ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ

ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΗΛΕΚΤΡΙΚΗΣ ΙΣΧΥΟΣ

Ανάλυση Μηχανισμών Πρόληψης και Ανίχνευσης Κυβερνοεισβολών στα Συστήματα Επικοινωνίας των Σύγχρονων Ηλεκτρικών Συστημάτων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Βασίλειος Αργυρός

Επιβλέπων : Γεώργιος Κορρές, Καθηγητής Ε.Μ.Π.

Αθήνα, Οκτώβριος 2023

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

Ανάλυση Μηχανισμών Πρόληψης και Ανίχνευσης Κυβερνοεισβολών στα Συστήματα Επικοινωνίας των Σύγχρονων Ηλεκτρικών Συστημάτων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Βασίλειος Αργυρός

Επιβλέπων : Γεώργιος Κορρές, Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την ….η Οκτωβρίου 2023.

.....	.....	.....
Γεώργιος Κορρές	Παύλος Γεωργιλάκης	Άρης-Ευάγγελος Δημέας
Καθηγητής Ε.Μ.Π	Καθηγητής Ε.Μ.Π	Επ. Καθηγητής Ε.Μ.Π

Αθήνα, Οκτώβριος 2023

.....

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

Περίληψη

Τα παραδοσιακά συστήματα παραγωγής, διανομής και διαχείρισης της ηλεκτρικής ενέργειας συνεχώς εξελίσσονται σε πιο προηγμένα και ευφυή δίκτυα. Η διαδικασία αυτή αποτελεί ένα σημαντικό και αναπτυσσόμενο πεδίο στον τομέα της ενεργειακής τεχνολογίας. Η δημιουργία ενός αποτελεσματικού, ασφαλούς, αειφόρου και ευφυούς ηλεκτρικού δικτύου απαιτεί την ενσωμάτωση εξελιγμένων τεχνολογιών πληροφορικής, επικοινωνιών και αυτοματισμού στα συστήματα ελέγχου ενεργειακών υποδομών. Έτσι, στα σύγχρονα ενεργειακά συστήματα, εισάγεται η έννοια του κυβερνοχώρου ως το πεδίο εκείνο που συναντώνται οι ψηφιακές τεχνολογίες, οι δικτυακές συνδέσεις και οι φυσικές υποδομές. Ο συνδυασμός των παραπάνω διαμορφώνει ένα κυβερνοφυσικό περιβάλλον, σύγχρονο ως προς τις λειτουργίες του και έξυπνο ως προς τον έλεγχο.

Η ανάπτυξη ενός σύγχρονου, αποδοτικού και αυτοματοποιημένου ηλεκτρικού συστήματος στοχεύει στην βελτιστοποίηση του ελέγχου και της απόδοσης της παραγωγής ηλεκτρικής ενέργειας. Από την άλλη όμως, τα δικτυακά και επικοινωνιακά συστήματα που εισάγονται, κάνουν το ενεργειακό σύστημα ακόμη πιο ευάλωτο απέναντι σε δυνητικές εξωτερικές απειλές. Η επικοινωνία στα ευφυή δίκτυα ηλεκτρικής ενέργειας χρησιμοποιεί συνήθως παραδοσιακά βιομηχανικά πρωτόκολλα, τα οποία δεν παρέχουν στο σύστημα μεγάλα επίπεδα ασφάλειας και είναι αρκετά ευάλωτα σε κυβερνοεπιθέσεις. Τέτοιες καταστάσεις μπορεί να κλονίσουν την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα των ψηφιακών δεδομένων. Αυτά τα δεδομένα, μεταδίδονται αδιάλειπτα μεταξύ του «έξυπνου» εξοπλισμού και βιομηχανικών εφαρμογών που εποπτεύουν την καθολική λειτουργία του συστήματος. Συνεπώς οι κυβερνοεπιθέσεις, ειδικά όταν προέρχονται από έμπειρους εισβολείς με καλή γνώση των πρωτοκόλλων του δικτύου, μπορούν να επηρεάσουν σε καταστροφικό βαθμό το σύστημα επικοινωνίας και κατ' επέκταση την φυσική υποδομή.

Την σημερινή εποχή, λόγω της μεγάλης αύξησης των κινδύνων στον κυβερνοχώρο, δημιουργείται μεγάλη ανάγκη για εξέλιξη των πληροφοριακών και δικτυακών συστημάτων με στόχο την αποτελεσματική προστασία του κυβερνοσυστήματος. Για αυτόν τον λόγο, η ανάδειξη της σημασίας της κυβερνοασφάλειας στα προηγμένα ηλεκτρικά δίκτυα αποτελεί και το βασικό ζητούμενο της παρούσας εργασίας. Η ασφάλεια των δικτύων και πρωτοκόλλων επικοινωνίας θα πρέπει να ενισχύεται επαρκώς τόσο μέσω πρόσθετων μηχανισμών πρόληψης, όσο και με την ανάπτυξη αποδοτικών συστημάτων ανίχνευσης επιθέσεων. Συνεπώς, το ζήτημα της κυβερνοασφάλειας στα ευφυή δίκτυα αναδεικνύεται ως ένα κρίσιμο ερευνητικό πεδίο. Μια σωστή αντιμετώπιση του ζητήματος οφείλει σε κάθε περίπτωση να περιλαμβάνει, βαθιά γνώση των πρωτοκόλλων επικοινωνίας που χρησιμοποιούνται, μελέτη των πιθανών κινδύνων και ανάλυση των διαθέσιμων μηχανισμών κυβερνοασφάλειας.

Λέξεις Κλειδιά

Ευφυή Δίκτυα Ενέργειας, Ενεργειακά Συστήματα Ελέγχου, Κυβερνοφυσικό Σύστημα, Βιομηχανικά πρωτόκολλα επικοινωνίας, Κυβερνοεπίθεση, Κυβερνοασφάλεια, Συστήμα Ανίχνευσης Εισβολής, Σύστημα Παρεμπόδισης Εισβολής.

ABSTRACT

Traditional systems for the generation, distribution, and management of electrical energy are continuously evolving into more advanced and intelligent grids. This process represents a significant and growing field in the energy technology sector. The creation of an efficient, secure, and sustainable smart grid requires the integration of advanced information, communication, and automation technologies into the energy control systems. Thus, in modern energy systems, the concept of the cyberspace is introduced as the domain, where digital technologies, network connections, and physical infrastructure converge. The combination of these elements ultimately shapes a cyber-physical environment, which includes contemporary functions and intelligent control methods.

The development of an advanced, efficient, and automated electrical system aims to optimize the control and performance of electricity generation. However, the introduced communication systems make the energy system more vulnerable to potential external threats. Communication in smart grids, typically relies on traditional industrial protocols, which do not provide the system with high levels of security and are susceptible to cyberattacks. Such situations could undermine the confidentiality, integrity, and availability of digital data. These data are continuously transmitted between the "smart" equipment and industrial applications that monitor the overall system operation. Especially, when cyberattacks are executed by experienced intruders with a good understanding of network protocols, they could have a devastating impact on the communication system and, consequently, on the physical infrastructure.

In the present era, due to the significant increase in cybersecurity risks, there is a pressing need for the enhancement of information and network systems to effectively protect the cybersecurity of energy infrastructure. For this reason, the primary goal of this work is to emphasize the importance of cybersecurity in advanced energy grids. The security of network protocols and communication systems should be significantly reinforced through both additional preventive measures and the development of efficient intrusion detection systems. Therefore, the issue of cybersecurity in smart grids emerges as a critical research field. A proper approach to this issue should include an in-depth understanding of the communication protocols used, an examination of potential risks, and an analysis of available cybersecurity mechanisms.

KEY WORDS

Smart Grid, Energy Control Systems, Cyber-Physical System, Industrial Communication Protocols, Cyber-attack, Cyber-security, Intrusion Detection Systems – IDS, Intrusion Prevention System -IPS.

ΕΥΧΑΡΙΣΤΙΕΣ

Η παράδοση της παρούσας διπλωματικής εργασίας ολοκληρώνει επιτυχώς τον κύκλο σπουδών μου στην Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών. Παρ' ότι ο δρόμος ήταν μακρύς και δύσκολος, η χαρά που φέρνει το τέλος της διαδρομής θα παραμείνει ανεξίτηλη στον χρόνο. Αναμφίβολα, η γνώση και οι εμπειρίες που αποκόμισα καθ' όλη την διάρκεια της φοίτησής μου αποτελούν απαραίτητα εφόδια για την επαγγελματική μου σταδιοδρομία. Από την μεριά μου, οφείλω να διατηρήσω τις αρχές, τις αξίες και τις ιδέες που απέκτησα στο Πολυτεχνείο με σκοπό να υπηρετήσω τις κοινωνικές ανάγκες από την σκοπιά του μηχανικού, αλλά και ενός ανθρώπου με ήθος και ευαισθησίες.

Συνοδοιπόροι σε αυτό το ταξίδι ήταν όλοι όσοι γνώρισα στο Αμφιθέατρο 1 και τους διαδρόμους της σχολής, με τους οποίους ανέπτυξα φιλικούς και συντροφικούς δεσμούς. Οι φίλοι μου, ο Κώστας, ο Νώντας, ο Μανώλης και ο Λεωνίδας, οι οποίοι ακολούθησαν διαφορετικές επαγγελματικές πορείες, αλλά η πρόοδος και οι επιτυχίες τους πάντα αποτελούσαν το μεγαλύτερο κίνητρο για να συνεχίσω την προσπάθεια προς τον τελικό στόχο. Οι σύντροφοι των ΑΝΑΦΗ, ο Πέτρος, ο Βασίλης και ο Βασίλης, ο Δημήτρης, ο Αντώνης, η Ευγενία, ο Κώστας, ο Γιάννης και πολλοί ακόμη, οι οποίοι μου έδωσαν το βήμα να μοιραστώ τις σκέψεις μου και μου έδειξαν τον συλλογικό δρόμο, ως τον τρόπο για να αντιμετωπίζω προβλήματα και δυσκολίες στην ζωή μου. Σε όλους αυτούς θα ήθελα να ευχηθώ μια επιτυχημένη και ευτυχισμένη ζωή και να τους πω ότι... σαν τα φοιτητικά μας χρόνια, δεν έχει!

Σε αυτό το σημείο θα ήθελα να ευχαριστήσω τους καθηγητές του τομέα μου, κύριο Νικόλαο Χατζηαργυρίου και Γεώργιο Κορρέ, που μου έδωσαν την ευκαιρία να μελετήσω σε βάθος το επιστημονικό πεδίο της κυβερνοασφάλειας στον τομέα της ηλεκτρικής ενέργειας, αλλά και για αυτά που μου δίδαξαν στα μαθήματά τους, τα οποία ήδη εφαρμόζω στην εργασία μου. Ένα μεγάλο ευχαριστώ στον υποψήφιο διδάκτορα και φίλο, Αντρέα Συρμακέση, του οποίου η επίβλεψη και στήριξη καθ' όλη την διάρκεια εκπόνησης της παρούσας εργασίας ήταν καθοριστική και επέφερε ένα πολύ όμορφο αποτέλεσμα.

Ένα μεγάλο ευχαριστώ στους γονείς μου, Δημήτρη και Μαρία, που θυσίασαν πάρα πολλά από την προσωπική τους ζωή ώστε να πετύχω τους στόχους μου και να φτάσω στο σημείο που βρίσκομαι τώρα. Η αγάπη και η στήριξή τους, σε όλη την διάρκεια της ζωής μου, ήταν και είναι ο βασικός παράγοντας αυτής της επιτυχίας.

Η διπλωματική μου εργασία αφιερώνεται επίσης στην παρέα μου, τον Δημήτρη και τον Δημήτρη που είναι στο πλευρό μου από τα μαθητικά μας χρόνια και μου δείχνουν συνεχώς την θετική πλευρά της ζωής, την Γεωργία και την Αννούλα που μαζί περάσαμε τα πιο όμορφα φοιτητικά καλοκαίρια, την Αθηνά και τον Νικόλα που είναι τα πιο λαμπρά αστέρια αυτής της ομάδας.

Η τελευταία και πιο σημαντική αφιέρωση είναι για την σύντροφό μου Αλίκη, η οποία έδωσε χρώμα στην καθημερινότητά μου και νόημα στους μελλοντικούς μου στόχους. Την ευχαριστώ πολύ που με υπέμεινε τους τελευταίους έξι μήνες σε μια δύσκολη περίοδο και της υπόσχομαι ότι μέλλον θα είναι γεμάτο από χαρές και ταξίδια.

Πίνακας περιεχομένων

1. Εισαγωγή στα Κυβερνοφυσικά Συστήματα Ενέργειας

1.1. Ευφυή Δίκτυα Ενέργειας

1.1.1. Η ανάγκη για σύγχρονα και ψηφιοποιημένα Ηλεκτρικά Δίκτυα

Οι παραδοσιακές υποδομές παραγωγής, διανομής και διαχείρισης της ηλεκτρικής ενέργειας, ολοένα και περισσότερο, εξελίσσονται σε πιο προηγμένα και «ευφυή δίκτυα» ("smart grids" κατά την αγγλική ορολογία) που επιτελούν έναν πιο σύγχρονο και περίπλοκο ρόλο, συγκριτικά με παλιότερα. Αυτή η εξελικτική διαδικασία αποτελεί ένα σημαντικό και αναπτυσσόμενο πεδίο στον τομέα της ενεργειακής τεχνολογίας. Συγκριτικά, τα παραδοσιακά δίκτυα ισχύος χρησιμοποιούνται κατά κύριο λόγο για τη μεταφορά ενέργειας από λίγες κεντρικές γεννήτριες σε ένα μεγάλο αριθμό χρηστών ή πελατών. Αντίθετα, ένα ευφυές δίκτυο χρησιμοποιεί δίκτυα διπλής κατεύθυνσης ενέργειας και πληροφοριών για να δημιουργήσει ένα αυτοματοποιημένο, κατανεμημένο και προηγμένο δίκτυο παροχής ενέργειας.

