονικές στιγμές έναρξης και λήξης αυτών (χρονική διάρκεια επίθεσης).
Είναι σημαντικό οι προτεινόμενες μέθοδοι να μπορούν να εφαρμοστούν και να εκτελεστούν στο κέντρο διαχείρισης και λήψης αποφάσεων του συστήματος - EMS, για να μπορούν να ελεγχθούν άμεσα τα αποτελέσματα από την εφαρμογή τους. Επίσης είναι εξίσου σημαντικό, οι μέθοδοι για την αντιμετώπιση των FDIAs επιθέσεων να μπορούν να κάνουν χρήση, παράλληλα με το υφιστάμενο σύστημα κρυπτογραφίας που χρησιμοποιεί κάθε κέντρο διαχείρισης. Δυστυχώς, όμως, οι αναφερόμενες μέθοδοι όπως έχει αποδειχθεί από τη σχετιζόμενη έρευνα και βιβλιογραφία, δεν είναι ικανές να ταυτοποιήσουν κάθε τύπο FDIAs ενώ έχουν καταδείξει αδυναμίες στην εφαρμογή τους [26], [36], [37]. Ειδικότερα στην περίπτωση που οι επιτιθέμενοι έχουν παραβιάσει το επίπεδο κρυπτογραφίας του συστήματος, τότε είναι ακόμη πιο δύσκολο για τους αλγορίθμους να εντοπίσουν τις καταστάσεις επίθεσης και τις εκπορευόμενες ενέργειες.
Είναι, τέλος, σημαντικό μία μέθοδος να μπορεί να κάνει χρήση του υπάρχοντος υλικού χωρίς να απαιτεί την προσθήκη εξειδικευμένων υποσυστημάτων.

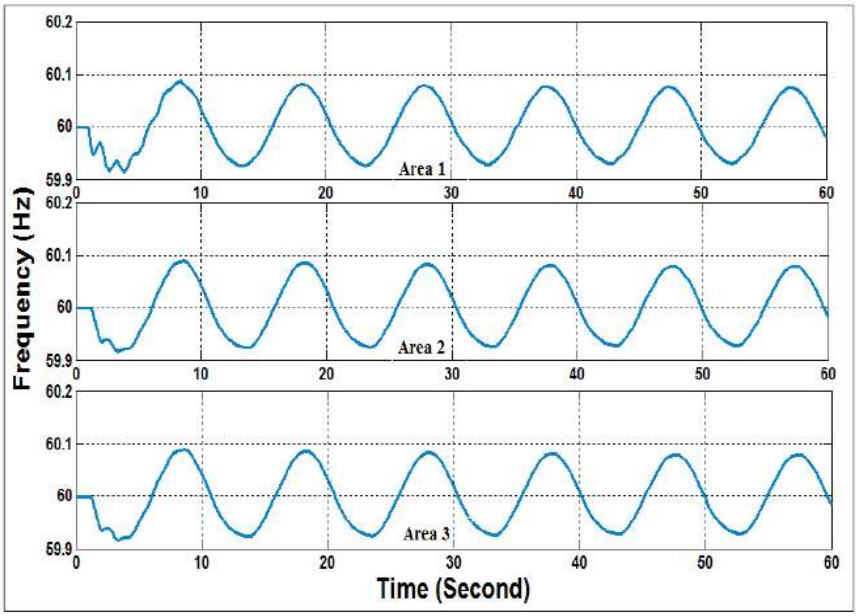
4.5 Αντιμετώπιση Επιθέσεων Με Έγχυση Χρονικά Καθυστερημένων Δεδομένων (Time Delay Attacks)

Όπως παρουσιάστηκε και στην αντίστοιχη ενότητα του Κεφαλαίου 3, οι κυβερνο-επιθέσεις τύπου Χρονικής Καθυστέρησης (Time Delay – TD Attacks), βασίζονται στην εισαγωγή μετρητικών δεδομένων στο AGC δίκτυο, με σκόπιμη χρονική καθυστέρηση, η οποία οδηγεί τον Διαχειριστή Ενέργειας – EMS, σε λανθασμένη (ετεροχρονισμένη) λήψη αποφάσεων [20]. Οι ετεροχρονισμένες αυτές αποκρίσεις οδηγούν επίσης σε καταστροφικά αποτελέσματα ως προς την ευσταθή λειτουργία του δικτύου παροχής ισχύος. Η εισαγωγή καθυστέρησης και οι παράγοντες που επιδρούν σε αυτήν, αναλύθηκαν διεξοδικά στην αντίστοιχη ενότητα.
Οι επιθέσεις χρονικής καθυστέρησης μπορούν να επιτευχθούν είτε από την σκόπιμη καθυστέρηση στη μετάδοση των δεδομένων μετρήσεων από τους αισθητήρες προς το Διαχειριστή, είτε εναλλακτικά προκαλώντας υπερφόρτωση των γραμμών μετάδοσης (jamming). Η υπερφόρτωση των τηλεπικοινωνιακών διαύλων μετάδοσης οδηγεί σε απώλεια δεδομένων, η οποία με τη σειρά της προκαλεί επαναπροώθηση των χαμένων δεδομένων, τα οποία θα περιέλθουν στον Διαχειριστή Ενέργειας με σημαντική καθυστέρηση. Κατά συνέπεια, η χρονική αυτή καθυστέρηση καθιστά πλέον άχρηστα τα παραπάνω δεδομένα, εφόσον αυτά δεν ανταποκρίνονται στην παρούσα χρονική κατάσταση λειτουργίας του δικτύου ισχύος.
Τα μοντέλα προσομοίωσης για τον χειρισμό κυβερνο-επιθέσεων τύπου χρονικής καθυστέρησης, προκαλούν σκόπιμες και ελεγχόμενες καθυστερήσεις στη μετάδοση των δεδομένων μετρήσεων και αξιολογούν με τον τρόπο αυτό την ικανότητα λήψης αποφάσεων από το κέντρο διαχείρισης. Για την εφαρμογή των διαδικασιών

προσομοιώσεων και εκτίμησης, συνήθως το δίκτυο παροχής ισχύος μοντελοποιείται με χρήση μαθηματικών μοντέλων προσομοίωσης. Στη συνέχεια επιβάλλονται διαταραχές στην καθυστέρηση επικοινωνίας των κόμβων μετρήσεων και εκτιμώνται τα σφάλματα ελέγχου συχνότητας στις περιοχές ενός δικτύου.
Στη συνέχεια παρουσιάζονται ενδεικτικά διαγράμματα που δείχνουν τις μεταβολές συχνότητας λειτουργίας σε ένα δίκτυο ισχύος, το οποίο αποτελείται από τρεις περιοχές, για διαφορετικές μεταβολές της χρονικής καθυστέρησης για τα σήματα μετρήσεων.



Σχήμα 21: Επίπεδο συχνότητας για τρεις περιοχές λειτουργίας που ελέγχονται από κοινό AGC χωρίς την επιβολή TD επίθεσης



Σχήμα 22: Επίπεδο συχνότητας για τρεις περιοχές λειτουργίας που ελέγχονται από κοινό AGC με επιβολή TD επίθεσης 2 sec καθυστέρησης για τα σήματα από την Περιοχή 1

Από τα διαγράμματα είναι εμφανές ότι η επιβολή καθυστερήσεων στη μετάδοση των μετρήσεων ακόμη και σε μία από τις περιοχές ελέγχου, προκαλεί άμεσες μεταβολές στη λειτουργία της συχνότητας για ολόκληρη την περιοχή ελέγχου από το κοινό AGC.
Οι μέθοδοι για την αντιστάθμιση των δυσμενών αποτελεσμάτων από την επίδραση των TD κυβερνο-επιθέσεων, βασίζονται στις ακόλουθες τεχνικές:

- Χρήση παραγόντων απόσβεσης φορτίου (load damping) για τον μετριασμό των αποτελεσμάτων επίδρασης. Μεγάλη ικανότητα απόσβεσης συνεπάγεται αδράνεια του δικτύου ισχύος η οποία θα αντιμετωπίσει επαρκώς γρήγορες και μικρές μεταβολές ισχύος κατά την εκδήλωση μίας επίθεσης.
- Χρήση αποκλειστικών και απομονωμένων δικτύων μετάδοσης (leased lines) για την ελαχιστοποίηση επιδράσεων καθυστέρησης.
- Κρυπτογράφηση των πακέτων μετρήσεων για την αποφυγή επίδρασης επί των δεδομένων τους.
- Βελτιστοποιημένα σχήματα δρομολόγησης της μετάδοσης δεδομένων για την όσο το δυνατόν σταθερότερη καθυστέρηση μετάδοσης (εξασφάλιση Quality of Service - QoS για την υπηρεσία) [38]. Οι παράμετροι που αφορούν τη διασφάλιση μίας σταθερής επικοινωνίας στο χρόνο αποτελούν μηχανισμούς οι οποίοι έχουν επιβληθεί στα δίκτυα μετάδοσης πακέτων για να μπορούν να φιλοξενήσουν υπηρεσίες που απαιτούν σταθερή ροή δεδομένων στο χρόνο.
- Περιοδικότητα στην επικοινωνία μεταξύ αισθητήρων και Κέντρου Διαχείρισης. Εφαρμογή τυπικών μετρήσεων (ping) για τον έλεγχο της χρονικής καθυστέρησης και μέτρηση της χρονικής λήψης των πακέτων για την εξαγωγή των μεταβολών της χρονικής διανομής (παράμετρος jitter) [39].
- Χρονικά πλαίσια αναφοράς μετάδοσης πακέτου (time stamps), για την ανίχνευση μεταβολής καθυστερήσεων μετάδοσης/λήψης.
- Λήψη Αποφάσεων βασισμένη σε μοντέλα πρόβλεψης – εκτίμησης τρέχουσας ζήτησης ισχύος από τον Διαχειριστή Ενέργειας, όταν υπάρχει απώλεια επικοινωνίας και λήψης μετρήσεων πραγματικού χρόνου από τους αισθητήρες προς το κέντρο Διαχείρισης.

Οι αναλύσεις των επιθέσεων τύπου χρονικής καθυστέρησης έχουν αποδείξει, ότι τα περισσότερο ευπαθή τμήματα μίας πολλαπλής περιοχής ελέγχου (multi-area), αφορούν κυρίως τα τμήματα που σχετίζονται με μικρές τιμές απόσβεσης φορτίου (load damping). Τα τμήματα αυτά του δικτύου ισχύος είναι περισσότερο ευπαθή, δεδομένου ότι κρίσιμες μεταβολές των επιπέδων παρεχόμενης ισχύος συνιστούν μεγάλες μεταβολές για τη συχνότητα λειτουργίας τους.
Η χρήση απομονωμένων διαδικτυακών υποδομών που δεν έρχονται σε άμεση επαφή με τις παγκόσμιες διαδικτυακές υποδομές (internet), ελαχιστοποιούν την επίδραση των χρονικών καθυστερήσεων από τις συνθήκες φορτίου λειτουργίας των δικτυακών παρόχων (congestion). Η εγγύηση επιπέδων ποιότητας για τους διαφορετικούς τύπους υπηρεσιών (παράμετρος Quality of Service των δικτύων), διασφαλίζει σε μέγιστο βαθμό την απρόσκοπτη ροή δεδομένων από/προς τους σχετιζόμενους