Οι αυξανόμενες απαιτήσεις της σύγχρονης κοινωνίας απαιτούν βελτίωση του κλασικού ηλεκτρικού δικτύου του 20ου αιώνα και προσαρμογή του στα νέα δεδομένα. Συνεπώς η **ανάπτυξη σύγχρονων και «έξυπνων» δικτύων απορρέει από μια σειρά απαιτήσεων και αναγκών** που έχουν διαμορφωθεί στον ενεργειακό τομέα τα τελευταία χρόνια. Πιο συγκεκριμένα, οι αυξημένες απαιτήσεις για διαρκή ενεργειακή απόδοση έχουν οδηγήσει στην ανάγκη για μια πιο αποτελεσματική διαχείριση της ηλεκτρικής ενέργειας. Μέσω της συλλογής, της ανάλυσης και της αξιοποίησης δεδομένων από το δίκτυο και της συμμετοχής των καταναλωτών, τα ευφυή δίκτυα επιτρέπουν την αποτελεσματική προσαρμογή της παραγωγής, της διανομής και της κατανάλωσης ενέργειας, με σκοπό την επίτευξη μιας καλύτερης λειτουργίας στο δίκτυο, τη βελτίωση της ενεργειακής απόδοσης και τη μείωση των εκπομπών αερίων του θερμοκηπίου. Επιπλέον, οι μεγάλες προκλήσεις που αντιμετωπίζει το σύγχρονο δίκτυο με τον αυξανόμενο αριθμό αξιοποίησης ανανεώσιμων πηγών ενέργειας, όπως η ηλιακή και η αιολική, απαιτούν νέες λύσεις για την ομαλή ενσωμάτωσή τους στην παραδοσιακή παραγωγή. Ακόμη, η αυξημένη ζήτηση ενέργειας, οι μεταβαλλόμενες καταναλωτικές συνήθειες και οι νέες απαιτήσεις των χρηστών απαιτούν πιο ευέλικτα δίκτυα που θα μπορούν να ανταποκρίνονται σε αυτές τις μεταβολές με αποδοτικό και αυτοματοποιημένο τρόπο. Αναμφίβολα, σε ένα σύγχρονο και ψηφιοποιημένο δίκτυο ενέργειας που αξιοποιεί προηγμένες επικοινωνιακές τεχνολογίες, η αξιοπιστία και η ασφαλής λειτουργία του αντιμετωπίζει και νέες προκλήσεις στον τομέα της κυβερνοασφάλειας. Η ανάδειξη αυτής της έννοιας αποτελεί και το βασικό ζητούμενο της παρούσας εργασίας.

Για να επιτευχθούν όλα τα παραπάνω, **τα ευφυή δίκτυα ενσωματώνουν τη χρήση εξελιγμένων τεχνολογιών πληροφορικής, επικοινωνιών και αυτοματισμού** για να παρέχουν έξυπνες λύσεις στην παραγωγή, μεταφορά, διανομή και κατανάλωση ηλεκτρικής ενέργειας. Η ανάπτυξη αυτών των τεχνολογιών βοηθά τα ευφυή δίκτυα στην δημιουργία ενός πιο αποτελεσματικού, ασφαλούς και αειφόρου ηλεκτρικού συστήματος που εξυπηρετεί τις ανάγκες των χρηστών και συμβάλλει στην ενεργειακή μετάβαση. Χρησιμοποιώντας σύγχρονες τεχνολογίες πληροφορικής, ένα ευφυές δίκτυο είναι ικανό να παρέχει ενέργεια με πιο αποδοτικούς τρόπους και να ανταποκρίνεται σε ευρεία γκάμα συνθηκών και γεγονότων. Έτσι αυτό, μπορεί να αντιδράσει σε γεγονότα που συμβαίνουν οπουδήποτε στο ηλεκτρικό δίκτυο (παραγωγή, μετάδοση, διανομή και κατανάλωση ενέργειας) και να εφαρμόσει τις ανάλογες στρατηγικές. Για παράδειγμα, όταν συμβεί

ένα περιστατικό βλάβης σε ένα μετασχηματιστή μεσαίας τάσης στο δίκτυο διανομής, το ευφυές δίκτυο μπορεί αυτόματα να αλλάξει τη ροή ενέργειας και να αποκαταστήσει την παροχή ηλεκτρικής ενέργειας προς κατανάλωση.

Παραδοσιακό Δίκτυο	Ευφυές Δίκτυο
Ηλεκτρομηχανολογικό	Ψηφιακό
Μονή κατεύθυνση επικοινωνίας	Διπλή κατεύθυνση επικοινωνίας
Κεντρική παραγωγή	Κατανεμημένη παραγωγή
Περιορισμένη χρήση αισθητήρων	Αισθητήρες σε όλο το σύστημα
Χειροκίνητη παρακολούθηση	Αυτόνομη και απομακρυσμένη παρακολούθηση
Χειροκίνητη αποκατάσταση	Αυτό-αποκατάσταση (self-healing)
Βλάβες και διακοπές ρεύματος	Προσαρμοστικότητα και απομονωμένη λειτουργία
Απλός και χειροκίνητος έλεγχος	Διευρυμένος και απομακρυσμένος έλεγχος
Ρύπανση του περιβάλλοντος	Πράσινη ενέργεια - ΑΠΕ

Σχήμα 1.1 – Σύγκριση παραδοσιακού δικτύου με ευφυή δίκτυα.

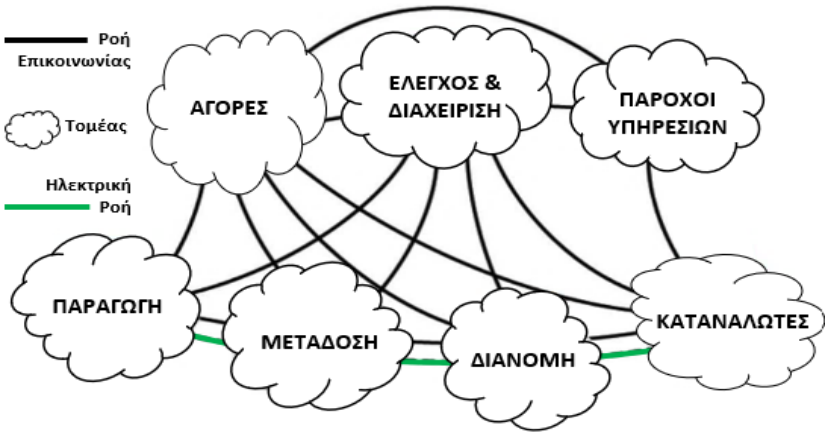
Ως Ευφυές Δίκτυο θεωρείται ένα ηλεκτρικό σύστημα που (α.) αξιοποιεί πληροφορίες προσφέροντας διπλή κατεύθυνση επικοινωνίας και χρησιμοποιεί (β.) κυβερνο-επικοινωνιακές τεχνολογίες και (γ.) υπολογιστική νοημοσύνη. Αυτή η περιγραφή καλύπτει ολόκληρο το φάσμα ενός ενεργειακού και έξυπνου συστήματος όπου όλα τα παραπάνω στοιχεία πρέπει να ενσωματώνονται με ολοκληρωμένο τρόπο σε όλη τη διάρκεια της παραγωγής, της μετάδοσης, της διανομής και της κατανάλωσης ηλεκτρικής ενέργειας. Το τελικό αποτέλεσμα θα πρέπει να είναι ένα ηλεκτρικό σύστημα καθαρό από θορύβους, ασφαλές, αξιόπιστο, ανθεκτικό στις μεταβολές, αποτελεσματικό και τελικά βιώσιμο για την παραγωγή και τον καταναλωτή.

Ειδικότερα, το ΕΔ πρόκειται για την αρμονική ένταξη συμπληρωματικών συστατικών, υποσυστημάτων, λειτουργιών και υπηρεσιών υπό τον έλεγχο προηγμένων διαχείρισης και ελέγχου. Η αρχική έννοια των Έξυπνων Δικτύων ξεκίνησε με την ιδέα μιας προηγμένης υποδομής μέτρησης (AMI) με στόχο την καλύτερη διαχείριση της ζήτησης και της ενεργειακής αποδοτικότητας. Ταυτόχρονα, ήταν αναγκαία η δημιουργία ενός αξιόπιστου -με δυνατότητες αυτό-αποκατάστασης (self-healing)- συστήματος προστασίας του δικτύου από κακόβουλες ενέργειες και φυσικές καταστροφές. Έτσι, το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας – NIST επικεντρώθηκε στην έρευνα για την ανάπτυξη ενός γενικού μοντέλου και αρχιτεκτονικής για τα ΕΔ, το οποίο θα ακολουθεί τους παρακάτω άξονες και απαιτήσεις:

- Βελτίωση της αξιοπιστίας και ποιότητας της ηλεκτρικής ενέργειας.
- Βελτιστοποίηση της χρήσης των εγκαταστάσεων και αποτροπή της κατασκευής εφεδρικών (υψηλού φορτίου) εργοστασίων ηλεκτρικής ενέργειας.
- Ενίσχυση της χωρητικότητας και της αποδοτικότητας των υφιστάμενων ηλεκτρικών δικτύων.
- Βελτίωση της ανθεκτικότητας σε διαταραχές με δυνατότητα προβλεπτικής συντήρησης και λειτουργία αυτοματοποιημένων ρυθμίσεων αυτο-αποκατάστασης (self-healing).
- Δυνατότητα διευρυμένης εγκατάστασης ανανεώσιμων πηγών ενέργειας.
- Προσαρμογή κατανεμημένων πηγών ενέργειας.
- Μείωση των εκπομπών αερίων θερμοκηπίου μέσω της ενεργοποίησης ηλεκτρικών μηχανών και νέων πηγών ενέργειας.
- Μείωση της κατανάλωσης πετρελαίου με τον περιορισμό μη αποδοτικής παραγωγής ενέργειας κατά τη διάρκεια υψηλής ζήτησης.
- Βελτίωση της ασφάλειας του δικτύου.

- Δυνατότητες μετάβασης σε ηλεκτρικά μέσα και σύγχρονες μορφές αποθήκευσης ενέργειας.
- Ποικιλία επιλογών για τους καταναλωτές.
- Δημιουργία νέων προϊόντων, υπηρεσιών και αγορών.

Για την δημιουργία μιας **τυποποιημένης αρχιτεκτονικής δικτύου**, το NIST παρείχε ένα μοντέλο (Σχήμα 1.2), το οποίο μπορεί να χρησιμοποιηθεί ως αναφορά για την ενσωμάτωση ΕΔ σε διάφορα μέρη του ηλεκτρικού συστήματος. Αυτό το μοντέλο είναι πολυεπίπεδο και περιλαμβάνει **επτά τομείς**, όπου ο καθένας μπορεί να απαρτίζεται από διάφορες συσκευές, επιμέρους συστήματα ή προγράμματα που λαμβάνουν αποφάσεις και ανταλλάσσουν απαραίτητες πληροφορίες για την εκτέλεση των δραστηριοτήτων τους.



Σχήμα 1.2 – Τυπική αρχιτεκτονική σύγχρονων ενεργειακών δικτύων

- **Αγορές**: Οι διαχειριστές της αγοράς ηλεκτρικής ενέργειας.
- **Έλεγχος και Διαχείριση**: Οι υπεύθυνοι για τη διαχείριση της μεταφοράς της ηλεκτρικής ενέργειας.
- **Πάροχοι υπηρεσιών**: Οι οργανισμοί που παρέχουν υπηρεσίες ηλεκτρικής ενέργειας σε πελάτες και επιχειρήσεις.
- **Μαζική παραγωγή**: Οι παραγωγοί ηλεκτρικής ενέργειας σε μεγάλες ποσότητες που παράγουν και αποθηκεύουν ενέργεια για μετέπειτα διανομή.
- **Μετάδοση**: Οι μεταφορείς της ηλεκτρικής ενέργειας σε μεγάλες αποστάσεις, οι οποίοι επίσης μπορούν να αποθηκεύσουν και να παράγουν ηλεκτρική ενέργεια.
- **Διανομή**: Οι διανομείς της ηλεκτρικής ενέργειας προς και από τους πελάτες.
- **Καταναλωτές/Πελάτες:** Οι τελικοί καταναλωτές της ηλεκτρικής ενέργειας, μπορούν να παράγουν, να αποθηκεύουν και να διαχειρίζονται τη χρήση της.

1.1.2. «Έξυπνα» συστήματα ενέργειας

Από σκοπιά τεχνικής ανάλυσης, θα επικεντρωθούμε σε **τρία βασικά έξυπνα συστήματα**, ο συνδυασμός των οποίων συνθέτει ένα ολοκληρωμένο σύστημα ευφυούς δικτύου. Το πρώτο σύστημα που θα αναλύσουμε είναι **το σύστημα έξυπνης υποδομής**, το **οποίο αποτελεί την ενεργειακή, πληροφοριακή και επικοινωνιακή υποδομή** που βρίσκεται στη βάση των έξυπνων δικτύων. Υποστηρίζει τη διπλή ροή ηλεκτρικής ενέργειας και πληροφοριών. Η "διπλή ροή ηλεκτρικής ενέργειας" υποδηλώνει ότι η παράδοση ηλεκτρικής ενέργειας δεν έχει μόνο μία κατεύθυνση, από την παραγωγή στην κατανάλωση. Για παράδειγμα, στο παραδοσιακό δίκτυο ηλεκτρικής ενέργειας, η ενέργεια παράγεται από το εργοστάσιο παραγωγής, μεταφέρεται μέσω του δικτύου μετάδοσης, του δικτύου διανομής και, τελικά, παραδίδεται στους χρήστες. Σε ένα ευφυές δίκτυο, η ηλεκτρική ενέργεια μπορεί επίσης να επιστραφεί στο δίκτυο από τους καταναλωτές διότι μπορούν πλέον να παράγουν ηλεκτρική ενέργεια χρησιμοποιώντας οικιακούς ηλιακούς συλλέκτες.

Συνεπώς θα πρέπει να υπάρχει δυνατότητα να την επιστρέψουν στο δίκτυο. Η διαδικασία αυτή μπορεί να είναι εξαιρετικά χρήσιμη σε ένα μικροδίκτυο (microgrid) που έχει απομονωθεί λόγω διακοπής ρεύματος. Σε μια τέτοια περίπτωση, το μικροδίκτυο μπορεί να λειτουργήσει, έστω σε μειωμένα επίπεδα, με τη βοήθεια της ενέργειας που τροφοδοτείται από τους υπόλοιπους χρήστες. Δεύτερον, **το σύστημα έξυπνης διαχείρισης παρέχει προηγμένες υπηρεσίες και λειτουργίες διαχείρισης και ελέγχου**. Με την ανάπτυξη νέων εφαρμογών και υπηρεσιών διαχείρισης που μπορούν να αξιοποιήσουν την εξέλιξη της τεχνολογίας, το δίκτυο συνεχίζει να γίνεται ακόμα πιο "έξυπνο" και προσαρμοσμένο σε νέα δεδομένα και δυνατότητες που δημιουργούνται μέρα με την μέρα. Ένα έξυπνο σύστημα διαχείρισης εκμεταλλεύεται την έξυπνη υποδομή για την επίτευξη διάφορων προηγμένων διοικητικών στόχων. Μέχρι σήμερα, οι περισσότεροι από αυτούς τους στόχους σχετίζονται με τη βελτίωση της ενεργειακής αποδοτικότητας, την ισορροπία προσφοράς και ζήτησης, τον έλεγχο των εκπομπών, τη μείωση του λειτουργικού κόστους και μεγιστοποίηση της γενικής ωφέλειας. Τρίτον, **το σύστημα έξυπνης προστασίας προσφέρει προηγμένη ανάλυση αξιοπιστίας του δικτύου**, **προστασία από σφάλματα και υπηρεσίες ασφάλειας και απορρήτου**. Αξιοποιώντας την έξυπνη υποδομή, το συνολικό ΕΔ πρέπει να αναπτύξει όχι μόνο ένα πιο έξυπνο σύστημα διαχείρισης, αλλά και ένα πιο έξυπνο σύστημα προστασίας. Το σύστημα αυτό θα πρέπει να είναι σε θέση να υποστηρίξει αποτελεσματικότερα και αποδοτικότερα μηχανισμούς προστασίας από βλάβες, να αντιμετωπίσει θέματα κυβερνοασφάλειας και να διαφυλάξει το απόρρητο.

Σε συνέχεια όσων αναφέρθηκαν παραπάνω γίνεται αντιληπτό ότι **το Έξυπνο Σύστημα Υποδομής εμπεριέχει** τρεις κατηγορίες (ενεργειακή, πληροφοριακή και επικοινωνιακή υποδομή), για τις οποίες ορίζονται τα αντίστοιχα **τρία έξυπνα υποσυστήματα**: το έξυπνο ενεργειακό υποσύστημα, το έξυπνο υποσύστημα πληροφοριών και το υποσύστημα έξυπνης επικοινωνίας. Τα υποσυστήματα αυτά αναλύονται παρακάτω και αναφέρονται αντίστοιχα στις εξής βασικές λειτουργίες: (α) την προηγμένη παραγωγή, την διάθεση και κατανάλωση ηλεκτρικής ενέργειας, (β) την προηγμένη μέτρηση, παρακολούθηση και διαχείριση των πληροφοριών και (γ) προηγμένες τεχνολογίες επικοινωνίας.

Α. «Έξυπνο» Υποσύστημα Ενέργειας

Γνωρίζουμε ήδη ότι στα παραδοσιακά ηλεκτρικά δίκτυα, η παραγόμενη ηλεκτρική ενέργεια ανυψώνεται σε υψηλή τάση για τη μετάδοσή της ώστε το δίκτυο μετάδοσης να μεταφέρει την ισχύ για μεγάλες αποστάσεις προς τους υποσταθμούς. Κατά την άφιξη σε έναν υποσταθμό, οι Μ/Σ τάσης υποβαθμίζουν την εισαγόμενη τάση στα επίπεδα τάσης διανομής και καθώς η ισχύς εξέρχεται από τον υποσταθμό, έπειτα εισέρχεται στο δίκτυο διανομής. Τελικά, κατά την άφιξη στην τοποθεσία χρήσης, η ισχύς μειώνεται ξανά από την τάση διανομής στην απαιτούμενη τάση χρήσης. Αντίθετα με το παραδοσιακό δίκτυο, η το πρότυπο παραγωγής και διάθεσης της ενέργειας σε ένα ΕΔ είναι πιο ευέλικτο, καθώς η παραγωγή ενέργειας μπορεί να συμβεί σε κάθε επιμέρους δίκτυο της παραδοσιακής αλυσίδας (πχ. χρησιμοποιώντας ηλιακούς συλλέκτες ή ανεμογεννήτριες).

Η κυρίαρχη μορφή παραγωγής ισχύος σε ένα ΕΔ είναι η **Κατανεμημένη Παραγωγή** (Distributed Generation), η οποία εκμεταλλεύεται συστήματα κατανεμημένων ενεργειακών πόρων (DERs) όπως φωτοβολταϊκά πάνελ και μικρές ανεμογεννήτριες. Αυτά συνήθως παράγουν ισχύ σε μικρή κλίμακα (3 kW - 10.000 kW) και ο σκοπός τους είναι η βελτίωση της ποιότητας και της αξιοπιστίας της παραγωγής. Ωστόσο, η υλοποίηση στην πράξη μιας κατανεμημένης παραγωγικής διαδικασίας δεν είναι μια εύκολη πρόταση λόγω πολλών αιτίων. Οι μεγάλες

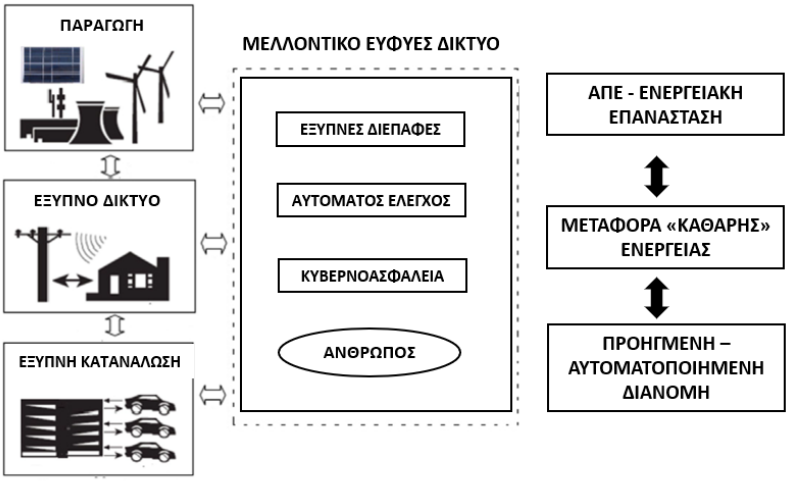
διακυμάνσεις παραγωγής των ανανεώσιμων πηγών και η μεγάλη αναντιστοιχία της παραγωγής με τα καταναλωτικά πρότυπα είναι τα δύο βασικά προβλήματα που αντιμετωπίζονται έως σήμερα, εάν συμμεριστούμε ότι το ζήτημα της βέλτιστης και αποδοτικής αποθήκευσης της ενέργειας δεν έχει ξεπεραστεί. Ένα επιπλέον ζήτημα είναι τα υψηλά λειτουργικά κόστη της κατανεμημένης παραγωγής σε σύγκριση με αυτό των παραδοσιακών κεντρικών εργοστασίων ισχύος μεγάλης κλίμακας. Παρ' όλα αυτά, λαμβάνοντας υπόψη τα νέα μεγάλα οφέλη που προκύπτουν ως προς την ποιότητα της ισχύος αλλά και την μελλοντική μείωση του κόστους παραγωγής και συντήρησης των κατανεμημένων μονάδων παραγωγής, το πρόβλημα αυτό θα ξεπεραστεί με την πάροδο των χρόνων. Σε κάθε περίπτωση, η υιοθέτηση κατανεμημένων παραγωγών για τη δημιουργία ενός πιο αποκεντρωμένου συστήματος παροχής ισχύος αποτελεί κεντρική στρατηγική σε πανευρωπαϊκή κλίμακα. Συνεπώς, η διείσδυση των ανανεώσιμων πηγών ενέργειας στο ηλεκτρικό σύστημα, σήμερα, αυξάνεται με μεγάλους ρυθμούς. Για να επιτευχθεί στο μέλλον **η καθολική μετάβαση προϋποθέτει τέσσερα βασικά στάδια**:

1. Η προσαρμογή της κατανεμημένης παραγωγής στο τρέχον ηλεκτρικό σύστημα.
2. Η εισαγωγή ενός αποκεντρωμένου συστήματος που θα συνεργάζεται με το κεντρικό σύστημα παραγωγής.
3. Η παροχή περισσότερης ισχύος από τους κατανεμημένους παραγωγούς και περιορισμός της κεντρικής παραγωγής.
4. Η εισαγωγή της κατανεμημένης παραγωγής σε μεγάλη κλίμακα θα αλλάξει ριζικά την παραδοσιακή μεθοδολογία σχεδιασμού του ηλεκτρικού δικτύου.

Στον τομέα της μετάδοσης ισχύος, τόσο οι προκλήσεις στην ενεργειακή υποδομή (αυξανόμενες απαιτήσεις φορτίου, γρήγορη φθορά εξαρτημάτων, κ.λπ.) όσο και οι διάφορες καινοτόμες τεχνολογίες (νέα υλικά, προηγμένη ηλεκτρονική ισχύος και σύγχρονες τεχνολογίες επικοινωνίας) οδηγούν στην ανάγκη για **ανάπτυξη ευφυών δικτύων μετάδοσης ισχύος**. Για να θεωρηθεί ολοκληρωμένο ένα τέτοιο ευφυές δίκτυο, εκτός από τις λειτουργίες μετάδοσης ισχύος, οφείλει επίσης να περιλαμβάνει έξυπνα κέντρα ελέγχου και έξυπνους υποσταθμούς. Τα έξυπνα κέντρα ελέγχου, για παράδειγμα, εισάγουν προηγμένες δυνατότητες ελέγχου, παρακολούθησης, αναλύσεις και οπτικοποίηση των διεργασιών στο δίκτυο μεταφοράς. Αντίστοιχα, τα ευφυή δίκτυα μετάδοσης ισχύος έχουν ως βάση την υπάρχουσα υποδομή μετάδοσης, ενσωματώνοντας νέες τεχνολογίες υλικών, συσκευών, αισθητήρων, επικοινωνιών, επεξεργασίας σημάτων κ.ά. για την βέλτιστη αξιοποίηση της μεταφερόμενης ισχύος και την ενίσχυση της ασφάλειας και αξιοπιστίας του συστήματος. Με την σειρά τους, οι έξυπνοι υποσταθμοί υψηλής τάσης περιλαμβάνουν σύγχρονες λειτουργίες αυτό-αποκατάστασης, ψηφιοποίησης και συντονισμού των διεργασιών. Με την υποστήριξη αυτών των χαρακτηριστικών, ένας έξυπνος υποσταθμός είναι σε θέση να ανταποκρίνεται γρήγορα και να παρέχει αυξημένη ασφάλεια για τους χειριστές. Ακόμη με την χρήση κοινής ψηφιακής πλατφόρμας, το τελικό και ολοκληρωμένο ευφυές δίκτυο μετάδοσης ισχύος μπορεί να προσφέρει τεράστια ευελιξία στον έλεγχο του δικτύου και στην ενίσχυση της ανθεκτικότητάς του.

Για την διανομή ηλεκτρικής ενέργειας στους τελικούς χρήστες, **το ζήτημα ενός σύγχρονου δικτύου διανομής ισχύος** γίνεται αρκετά πιο σύνθετο. Η ενσωμάτωση πολλών παραγωγών στο έξυπνο κατανεμημένο δίκτυο, ναι μεν αυξάνει την ευελιξία του συστήματος για την παραγωγή ισχύος ωστόσο περιπλέκει τον έλεγχο της ροής ισχύος, πράγμα που απαιτεί βαθύτερη έρευνα για την ανάπτυξη πιο έξυπνων μηχανισμών διανομής ισχύος. Το δίκτυο διανομής είναι η τελευταία φάση στη μετάδοση της ισχύος προς τους καταναλωτές, όπου η πρωτεύον και δευτερεύον παροχή ισχύος παρέχει ηλεκτρική ενέργεια σε βιομηχανικούς, εμπορικούς και

οικιακούς καταναλωτές. Σε αυτήν την διαδικασία έχουν αναπτυχθεί έξυπνες υποστηρικτικές μέθοδοι με δυνατότητες παρακολούθησης χρησιμοποιώντας συνδέσεις επικοινωνίας μεταξύ παρόχων και καταναλωτών, έξυπνων μετρητών, συστημάτων AMI και διαχείρισης ενέργειας. Οι αντίστοιχες λειτουργίες αυτοματισμού περιλαμβάνουν δυνατότητες αυτοματοποιημένης εκμάθησης, αυτόματης χρέωσης, ανίχνευσης βλαβών, αποκατάστασης, αναδιαμόρφωσης της παροχής και βελτιστοποίησης στην μεταφορά φορτίου.