κόμβους επικοινωνίας στους οποίους αντιστοιχεί η δεδομένη μετρική ποιότητας. Επομένως, σταθερά επίπεδα ανταλλαγής δεδομένων στο χρόνο (Constant Bit Rate – CBR communication profiles), μπορούν να επιτευχθούν διασφαλίζοντας την όσο το δυνατόν χρονικά σταθερότερη διανομή των πακέτων μετρήσεων προς το Κέντρο Λήψης Απόφασης.
Η παράμετρος χρονικής μεταβολής της μεταδιδόμενης πληροφορίας (jitter) επίσης συνιστά έναν παράγοντα επικοινωνίας ο οποίος θα πρέπει να παραμένει σε καθορισμένα χρονικά πλαίσια. Η διασφάλιση της ποιότητας επικοινωνίας (QoS) επίσης μπορεί διασυνεχώς να μετρηθεί στο υφιστάμενο δίκτυο χωρίς να φορτώσει με επιπλέον δεδομένα τη μετάδοση, με την αποστολή σύντομων πακέτων που ελέγχουν το συνολικό χρόνο αποστολής και λήψης (πακέτα ping). Οι μετρήσεις διακύμανσης (jitter) για τη χρονική καθυστέρηση των πακέτων μπορούν να γίνουν χωρίς επιβάρυνση των δομών του δικτύου διασύνδεσης με χρήση ενσωματωμένων πεδίων πραγματικού χρόνου στα αποστελλόμενα πακέτα μετρήσεων (real time stamps).
Μία ανάλογης φύσης τεχνική που κάνει χρήση σκόπιμων προτύπων (patterns) για την ανίχνευση αλλοιωμένων δεδομένων κατά τη φάση επιθέσεων είναι και η τεχνική υδατογράφησης. Η τεχνική **δυναμικής υδατογράφησης** (**Dynamic Watermarking-based Defence**) χρησιμοποιείται ως ο βασικός αλγόριθμος για την ανίχνευση τυχόν παραβιαζόμενων μετρήσεων που τροφοδοτούν το σύστημα AGC. Μέσω της σκόπιμης επικάλυψης ενός ιδιωτικού σήματος μικρού μεγέθους στις εντολές ελέγχου που αποστέλλονται από τον AGC, "υδατογραφούνται" έτσι οι μετρήσεις που τροφοδοτούν τον AGC με ορισμένα ανεξίτηλα χαρακτηριστικά (patterns), με τα οποία μπορούν να εντοπιστούν κυβερνο-επιθέσεις στον AGC. Η τεχνική της Δυναμικής Υδατογράφησης παρουσιάζει σημαντικά πλεονεκτήματα, όπως:

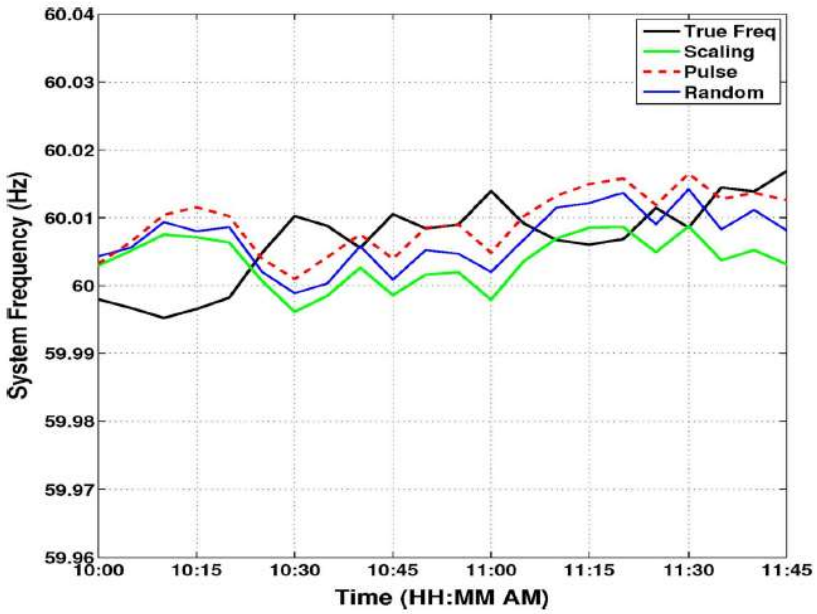
- Οποιοσδήποτε χειρισμός των μετρήσεων που τροφοδοτούν το AGC μπορεί να ανιχνευθεί ανεξάρτητα από τη στρατηγική επίθεσης που ακολουθούν οι επιτιθέμενοι.
- Ο αλγόριθμος μπορεί να χρησιμοποιηθεί όταν οι επιτιθέμενοι έχουν λεπτομερείς πληροφορίες σχετικά με τα φυσικά/στατιστικά μοντέλα του συστήματος ισχύος.
- Η μέθοδος είναι πρακτικά εφαρμόσιμη, καθώς δε χρειάζεται ενημέρωση υλικού (hardware) στις μονάδες παραγωγής.

Η χρήση κλειδιών κρυπτογράφησης της ανταλλασσόμενης στο δίκτυο πληροφορίας μπορεί να δράσει ενισχυτικά στο παραπάνω πρότυπο, δυσχεραίνοντας τη διαδικασία αποκωδικοποίησης και εξαγωγής του προτύπου προστασίας από έναν επιτιθέμενο. Οι σύγχρονοι αλγόριθμοι κρυπτογραφίας με χρήση μεγάλου μήκους κλειδιών απαιτούν σημαντική υπολογιστική ισχύ για την αποκωδικοποίησή τους. Κατά συνέπεια, η χρήση δυναμικών κλειδιών τα οποία μεταβάλλονται και ανταλλάσσονται στο χρόνο, καθιστούν δυσχερή τη διαδικασία αποκωδικοποίησης για έναν επιτιθέμενο.
Τέλος, η λήψη αποφάσεων από τον Κεντρικό Διαχειριστή Ενέργειας, η οποία βασίζεται σε μοντέλα πρόβλεψης ισχύος, ειδικά σε επιθέσεις χρονοκαθυστέρησης, μπορεί να υποκατασταθεί για μικρό χρονικό διάστημα. Το Κέντρο Λήψης Απόφασης βασίζει τις επιλογές του όχι στις λαμβανόμενες αλλοιωμένες μετρήσεις, αλλά σε προηγούμενες, οι οποίες ήταν μη αλλοιωμένες, αποτρέποντας ενέργειες για σημαντικές μεταβολές φορτίου.

4.6 Αντιμετώπιση Επιθέσεων Με Χρήση Μοντέλων (Model based Attacks)

Τα μοντέλα κυβερνο-επιθέσεων στα συστήματα AGC, παρουσιάστηκαν στην αντίστοιχη ενότητα του Κεφαλαίου 3 και σχετίζονται με τον τύπο και τη μορφή των σημάτων αλλοίωσης, που επιφέρουν στα πραγματικά δεδομένα των αισθητήρων. Οι αλλοιώσεις μπορούν να θεωρηθούν είτε ότι υποκαθιστούν τα πραγματικά δεδομένα μετρήσεων από τους αισθητήρες, είτε ότι προσβάλλουν τα πραγματικά δεδομένα σε μορφή θορύβου [21]. Οι μορφές αυτών των επιθέσεων (scaling, ramp, pulse, random attacks) αλλοιώνουν τα επίπεδα μετρήσεων συχνότητας, δίνοντας την αίσθηση στον Κεντρικό Διαχειριστή, για μη πραγματικές αλλαγές φορτίου, τις οποίες καλείται λανθασμένα να αντισταθμίσει με ενδεχόμενη μεταβολή της παρεχόμενης ισχύος προς τα υποδίκτυα. Η επίδραση των κυβερνο-επιθέσεων αυτού του τύπου έχουν μεταβλητά αποτελέσματα εξαρτώμενα από τον τύπο του δικτύου ελέγχου (μίας – πολλαπλών περιοχών), τη μεταβολή των φορτίων ανά περιοχή, και τις εμφανιζόμενες μεταβολές συχνότητας που επιφέρουν οι επιθέσεις.

Για την επιβολή προσομοιώσεων λειτουργίας, είναι σημαντική η ανάπτυξη μαθηματικών μοντέλων περιγραφής της τοπολογίας του δικτύου υπό τον AGC έλεγχο. Ένα ενδεικτικό διάγραμμα από διαδικασίες προσομοίωσης στην αναφορά [21] για αυτούς τους τύπους κυβερνο-επιθέσεων, παρουσιάζεται στο σχήμα που ακολουθεί:



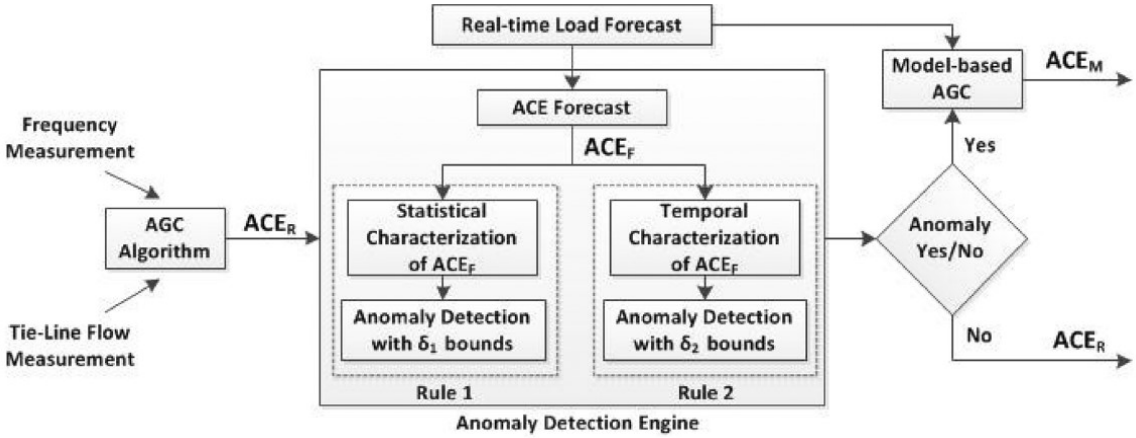
Σχήμα 23: Μεταβολές των επιπέδων συχνότητας λειτουργίας για διαφορετικούς τύπους επίθεσης

Από το παραπάνω σχήμα γίνεται φανερό ότι ανάλογα με τον τύπο της επίθεσης (scaling, pulse, random) το AGC αναγκάζεται σε μεταβολές που επιδρούν στην πραγματική συχνότητα λειτουργίας του δικτύου ισχύος.

Στόχος των αναπτυσσόμενων αλγορίθμων για την αποφυγή αυτών των επιθέσεων είναι η διαμόρφωση ενός ανεκτικού δικτύου (attack resilient network).

Ορισμός: Ως **Ανεκτικό Δίκτυο**, ορίζεται το δίκτυο, που υπό το καθεστώς των κυβερνο-επιθέσεων μπορεί να ανιχνεύσει τις επιθέσεις και να μετριάσει την επίδραση των αποτελεσμάτων τους (smart attack detection and mitigation) [21].

Η πραγμάτωση ενός ανεκτικού δικτύου απαιτεί την ανάπτυξη αλγορίθμων, που επαληθεύουν την ακεραιότητα (integrity) των λαμβανόμενων σημάτων από τους αισθητήρες, με προσομοίωση και παραγωγή ανάλογων σημάτων από εξισώσεις που περιγράφουν τα ανάλογα σήματα, με βάση την κατάσταση του δικτύου. Η διαδικασία αυτή καλείται **ανίχνευση ανωμαλιών** (anomaly detection). Ένα διάγραμμα ελέγχου που βασίζεται στη διαδικασία της ανίχνευσης ανωμαλιών παρουσιάζεται στο σχήμα που ακολουθεί:



Σχήμα 24: Διάγραμμα ροής για την ανίχνευση και το χειρισμό των ανωμαλιών [21]

Οι τεχνικές μετρίασης των αποτελεσμάτων της επίθεσης (smart mitigation), αφορούν στην ανάπτυξη τεχνικών λειτουργίας με πρόβλεψη, όταν οι παρεχόμενες μετρήσεις από τους αισθητήρες έχουν χαθεί ή είναι αναξιόπιστες λόγω της επίθεσης.
Κάθε υποσύστημα το οποίο συνιστά το AGC, έχει τις ιδιαιτερότητες καθώς και τα ευαίσθητα σημεία του, ανάλογα με τον τύπο της επίθεσης που δέχεται συνολικά το σύστημα ελέγχου. Επομένως, ένα σύστημα για την αντιμετώπιση κυβερνο-επιθέσεων βασισμένες σε μοντέλα σημάτων θα πρέπει να διαθέτει ταξινόμηση της πληροφορίας στις ακόλουθες κλάσεις, με στόχο τη δημιουργία ενός ανεκτικού δικτύου [21]:

- Πρόβλεψη (Forecasts)
- Ευαισθησία ανά Κατάσταση (Situational Awareness)
- Γνώση των υποδομών του (system resources)
- Καταχώρηση των προτύπων των επιθέσεων (Attack Templates)
- Παράμετροι Λειτουργίας του Δικτύου (System Data)

Οι προβλέψεις αναφέρονται στην ικανότητα των αλγορίθμων να εντοπίσουν συνθήκες οι οποίες είναι ευεπίφορες για την εφαρμογή επιθέσεων (π.χ. μεταβολές ισχύος στο σύστημα παραγωγής εξαιτίας καιρικών συνθηκών οι οποίες θα μεταβάλλουν τα μετεωρολογικά δεδομένα λειτουργίας ανεμογεννητριών).
Η ευαισθησία ανάλογα με την κατάσταση λειτουργίας ενός δικτύου αφορά στη γνώση των συνθηκών ευσταθούς λειτουργίας για το δίκτυο, έτσι ώστε να ληφθούν οι

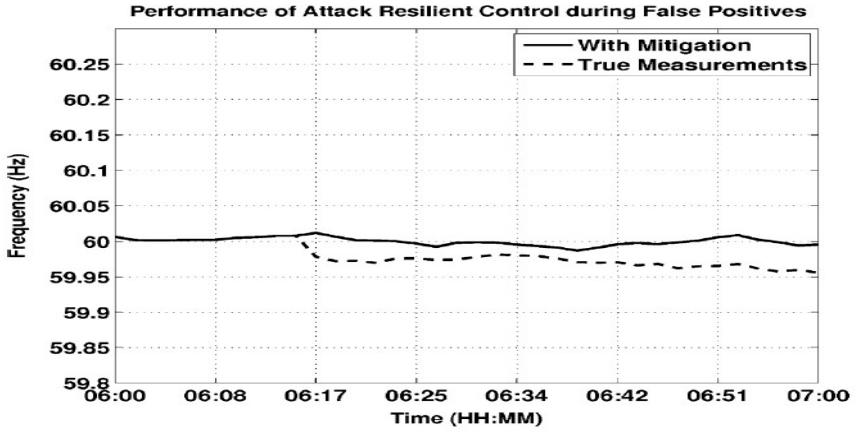
καλύτερες δυνατές αποφάσεις για την μείωση των βλαβών που επιφέρει η επίθεση (π.χ. γραμμές ισχύος σε ευαίσθητα φορτία όπως νοσοκομεία, τα οποία σε καμία συνθήκη δεν πρέπει να βρεθούν εκτός τροφοδότησης). Σε αυτό συνεισφέρει και η γνώση των υποδομών του δικτύου για τη μετρίαση των καταστροφικών επιδράσεων κατά την επίθεση.

Η γνώση των μορφών επίθεσης (attack signatures) βοηθά στην ανίχνευση των σημάτων επίθεσης από το σύστημα ελέγχου, εξετάζοντας μέσω ειδικών αλγορίθμων τη μορφή των λαμβανόμενων σημάτων από τους αισθητήρες.

Οι παράμετροι λειτουργίας του δικτύου, όπως η σταθερά αδράνειας *H* (inertia) διαδραματίζει έναν πολύ σημαντικό ρόλο στην απόρριψη διαταραχών από το δίκτυο.

Τα συστήματα προστασίας από επιθέσεις τύπου μοντέλου αποτελούνται κατά κύριο λόγο από έναν κεντρικό αλγόριθμο για την ανίχνευση ανωμαλιών (Anomaly Detection Engine - ADE). Ο αλγόριθμος αξιοποιεί τις παραπάνω κλάσεις πληροφορίας με το διπλό στόχο, (i) να εντοπίσει τη χρονική περίοδο μίας επίθεσης και επιπλέον (ii) να ελαχιστοποιήσει την επίδρασή της στο σύστημα με λήψη σωστών αποφάσεων διαχείρισης. Η λειτουργία του αλγορίθμου πρέπει να είναι διασυνεχής και πραγματικού χρόνου.

Με βάση την παραπάνω ανάπτυξη των αμυντικών μηχανισμών, ένα παράδειγμα προσομοίωσης για την ελαχιστοποίηση των επιδράσεων επίθεσης τύπου μοντέλου από την εργασία [21] παρουσιάζεται στο σχήμα που ακολουθεί:



Σχήμα 25: Προσομοίωση επιθέσεων τύπου μοντέλου

Με βάση τα παρεχόμενα δεδομένα από τους επιμολυσμένους αισθητήρες κατά τη διάρκεια επίθεσης, οι αντιδράσεις του συστήματος διαχείρισης δίνουν αποτελέσματα τα οποία αντιστοιχούν σε σχετικά σημαντικές μεταβολές συχνότητας. Το μοντέλο πρόβλεψης και ανίχνευσης ανωμαλιών (συνεχής γραμμή) παράγει πιο μετριοπαθείς αντιδράσεις οι οποίες αντιστοιχούν σε ηπιότερες μεταβολές συχνότητας για το δίκτυο κατά τη διάρκεια μίας επίθεσης.

5 Ανοικτά Θέματα και Ερευνητικές Προκλήσεις από τις Μεθόδους Αντιμετώπισης των Επιθέσεων σε συστήματα AGC

5.1 Ανοικτά θέματα και επισφάλειες από το φυσικό επίπεδο προστασίας

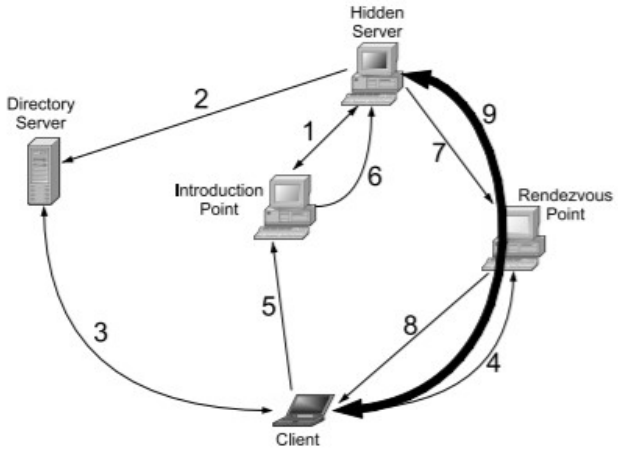
Σε προηγούμενο κεφάλαιο δόθηκε ο ορισμός του φυσικού επιπέδου προστασίας, που αποτελεί τη βάση των μηχανισμών προστασίας για τα συστήματα AGC. Οι βασικές διεργασίες που το φυσικό επίπεδο προστασίας υλοποιεί, είναι οι διαδικασίες της Ταυτοποίησης (Authentication) και του Επιπέδου Πρόσβασης (Authorization) για οποιονδήποτε αιτείται πρόσβαση χρήσης στο σύστημα.

Η ταυτοποίηση αποτελεί μία διεργασία που στηρίζεται κατά κύριο λόγο σε πληροφοριακά συστήματα διαχείρισης δεδομένων, με στόχο την αναγνώριση (ταυτοποίηση) του φυσικού προσώπου που αιτείται την πρόσβαση διαχείρισης – λειτουργίας στο σύστημα AGC. Κατά συνέπεια, ένα τέτοιο πληροφοριακό σύστημα είναι υποκείμενο στους κινδύνους και τις προκλήσεις ανάλογων ηλεκτρονικών πληροφοριακών συστημάτων. Η διαδικασία της ταυτοποίησης εφόσον βασίζεται σε εισαγωγή/είσοδο ενός χρήστη – ηλεκτρονικά σε ένα σύστημα (login process), είναι άμεσα υποκείμενη στις επισφάλειες που δημιουργεί η απώλεια και η λανθασμένη χρήση των κωδικών πρόσβασης (passwords) στο σύστημα.

Η ανάκτηση των κωδικών πρόσβασης ενός χρήστη (login accounts – passwords) μπορεί να τεθεί άμεσα σε κίνδυνο μέσω πολλών τεχνικών ανίχνευσης. Τέτοιες διαδικασίες είναι το 'ψάρεμα των δεδομένων' (data phishing), η συγκέντρωση πληροφοριών και δεδομένων από τα δίκτυα κοινωνικής δικτύωσης καθώς και η πρόσβαση σε υπολογιστές που ο χρήστης χειρίζεται. Πάντα υπάρχει πιθανότητα ανάκτησης αυτής της πληροφορίας, αν και πιο μειωμένη της απευθείας επίθεσης στα πληροφοριακά συστήματα που διαχειρίζονται τις δομές πληροφορίας για το σύστημα AGC. Η ανάλυση των ανταλλασσόμενων πακέτων δεδομένων – πληροφορίας στο σύστημα AGC, αποτελεί μία συνήθη τεχνική επίθεσης στα δίκτυα δεδομένων. Ο επιτιθέμενος συγκεντρώνει τα ανταλλασσόμενα δεδομένα ως ενδιάμεσος (Man-in-the-middle - MiM) με στόχο να 'αλιεύσει' την κρίσιμη πληροφορία που αφορά στις διαδικασίες login στο σύστημα. Κατά συνέπεια, τα ανοικτά θέματα που αφορούν στο φυσικό επίπεδο προστασίας και για τα συστήματα AGC, παραμένουν ανάλογα των ανοικτών θεμάτων διαχείρισης – κρυπτογράφησης και ανάκτησης διαπιστευμένης πληροφορίας σε ένα ηλεκτρονικό σύστημα. Οι αλγόριθμοι κρυπτογράφησης (encryption process) και ελέγχου των διαδικασιών εισόδου (login process) διαρκώς είναι υποκείμενοι σε νέες τεχνικές επίθεσης και ισχυρότερα υπολογιστικά συστήματα (από πλευράς των επιτιθέμενων). Αυτό έχει ως αποτέλεσμα να χρειάζονται διαρκώς βελτιώσεις και ενημερώσεις σε ενδεχόμενα κενά δικτυακής ασφάλειας που παρουσιάζουν από τη χρήση των πρωτοκόλλων επικοινωνίας και κρυπτογράφησης. Η εμπειρία από τα δίκτυα επικοινωνιών έχει δείξει ότι σε οποιοδήποτε πρωτόκολλο επικοινωνίας μπορούν να υπάρξουν πάντοτε μικρά ή μεγάλα κενά ασφαλείας, τα οποία μπορεί να τύχουν αντικείμενο εκμετάλλευσης από πλευράς του επιτιθέμενου (protocol vulnerabilities) [43], [44].