Σχήμα 1.3 – Μελλοντικό Ευφυές Δίκτυο

Β. «Έξυπνο» Υποσύστημα Πληροφοριών

Το σύγχρονο ΕΔ είναι συνυφασμένο με έννοιες όπως ο αυτόματος έλεγχος και η απομακρυσμένη παρακολούθηση του ηλεκτρικού συστήματος. Συνεπώς, η εξέλιξή του εξαρτάται σε μεγάλο βαθμό από προηγμένα υπολογιστικά συστήματα παρακολούθησης, ανάλυσης, βελτιστοποίησης και ελέγχου από κεντρικά σημεία, για τις υπηρεσίες διανομής και μετάδοσης. Για να επιτευχθεί αυτό θα πρέπει να εξασφαλίζεται η ψηφιοποίηση της πληροφορίας, η διαλειτουργικότητα στην ανταλλαγή δεδομένων και η ενσωμάτωση με υπάρχουσες και μελλοντικές συσκευές, συστήματα και εφαρμογές. Επομένως, ένα έξυπνο υποσύστημα πληροφοριών χρησιμοποιείται για να υποστηρίξει την **παραγωγή, μοντελοποίηση, ενσωμάτωση, ανάλυση και βελτιστοποίηση πληροφοριών**. Στα πλαίσια των ΕΔ τα πληροφοριακά συστήματα περιλαμβάνουν τους εξής τομείς:

- **Μέτρηση Πληροφοριών**: Η έξυπνη μέτρηση είναι ο σημαντικότερος μηχανισμός που χρησιμοποιείται για την απόκτηση πληροφοριών ελέγχου και συμπεριφοράς των συσκευών. Τα προηγμένα συστήματα αυτόματης μέτρησης AMI συλλέγουν συνεχώς, σε έναν κεντρικό σύστημα βάσης δεδομένων, τα διάφορα διαγνωστικά δεδομένα και δεδομένα κατάστασης από τους μετρητές και αναλυτές ενέργειας, στην λογική επικοινωνίας διπλής κατεύθυνσης. Έτσι όλες αυτές οι πληροφορίες είναι διαθέσιμες σε πραγματικό χρόνο επιτρέποντας τη βέλτιστη λειτουργία του συστήματος και διαχείριση της ζήτησης από τους καταναλωτές.
- **Παρακολούθηση Πληροφοριών:** Η αποτελεσματική παρακολούθηση των πληροφοριών προϋποθέτει την χρήση δικτύων αισθητήρων και μονάδων μέτρησης φάσης, για την αξιολόγηση των μηχανολογικών και ηλεκτρικών συνθηκών στις γραμμές μεταφοράς. Έτσι τα κέντρα ελέγχου αποκτούν μια πλήρη εικόνα του συστήματος ηλεκτρικής ενέργειας, σε πραγματικό χρόνο,

έχοντας δυνατότητες έγκαιρης διάγνωσης βλαβών και αρά καθορισμού κατάλληλων μέτρων αντιμετώπισης. Από την άλλη, οι μετρητές φάσης (PMU) ελέγχουν την κατάσταση και ποιότητα της ηλεκτρικής ενέργειας που μεταφέρεται (γωνία, κυματομορφές, κλπ.) προσδίδοντας μια εξελιγμένη μορφή παρακολούθησης του δικτύου.

- **Διαχείριση Πληροφορίας**: Τέλος, οι μεγάλες ποσότητες δεδομένων που δημιουργούνται από τους παραπάνω τομείς διαμορφώνουν μια ξεχωριστή ενότητα, που αφορά την αποτελεσματική διαχείριση της πληροφορίας. Τα ΕΔ οφείλουν να υποστηρίζουν προηγμένες λειτουργίες διαχείρισης της πληροφορίας, όπως η μοντελοποίηση δεδομένων, η ανάλυση πληροφοριών και η βελτιστοποίηση.

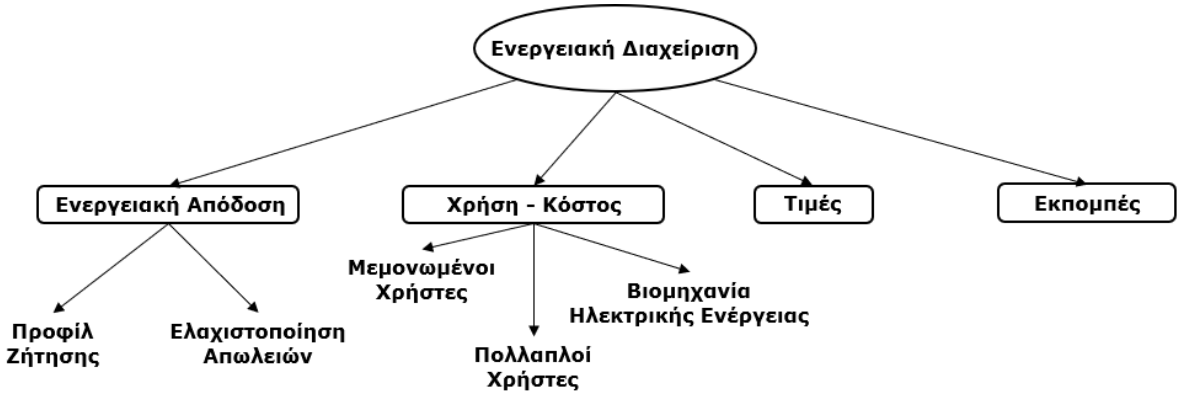
Γ. «Έξυπνο» Υποσύστημα Επικοινωνιών

Το τελευταίο μέρος του συστήματος υποδομής αφορά την **επικοινωνιακή συνδεσιμότητα και μετάδοση των παραπάνω πληροφοριών** μεταξύ των διάφορων συστημάτων, συσκευών και εφαρμογών που απαρτίζουν την συνολική υποδομή. Εδώ αποφασίζονται οι στρατηγικές και οι τεχνολογίες επικοινωνίας και δικτύωσης που θα χρησιμοποιηθούν για να ικανοποιήσουν τις απαιτήσεις του εκάστοτε ΕΔ. Διάφορες επιλογές δικτύων επικοινωνίας μπορεί να είναι: (α) εταιρικοί δίαυλοι επικοινωνίας που συνδέουν εφαρμογές κέντρου ελέγχου, αγορές και γεννήτριες, (β) δίκτυα WAN που συνδέουν γεωγραφικά απομακρυσμένες τοποθεσίες, (γ) δίκτυα πεδίου που συνδέουν τις διάφορες ηλεκτρονικές συσκευές, (δ) δίκτυα στην περιοχή των καταναλωτών/πελατών. Οι παραπάνω στρατηγικές επικοινωνίας μπορούν, πλέον, να υλοποιηθούν διάφορες τεχνολογίες, είτε ενσύρματές είτε ασύρματες ανάλογα με τις ιδιαιτερότητες της κάθε εφαρμογές.

Δ. «**Έξυπνο» Σύστημα Διαχείρισης**

Η βελτίωση της ενεργειακής αποδοτικότητας, η μείωση του κόστους λειτουργίας, η ισορροπία της ζήτησης και προσφοράς, ο έλεγχος εκπομπών και η μεγιστοποίηση της χρησιμότητας της παραγόμενης ηλεκτρικής ενέργειας δεν εξασφαλίζονται μόνο από ευφυή ενεργειακά, πληροφοριακά και επικοινωνιακά συστήματα. Παράλληλα με την ανάπτυξη του ενός έξυπνου συστήματος υποδομής, χρειάζονται νέα έξυπνα συστήματα και εφαρμογές διαχείρισης που θα μπορούν να αξιοποιήσουν τα αναβαθμισμένα χαρακτηριστικά της προηγμένης υποδομής και θα εξασφαλίζουν ότι το δίκτυο θα συνεχίσει να γίνεται "εξυπνότερο". Το παράδειγμα του προβλήματος ζήτησης και προσφοράς είναι χαρακτηριστικό και αναδεικνύει την σημασία της διαχείρισης της ενέργειας. Παραδοσιακά, η επίτευξη της ισορροπίας μεταξύ προσφοράς-ζήτησης ήταν ένα ανυπέρβλητο εμπόδιο σε μακροπρόθεσμη κλίματα, διότι το συνολικό ποσό ζήτησης ισχύος από τους χρήστες μπορεί να έχει μια πολύ ευρεία κατανομή πιθανοτήτων. Αυτό, απαιτεί εφεδρικά – και σε κατάσταση ετοιμότητας - εργοστάσια γεννητριών για την άμεση ανταπόκριση στην γρήγορα μεταβαλλόμενη χρήση ενέργειας. Αυτές οι προσπάθειες ανταπόκρισης στη ζήτηση δεν πετυχαίνουν πάντα και έχουν ως πιθανές επιπτώσεις την μείωση της τάσης ή διακοπές ηλεκτρικής ενέργειας. Αντίθετα, **ένα ευφυές δίκτυο διαχειρίζεται την ζήτηση ενέργειας ως αντίδραση στις συνθήκες προσφοράς**. Δηλαδή προσπαθεί να ταιριάξει την κατανάλωση με τη διαθέσιμη προσφορά χρησιμοποιώντας τεχνολογίες ελέγχου ή πείθοντας τους καταναλωτές (πχ. μέσω μεταβλητής τιμολόγησης) να μεταβάλλουν τις καταναλωτικές συνήθειες. Συνεπώς ένας έξυπνος μετρητής στην πλευρά του καταναλωτή μπορεί να μειώσει την κατανάλωση απενεργοποιώντας μη ουσιαστικές συσκευές κατά τη διάρκεια αιχμών (περίοδοι υψηλής ζήτησης). Οι διάφορες διεργασίες κατά την Έξυπνη Διαχείριση έξυπνη διαχείριση εστιάζουν κυρίως στους εξής τρεις στόχους:

1. Βελτίωση της ενεργειακής απόδοσης και του προφίλ ζήτησης.
2. Βελτιστοποίηση χρήσης, κόστους και σταθεροποίηση τιμών.
3. Έλεγχος εκπομπών.



Σχήμα 1.4 – Τομείς εργασιών «Έξυπνου» Συστήματος Διαχείρισης

Ε. «**Έξυπνα» Σύστημα Προστασίας**

Είναι επιτακτικό σε κάθε Ευφυές Δίκτυο να αναπτύσσονται διατάξεις ασφαλείας και προστασίας τόσο της υποδομής, όσο και της πληροφορίας και τον επικοινωνιών. Ένα **Έξυπνο Σύστημα Προστασίας** οφείλει να αντιμετωπίζει όχι μόνο τις ακούσιες βλάβες του δικτύου από σφαλμάτων χρηστών, πιθανές βλάβες του εξοπλισμού ή φυσικές καταστροφές, αλλά και πιθανές κυβερνοεπιθέσεις, που μπορούν να προκληθούν από υπαλλήλους ή εξωτερικούς κατασκόπους. Οι μηχανισμοί αυτοί μπορεί να στοχεύουν είτε στην πρόληψη ενάντια σε πιθανές βλάβες είτε στην ανίχνευση και αντιμετώπιση σφαλμάτων που ήδη έχουν συμβεί στο σύστημα. Σε κάθε περίπτωση, το σύστημα προστασίας θα πρέπει να εξασφαλίζει τρεις βασικούς άξονες: (α.) την Αξιοπιστία του Συστήματος όταν αντιμετωπίζει βλάβες, (β.) την συνολική **Ασφάλεια και Ιδιωτικότητα** όλων των διεργασιών και (γ.) την **ασφαλή Μετάδοση των Πληροφοριών**.

Το κύριο ζητούμενο των επόμενων κεφαλαίων της παρούσας εργασίας επικεντρώνεται στον τρίτο άξονα, καθώς αποτελεί ένα σχετικά πρόσφατο πεδίο έρευνας για τα ενεργειακά συστήματα, αλλά ταυτόχρονα κομβικό για την ασφάλεια και αξιοπιστία των συστημάτων επικοινωνίας στα σύγχρονα βιομηχανικά περιβάλλοντα παραγωγής ηλεκτρικής ενέργειας.

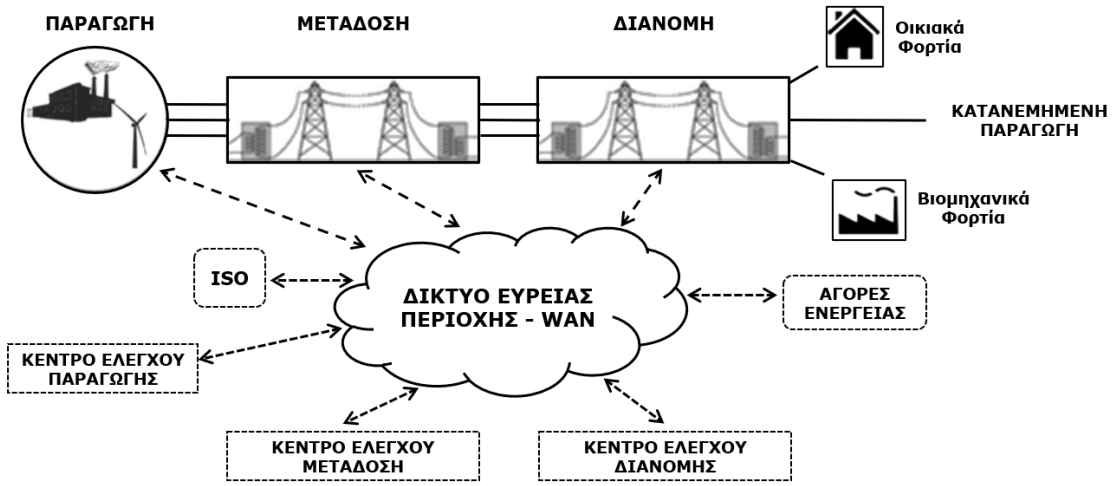
1.2. Υποδομή και Ασφάλεια Κυβερνοφυσικών Συστημάτων

1.2.1. Ευφυή Δίκτυα και Κυβερνησιμότητα

Η διαρκής αυξανόμενη ζήτηση για μια αξιόπιστη ηλεκτρική ενέργεια σε συνδυασμό με τις πολυάριθμες τεχνολογικές εξελίξεις διαμορφώνουν το παρόν και το μέλλον των συστημάτων ηλεκτρικής ενέργειας με τρόπο που είναι συνυφασμένος με έξυπνα και αυτοματοποιημένα δίκτυα. Η ανάπτυξη των ΕΔ, σήμερα, θα επεκτείνει τις υφιστάμενες δυνατότητες των συστημάτων παραγωγής, μετάδοσης και διανομής δημιουργώντας μια υποδομή, ικανή να ανταποκριθεί στις μελλοντικές απαιτήσεις για την κατανεμημένη παραγωγή, τις ανανεώσιμες πηγές ενέργειας, τα ηλεκτρικά οχήματα και την βέλτιστη διαχείριση της ζήτησης ηλεκτρικής ενέργειας. Παρά το γεγονός ότι οι διάφορες προηγμένες τεχνολογίες που αναφερθήκαμε προηγουμένως χρησιμοποιούνται για να επιτευχθούν οι παραπάνω στόχοι, παρουσιάζουν επίσης αυξημένη εξάρτηση από τον κυβερνοχώρο και τα όποια επικίνδυνα μονοπάτια ανοίγει αυτό το νέο πεδίο.

Ο όρος "κυβερνοχώρος" αναφέρεται στο πεδίο όπου συναντώνται οι ψηφιακές τεχνολογίες, οι δικτυακές συνδέσεις και οι φυσικές υποδομές, ο συνδυασμός των οποίων διαμορφώνει ένα κυβερνοφυσικό (cyber-physical) περιβάλλον. Στα πλαίσια του Ευφυούς Δικτύου, ο κυβερνοχώρος συνδυάζει το (φυσικό) ηλεκτρικό δίκτυο με προηγμένες τεχνολογίες και αυτοματοποιημένα συστήματα ελέγχου και διαχείρισης, όπως μονάδες μέτρησης φάσης, συστήματα μέτρησης ευρείας ζώνης, υποδομές AMI ή την γενικότερη αυτοματοποίηση των υποσταθμών. **Η εξάρτηση του ΕΔ από τον κυβερνοχώρο** είναι σημαντική καθώς η παρακολούθηση, ο έλεγχος, η διαχείριση και η ανταλλαγή δεδομένων μεταξύ των διάφορων συστημάτων και συσκευών του φυσικού δικτύου απαιτούν την ενσωμάτωση των παραπάνω ψηφιακών τεχνολογιών. Αυτό, αναπόφευκτα, θα έχει ως αποτέλεσμα την αυξημένη ευαισθησία σε κυβερνοεπιθέσεις και κακόβουλες παρεμβολές στις συνδέσεις επικοινωνίας, στις ψηφιακές εφαρμογές και κατ' επέκταση στη γενική λειτουργία του δικτύου ηλεκτρικής ενέργειας.

Μια ολοκληρωμένη προσέγγιση για την κατανόηση των ζητημάτων ασφάλειας στα ΕΔ θα πρέπει οπωσδήποτε να λαμβάνει υπόψιν τις αλληλεπιδράσεις των διαφόρων Κυβερνο-Φυσικών Συστημάτων (ΚΦΣ). Χωρίς αυτή την προϋπόθεση δεν θα μπορούσαν να αξιολογηθούν κατάλληλα οι επιπτώσεις πιθανών κυβερνοεπιθέσεων και η αποτελεσματικότητα των αντίμετρων που αναπτύσσονται. **Η έννοια της ασφάλειας για τα ΚΦΣ** των δικτύων ηλεκτρικής ενέργειας περιλαμβάνει τον λειτουργικό συνδυασμό των εξής στοιχείων: (α.) Τα φυσικά συστατικά και οι εφαρμογές ελέγχου, (β.) οι κυβερνο-υποδομές που απαιτούνται για την υποστήριξη των απαραίτητων υπηρεσιών σχεδιασμού, λειτουργίας και αγοράς, (γ.) η συσχέτιση μεταξύ των κυβερνοεπιθέσεων και των επιπτώσεών τους στο φυσικό σύστημα και (δ.) τα αντίμετρα για τη μείωση των κινδύνων που επιφέρουν οι αντίστοιχες απειλές.



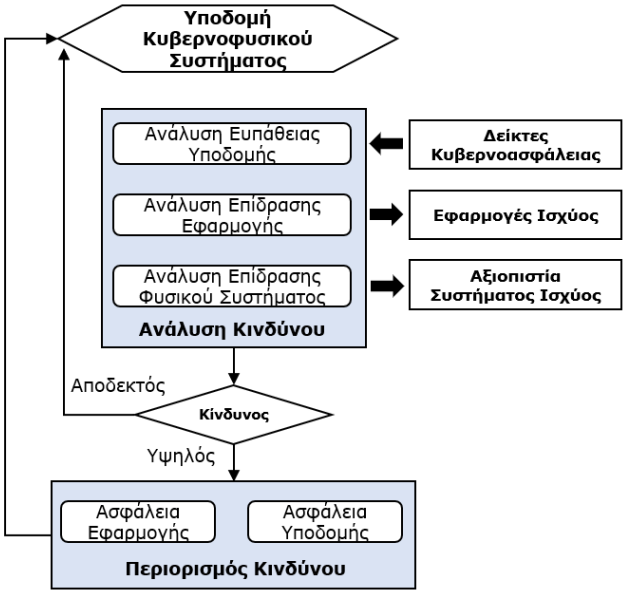
Σχήμα 1.5 – Η Κυβερνοφυσική υποδομή του ηλεκτρικού δικτύου

Όλα τα κυβερνοσυστήματα αποτελούνται από ηλεκτρονικές συσκευές πεδίου, δίκτυα επικοινωνίας, συστήματα αυτοματισμού υποσταθμών και κέντρα ελέγχου, τα οποία είναι ενσωματωμένα σε ολόκληρο το φυσικό δίκτυο. Το κέντρο ελέγχου είναι υπεύθυνο για την παρακολούθηση σε πραγματικό χρόνο, τον έλεγχο και την λήψη αποφάσεων για την λειτουργία ολόκληρου του συστήματος. Από την άλλη, οι ανεξάρτητοι φορείς λειτουργίας (ISOs) πραγματοποιούν τον συντονισμό μεταξύ εταιρειών ενέργειας, αποστέλλουν εντολές στα κέντρα ελέγχου τους και υποστηρίζουν τις αγορές ενέργειας διαθέτοντας κατάλληλες λειτουργίες που βασίζονται στην πραγματική παραγωγή, μετάδοση και ζήτηση ισχύος.

Στην συνέχεια σχολιάζονται οι αβεβαιότητες που υπάρχουν για την ασφάλεια ενός ευφυούς δικτύου εξετάζοντας τον συσχετισμό μεταξύ των εφαρμογών ελέγχου ισχύος και των βασικών κυβερνο-συστημάτων.

1.2.2. Αξιολόγηση κινδύνου και επιπτώσεις στο σύστημα ισχύος

Η πολυπλοκότητα στην σχέση του κυβερνοσυστήματος και του φυσικού συστήματος ισχύος μπορεί να παρουσιάζει πολλές φορές ακατανόητες εξαρτήσεις στο σύστημα. Η διεξαγωγή αξιόπιστων αξιολογήσεων κινδύνου απαιτεί την ανάπτυξη μοντέλων που παρέχουν μια βάση για την ανάλυση όλων των εξαρτήσεων και την ποσοτικοποίηση των αντίστοιχων επιπτώσεων. Αυτή η συσχέτιση των κύριων χαρακτηριστικών μεταξύ κυβερνοχώρου και φυσικής υποδομής θα βοηθήσει στην αξιολόγηση των κινδύνων και στις διαδικασίες αντιμετώπισης αυτών. Στην συνέχεια παρουσιάζεται μια συνοπτική μεθοδολογία αξιολόγησης για την ανάδειξη της εξάρτησης μεταξύ των εφαρμογών ισχύος και της υποστηρικτικής υποδομής. Μια αναπαράσταση της μεθοδολογίας παρουσιάζεται στο παρακάτω διάγραμμα (Σχ. 1.6). Ο κίνδυνος καταρτίζεται θεωρητικά ως ο πολλαπλασιασμός της επίδρασης με την πιθανότητα ενός γεγονότος. Η πιθανότητα θα προκύπτει μέσω της ανάλυσης της ευπάθειας της υποδομής, η οποία αξιολογεί την ικανότητα της υποστηρικτικής υποδομής να περιορίσει την πρόσβαση επιτιθέμενων σε κρίσιμες λειτουργίες ελέγχου. Αφού ανιχνευθούν πιθανές ευπάθειες, στην συνέχεια πρέπει να γίνει ανάλυση της επίδρασης στις εφαρμογές για να προσδιοριστούν οι επηρεαζόμενες λειτουργίες ελέγχου του δικτύου. Τελικά, το σύνολο αυτών των πληροφορίων θα χρησιμοποιηθούν για την αξιολόγηση της επίδρασης των κινδύνων στο φυσικό σύστημα.



Σχήμα 1.6 – Διάγραμμα Αξιολόγησης Κινδύνου

Το αρχικό βήμα στη **διαδικασία ανάλυσης κινδύνου** είναι, όπως αναφέραμε προηγουμένως, η ανάλυση ευπαθειών της υποδομής. Λόγω των υψηλών απαιτήσεων διαθεσιμότητας και των μεγάλων εξαρτήσεων από παλαιά και παραδοσιακά συστήματα και πρωτόκολλα επικοινωνίας, αντιμετωπίζονται πολλές δυσκολίες κατά τον προσδιορισμό των κυβερνο-ευπαθειών στο περιβάλλον των συστημάτων ελέγχου. Μια περιεκτική ανάλυση των κυβερνο-ευπαθών σημείων, θα πρέπει να συμπεριλαμβάνει το λογισμικό, τον εξοπλισμό και τα πρωτόκολλα επικοινωνίας που χρησιμοποιεί η υποδομή. Παραδείγματα εξειδικευμένων διαγνωστικών δοκιμών στο σύστημα μπορεί να είναι δοκιμές διείσδυσης με σάρωση ευπαθειών, προσδιορίζοντας κάποια πιθανά ευάλωτα σημεία στο περιβάλλον. Επιπλέον απαραίτητες ενέργειες είναι η συνεχόμενη χρήση ενημερώσεων ασφαλείας των προμηθευτών, αρχεία καταγραφής συστήματος και εγκατεστημένα συστήματα ανίχνευσης εισβολών. Αφού καταγραφούν οι κυβερνο-ευπάθειες του συστήματος,

θα πρέπει να πραγματοποιηθεί η ανάλυση επιπτώσεων στην εφαρμογή και σύμφωνα με την κατηγοριοποίηση των συστημάτων ελέγχου ισχύος που γίνεται στην συνέχεια (1.2.3), ώστε να προσδιοριστεί το σύνολο των επηρεαζόμενων μηχανισμών επικοινωνίας και ελέγχου. Τέλος, αφού προσδιοριστούν οι επιπτώσεις στις εφαρμογές ισχύος, πρέπει να πραγματοποιηθεί η ανάλυση των φυσικών επιπτώσεων. Αυτό μπορεί να πραγματοποιηθεί με χρήση μεθόδων προσομοίωσης συστημάτων ισχύος που αξιολογούν τις επιδόσεις σε σταθερή ή μεταβατικές καταστάσεις και των μεταβολών σε βασικές παραμέτρους που υποδεικνύουν την σταθερότητα του δικτύου (τάση, συχνότητα, γωνία, κλπ.). Μετά την ανάλυση των κινδύνων ακολουθούν οι προσπάθειες για τον περιορισμό τους (risk mitigation). Αυτό μπορεί να επιτευχθεί μέσω της ανάπτυξης μιας πιο ανθεκτικής υποστηρικτικής υποδομής ή εφαρμογών ισχύος, όπως θα δούμε στην συνέχεια.

Συχνές ευπάθειες των συστημάτων ελέγχου έχουν αξιολογηθεί στο παρελθόν από το Τμήμα Εθνικής Ασφάλειας των Ηνωμένων Πολιτειών (DHS) και παρουσιάζονται παρακάτω. Στον πίνακα (Σχ. 1.7) αυτές οι ευπάθειες κατηγοριοποιούνται ανάλογα με το αν οφείλονται σε εσφαλμένη διαμόρφωση του συστήματος ή στις ευπάθειες του δικτύου επικοινωνίας.

Ευπάθειες Λογισμικού και Διαμόρφωσης	**Ευπάθειες Ασφάλειας Δικτύου**
Ακατάλληλη επικύρωση εισόδου	Κοινότυπες ευπάθειες στον σχεδιασμό του δικτύου
Κακή ποιότητα κώδικα	
Έλεγχος/Διαχείριση πρόσβασης	Αδύναμα τείχη προστασίας - firewalls
Ελλιπής αυθεντικοποίηση	
Ανεπαρκής επαλήθευση αυθεντικότητας δεδομένων	Ευάλωτα τμήματα και συσκευές του δικτύου
Προβλήματα στην κρυπτογράφηση	
Μη διαμόρφωση ή συντήρηση μηχανισμών ασφάλειας	Απουσία ελέγχου διασφάλισης ποιότητας και ασφάλειας του δικτύου
Κακή διαμόρφωση παραμέτρων ελέγχου	

Σχήμα 1.7 – Συχνές ευπάθειες κυβερνοσυστήματος

Ορισμένες ερευνητικές προσπάθειες που έχουν επικεντρωθεί στην σχέση κυβερνοχώρου και φυσικής υποδομής στα πλαίσια της αξιολόγησης του κινδύνου (πχ. έρευνα «για την αλληλεξάρτηση», C. Laprie) δίνουν βάρος στην ανάλυση κλιμακούμενων, διαδοχικών και κοινών σφαλμάτων μέσα σε μια κυβερνο-φυσική σχέση. Αυτές δείχνουν πώς οι μεταβολές που προκύπτουν από επιθέσεις στο κυβερνοσύστημα μπορεί να οδηγήσουν σε καταστάσεις βλάβης του φυσικού συστήματος. Άλλες έρευνες περιλαμβάνουν αναλύσεις γραφημάτων με στόχο να αξιολογηθεί ποια είναι η επίδραση του ελέγχου σε μια φυσική οντότητα. Δηλαδή πώς ακριβώς η παραγωγή ενέργειας μπορεί να επηρεαστεί από αποτυχίες ή επιθέσεις σε πόρους του κυβερνοχώρου. Ακόμη, υπάρχουν διάφορες πιθανοτικές μέθοδοι (βασισμένες σε Petri-nets και δέντρα επίθεσης) για να ανιχνεύσουν ευάλωτα σημεία σε υποσταθμούς και κέντρα ελέγχου, τις οποίες μπορούν στη συνέχεια να χρησιμοποιήσουν για να αναγνωρίσουν την απώλεια φορτίου ως ποσοστό του συνολικού φορτίου στο σύστημα ηλεκτρικής ενέργειας. Συμπερασματικά, η βαθιά ανάλυση και κατανόηση όλων των προσεγγίσεων και με συνδυασμούς αυτών μπορεί να οδηγήσει σε νέες στρατηγικές μείωσης του κινδύνου.