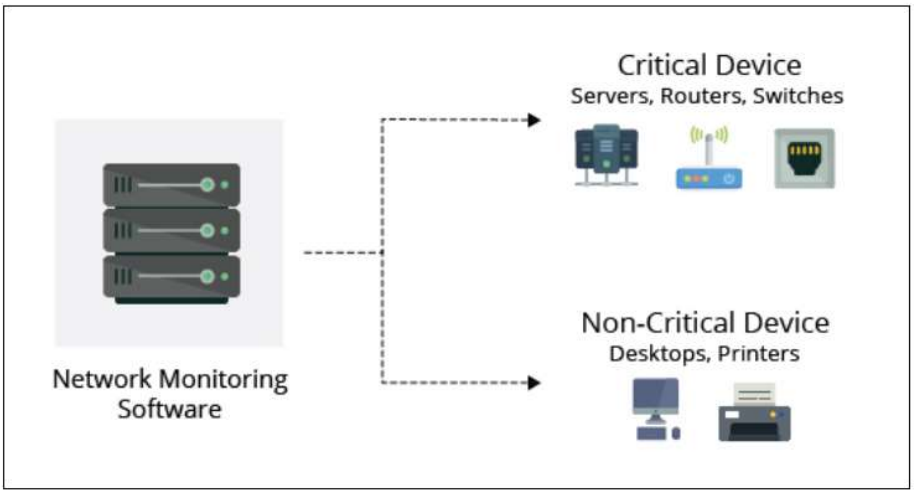
Η απομακρυσμένη διαχείριση και η πρόσβαση των πληροφοριακών συστημάτων

(remote access), εγκυμονούν έναν επίσης σημαντικό κίνδυνο για τη λειτουργία των συστημάτων διαχείρισης και ελέγχου του AGC. Η απομακρυσμένη πρόσβαση και διαχείριση σε ένα τέτοιο σύστημα, επιτρέπει σε μία κακόβουλη ομάδα, τον απομακρυσμένο (μερικό ή πλήρη) έλεγχο των συστημάτων ισχύος, χωρίς καν να απαιτείται η φυσική πρόσβαση της ομάδας στο χώρο και την έκταση των πραγματικών εγκαταστάσεων λειτουργίας.
Η διαχείριση υπολογιστικών συστημάτων από κακόβουλες ομάδες και η μετατροπή τους σε υπολογιστικά συστήματα επίθεσης (μηχανήματα zombies), σε συνδυασμό με τις δικτυακές διασυνδέσεις τύπου VPN (Virtual Private Networks) [30] μέσω εξωτερικών εξυπηρετητών (proxies), δυσχεραίνουν ακόμη περισσότερο τον εντοπισμό σε χώρο και χρόνο των παραπάνω επιθέσεων στα συστήματα AGC. Επομένως, όταν οι επιτιθέμενες ομάδες κάνουν χρήση αυτών των τεχνικών, είναι δύσκολο να εντοπιστούν σε φυσικό επίπεδο και επιπλέον οι επιθέσεις τους είναι δυνατόν να εκδηλωθούν οποιαδήποτε χρονική στιγμή για το σύστημα.
Συνολικά, λοιπόν, οι δομές φυσικής προστασίας μέσω των διεργασιών ταυτοποίησης και επιπέδου πρόσβασης, όταν αυτές βασίζονται σε υπολογιστικά συστήματα, εξακολουθούν να πάσχουν από τα ανοικτά θέματα και προβλήματα που αντιμετωπίζουν όλες οι υπολογιστικές δομές για τη διαχείριση και εξυπηρέτηση μέσω ηλεκτρονικών υπολογιστικών συστημάτων.
Ένα θωρακισμένο σύστημα φυσικής προστασίας απαιτεί ισχυρούς αλγορίθμους κρυπτογράφησης και ανάκτησης πληροφορίας (encryption/decryption algorithms). Επίσης, απαιτεί την ύπαρξη, διαχείριση και δημιουργία ασφαλών εξυπηρετητών (servers) οι οποίοι δεν είναι εξωτερικά εντοπίσιμοι και προσβάσιμοι από τα εξωτερικά δίκτυα διασύνδεσης (hidden servers) [40].



Σχήμα 26: Τυπική Δικτυακή χρήση κρυμμένων εξυπηρετητών (hidden – rendezvous servers)

Επιπλέον, ο εντοπισμός των επιθέσεων στα συστήματα AGC απαιτεί διασυνεχή έλεγχο και παρακολούθηση [41], συνθήκες που δεν μπορούν να διασφαλιστούν παρά μόνο με τη χρήση αυτοματοποιημένων συστημάτων ανάλυσης και παρακολούθησης των δεδομένων του δικτύου.



Σχήμα 27: Διαδικασία Δικτυακής Παρακολούθησης (Network Monitoring)

Τα ανοικτά θέματα και οι προκλήσεις που αφορούν κυρίως στο επίπεδο φυσικής προστασίας σχετίζονται με τα παρακάτω ερευνητικά θέματα [27], [30]:

- Ασφαλείς αλγόριθμοι κρυπτογράφησης με χρήση μεγάλων και δύσκολο να αναλυθούν κλειδιών.
- Υπολογιστικά συστήματα – εξυπηρετητές οι οποίοι δεν είναι εντοπίσιμοι από εξωτερικά δίκτυα.
- Δημιουργία και χρήση ασφαλών πρωτοκόλλων μετάδοσης και λήψης πληροφορίας.
- Λογισμικό ανάλυσης και παρακολούθησης των συντελούμενων διεργασιών εισόδου – εξόδου (login – logout process) και εφαρμογής ενεργειών επί του δικτύου AGC κατά την πάροδο του χρόνου (monitoring process and logs keeping).
- Δημιουργία απομονωμένων δικτυακών κόμβων (isolated networks), οι οποίοι έρχονται σε όσο το δυνατόν λιγότερη επαφή με το παγκόσμιο διαδίκτυο (internet).
- Προσωπικό που υποστηρίζει και επιμελείται ασφαλώς και καλόπιστα τις λειτουργίες του συστήματος AGC.

5.2 Η έννοια της εισβολής στα συστήματα AGC και τα ανοικτά θέματα στον εντοπισμό της

Ένα επίσης σημαντικό θέμα για την προστασία των συστημάτων ελέγχου και διαχείρισης ισχύος AGC, είναι η ακρίβεια του εντοπισμού μίας επίθεσης στο σύστημα. Ο εντοπισμός της επίθεσης αφορά τόσο στον καθορισμό της χρονικής στιγμής που το δίκτυο δέχεται την επίθεση, καθώς επίσης και στον καθορισμό των εσφαλμένων ενεργειών διαχείρισης που το σύστημα υφίσταται εξαιτίας της επίθεσης. Σημαντικό, επίσης, θέμα κατά την εκδήλωση των επιθέσεων είναι ο εντοπισμός των υποσυστημάτων που τελούν υπό τον έλεγχο των επιτιθέμενων στο σύστημα, παρέχοντας αναληθείς μετρήσεις, οδηγώντας το Διαχειριστή Λήψης Αποφάσεων

(EMS) σε λανθασμένες ενέργειες. Οι τεχνικές που χρησιμοποιούνται για τον εντοπισμό της έννοιας της επίθεσης στο δίκτυο AGC βασίζονται, είτε στον εντοπισμό καθορισμένων προτύπων επίθεσης (signature based detection) είτε στον καθορισμό συνθηκών ανώμαλης λειτουργίας (anomaly based detection).
Οι τεχνικές signature based detection βασίζονται σε εντοπισμό καθορισμένων προτύπων δράσεων – σημάτων επί του δικτύου AGC. Οι τεχνικές αυτές μοιάζουν στην προσέγγισή τους με τις τεχνικές που χρησιμοποιούνται για την ανίχνευση και τον εντοπισμό κακόβουλου λογισμικού (viruses) στα υπολογιστικά συστήματα. Το λογισμικό που είναι επιφορτισμένο με την προστασία των δομών AGC θα πρέπει να ανιχνεύσει από τα αναπτυσσόμενα πρότυπα δράσης στο δίκτυο, την πιθανή παρουσία επίθεσης στη δεδομένη χρονική στιγμή. Ο έλεγχος των προτύπων γίνεται μέσω μίας βάσης προτύπων (IDS), η οποία διαρκώς ενημερώνεται με την πάροδο του χρόνου για τα νέα και εξελισσόμενα πρότυπα επίθεσης (διαδικασία ανάλογη με την ενημέρωση του λογισμικού antivirus). Οι τεχνικές αυτού του τύπου είναι λογικό να βρίσκονται διαρκώς ένα βήμα πίσω από ενδεχόμενους νέους τύπους επιθέσεων, οι οποίοι μπορεί να δράσουν με νέα πρότυπα ή/και παραλλαγές των υφισταμένων προτύπων. Επομένως, ένα ανοικτό θέμα για τις δομές παρακολούθησης που βασίζουν τη λειτουργία τους σε signature based τεχνικές, είναι η μετεξέλιξη του λογισμικού με χρήση ευριστικών ή και άλλων αλγορίθμων για να μπορεί να εντοπίσει νέου τύπου επιθέσεις, οι οποίες εκδηλώνονται μέσω παραλλαγμένων προτύπων δράσεως [45].
Η εναλλακτική αρχιτεκτονική δράσης, όπως παρουσιάστηκε και στο προηγούμενο κεφάλαιο είναι η τεχνική ‘’anomaly based detection’’. Με αυτή την αρχιτεκτονική, το υποσύστημα παρακολούθησης και ανάλυσης εισβολών, εκπαιδεύεται με την πάροδο του χρόνου και μαθαίνει τα ορθά επίπεδα των σημάτων του δικτύου και των μηχανισμών δράσεων στο σύστημα AGC που επιβλέπει. Κατά συνέπεια, στην πορεία του χρόνου, το σύστημα είναι ικανό να αναγνωρίσει και να διαχωρίσει (σε ένα βαθμό πιθανότητας) τυχόν ανώμαλες συνθήκες λειτουργίας, οι οποίες σε ένα ποσοστό πιθανότητας μπορεί να περιλαμβάνουν δράσεις επιθέσεων στο σύστημα AGC.
Όμως, και οι δύο τεχνικές που παρουσιάστηκαν, μπορεί είτε να μην εντοπίσουν την εκδηλούμενη επίθεση εφόσον πρόκειται για ένα νέο και άγνωστο πρότυπο, ή να δημιουργήσουν ψευδή σήματα συναγερμών (False alerts) στην περίπτωση που εντοπίσουν ακραίες αλλά πραγματικές καταστάσεις κατά τη λειτουργία του δικτύου παροχής ισχύος.
Ανοικτό θέμα και για τις δύο αρχιτεκτονικές, αποτελεί η ανάπτυξη ευφυών αλγορίθμων οι οποίοι θα μπορούν να εκτελούν τις παρακάτω διεργασίες [45]:

- Να αναγνωρίζουν τις ομαλές συνθήκες λειτουργίας του δικτύου.
- Να εντοπίζουν ακραίες καταστάσεις κατά τη λειτουργία του δικτύου και να καταχωρούν τις συνθήκες σε δυναμικά συστήματα βάσεων δεδομένων.
- Να μαθαίνουν από το χειρισμό και τον εντοπισμό των συνθηκών λειτουργίας του δικτύου ισχύος.
- Να ανακαλούν γραμμές άμυνας (δράσεις) και διαχείρισης στην περίπτωση που εντοπίσουν τυχόν επιθέσεις στο δίκτυο AGC.
- Να προβλέψουν μέσω των συνθηκών λειτουργίας, χρονικές περιόδους που ευνοούν την εφαρμογή επιθετικών δράσεων στο σύστημα AGC.

Οι γενετικοί αλγόριθμοι, καθώς και τα νευρονικά δίκτυα διαχείρισης και ανάλυσης ψηφιακών δεδομένων, αποτελούν σημαντικές τεχνολογίες που αναμένεται με την πάροδο του χρόνου να συμβάλλουν καθοριστικά τόσο στην ανίχνευση όσο και στις ενέργειες που θα εφαρμόσουν για τον έλεγχο της εκδηλούμενης επίθεσης στο δίκτυο AGC [25]. Η διαδικασία εκμάθησης έχει αποδειχθεί ότι αποτελεί ένα εγγενές πλεονέκτημα – χαρακτηριστικό αυτών των τεχνολογιών. Η ταυτόχρονη υποστήριξη των αλγορίθμων με υπολογιστικά συστήματα παράλληλης αρχιτεκτονικής/εκτέλεσης πολλαπλών επεξεργαστών, αυξάνουν σημαντικά την απόδοση και την ταχύτητα δράσης αυτών των αλγορίθμων.
Στόχος αυτών των συστημάτων είναι η διασυνεχής (online) παρακολούθηση, η οποία μπορεί αυτοματοποιημένα να εντοπίσει και να αντιδράσει με τις απαραίτητες ενέργειας μετριασμού της επίθεσης στο υφιστάμενο δίκτυο ισχύος μέσω των μηχανισμών ελέγχου που δίνουν τα συστήματα AGC.