1.2.3. Εφαρμογές ελέγχου συστήματος ισχύος και κυβερνοασφάλεια

Σε κάθε μία από τις τρεις βασικές λειτουργίες του ΚΦΣ ισχύος (παραγωγή, μεταφορά, διανομή) μπορεί να γίνει μια **ταξινόμηση των μεθόδων ελέγχου**. Σε κάθε ελεγκτικό βρόχο που χρησιμοποιείται προσδιορίζονται σήματα και πρωτόκολλα επικοινωνίας, μηχανές και βιομηχανικές συσκευές, υπολογιστικές διαδικασίες και

ελεγκτικές ενέργειες που συνδέονται με κάθε λειτουργία. Παρακάτω δίνεται το διάγραμμα ενός τυπικού βρόχου ελέγχου που αναπαριστά την αλληλεπίδραση μεταξύ του κέντρου ελέγχου και του φυσικού συστήματος:

Σχήμα 1.8 – Βρόχος ελέγχου κυβερνοφυσικού συστήματος

Μια **συνοπτική περιγραφή των λειτουργιών που εκτελούνται στον βρόχο ελέγχου** είναι ως εξής: Τα κέντρα ελέγχου λαμβάνουν διάφορες μετρήσεις από αισθητήρες που αλληλοεπιδρούν με συσκευές στο πεδίο (γραμμές μετάδοσης, μετασχηματιστές, κλπ.). Οι αλγόριθμοι που εκτελούνται στο κέντρο ελέγχου επεξεργάζονται αυτές τις μετρήσεις για να ληφθούν σημαντικές αποφάσεις για την λειτουργία του συστήματος. Έπειτα, οι αποφάσεις αυτές πρέπει να μεταδοθούν στους ενεργοποιητές οι οποίοι θα τις εκτελέσουν σε φυσικό επίπεδο. Οι μετρήσεις από τους αισθητήρες και τα ελεγκτικά μηνύματα των ελεγκτών, μπορούν να αναπαρασταθούν συναρτήσει του χρόνου ($y_i(t)$ και $u_i(t)$). Οι μετρούμενες φυσικές παράμετροι $y_i(t)$ που λαμβάνονται από υποσταθμούς, γραμμές μετάδοσης ή διάφορες μηχανές αναφέρονται σε μεγέθη όπως η τάση, συχνότητα, αρμονικές, ένταση ρεύματος, κ.ά. και αποστέλλονται στο κέντρο ελέγχου χρησιμοποιώντας καθορισμένα πρωτόκολλα επικοινωνίας. Στην συνέχεια το κέντρο ελέγχου τις επεξεργάζεται μέσω ενός συνόλου υπολογιστικών αλγορίθμων (Σύστημα Διαχείρισης Ενέργειας - EMS) και οι μεταβλητές απόφασης $u_i(t)$ μεταδίδονται στους ενεργοποιητές που σχετίζονται άμεσα με τις συσκευές πεδίου.

Από την σκοπιά της ασφάλειας, **ένας επιτιθέμενος μπορεί να εκμεταλλευτεί τις ευπάθειες κατά μήκος των συνδέσεων επικοινωνίας** και να δημιουργήσει πρότυπα επιθέσεων που επιτίθονται στην ακεραιότητα της επικοινωνίας (πχ. σχεδιασμένα για να αλλοιώνουν το περιεχόμενο μηνυμάτων), να εισάγουν καθυστέρηση στην μεταφορά της πληροφορίας ή ακόμη να μην επιτρέπουν την επικοινωνία (π.χ. άρνηση υπηρεσίας DoS, επιθέσεις χρονισμού) και την ανταλλαγή σημάτων ελέγχου και μέτρησης. Είναι σημαντικό λοιπόν να μελετηθούν και να αναλυθούν οι επιπτώσεις αυτών των επιθέσεων στο ηλεκτρικό σύστημα, καθώς μπορεί να επηρεάσουν σοβαρά την ασφάλεια και την αξιοπιστία του. Για παράδειγμα, αυτές οι επιπτώσεις μπορούν να μετρηθούν σε όρους απώλειας φορτίου ή παρεμβολών στην συχνότητα και την τάση λειτουργίας του συστήματος. Η μελέτη πιθανών επιθέσεων στα πρότυπα επικοινωνίας θα διεκπεραιωθεί σε επόμενα κεφάλαια και θα βοηθήσει τελικά και στην ανάπτυξη στρατηγικών και μοντέλων για την ανάπτυξη αντίμετρων, ικανών να προλάβουν ή να ανιχνεύουν επιθέσεις.

Σε αυτήν την ενότητα, επικεντρωνόμαστε στην κατηγοριοποίηση των κυριότερων μεθόδων ελέγχου επισημαίνοντας συνηθισμένες ευπάθειες, πρότυπα επιθέσεων, δυνητικές κατευθύνσεις έρευνας και πρότυπα επικοινωνίας.

Α. Έλεγχος Παραγωγής

Στην παραγωγική διαδικασία του συστήματος ισχύος, οι βρόχοι ελέγχου αφορούν κυρίως τον έλεγχο της τάσης και της ισχύος εξόδου της γεννήτριας. Η παραγωγή ελέγχεται είτε από τοπικά (αυτόματος ρυθμιστής τάσης και έλεγχος τοποτηρητή) είτε από ευρείας-ζώνης (αυτόματος έλεγχος παραγωγής) συστήματα ελέγχου. Παρακάτω δίνεται ο ένας πίνακας που κατηγοριοποιεί σημαντικές παραμέτρους για τις τρεις βασικές μεθόδους ελέγχου στο σύστημα παραγωγής.

Συστήματα Ελέγχου	**AVR**	**Governor**	**AGC**
Φυσική Παράμετρος	Τάση	Γωνιακή ταχύτητα	Συχνότητα
Μετρήσεις & είσοδοι συστήματος	Τάση εξόδου της γεννήτριας, τάση αναφοράς	Μετρούμενη ταχύτητα δρομέα γεννήτριας	Συχνότητα δικτύου, Ισχύς εξόδου
Απόκτηση Δεδομένων	Τοπική μέτρηση στους ακροδέκτες	Τοπικός αισθητήρας περιστροφής	Σύστημα SCADA σε δίκτυα WAN
Εντολές ελέγχου	Τοπικός έλεγχος του διεγέρτη ελεγκτή	Τοπικός έλεγχος του κύριου ελεγκτή κίνησης (τοποτηρητής βαλβίδας)	Μεμονωμένες σε κάθε εργοστάσιο παραγωγής
Συχνά πρωτόκολλα Επικοινωνίας	-	-	Modbus / DNP3 / IEC 60870-5/ ICCP
Υπολογισμός	Ρεύμα διέγερσης, έλεγχος PID	Έλεγχος ροής καυσίμου, PID έλεγχος	Ρυθμός αύξησης παρεχόμενης ισχύος, σφάλμα ελέγχου περιοχής (ACE)
Μηχανή ή Συσκευή	Γεννήτρια, σύστημα διέγερσης	Κινητήρια μηχανή	Μονάδες παραγωγής, γεννήτριες, AGC ελεγκτές
Ενέργειες Ελέγχου	Ρύθμιση ρεύματος διέγερσης	Ρύθμιση βαλβίδας	Ρύθμιση παραγωγής

Σχήμα 1.9 – Παράμετροι ελέγχου στο σύστημα παραγωγής ηλεκτρικής ενέργειας

1. **Αυτόματος Ρυθμιστής Τάσης (Automatic Voltage Regulator ή AVR):** Ο έλεγχος της διέγερσης της γεννήτριας χρησιμοποιείται για τη βελτίωση της ευστάθειας του συστήματος ισχύος, ελέγχοντας ουσιαστικά την ποσότητα της άεργου ισχύος που απορροφάται ή εισάγεται στο σύστημα. Γενικότερα, ο AVR είναι ο πλέον αποδοτικός στην παραγωγή και προτιμάται ευρέως από τους οργανισμούς παραγωγής ηλεκτρικής ενέργειας. Ο ψηφιακός εξοπλισμός ελέγχου που χρησιμοποιείται, επιτρέπει τη δοκιμή διάφορων αλγορίθμων για τη βελτίωση της ευστάθειας αυτής. Συγκεκριμένα, ένας ηλεκτρονικός διεγέρτης αλληλοεπιδρά με το κέντρο ελέγχου του εργοστασίου με στόχο την σωστή ρύθμιση της γεννήτριας. Για να επιτευχθεί αυτή η αλληλεπίδραση συνδέεται στο δίκτυο επικοινωνίας του κέντρου ελέγχου και ανταλλάσσει κατάλληλα μηνύματα ελέγχου χρησιμοποιώντας βιομηχανικά πρωτόκολλα ανταλλαγής μηνυμάτων όπως το Modbus. Μέσω αυτής της δικτυακής σύνδεσης, ο διεγέρτης προγραμματίζεται κατάλληλα και θέτει τους επιθυμητούς στόχους για την τάση και την συχνότητα. Ο βρόχος ελέγχου AVR λαμβάνει ανατροφοδότηση από την γεννήτρια και συγκρίνει τη μέτρηση με την τιμή-στόχο που έχει αποθηκευτεί στη μνήμη του ηλεκτρονικού διεγέρτη. Βάσει της διαφοράς μεταξύ της μέτρησης και της επιθυμητής τιμής και τις αντίστοιχης μεθόδου ελέγχου που έχει προγραμματιστεί, το ρεύμα τροποποιείται ώστε να διατηρεί την τάση στο επιθυμητό επίπεδο.

2. **Τοποτηρητής (ή Governor Control):** Αποτελεί τον κύριο τοπικό μηχανισμό ελέγχου της συχνότητας. Αυτός ο μηχανισμός χρησιμοποιεί έναν αισθητήρα που ανιχνεύει τις αλλαγές στην ταχύτητα που προέρχονται από διαταραχές και τροποποιεί αναλόγως τις ρυθμίσεις στην ατμοβαλβίδα για να μεταβληθεί η ισχύς

εξόδου της γεννήτριας. Οι ελεγκτές που χρησιμοποιούνται σε σύγχρονα ψηφιακά ελεγκτικά μοντέλα τοποτηρητών χρησιμοποιούν συνήθως το πρωτόκολλο επικοινωνίας Modbus για να επικοινωνήσουν με τους υπολογιστές στο κέντρο ελέγχου. Όπως και στην περίπτωση του AVR, αυτή η σύνδεση επικοινωνίας χρησιμοποιείται για τον καθορισμό της επιθυμητής τιμής λειτουργίας για τον έλεγχο του κυβερνήτη.

Τόσο ο AVR όσο και ο τοποτηρητής είναι τοπικοί βρόχοι και η λειτουργία τους δεν εξαρτάται από την υποδομή τηλεμετρίας του SCADA, διότι η τάση εξόδου και η ταχύτητα περιστροφής του άξονα ανιχνεύονται τοπικά. Επομένως, το πεδίο έρευνας για μια πιθανή εισβολή είναι σχετικά περιορισμένο. Ωστόσο, αυτές οι εφαρμογές εξακολουθούν να είναι ευάλωτες σε κακόβουλο λογισμικό που μπορεί να εισέλθει στο τοπικό δίκτυο του υποσταθμού μέσω τοπικών εισόδων (πχ. USB). Επιπλέον, τα ψηφιακά ελεγκτικά μοντέλα και στα δύο συστήματα έχουν συνδέσεις επικοινωνίας με το κέντρο ελέγχου του εργοστασίου. Σε αυτό το σημείο, ένας επιτιθέμενος μπορεί να παραβιάσει τους μηχανισμούς κυβερνοασφάλειας του εργοστασίου και να αποκτήσει πρόσβαση στο τοπικό δίκτυο. Εάν επιτευχθεί μια τέτοια εισβολή, ο επιτιθέμενος μπορεί να διαταράξει την κανονική λειτουργία παραμορφώνοντας ρυθμίσεις στις ψηφιακές ελεγκτικές κάρτες. Επομένως, πρέπει να εφαρμοστούν μέτρα ασφαλείας που επαληθεύουν τις εντολές ελέγχου που προέρχονται ακόμα και από το κέντρο ελέγχου.

3. **Αυτόματος Έλεγχος Παραγωγής (Automatic Generation Control ή AGC):** Ο αυτόματος έλεγχος της παραγόμενης ενέργειας είναι ο δευτερεύων τρόπος ελέγχου της συχνότητας και στοχεύει στην ακριβή ρύθμιση της συχνότητας στα επίπεδα της ονομαστικής της τιμή. Ο ρόλος του AGC είναι να πραγματοποιεί διορθώσεις στη ροή ισχύος και στις αποκλίσεις της συχνότητας, αντισταθμίζοντας έτσι τις αλλαγές του φορτίου και περιορίζοντας την ανταλλαγή ισχύος μεταξύ δύο περιοχών ελέγχου στην προκαθορισμένη τιμή. Συγκεκριμένα, ο αλγόριθμος συσχετίζει την απόκλιση της συχνότητας και τις μετρήσεις της καθαρής ροής του διασυνοριακού συνδέσμου για να υπολογίσει το σφάλμα ελέγχου της περιοχής (area control error). Αυτή η αντιστάθμιση φτάνει ως πληροφορία σε κάθε εργοστάσιο παραγωγής και προσαρμόζει κατάλληλα τα σημεία λειτουργίας, συνήθως κάθε πέντε δευτερόλεπτα. Μέσω αυτού του σήματος, ο αυτόματος έλεγχος εξασφαλίζει ότι κάθε αρχή ισορροπίας αντιμετωπίζει τις αλλαγές του φορτίου της και η πραγματική ισχύς που ανταλλάσσεται παραμένει όσο το δυνατόν πιο κοντά στην προγραμματισμένη.

   Οι ηλεκτρικές μετρήσεις του συστήματος ελέγχου παρέχονται από το σύστημα τηλεμετρίας SCADA, πράγμα που σημαίνει ότι η γκάμα των ευάλωτων σημείων του συστήματος επικοινωνίας μεγαλώνει. Μια επιτυχημένη επίθεση στον AGC είναι πολύ σοβαρή και θα έχει άμεσες επιπτώσεις στη συχνότητα και στην γενικότερη σταθερότητα και οικονομική λειτουργία του συστήματος. Αρκετές ερευνητικές προσπάθειες επισημαίνουν περιπτώσεις εισβολής στον βρόχο AGC έχοντας εντοπίσει παραποίηση των δεδομένων που ανταλλάσσονται. Χαρακτηριστικό παράδειγμα είναι το σχετικό πείραμα [68] όπου αναπτύχθηκε ένα πρότυπο επίθεσης το οποίο τροποποιεί τις μετρήσεις συχνότητας και ροής στη γραμμή σύνδεσης, οδηγώντας τη συχνότητα σε ανώμαλες τιμές λειτουργίας.

Β. Έλεγχος Μετάδοσης

Συστήματα Ελέγχου	State Estimation	VAR	WAMS
Φυσική Παράμετρος	Παραγωγή ισχύος & τοπολογία δικτύου	Τάση και άεργος ισχύς	Γωνία φάσης
Μετρήσεις & είσοδοι συστήματος	Τάση, Ενεργός και Άεργος Ισχύς, ροή ρεύματος, ρυθμίσεις Μ/Σ	Τάση, ροή αέργου, συντελεστής ισχύος	Φάσεις τάσης και ρεύματος, Ρυθμός αλλαγής συχνότητας
Απόκτηση Δεδομένων	Απομακρυσμένα μέσω WAN	Τοπική μέτρηση	Τοπική μέτρηση, Απομακρυσμένη παρακολούθηση
Εντολές ελέγχου	Μεμονωμένα στους παραγωγικούς σταθμούς	Τοπικά μηνύματα στις τοπικές συσκευές (FACTS)	Παρακολούθηση τιμών
Συχνά πρωτόκολλα Επικοινωνίας	IEC 61850	DNP3 / IEC 61850	IEC 61850 / ICCP/ IEEE C37.118
Υπολογισμός	Τάση συστήματος, γωνία φάσης, ελλαττωματικά δεδομένα συστήματος	Βελτιστοποίηση ροής και κατανομής ισχύος	Ανάλυση δεδομένων φάσης, απόσβεση ταλάντωσης και αξιολόγηση ευστάθειας
Μηχανή ή Συσκευή	Μεταγωγικές συσκευές, διακόπτες ισχύος	FACTS, Συσσωρευτές	PMU, συλλέκτες δεδομένων
Ενέργειες Ελέγχου	Απελευθέρωση παραγωγής	Παροχή ή απορρόφηση αέργου, ρύθμιση τάσης	Ενημέρωση κέντρου ελέγχου

Σχήμα 1.10 – Παράμετροι ελέγχου στο σύστημα μετάδοσης ηλεκτρικής ενέργειας

Το σύστημα μετάδοσης λειτουργεί συνήθως σε τάσεις άνω των 13 KV και στον υπό έλεγχο εξοπλισμό περιλαμβάνονται συσκευές μεταβολής και υποστήριξης ενεργού ισχύος. Η βασική ευθύνη του ελέγχου, εδώ, είναι να εξασφαλίζει ότι η ισχύς που διαρρέει τις γραμμές βρίσκεται εντός ασφαλών ορίων λειτουργίας και να διατηρείται η σωστή τάση κατά μήκος της γραμμής μετάδοσης. Οι παρακάτω βρόχοι ελέγχου υποστηρίζουν τους χειριστές σε αυτήν τη λειτουργία.

4. **Εκτίμηση Κατάστασης (State Estimation)**: Η εκτίμηση κατάστασης του ηλεκτρικού συστήματος είναι μια τεχνική με την οποία γίνονται εκτιμήσεις των μεταβλητών του συστήματος, όπως η τάση και η γωνία φάσης (μεταβλητές κατάστασης), βασιζόμενες σε πιθανές εσφαλμένες μετρήσεις από συσκευές του πεδίου. Αυτή η μέθοδος παρέχει ουσιαστικά μια εκτίμηση των μεταβλητών κατάστασης, όχι μόνο όταν οι συσκευές του πεδίου παρέχουν εσφαλμένες μετρήσεις, αλλά και όταν το κέντρο ελέγχου δεν λαμβάνει μετρήσεις λόγω κάποιας βλάβης της συσκευής ή του δικτύου επικοινωνίας. Παρέχονται λοιπόν στον χειριστή λεπτομέρειες σχετικά με τη ροή ισχύος και την τάση σε διάφορα τμήματα του δικτύου μετάδοσης συνδράμοντας έτσι στη λήψη κρίσιμων λειτουργικών αποφάσεων. Το κέντρο ελέγχου πραγματοποιεί υπολογισμούς χρησιμοποιώντας χιλιάδες μετρήσεις που λαμβάνει μέσω δικτύου ευρείας περιοχής. Οι τεχνικές για την ανίχνευση ελαττωματικών δεδομένων έχουν αναπτυχθεί σε μεγάλο βαθμό τα τελευταία χρόνια και παρέχουν καλές εκτιμήσεις των μεταβλητών κατάστασης παρά τα συχνά σφάλματα που προκαλούνται. Από την άλλη πλευρά όμως, αυτές δεν έχουν σχεδιαστεί για να είναι ανθεκτικές σε λανθασμένα δεδομένα που εισάγονται με πρόθεση μετά από μία εισβολή στην επικοινωνία.

   Ενώ η ανίχνευση λανθασμένων δεδομένων στην Εκτίμηση Κατάστασης έχει μελετηθεί εκτενώς, σε περιπτώσεις που ένας εισβολέας εκτελεί μια επίθεση στοχεύοντας στην διατάραξη της ομαλής λειτουργίας ελέγχου, οι παραδοσιακές τεχνικές μπορεί να μην είναι σε θέση να ανιχνεύσουν την παρουσία κακόβουλων στοιχείων. Μετά από έρευνες και μελέτες, που συναντάμε στην διαθέσιμη βιβλιογραφία, δημιουργείται μια ξεχωριστή κατηγορία επιθέσεων που ονομάζονται «επιθέσεις έγχυσης πλασματικών δεδομένων», οι οποίες διαφεύγουν της ανίχνευσης από τους υπάρχοντες αλγορίθμους αναγνώρισης εσφαλμένων μετρήσεων. Από τις μελέτες αυτές, προκύπτει ότι για να εισαχθούν πλασματικά δεδομένα σε μια μεταβλητή κατάστασης, αρκεί να χειραγωγηθούν

δέκα μετρητές. Οι συγγραφείς προτείνουν μια θεωρητική προσέγγιση γραφημάτων για να προσδιορίσουν το ελάχιστο σύνολο χειραγωγημένων μετρήσεων που διατηρεί το δίκτυο σε ικανοποιητικά επίπεδα αξιοπιστίας και ασφάλειας. Αυτές οι αρχικές ερευνητικές διαπιστώσεις δεν μπορούν να θεωρηθούν μηχανισμοί άμυνας του συστήματος ωστόσο τα συμπεράσματά τους βάζουν τα θεμέλια για την μετέπειτα ανάπτυξη τεχνικών ανίχνευσης τέτοιων επιθέσεων. Μια επόμενη αρχειακή πειραματική ιδέα ήταν η παρατήρηση ενός υποσυνόλου μετρήσεων και βάσει αυτών, η διεξαγωγή υπολογισμών για την ανίχνευση κακόβουλων δεδομένων και των επιπτώσεών τους. Το πείραμα αυτό έδειξε ότι μια επιτυχημένη επίθεση στην εκτίμηση κατάστασης μπορεί να χρησιμοποιηθεί στις αγορές ηλεκτρικής ενέργειας, καθώς οι διακανονισμοί μεταξύ των ενεργειακών εταιρειών υπολογίζονται βάσει τιμών από την εκτίμηση κατάστασης.

5. **Αποζημίωση Άεργου (VAR Compensation):** Αποτελεί την διαδικασία ελέγχου εισαγωγής ή απορρόφησης άεργου ισχύος σε ένα σύστημα ηλεκτρικής ενέργειας για τη βελτίωση της απόδοσης του συστήματος μεταφοράς. Ο κύριος στόχος των συσκευών που απαρτίζουν αυτήν την μέθοδο ελέγχου είναι η παροχή υποστήριξης στην τάση του δικτύου μεταφοράς, δηλαδή η ελαχιστοποίηση των διακυμάνσεων τάσης σε κάποιο άκρο μιας γραμμής μετάδοσης. Αυτές οι συσκευές μπορούν επίσης να αυξήσουν τη μεταφερόμενη ισχύ μέσω της γραμμής μετάδοσης και έχουν τη δυνατότητα να βοηθήσουν στην αποφυγή καταστάσεων blackout. Οι παραδοσιακές συσκευές VAR ελέγχου είναι σύγχρονοι συμπυκνωτές και μηχανικά εναλλασσόμενοι πυκνωτές και πηνία. Ωστόσο, με την μετάβαση στους ελεγκτές με θυρίστορ, αποκτούν ευρεία εφαρμογή συσκευές που ανήκουν στην οικογένεια των ευέλικτων συστημάτων εναλλασσόμενου ρεύματος (FACTS). Τα FACTS αλληλοεπιδρούν μεταξύ τους για να ανταλλάσσουν λειτουργικές πληροφορίες σε ένα αυτόνομο πλαίσιο. Έτσι δημιουργείται μια μεγαλύτερη εξάρτηση από την επικοινωνία, για την ανταλλαγή δεδομένων με άλλες συσκευές FACTS και τη λήψη ρυθμίσεων που καθορίζουν το την λειτουργικότητά τους.

   Οι συσκευές FACTS είναι αρκετά ευάλωτες σε επιθέσεις απόρριψης υπηρεσίας, αποσυγχρονισμού και έγχυσης πλαστών δεδομένων. Επιθέσεις δηλαδή που πλημμυρίζουν το δίκτυο επικοινωνίας με πλαστά πακέτα μπορούν να οδηγήσουν τις συσκευές αυτές σε καταστάσεις αδρανοποίησης και τελικά στην απώλεια κρίσιμων πληροφοριών και της δυνατότητα μακροπρόθεσμου και δυναμικού ελέγχου. Επιπλέον, οι αλγόριθμοι ελέγχου που χρησιμοποιούνται από συνεργαζόμενες συσκευές FACTS εξαρτώνται από τον χρόνο και απαιτούν αυστηρό συγχρονισμό. Συνεπώς, μια επίθεση βασισμένη στον χρονισμό μπορεί να διαταράξει τη σταθερή λειτουργία του περιβάλλοντος συνεργασίας. Τέλος, οι επιτιθέμενοι με βαθιά κατανόηση του πρωτοκόλλου επικοινωνίας που χρησιμοποιείται μπορεί να στείλει εσφαλμένα λειτουργικά δεδομένα και να επιφέρει αστάθειες στην διαδικασία αποζημίωσης αέργου ισχύος.

6. **Συστήματα Παρακολούθησης Ευρείας Περιοχής (Wide-Area Monitoring ή WAMS):** Τα συστήματα μέτρησης ευρείας περιοχής επικεντρώνονται στην παρακολούθηση της γενικότερης κατάστασης του ευφυούς δικτύου σε μια μεγάλη γεωγραφική περιοχή και η λειτουργία τους εξαρτάται από PMU μονάδες. Ο όρος PMU αναφέρεται σε Μονάδες Φασικών Μετρήσεων και είναι συσκευές που χρησιμοποιούνται στα ηλεκτρικά συστήματα για τη μέτρηση των φασικών ποσοτήτων της τάσης και του ρεύματος, σε συγκεκριμένες θέσεις. Οι φάσεις των παραγόμενων τάσεων που μετρούνται από τις PMU βοηθούν στον απευθείας υπολογισμό των πραγματικών ροών ισχύος στο δίκτυο και μπορούν έτσι να

συμβάλλουν στη λήψη αποφάσεων στο κέντρο ελέγχου. Τα συστήματα Υψηλής DC Τάσης (HVDC), τα κεντρικά συστήματα διέγερσης, οι ελεγκτές FACTS και οι σταθεροποιητές ισχύος μπορούν να επωφεληθούν από τις μετρήσεις ευρείας περιοχής που προσφέρουν οι PMU και να ενισχύσουν την απόδοση και την αποτελεσματικότητά τους.

Οι μονάδες μέτρησης φάσης PMU χρησιμοποιούν την τεχνολογία του παγκόσμιου συστήματος θέσης (GPS) για να προσδιορίσουν με ακρίβεια τις μετρήσεις των φάσεων. Έτσι, η διαφορά φάσης μεταξύ των τάσεων στα δύο άκρα μιας γραμμής μετάδοσης, σε ένα δεδομένο στιγμιότυπο, μπορεί να μετρηθεί με ακρίβεια χρησιμοποιώντας αυτήν την τεχνολογία. Οι συλλέκτες δεδομένων φάσης συνδυάζουν τα δεδομένα από διάφορα PMU και παρέχουν ένα σύνολο δεδομένων με χρονοσήμανση για μια συγκεκριμένη περιοχή στο κέντρο ελέγχου. Η ραγδαία ανάπτυξη της παραπάνω διαδικασίας έχει οδηγήσει τις έρευνες να επικεντρωθούν στην ανάπτυξη ασφαλούς και αξιόπιστου δικτύου ευρείας περιοχής ώστε να εξασφαλιστεί η σταθερότητα του ηλεκτρικού συστήματος.

Γ. Έλεγχος Διανομής

Συστήματα Ελέγχου	Μείωση Φορτίου	AMI
Φυσική Παράμετρος	Φορτίο και συχνότητα συστήματος	Κατανάλωση ηλεκτρικής ενέργειας
Μετρήσεις & είσοδοι συστήματος	Παραγωγή ισχύος, όρια παραγωγής, επίπεδα ζήτησης	Χρήση ενέργειας, ποιότητα ισχύος, εισαγωγή αρμονικών στο δίκτυο
Απόκτηση Δεδομένων	Υποσταθμοί, τοπική μέτρηση στους Μ/Σ διανομής	Τοπικές μετρήσεις στην πλευρά του καταναλωτή
Εντολές ελέγχου	Μηνύματα ενεργοποίησης διακοπτών διανομής και ρελέ στην κατανεμημένη παροχή	Απόρριψη φορτίων, αποστολή δεδομένων παρακολούθησης
Συχνά πρωτόκολλα Επικοινωνίας	IEC 61850	Ασύρματα πρότυπα επικοινωνίας
Υπολογισμός	Ποσότητα και σημεία φορτίου, προτεραιοποίηση φορτίων, στρατηγικές περιορισμού φορτίου	Λειτουργίες μέτρησης, προφίλ καταναλωμένων φορτίων, τιμολόγηση, ανίχνευση διακοπών
Μηχανή ή Συσκευή	Πίνακες παροχής, διακόπτες διανομής, κλπ.	Έξυπνοι Μετρητές, Προηγμένα Υπολογιστικά Συστήματα
Ενέργειες Ελέγχου	Άνοιγμα παροχικών διακοπτών	Ανάλυση μετρήσεων, διακοπές φορτίων

Σχήμα 1.11 – Παράμετροι ελέγχου στο σύστημα διανομής ηλεκτρικής ενέργειας

Το σύστημα διανομής είναι υπεύθυνο για την παροχή ηλεκτρικής ενέργειας στους καταναλωτές. Ωστόσο, με την ολοένα και μεγαλύτερη εφαρμογή των ευφυών δικτύων, το σύστημα διανομής εισάγει νέες δραστηριότητες παρακολούθησης που επιτρέπουν τον άμεσο έλεγχο του φορτίου στο επίπεδο του τελικού χρήστη. Στην συνέχεια παρουσιάζονται οι βασικοί έλεγχοι που συντελούν στην επίτευξη του παραπάνω στόχου και στον παρακάτω πίνακα ταξινομούνται σημαντικοί παράμετροι των αντίστοιχων ελεγκτικών βρόχων.