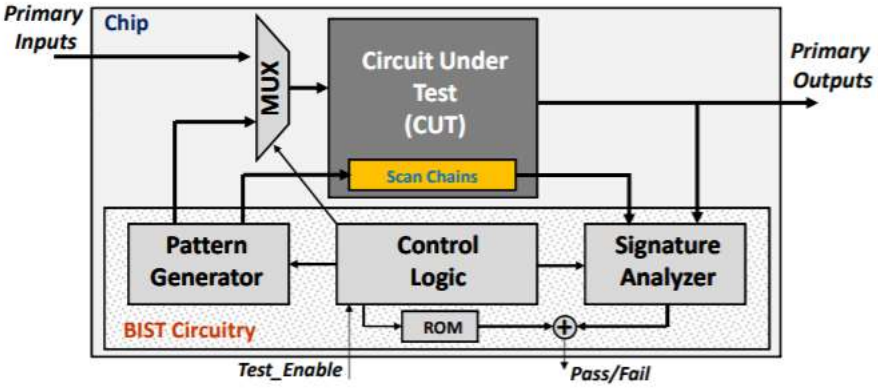
5.3 Αντιμετώπιση επιθέσεων με αλλοιωμένα σήματα αισθητήρων

Η αντιμετώπιση των επιθέσεων με αλλοιωμένα σήματα αισθητήρων βασίζεται στη δημιουργία ψευδών και αλλοιωμένων σημάτων που προέρχονται από τους αισθητήρες και κατευθύνονται προς το κέντρο Λήψης Αποφάσεων και Διαχείρισης (EMS) του συστήματος AGC. Η κατηγοριοποίηση και περιγραφή αυτών των επιθέσεων βασίζεται στα πρότυπα και τους τύπους αλλοιώσεων των σημάτων του αισθητήρα. Στην αλλοίωση των δεδομένων των αισθητήρων μπορούμε να διακρίνουμε δύο εναλλακτικούς τρόπους δράσης ως προς την αλλοίωση:

- Αλλοίωση των σημάτων κατά τη γένεσή τους στον αισθητήρα
- Αλλοίωση των πακέτων δεδομένων του αισθητήρα κατά την αποστολή τους μέσω του δικτύου διασύνδεσης

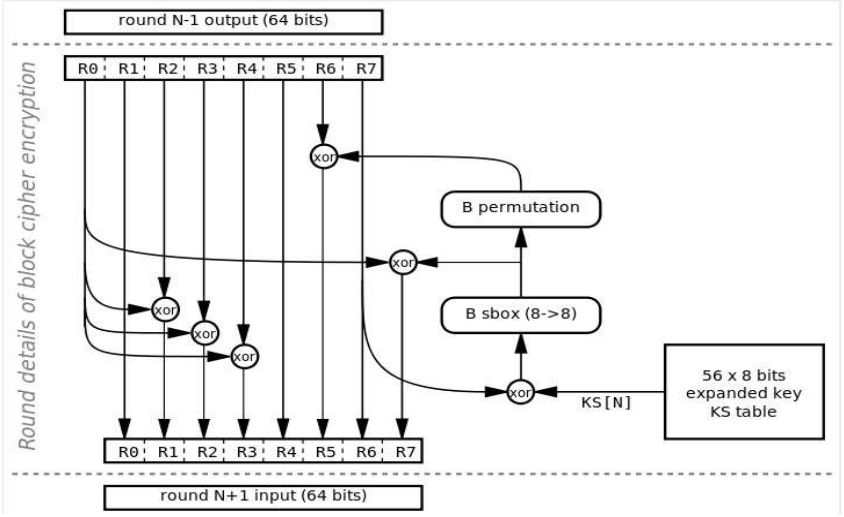
Στην πρώτη περίπτωση, τα δεδομένα του αισθητήρα επιμολύνονται από την προσθήκη κυκλωμάτων δράσης επί των φυσικών κυκλωμάτων του αισθητήρα, με τρόπο που να παραλλάσει – αλλοιώνει τα παραγόμενα δεδομένα μετρήσεων. Στη δεύτερη περίπτωση, η αλλοίωση των δεδομένων του αισθητήρα γίνεται σε δευτερογενές επίπεδο. Ο αισθητήρας δημιουργεί τα ορθά δεδομένα εκτίμησης λειτουργίας και μετρήσεων και αυτά αντικαθίστανται ή αλλοιώνονται μέσω των πακέτων αποστολής προς το κέντρο διαχείρισης.
Για την αντιμετώπιση της πρώτης περίπτωσης απαιτείται η ανάπτυξη κυκλωμάτων που δεν επιτρέπουν φυσικές κυκλωματικές διασυνδέσεις (tapping), με τις οποίες να αλλοιώνονται τα δεδομένα μετρήσεων. Η φυσική τοποθέτηση των αισθητήρων θα πρέπει να είναι προστατευμένη από τους μηχανισμούς φυσικής πρόσβασης, δίνοντας τη δυνατότητα μόνο σε εξουσιοδοτημένο προσωπικό για τη διαχείρισή τους. Αυτοματοποιημένοι αλγόριθμοι ελέγχου (self-tests) με τεχνικές BIST (Bult In Self Tests) ή POST (Power On Self Tests) [42], [46], επιτρέπουν την ασφαλή εκτίμηση των επιπέδων λειτουργικότητας του αισθητήρα.
Και οι δύο έλεγχοι αυτού του τύπου είναι ικανοί να εξακριβώσουν την κατάσταση λειτουργικότητας του αισθητήρα. Για την εφαρμογή τους κάνουν χρήση, ο μεν BIST εσωτερικών κυκλωμάτων που ενυπάρχουν από κατασκευής στο κύκλωμα του

αισθητήρα, ο δε POST μπορεί να συμπεριλαμβάνει και εξωτερικά κυκλώματα συνοδευτικά για τον έλεγχο της λειτουργίας. Ο BIST συνήθως υλοποιείται αυτόματα κατά την εκκίνηση του συστήματος, ενώ ο POST μπορεί να εφαρμοσθεί με δυναμικό τρόπο από το χρήστη του συστήματος.



Σχήμα 28: Αρχιτεκτονική Αναπαράσταση ενός BIST ελέγχου για ένα κύκλωμα

Στην περίπτωση που οι αυτοματοποιημένοι έλεγχοι αποτυγχάνουν, αυτό συνιστά ένα σημαντικό λόγο για την παρακολούθηση και ενδεχόμενα αντικατάσταση ενός αισθητήρα. Επιπλέον, η συγκέντρωση των δεδομένων του αισθητήρα και η μετατροπή τους σε ψηφιακά δεδομένα θα πρέπει να μη γίνεται αμορφοποίητα (raw measurements data), έτσι ώστε να μη δίνουν τη δυνατότητα παρακολούθησης απευθείας των παραγόμενων δεδομένων τους.
Για την αντιμετώπιση του δεύτερου τύπου επίθεσης απαιτείται η οργάνωση των δεδομένων του αισθητήρα σε πακέτα ψηφιακής πληροφορίας, τα οποία είναι κωδικοποιημένα με τη χρήση ισχυρών κλειδιών, τα οποία μπορεί να είναι δυναμικά και μεταβαλλόμενα στο χρόνο. Κατά συνέπεια, η ανάλυση των παρεχόμενων δεδομένων από τον αισθητήρα, μπορεί να γίνει μόνο μετά την αποκωδικοποίησή τους από έναν πιθανό επιτιθέμενο, αποτρέποντας τυχόν αλλοιώσεις οι οποίες θα μπορούσαν να συντελεστούν. Η χρήση δομών προστασίας μπορεί εντός του ίδιου του πακέτου δεδομένων, να προστατεύσει τα παραγόμενα δεδομένα από τυχόν αλλοιώσεις οι οποίες μπορούν εύκολα να εντοπιστούν [50].



Σχήμα 29: Αρχιτεκτονική Αναπαράσταση της διαδικασίας προστασίας δεδομένων πακέτου με χρήση κλειδιών (scrambling)

Η περιοδικότητα στην ανταλλαγή των δεδομένων του αισθητήρα προς τον κεντρικό διαχειριστή σε καθορισμένα χρονικά πλαίσια, συνιστά ένα ακόμη επίπεδο προστασίας. Η χρήση καθορισμένων χρονοθυρίδων (timeslots) για την επικοινωνία, μπορεί να διασφαλιστεί με τη χρήση συντελεστών ποιότητας επικοινωνίας (QoS), καθώς επίσης και με τη χρήση απομονωμένων δικτύων τα οποία δεν έρχονται σε άμεση διεπαφή με τον παγκόσμιο ιστό (leased lines).
Ανοικτά θέματα, λοιπόν, για την προστασία από τις αλλοιώσεις δεδομένων των αισθητήρων, αποτελούν [50], [51]:

- η δημιουργία ασφαλών πρωτοκόλλων κρυπτογράφησης με χρήση δεδομένων πραγματικού χρόνου (real time stamps) για τις ανάγκες των δικτύων AGC, τα οποία καθορίζουν την αποστελλόμενη πληροφορία στο χρόνο.
- Η αμφίδρομη επικοινωνία με τη δημιουργία έξυπνων αισθητήρων – smart sensors (αισθητήρας → κεντρικό διαχειριστή και αντίστροφα), μπορεί να επιτρέψει την εκτέλεση ειδικών λειτουργιών επί του αισθητήρα, μέρος αυτών και οι διαδικασίες ορθής λειτουργίας του τελευταίου, οι οποίες αφορούν στην αποστολή και την ακρίβεια των δεδομένων. Σε φάσεις ακραίων συνθηκών λειτουργίας, ο έξυπνος αισθητήρας ενεργοποιείται και αποστέλλει περισσότερα δεδομένα στη μονάδα του χρόνου δίνοντας ρεαλιστικότερη εικόνα για την εκτίμηση της διαχείρισης ισχύος στον τομέα ελέγχου του.
- Οι δομές των έξυπνων αισθητήρων επικοινωνούν με τον κεντρικό διαχειριστή αλλά και μεταξύ τους, δίνοντας τη δυνατότητα για παράλληλο έλεγχο των δεδομένων όλης της ομάδας στο κοινό υποδίκτυο ισχύος. Το ιδιαίτερο αυτό χαρακτηριστικό επιτρέπει τον ταυτόχρονο έλεγχο και την εκτίμηση της ομάδας των αισθητήρων για το ίδιο υποσύστημα του δικτύου ισχύος. Με τον τρόπο αυτό, είναι ευκολότερη η απομόνωση και ο εντοπισμός του πλήθους των αισθητήρων που αναφέρουν λανθασμένα δεδομένα για το τμήμα του υποδικτύου, καθιστώντας εύκολη την ανίχνευση επίθεσης και απομόνωσης των αισθητήρων που έχουν τεθεί σε έλεγχο από τον επιτιθέμενο.

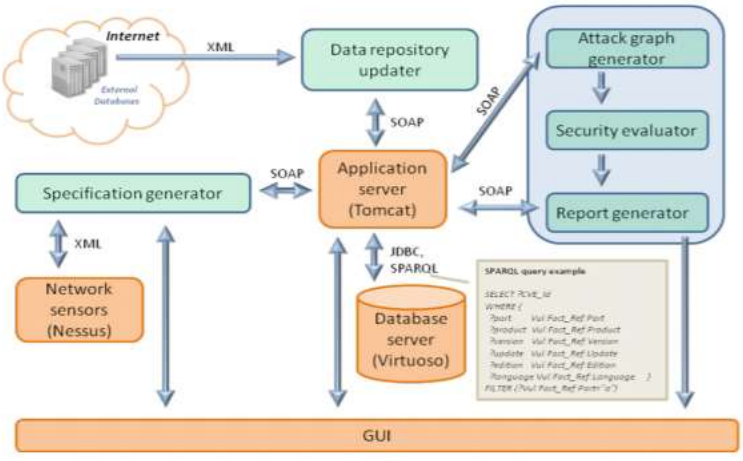
5.4 Αντιμετώπιση επιθέσεων με Έγχυση Λανθασμένων Δεδομένων (FDIAs)

Στο προηγούμενο κεφάλαιο της εργασίας παρουσιάστηκε ένα σημαντικό σύνολο από ερευνητικές εργασίες και αλγορίθμους που χρησιμοποιούνται για την ανίχνευση και τη διόρθωση – μετριασμό των αποτελεσμάτων επιθέσεων με έγχυση λανθασμένων δεδομένων (FDIAs). Σε αυτό τον τύπο της επίθεσης, η αλλοίωση των δεδομένων δεν προέρχεται απευθείας από τους αισθητήρες του δικτύου, αλλά δευτερογενώς θεωρούμε ότι οι επιτιθέμενοι έχουν αναλάβει, μέσω του δικτύου διασύνδεσης των αισθητήρων, δράσεις στην αποστολή και κατασκευή ψευδών πακέτων μετρήσεων προς τον κεντρικό διαχειριστή [19].

Οι αλγόριθμοι που παρουσιάστηκαν για την αντιμετώπιση του προβλήματος, ανέλυσαν ένα ευρύ σύνολο από παραμέτρους και χαρακτηριστικά για την αξιολόγηση και εκτίμηση των επιθέσεων. Οι αλγόριθμοι βασίζονταν σε:

- χρήση συναρτήσεων δυναμικού και ευαισθησίας **[31]**, **[32]**,
- εντόπιζαν μέσω ανάλυσης την βέλτιστη πολιτική επίθεσης από την πλευρά του επιτιθέμενου στο δίκτυο **[33]**,
- αναζητούσαν τις επιδράσεις των επιθέσεων στο δίκτυο AGC **[34]**,
- προσέγγιζαν το θέμα πειραματικά με αναλύσεις σε πραγματικά συστήματα παραγωγής και διανομής **[35]**, **[24]**,
- έκαναν χρήση μοντέλων πρόβλεψης για την εκτίμηση των επιπέδων ισχύος στις φάσεις εκδήλωσης επιθέσεων **[25]**,
- έκαναν χρήση παρατηρητών κατάστασης (UIO/SMO) για το δίκτυο ισχύος **[19]**, **[29]**.

Από τις παραπάνω προσεγγίσεις καθίσταται εμφανής η ετερογένεια των προτεινόμενων μεθόδων και αλγορίθμων. Όλες οι μέθοδοι στόχευαν στον εντοπισμό και τον μετριασμό των επιδράσεων από τη δράση της επίθεσης, εκκινώντας όμως από διαφορετικά επίπεδα δεδομένων και γνώσης του συστήματος διαχείρισης ισχύος. Καθίσταται, λοιπόν, προφανές ότι παρά την ερευνητική προσπάθεια, δεν υφίσταται ένα κοινό πλαίσιο έρευνας τόσο για την αρχιτεκτονική όσο και για τους στόχους των παραπάνω αλγορίθμων. Όλες οι μέθοδοι καταλήγουν στο συμπέρασμα ότι οι επιθέσεις αυτού του τύπου είναι εξαιρετικά επικίνδυνες για τη λειτουργία των δικτύων ισχύος, αλλά είναι επίσης εξαιρετικά δύσκολο να προστατευτούν τα δίκτυα ισχύος από αυτές **[32]**. Στόχος των μεθόδων είναι ο εντοπισμός κάποιων από τους τύπους των επιθέσεων έγχυσης λανθασμένων δεδομένων (FDIAs).

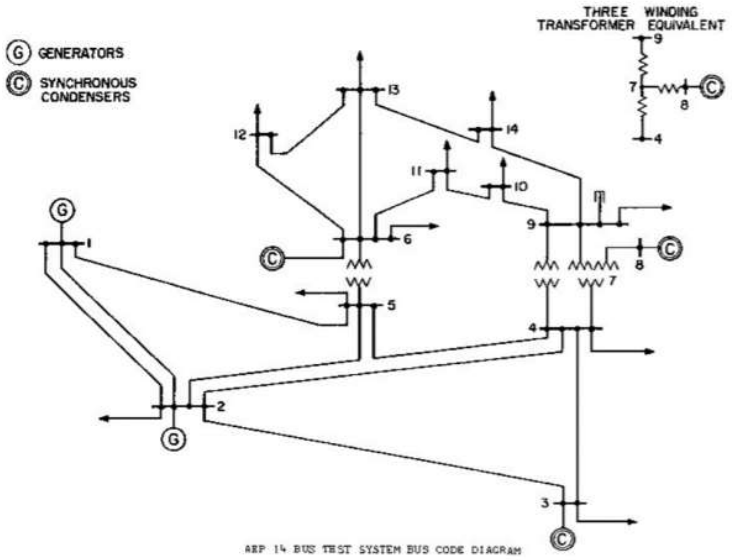


Σχήμα 30: Αρχιτεκτονική Cyber Attacks Impact Assessment – CAIA methodology

Ανοικτά θέματα για το συγκεκριμένο πεδίο αποτελούν [32]:

- Οι εφαρμογές προσομοιώσεων (Cyber Attacks Impact Assessment – CAIA methodology) για τον εντοπισμό των επιδράσεων των επιθέσεων FDIAs στα υφιστάμενα δίκτυα ισχύος.

- Η ανάπτυξη λεπτομερών μοντέλων περιγραφής των δικτυακών υποδομών ισχύος.
- Η χρήση μοντέλων προσομοίωσης φυσικών διεργασιών που αναφέρονται στις πραγματικές υλοποιήσεις των δικτύων ισχύος (IEEE 14-bus, IEEE 300-bus, etc).



Σχήμα 31: Αρχιτεκτονική Διασύνδεσης του IEEE-14 bus συστήματος ελέγχου (test system) [48]

- Η ανάπτυξη πολύπλοκων σεναρίων επίθεσης.
- Η ακριβής εκτίμηση των επιδράσεων μίας επίθεσης.
- Η αξιολόγηση της εφαρμοσιμότητας των μεθόδων προσομοίωσης (CAIA) στα πραγματικά συστήματα παραγωγής και διαχείρισης ισχύος **[32]**.
- Η χρήση των αποτελεσμάτων των προσομοιώσεων στη μεθοδολογία του σχεδιασμού των δικτύων παραγωγής και διαχείρισης ισχύος.
- Η εκτίμηση της ικανότητας του επιτιθέμενου μέσω FDIA για τη δημιουργία επιθέσεων σε κάθε κύκλο λειτουργίας του συστήματος AGC, λόγω της απαιτούμενης υπολογιστικής ισχύος που απαιτείται για την αποκρυπτογράφηση των πακέτων μετρήσεων του δικτύου.
- Η θεώρηση της αρχής Kerckhoff δηλ, κατά πόσο ο επιτιθέμενος έχει ακριβή γνώση των δομών του συστήματος ισχύος και εκτίμηση της πραγματικής κατάστασης του δικτύου. Διαφορετικά επίπεδα θεώρησης επί της αρχής δημιουργούν και διαφορετικές βάσεις ανάλυσης για την προσέγγιση του προβλήματος **[24]**.
- Έλεγχος κατά πόσον ένα μεγάλο σύστημα ισχύος είναι υποκείμενο σε μία συνολική επίθεση ή σε επικέντρωση πολλών μικρών επιθέσεων στα υποδίκτυα που συνιστούν το συνολικό δίκτυο ισχύος. Η ερευνητική εμπειρία υποδεικνύει συνήθως ότι οι επιθέσεις επικεντρώνονται στα μικρά υποδίκτυα του συστήματος ισχύος (λόγω του βαθμού δυσκολίας που ο επιτιθέμενος αντιμετωπίζει από πλευράς υπολογιστικής ισχύος για τη συνολική αποκωδικοποίηση όλων των ανταλλασσόμενων δεδομένων στο δίκτυο).

- Η ανάπτυξη στρατηγικών μετριασμού των επιδράσεων (mitigation strategy) για επιθέσεις οι οποίες βασίζονται στην αγορά ηλεκτρικής ενέργειας σε συνδυασμό με επιθέσεις στα συστήματα AGC. Ο στόχος αυτών των μορφών επιθέσεων είναι ο εξαναγκασμός του Διαχειριστή Ενέργειας (EMS) σε αγορά ισχύος η οποία οδηγεί σε οικονομική ζημιά για το δίκτυο.
- Η εφαρμογή ευφυών αλγορίθμων (Genetic Algorithms – GA, Simulated Annealing - SA, Particle Swarm Optimization - PSO, Ant Colony Optimization - ACO, Fuzzy Logic - FL, Artificial Neural Network - ANN και αντίστοιχα υβριδικά τους μοντέλα), για το σχεδιασμό εύρωστων συστημάτων AGC **[19]**.

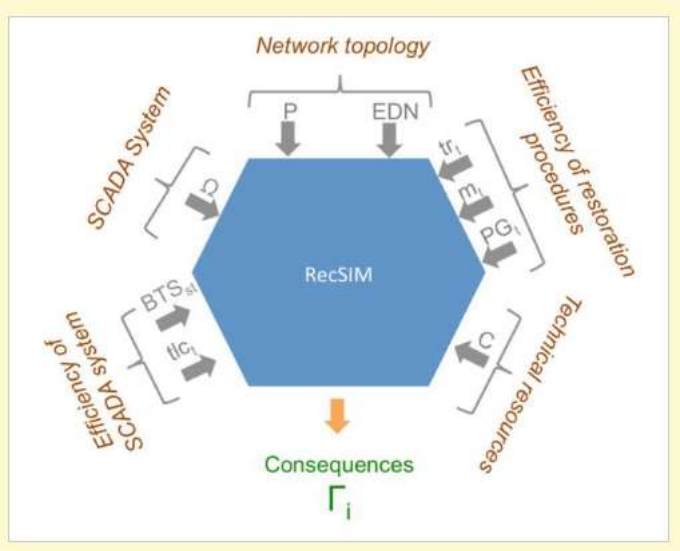
5.5 Αντιμετώπιση επιθέσεων με Έγχυση Χρονικά Καθυστερημένων Δεδομένων (Time Delay Attacks)

Στις επιθέσεις αυτού του τύπου, όπως παρουσιάστηκε και στο προηγούμενο κεφάλαιο, τα δεδομένα που προορίζονται από τους αισθητήρες προς το κέντρο Λήψης Αποφάσεων και Διαχείρισης του συστήματος AGC, υπόκεινται σε χρονικές καθυστερήσεις/απώλειες πακέτων δεδομένων, με αποτέλεσμα τα δεδομένα μετρήσεων που παρέχονται να δίνουν μία καθυστερημένη χρονική εικόνα της κατάστασης του δικτύου ισχύος. Κατά συνέπεια, πρόκειται για πραγματικά – μη αλλοιωμένα δεδομένα, τα οποία λόγω της επίθεσης έρχονται με σκόπιμη καθυστέρηση, δημιουργώντας στο διαχειριστή ισχύος λανθασμένη εικόνα για την τρέχουσα κατάσταση του δικτύου, οδηγώντας έτσι στη λήψη λανθασμένων ενεργειών προς τα υποσυστήματα παραγωγής.
Ανοικτά θέματα για την αποφυγή και την αντιμετώπιση των επιθέσεων χρονοκαθυστέρησης αποτελούν **[17]**:

- Η ανάπτυξη ευφυών συντελεστών ποιότητας (QoS) και προσαρμοσμένων πρωτοκόλλων για τη δυναμική δρομολόγηση των δεδομένων των αισθητήρων προς το κέντρο λήψης αποφάσεων με δυνατότητα ανίχνευσης της απώλειας και της καθυστέρησης. Σημαντικό χαρακτηριστικό αυτής της ερευνητικής προσπάθειας είναι η χρονική διασφάλιση της διανομής των πακέτων μετρήσεων προς τον Διαχειριστή.
- Επιλογή του τύπου και της τεχνολογίας κορμού των δικτύων προσπέλασης με βάση τις επαγόμενες καθυστερήσεις μετάδοσης. Στόχος είναι η υιοθέτηση δικτυακών υποδομών στις οποίες να μπορούν να ελεγχθούν οι χρονικές καθυστερήσεις δρομολόγησης.
- Βελτιστοποίηση των αλγορίθμων υπολογισμού και επεξεργασίας των μετρήσεων, για την ελαχιστοποίηση των χρόνων επεξεργασίας, ο οποίος προστίθεται στο συνολικό χρόνο απόδοσης των δεδομένων (καθυστέρηση + επεξεργασία) προς το Κέντρο Λήψης Απόφασης (EMS).
- Κατανομή της αδράνειας (inertia) των υποσυστημάτων παραγωγής ισχύος για το μετριασμό των επιδράσεων των επιθέσεων **[20]**.

5.6 Αντιμετώπιση Επιθέσεων Με Χρήση Μοντέλων (Model based Attacks)

Οι επιθέσεις που βασίζονται στη χρήση μοντέλων αφορούν στη χρήση μεταβλητών σημάτων από τους αισθητήρες προς τον Κεντρικό Διαχειριστή, με στόχο τη δημιουργία επισφαλειών στη λειτουργία του συστήματος AGC. Η διαχείριση αυτού του τύπου των επιθέσεων, κυρίως βασίζεται σε αποτελέσματα από την εφαρμογή προσομοιώσεων, τα οποία στηρίζονται από τα μοντέλα λειτουργίας του δικτύου AGC. Η ερευνητική βιβλιογραφία δείχνει ότι η επίδραση διαφορετικών μοντέλων στα σήματα που ανταλλάσσουν οι αισθητήρες, έχει διαφορετικά αποτελέσματα στην εκδήλωση των επιπέδων επίθεσης προς το δίκτυο, δημιουργώντας συνθήκες υπέρ-, υπό- μεταβολών για την πραγματική συχνότητα λειτουργίας του δικτύου ισχύος.



Σχήμα 32: Το Ανεκτικό Δίκτυο Παραγωγής και Διανομής Ισχύος [49]

Καθοριστικοί στη λήψη αποφάσεων είναι παράμετροι ευαισθησίας και η αδράνεια (inertia) των υποδικτύων, για τα επίπεδα εκδήλωσης των επιθέσεων. Στόχος των αντίστοιχων μελετών **[21]**, είναι η ανάπτυξη ενός ανεκτικού (resilient) δικτύου με σκοπό την ελαχιστοποίηση των επιδράσεων των επιθέσεων.

Τα ανοικτά θέματα με αυτού του τύπου τις επιθέσεις αφορούν **[21]**:

- Στην ανάπτυξη ακριβών περιγραφών – μοντέλων για τη διαδικασία προσομοίωσης των δικτύων ισχύος.
- Την ανάπτυξη σεναρίων προσβολής – επίθεσης για τον έλεγχο των αποτελεσμάτων.
- Τη στάθμιση των παραμέτρων λειτουργίας ενός δικτύου ισχύος.
- Την ανάπτυξη ανεκτικών δικτύων (resilient networks) και την αποτίμηση των αποτελεσμάτων προσομοίωσης στο σχεδιασμό των δικτύων AGC.

6 Συμπεράσματα

6.1 Ανοικτά Θέματα και Προκλήσεις

Από την παρουσίαση και μελέτη των διαφορετικών τύπων κυβερνο-επιθέσεων, όπως αυτές εκδηλώνονται στα δίκτυα παραγωγής και διαχείρισης ισχύος AGC, είναι προφανές ότι η ετερογένεια αυτών των επιθέσεων δεν επιτρέπει τη γενική ανάπτυξη ενός 'καθολικού' αλγορίθμου αντιμετώπισης. Ένας καθολικός αλγόριθμος θα επέτρεπε την ανίχνευση όλων των τύπων επίθεσης, καθώς και τη βέλτιστη διαχείριση των σημάτων ελέγχου από το Κέντρο Αποφάσεων (EMS), με στόχο το μετριασμό των επιδράσεων των επιθέσεων στην υποδομή και λειτουργία του δικτύου ισχύος **[19] – [47]**.

Μέσα στα γενικότερα πλαίσια των ανοικτών θεμάτων και προκλήσεων που καλούνται να αντιμετωπιστούν από τους αλγορίθμους που αναπτύσσει η έρευνα για τα δίκτυα AGC, είναι ο καθορισμός και η ενσωμάτωση μετρικών επίδοσης για το δίκτυο, καθώς και η συμπερίληψη γενικότερων κανόνων για τη διαχείριση των συνθηκών επίθεσης (optimal mitigation strategy).

Η διερεύνηση του εντοπισμού των χρονικών στιγμών επίθεσης (time of attack) για ένα δίκτυο ισχύος, αποτελεί επίσης ένα σημαντικό θέμα προς επίλυση, το οποίο μπορεί να καθορισθεί μόνο ως «πιθανότητα ορθής ανίχνευσης επίθεσης», με βάση τις επαγόμενες συνθήκες λειτουργίας του δικτύου κατά την εκδήλωσή της. Επομένως, η εκδήλωση και ο χαρακτηρισμός συνθηκών ως επιθέσεις (που μπορεί να είναι ψευδείς, δηλ. χωρίς στην πραγματικότητα να ισχύει αυτό), δίνει επίσης μία πιθανότητα για τη δημιουργία «ψευδών σημάτων συναγερμού» για το δίκτυο παραγωγής και διαχείρισης ισχύος. Το τελευταίο χαρακτηριστικό επιφέρει συνθήκες συναγερμού στον Διαχειριστή Ενέργειας (EMS), αναγκάζοντάς τον στην εφαρμογή πρωτοκόλλων διαχείρισης που μπορεί να μην είναι απαραίτητα στη συγκεκριμένη χρονική φάση. Άρα, είναι σημαντικό οι αλγόριθμοι που έχουν αναπτυχθεί και θα επεκταθούν στο μέλλον, να λάβουν υπόψιν τους αυτή τη σοβαρή συνθήκη, για την ελαχιστοποίηση ψευδών και λανθασμένων επιδράσεων εξαιτίας ακραίων χαρακτηριστικών λειτουργίας, που το σύστημα προστασίας λανθασμένα αντιλαμβάνεται ως επιθέσεις. Επομένως, η υπερευαισθησία των αλγορίθμων στην ανίχνευση επιθέσεων διαφαίνεται ότι μπορεί να προκαλέσει προβλήματα ανάλογα με τα προβλήματα που τα δίκτυα ισχύος βιώνουν και κατά την εκδήλωση πραγματικών επιθέσεων. Οι αλγόριθμοι, λοιπόν, θα πρέπει να δίνουν τη δυνατότητα για μία αυτορρύθμιση (self-tuning), λαμβάνοντας υπόψιν τα ιδιαίτερα χαρακτηριστικά του δικτύου ισχύος που διαχειρίζονται και προστατεύουν.

Γενικότερα, διαφαίνεται ότι λόγω της ετερογένειας των επιθέσεων και των διαφορετικών προσεγγίσεων στην προσπάθεια αντιμετώπισης του προβλήματος, η χρήση προσομοιώσεων μέσω υπολογιστικών συστημάτων αποτελεί μία επαρκή βάση για την τοποθέτηση και μελέτη του προβλήματος. Η ανάπτυξη αλγορίθμων, οι οποίοι βασίζονται στις διαδικασίες εκπαίδευσης – μάθησης, αποτελεί επίσης ένα τομέα πρόκλησης για την ανάπτυξη ευφυών αλγορίθμων ανίχνευσης και διαχείρισης των επιθέσεων. Το μαθηματικό υπόβαθρο για αυτήν την προσέγγιση είναι εκτενές, δεδομένης της ανάλογης ερευνητικής εργασίας για γενικότερα μαθηματικά μοντέλα προσομοίωσης (ασαφής λογική, γενετικοί αλγόριθμοι, κλπ). Επιπρόσθετα, οι

εκπαιδευόμενοι – ευφυείς αλγόριθμοι, εφόσον η υλοποίησή τους βασιστεί σε ένα συμπαγές αλλά επεκτάσιμο πυρήνα λογισμικού που εκτελείται στα υπολογιστικά συστήματα του Διαχειριστή Ενέργειας, μπορούν να εκπαιδευτούν στην αντιμετώπιση τόσο των υφιστάμενων, αλλά και των μελλοντικών τεχνικών επίθεσης που μπορεί να κάνει χρήση ένας επιτιθέμενος. Με το χαρακτηριστικό αυτό, αποτελούν μία ανοικτή και επεκτάσιμη βάση προς την κατεύθυνση ενός καθολικού αλγορίθμου για την επιτυχή αναγνώριση και αντιμετώπιση των επιθέσεων.

Ένα επίσης σημαντικό χαρακτηριστικό που πρέπει να ληφθεί υπόψιν, είναι ότι η αξιοποίηση των μεθόδων και των αλγορίθμων που καλούνται να αναπτυχθούν για την αντιμετώπιση του προβλήματος των επιθέσεων, θα πρέπει να συνδυασθεί με τα Κέντρα Λήψεως Απόφασης και Διαχείρισης, και εάν είναι δυνατόν να συμπεριληφθεί ως μέρος του υφιστάμενου συστήματος διαχείρισης ενέργειας. Επομένως, δεν αναφερόμαστε σε αυτόνομους και ανεξάρτητους αλγορίθμους ως προς το σύστημα AGC, αλλά σε ενσωματωμένους αλγορίθμους που εκτελούνται επί του συστήματος AGC (built-in realizations). Ο λόγος για την παραπάνω προσέγγιση οφείλεται στην ικανότητα των συστημάτων για γρήγορη λήψη αποφάσεων με αυτοματοποιημένο τρόπο, εφόσον εκτελούνται στον Διαχειριστή Ενέργειας, σε αντίθεση με τους χρονικούς περιορισμούς αντίδρασης του ανθρώπινου παράγοντα ή ενός εξωτερικού συστήματος, το οποίο θα πρέπει να επικοινωνήσει με τον Διαχειριστή Ενέργειας.

Επιπρόσθετα, έχει καταδειχθεί ότι η δημιουργία των αλγορίθμων ανίχνευσης και αντιμετώπισης των επιθέσεων, θα πρέπει να επιτρέπει την εκτέλεσή τους σε υπολογιστικά συστήματα εντός του διαχειριστή ενέργειας (EMS) χωρίς να απαιτείται επιπλέον χρήση ειδικού εξοπλισμού **[19**], μην εισάγοντας έτσι την επιπρόσθετη ανάγκη για νέα δομικά στοιχεία επί της υπάρχουσας δομής του δικτύου AGC **[21**], **[25**]. Κατά συνέπεια, μία επίσης σημαντική πρόκληση κατά τη διαδικασία ανάπτυξης και υλοποίησης αλγορίθμων αυτού του τύπου, είναι η ικανότητα ενσωμάτωσής τους στα υφιστάμενα συστήματα διαχείρισης και λήψης αποφάσεων στα δίκτυα ισχύος. Η χρήση υπολογιστικών συστημάτων συντελεί προς την παραπάνω κατεύθυνση, δεδομένου ότι κάθε αλγόριθμος που υλοποιείται για την επίλυση του προβλήματος, μπορεί πάντοτε να εκτελεστεί και να εξάγει αυτοματοποιημένα τα αποτελέσματά του εντός του Κέντρου Διαχείρισης.

Επίσης, ένα ακόμη σημαντικό ερευνητικό θέμα, αποτελεί ενδεχόμενα, η συναρμογή όλων των προτεινόμενων αλγορίθμων από τη βιβλιογραφία και την έρευνα για τα συστήματα AGC, και η ενσωμάτωσή τους σε έναν συνολικό αλγόριθμο δράσης **[32**]. Μία κοινή βάση για αυτήν την προσέγγιση δίνουν οι τεχνικές προσομοίωσης, οι οποίες μπορούν να βασιστούν σε δεδομένα πραγματικού χρόνου (real time measurements) από το δίκτυο, εφόσον η απαιτούμενη υπολογιστική ισχύς για την εκτέλεσή τους δε δημιουργεί χρονικές καθυστερήσεις (processing time delays), οι οποίες να είναι απαγορευτικές για την ταχύτητα λήψης αποφάσεων στο δίκτυο.

Επομένως, ο καθολικός αλγόριθμος θα αποτελέσει συνδυασμό μέρους των αλγορίθμων που έχουν ερευνητικά μελετηθεί, καθώς και άλλων που θα προκύψουν στο μέλλον. Οι εκτελέσεις αυτών των αλγορίθμων μπορεί να είναι παράλληλες και τα αποτελέσματά τους να αποτελούν σήματα προς χειρισμό και λήψη αποφάσεων από το Διαχειριστή Ενέργειας, ο οποίος θα σταθμίζει τα παραγόμενα αποτελέσματα.

6.2 Γενικά Συμπεράσματα

Το πρόβλημα της παραγωγής και διαχείρισης ισχύος παραμένει ένα ανοικτό και πολύ σημαντικό θέμα για τη σύγχρονη λειτουργία συστημάτων που λειτουργούν με ηλεκτρική ενέργεια. Δεδομένου ότι η ηλεκτρική ισχύς δεν μπορεί να αποθηκευτεί και θα πρέπει να διατίθεται άμεσα προς κατανάλωση, η εξισορρόπηση παραγωγής και ζήτησης παραμένει το κλειδί για την ευσταθή λειτουργία ενός δικτύου ισχύος. Η προσβολή από επιθέσεις για οποιονδήποτε λόγο και αιτία καθώς και οποιασδήποτε μορφής (όπως παρουσιάστηκε στις προηγούμενες ενότητες της εργασίας), συντελούν άμεσα στην καταστροφή της εξισορροπημένης λειτουργίας. Η διατάραξη της εξισορρόπησης αποσκοπεί είτε στο να πλήξει τη λειτουργία του δικτύου ισχύος είτε στο να προκαλέσει οικονομική ζημιά.

Οι κεντρικές δομές λήψης απόφασης (EMS) για έλεγχο μίας περιοχής/πολλών περιοχών βασίζουν τη λειτουργία τους στην εφαρμογή μετρήσεων και στη λήψη αποφάσεων. Οι αποφάσεις αποτελούν δράσεις – εντολές επί των συστημάτων AGC του δικτύου. Ένα πολύ σημαντικό πλήθος παραμέτρων επηρεάζουν τη λειτουργία του δικτύου ισχύος. Αυτό έχει ως αποτέλεσμα το πρόβλημα της ορθής λήψης αποφάσεων να είναι αρκετά σύνθετο κατά την εφαρμογή του.

Η πολυπλοκότητα των σύγχρονων δικτύων παραγωγής ισχύος σε συνδυασμό με την πολυπλοκότητα των τεχνικών εκδήλωσης επιθέσεων στα συστήματα αυτά, καταδεικνύουν ότι είναι δύσκολο για το σύστημα διαχείρισης, τόσο στο να προβλέψει τις επιθέσεις αυτές όσο και στο να μετριάσει τα αποτελέσματα επίδρασής τους.

Η έρευνα έχει κατατάξει τις επιθέσεις αυτές σε διάφορους τύπους προτείνοντας διαφορετικές και επικεντρωμένες τεχνικές για την αντιμετώπισή τους. Η ετερογένεια, όμως, όλων αυτών των ιδιαίτερων τύπων, καταδεικνύει ότι μάλλον οι διαδικασίες προσομοίωσης είναι οι καταλληλότερες για την τοποθέτηση και ανάλυση του προβλήματος των επιθέσεων στα δίκτυα ισχύος. Τα μαθηματικά μοντέλα περιγραφής των δικτύων ισχύος θα πρέπει να είναι όσο το δυνατόν πιο ακριβή, βοηθώντας στην ακρίβεια εφαρμογής των προσομοιώσεων στο δίκτυο. Επιπρόσθετα, τα αποτελέσματα των προσομοιώσεων μπορούν να χρησιμοποιηθούν ως βάση για την υιοθέτηση αρχιτεκτονικών σχεδιασμού για τα σύγχρονα δίκτυα ισχύος.

Η αύξηση της επεξεργαστικής ισχύος των συστημάτων δίνει τη δυνατότητα σε εκτέλεση όλο και πιο πολύπλοκων αλγορίθμων με μεγάλη αριθμητική ακρίβεια. Οι αλγόριθμοι αυτοί μπορούν να εκτελεστούν εντός των κέντρων Λήψης Απόφασης, συμβάλλοντας στην αμεσότητα των δράσεων καθώς και στον έλεγχο ακρίβειας των αποτελεσμάτων τους.

Το πρόβλημα της επιτυχούς παραγωγής και διαχείρισης της ηλεκτρικής ισχύος αποτελεί ένα ανοικτό ερευνητικό θέμα. Η λύση του προβλήματος θα προσεγγισθεί με τη χρήση και εφαρμογή νέων τεχνολογιών και αλγορίθμων, που θα μετεξελίξουν τα παραδοσιακά συστήματα AGC, σε κέντρα λήψης ευφυών αποφάσεων με αμεσότητα και ακρίβεια στη δράση τους.

Βιβλιογραφία

[1] Intelligent Automatic Generation Control, H. Bevrani, T. Hiyama, CRC Press © 2011.

[2] Power System Load Frequency Control, Classical and Adaptive Fuzzy Approaches, H. A. Yousef, CRC Press, © 2017.

[3] Power System Analysis and Design J. Duncan Glover, Mulucutla S. Sarma, Thomas J. Overbye, Cambridge, © 2012.

[4] Robust power system frequency control. H. Bevrani, Springer, © 2014.

[5] Advances in Power Systems and Energy Management, Lecture Notes in Electrical Engineering 436, Amik Garg, Akash Kumar Bhoi, Padmanaban Sanjeevikumar, K. K. Kamani, Springer, © 2018.

[6] Market operations in Electric Power Systems: Forecasting, Scheduling, and Risk Management, M. Shahidehpour, H. Yamin, Z. Li, New York: John Wiley & Sons, © 2002.

[7] Power generation, operation and control, A. J. Wood, B. F. Wollenberg, New York: John Wiley & Sons, © 1996.

[8] Electric power systems, D. Das, New Delhi, New Age International Ltd, © 2006.

[9] Power system stability and control, P. Kundur, New York: McGraw-Hill, © 1994.

[10] An Online Detection Framework for Cyber Attacks on Automatic Generation Control, T. Huang, B. Satchidanandan, P. R. Kumar, L. Xie, IEEE © 2018.

[11] A Survey of Recent Automatic Generation Control Strategies in Power Systems, Omveer Singh, P.Tiwari, Ibraheem and Arunesh Kr. Singh, © 2013.

[12] SCADA Wikipedia © 2020

[13] Έλεγχος Βιομηχανικών Διεργασιών – Συστήματα Εποπτικού Ελέγχου και Συλλογής Πληροφοριών (SCADA), ΤΕΙ Πειραιά

[14] Power System Monitoring and Control, H. Bevrani, M. Watanabe, Y. Mitani, IEEE Wiley, © 2014

[15] Open System Interconnection Model, Wikipedia © 2020

[16] A Comparative Analysis of Network Dependability, Fault-Tolerance, Reliability, Security, and Survivability, M. Al-Kuwaiti, N. Kyriakopoulos, S. Hussein

[17] Quality of Service: Delivering QoS on the Internet and in Corporate Networks, P. Ferguson, G. Huston, John Wiley, © 1998

[18] Cyber Attack Wikipedia © 2020

[19] Attack Detection and Identification for Automatic Generation Control Systems, A. Ameli, A. Hooshyar, F. Saadany, A. Youssef, 0885-8950, IEEE © 2018

[20] Effect of Communication Time-Delay Attacks on the Performance of Automatic Generation Control, K. Rahirni, A. Parchure, V. Centeno, R. Broadwater

[21] Model-Based Attack Detection and Mitigation for Automatic Generation Control, S. Sridhar, M. Govindarasu, IEEE, Vol 5 No 2, © 2014

[22] Authentication Wikipedia © 2020

[23] Authorization Wikipedia © 2020

[24] R. Tan *et al.*, "Modeling and mitigating impact of false data injection attacks on automatic generation control," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 7, pp. 1609–1624, Jul. 2017.

[25] 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.

[26] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Comput. Netw.*, vol. 57, no. 5, pp. 1344–1371, Apr. 2013.

[27] Emerging Technologies for Authorization and Authentication First International Workshop, Barcelina Spain Sep 7, 2018, Springer

[28] Assymetric Warfare Wikipedia © 2020

[29] A. F. Taha, J. Qi, J.Wang, and J. H. Panchal, "Risk mitigation for dynamic state estimation against cyber-attacks and unknown inputs," *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 886–899, Mar. 2018.

[30] VPN Wikipedia © 2020

[31] L. Cazorla, C. Alcaraz, and J. Lopez, "Cyber stealth attacks in critical information infrastructures," *IEEE Syst. J.*, vol. 12, no. 2, pp. 1778–1792, Jun. 2018.

[32] B. Genge, I. Kiss, and P. Haller, "A system dynamics approach for assessing the impact of cyber-attacks on critical infrastructures," *Int. J. Crit Infrastruct. Protection*, vol. 10, pp. 3–17, Sep. 2015.

[33] Y. W. Law, T. Alpcan, and M. Palaniswami, "Security games for risk minimization in automatic generation control," *IEEE Trans. Power Syst.*, vol. 30, no. 1, pp. 223–232, Jan. 2015.

[34] M. Vrakopoulou, P. M. Esfahani, K. Margellos, J. Lygeros, and G. Andersson, "Cyber-attacks in the automatic generation control," in *Cyber Physical Systems Approach to Smart Electric Grid*. New York, NY, USA: Springer, 2015, pp. 303–328.

[35] A. Ashok, P.Wang, M. Brown, and M. Govindarasu, "Experimental evaluation of cyber-attacks on automatic generation control using a CPS security testbed," in *Proc. IEEE Power Energy Soc. General Meeting*, Jul. 2015, pp. 1–5.

[36] P. Jovanovic and S. Neves, *Practical Cryptanalysis of the Open Smart Grid Protocol*. Berlin, Germany: Springer, 2015, pp. 297–316.

[37] K. Kursawe and C. Peters, "Structural weaknesses in the open smart grid protocol," in *Proc. 10th Int. Conf. Availability, Rel. Security*, Aug. 2015, pp. 1–10.

[38] QoS in modern networks, Wikipedia © 2020

[39] Jitter Wikipedia © 2020

[40] Locating Hidden Servers L. Overlier, P. Syverson, IEE Synposium of Security and Privacy, May 2006

[41] Network Monitoring Wikipedia © 2020

[42] CMOS Integrated Circuit Design Techniques, University of Ioannina, Dept. of computer Science and Eng.

[43] Vulnerability (computing) Wikipedia © 2020

[44] Analysis of Network Security Threats and Vulnerabilities by Development and Implementation of a Security Network Monitoring Solution, Master Thesis, N. Ahmad, M. K. Habib, Blekinge Institute of Technology, Sweden

[45] Machine Learning Algorithms and Applications M. Mohammed, M. Badruddin Khan, E. Bashier, CRC Press, © 2017

[46] Built IN Self-Test Wikipedia © 2020

[47] A Cyber Attack Modeling and Impact Assessment Framework, I. Kotenko, A. Chechulin, 5th International Conference on Cyber Conflict, © 2013

[48] Design, Simulation and Construction of IEEE 14-Bus Power System, J.A. Boudreaux, LSU Digital Commons

[49] Modeling Resilience in Electrical Distribution Networks, A. Torami, G. D'Agostino, A. Di Pietro, S. Giovinazzi, L. La Porta, DOI: 10.5772/intechopen.85917

[50] Computer and Information Security Handbook, J. R. VaccaMK, © 2009

[51] Learning from Data Streams, Processing Techniques in Sensor Networks, J. Gama, M. Gaber, Springer, © 2007

[52] The Design and Evaluation of Physical Protection Systems, M.L. Garcia, CPP, Elsevier © 2008

[53] A Review of Physical Layer Security Techniques for Internet of Things: Challenges and Solutions, L. Sun, Q. Du, entropy MDPI, Entropy 2018, 20, 730

[54] A Layered Security Model: OSI and Information Security, K. Pace, GSEC Practical Assignment, June 1 2004

[55] R. Tan, H. H. Nguyen, E. Y. S. Foo, D. K. Y. Yau, Z. Kalbarczyk, R. K. Iyer, and H. B. Gooi, "Modeling and mitigating impact of false data injection attacks on automatic generation control," IEEE Transactions on Information Forensics and Security, vol. 12, no. 7, pp. 1609–1624, July 2017.

[56] Sudha KR, Santhi RV. (2012). LFC of an interconnected reheat thermal system. Load frequency control of an interconnected reheat thermal system using type-2 fuzzy system including SME Sunits., 1383- 92.

[57] J. Park, and P. Chandramohan, "Static vs. dynamic recovery models for survivable distributed systems", *Proc. 37th Annual Hawaii International Conference on System Science*, Maui, HI, 5-8 Jan. 2004, IEEE Comp. Soc. Press, 2004, pp. 55-63.