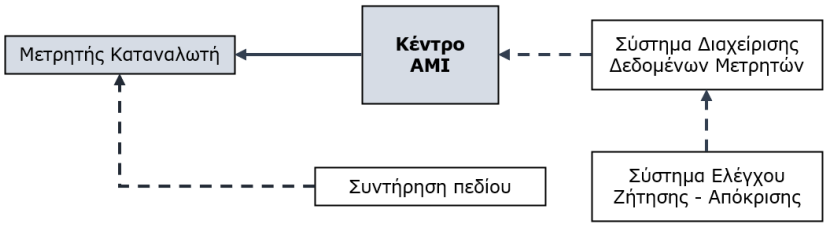
7. **Μείωση Φορτίου:** Οι μηχανισμοί μείωσης φορτίου είναι χρήσιμοι για την αποτροπή κατάρρευσης του συστήματος κατά τη διάρκεια καταστάσεων έκτακτης ανάγκης. Αυτοί οι μηχανισμοί μπορούν να κατηγοριοποιηθούν σε προληπτικούς, ενεργούς και χειροκίνητους. Οι πρώτοι δύο είναι αυτόματοι μηχανισμοί μείωσης φορτίου και λειτουργούν με τη χρήση ρελέ ισχύος. Για παράδειγμα, σε περιπτώσεις όπου η παραγωγή του συστήματος είναι ανεπαρκής για να ανταποκριθεί στο ζητούμενο φορτίο, μπορούν να χρησιμοποιηθούν

αυτόματοι μηχανισμοί μείωσης φορτίου για να διατηρηθεί η συχνότητα του συστήματος εντός των ασφαλών ορίων λειτουργίας ώστε να προστατευθούν οι συνδεδεμένες με το σύστημα συσκευές. Όταν υπάρχει ανάγκη, το φορτίο μειώνεται από το επίπεδο διανομής με τη χρήση των ρελέ υποσυχνότητας το οποίο είναι συνδεδεμένο στον διανομέα τροφοδοσίας. Σήμερα, τα ρελέ αυτά είναι πολύ πιο σύγχρονα και «έξυπνα» συγκριτικά με τα παραδοσιακά βιομηχανικά ρελέ. Για παράδειγμα μπορούν να υποστηρίξουν βιομηχανικά πρωτόκολλα επικοινωνίας (όπως το IEC 61850) ή το Πρωτόκολλο Διαδικτύου (IP).

Συνεπώς, μια κυβερνοεπίθεση στην υποδομή επικοινωνίας αυτών των ρελέ ή μια κακόβουλη αλλαγή στη λογική ελέγχου μπορεί πιθανότατα να οδηγήσει σε απρογραμμάτιστη απενεργοποίηση καλωδίων διανομής, εμποδίζοντας την εξυπηρέτηση τμημάτων του φορτίου. Η μεγάλη διακοπή που σημειώθηκε στο Tempe, AZ, το 2007, είναι ένα παράδειγμα του πώς ένα κακώς διαμορφωμένο πρόγραμμα μείωσης φορτίου μπορεί να οδηγήσει σε μια μαζική πτώση. Συγκεκριμένα, το σχετικό πρόγραμμα μείωσης φορτίου ενεργοποιήθηκε απροσδόκητα, με αποτέλεσμα το άνοιγμα 141 διακοπτών και την απώλεια 399 MW. Η διακοπή κράτησε 46 λεπτά και επηρέασε 98.700 χρήστες. Παρόλο που το περιστατικό συνέβη λόγω κακής διαχείρισης, αποδεικνύει το αντίκτυπο που μπορεί να προκαλέσει μια επιτυχημένη κακόβουλη εισβολή στο κυβερνοσύστημα.

8. **Προηγμένη Υποδομή Μέτρησης και Διαχείριση Ζήτησης (Advanced Metering Infrastructure ή AMI):** Τα μελλοντικά συστήματα διανομής θα βασίζονται σε μεγάλο βαθμό στα AMI διότι προσφέρουν μεγάλη αύξηση της αξιοπιστίας, την ενσωμάτωση ανανεώσιμων πηγών ενέργειας και την δυνατότητα στους καταναλωτές να παρακολουθούν την κατανάλωσή τους με λεπτομερείς πληροφορίες. Οι προηγμένες υποδομές μετρήσεων βασίζονται κυρίως στην εγκατάσταση έξυπνων μετρητών σε τοποθεσίες όπου συμβαίνει η πραγματική κατανάλωση ενέργειας, με στόχο την διεξαγωγή μετρήσεων πραγματικού χρόνου. Οι έξυπνοι μετρητές παρέχουν στις υπηρεσίες διανομής τη δυνατότητα διακοπής φορτίου (load control switching - LCS) και την απενεργοποίηση συσκευών των καταναλωτών όταν αυξάνεται η συνολική ζήτηση. Επιπλέον, η διαχείριση της ζήτησης (demand side management - DSM) εισάγει μια κυβερνο-φυσική σύνδεση μεταξύ της κυβερνο-υποδομής μέτρησης και της παρεχόμενης ισχύος στους καταναλωτές.

   Η διαμόρφωση του μετρητή ελέγχεται από ένα σύστημα διαχείρισης δεδομένων μέτρησης (MDMS) στο κέντρο ελέγχου το οποίο συνδέεται με μια κύρια συσκευή του AMI (AMI headend device). Η κύρια συσκευή από την μεριά της μεταδίδει εντολές και συγκεντρώνει τα δεδομένα που συλλέγονται από τους μετρητές σε όλο το σύστημα υποδομής. Οι δικτυακές συνδέσεις εντός της υποδομής του AMI εξαρτώνται από πολλές διαφορετικές τεχνολογίες, όπως RF mesh, WiMax, WiFi. και τα πρωτόκολλα επικοινωνίας, όπως το C12.22 ή το IEC 61850, χρησιμοποιούνται για τη μετάδοση τόσο της κατανάλωσης ηλεκτρικής ενέργειας όσο και των λειτουργιών ελέγχου των μετρητών προς το MDMS. Παρακάτω δίνεται το σχετικό **διάγραμμα των ροών ελέγχου** που μπορεί να επηρεάσουν τη διαθεσιμότητα ισχύος των καταναλωτών.



Σχήμα 1.12 – Διάγραμμα ελέγχου συστήματος AMI

Από την σκοπιά της ασφάλειας, οι έξυπνοι μετρητές στις τοποθεσίες των καταναλωτών εγείρουν όπως είναι κατανοητό ζητήματα ευπάθειας. Οι έλεγχοι κατάστασης στους μετρητές (ενεργοποιημένος ή απενεργοποιημένος) και η δυνατότητα απομακρυσμένης απενεργοποίησης συσκευών μέσω του μηχανισμού ελέγχου φορτίου προσφέρουν δυνητικούς κινδύνους από κυβερνοαπειλές. Μια κακόβουλη εντολή απενεργοποίησης του μετρητή μπορεί να αποτραπεί πιθανότατα μέσω της χρήσης περιόδων αναμονής, καθώς η απενεργοποίηση του μετρητή δεν απαιτεί ανταπόκριση σε πραγματικό χρόνο. Θα μπορούσαν λοιπόν οι μετρητές να προγραμματιστούν ώστε να περιμένουν κάποιο χρονικό διάστημα μετά τη λήψη μιας εντολής πριν απενεργοποιήσουν τη συσκευή. Αυτός ο προληπτικός μηχανισμός ωστόσο θα απέτρεπε μόνο απομακρυσμένες επιθέσεις, διότι η λογική πρόληψης δεν θα ήταν αποτελεσματική σε περίπτωση που ο εισβολέας έχει ήδη εισβάλει στον μετρητή.

2. Πρωτόκολλα Επικοινωνίας Ηλεκτρικών Συστημάτων

2.1. Εισαγωγή στα βιομηχανικά πρωτόκολλα επικοινωνίας

Τα βιομηχανικά πρωτόκολλα επικοινωνίας είναι στοιχείο ζωτικής σημασίας για ένα κυβερνο-φυσικό σύστημα, καθώς διασφαλίζουν την επικοινωνία και τον έλεγχο των βιομηχανικών συστημάτων, υποσυστημάτων και εγκαταστάσεων. Ωστόσο, αυτά τα πρωτόκολλα αντιμετωπίζουν σοβαρές προκλήσεις στον τομέα της κυβερνοασφάλειας, καθώς είναι εκτεθειμένα σε πολλούς κινδύνους και ευπαθή σε διάφορες επιθέσεις. Η παρούσα έρευνα επικεντρώνεται στην ανάλυση του ζητήματος της κυβερνοασφάλειας που αφορά τα κύρια και πιο διαδεδομένα βιομηχανικά πρωτόκολλα, όπως το Modbus, το DNP3, και άλλα. Σε επόμενα κεφάλαια θα εξεταστούν εργαλεία ανίχνευσης εισβολών που μπορούν να χρησιμοποιηθούν για τον εντοπισμό κυβερνοεπιθέσεων που επηρεάζουν αυτά τα πρωτόκολλα. Αρχικά, μελετώντας τα βασικά βιομηχανικά πρωτόκολλα και πιθανά τρωτά σημεία που εμπεριέχονται σε αυτά, μπορούμε να αναπτύξουμε μια καλύτερη κατανόηση των απειλών σε επίπεδο κυβερνοασφάλειας και των μέτρων προστασίας που απαιτούνται για την προστασία των βιομηχανικών συστημάτων και των ευφυών δικτύων.

Στο παρόν κεφάλαιο θα γίνει μια εκτενής ανάλυση των βασικών βιομηχανικών πρωτοκόλλων επικοινωνίας που έχουμε επιλέξει, προκειμένου να γίνει κατανοητή η λειτουργία τους και να εντοπιστούν τα τρωτά τους σημεία σε επίπεδο κυβερνοασφάλειας. Αρχικά θα αναφερθούν κάποια γενικά στοιχεία (υποενότητα 1.) που προσδιορίζουν το κάθε πρωτόκολλο επικοινωνίας. Στην συνέχεια και τις υποενότητες 2. και 3. θα εξετάσουμε την δομή κάθε πρωτοκόλλου σε επίπεδο μηνυμάτων, σημαντικές λειτουργίες που τα διακρίνουν και τις αρχιτεκτονικές διαμόρφωσης του δικτύου ανά περίπτωση. Στις υποενότητες 4. δίνεται εκτενής σχολιασμός για κάθε ενότητα πρωτοκόλλου, που θα περιλαμβάνει πλεονεκτήματά και μειονεκτημάτων τους. Διερευνώνται επίσης στην υποενότητα 5. πιθανά σημεία ευπαθείας για κάθε πρωτόκολλο, όπως αδυναμίες στην

αυθεντικοποίηση, την αποτελεσματικότητα των μηχανισμών κρυπτογράφησης, την επαλήθευση της ακεραιότητας των δεδομένων και τις αδυναμίες στον έλεγχο πρόσβασης. Τέλος, στην υποενότητα 6. θα αναφέρουμε τα κύρια πεδία εφαρμογής του κάθε πρωτοκόλλου, στον τομέα της ηλεκτρικής ενέργειας.

Ο κυρίαρχος στόχος της εργασίας είναι να γνωρίσουμε τους κινδύνους που αναδύονται ολοένα και περισσότερο στον κυβερνοχώρο των συστημάτων ελέγχου και διαχείρισης του ηλεκτρικού δικτύου, και να προτείνουμε μέτρα πρόληψης και αντιμετώπισης. Αυτό θα επιτευχθεί αρχικά από την με την μελέτη των πρωτοκόλλων καθώς οι βασικές απειλές που αντιμετωπίζουν τα έξυπνα συστήματα ισχύος βρίσκονται σε πεδίο της επικοινωνίας, λόγω των κρίσιμων πληροφοριών που μεταφέρονται.

Πριν όμως αναλύσουμε τα πέντε βασικά πρωτόκολλα που χρησιμοποιούνται κατά κόρον σε εφαρμογές και συστήματα ηλεκτρικής ενέργειας είναι απαραίτητο να οριστούν βασικές έννοιες που σχετίζονται με τα πρωτόκολλα επικοινωνίας ή την επικοινωνία γενικότερα ως έννοια. Οι παρακάτω **σημαντικοί ορισμοί** θα συμβάλουν στην καλύτερη κατανόηση της μελέτης των πρωτοκόλλων που διεξάγεται στις επόμενες ενότητες του παρόντος κεφαλαίου.

- **Πρωτόκολλο Επικοινωνίας**: Ένα πρωτόκολλο επικοινωνίας είναι ένα σύνολο κανόνων και διαδικασιών που καθορίζουν τον τρόπο με τον οποίο δύο ή περισσότερες συσκευές ή εφαρμογές ανταλλάσσουν πληροφορίες. Το πρωτόκολλο καθορίζει τον τύπο και τον χρόνο ανταλλαγής των μηνυμάτων μεταδίδονται, τη μορφή και τη σειρά των δεδομένων που περιέχονται στα μηνύματα, καθώς και τις διαδικασίες που ακολουθούνται για την αρχή και τη λήξη της επικοινωνίας. Είναι δηλαδή μια δέσμη κανόνων στους οποίους στηρίζεται μια επικοινωνία μεταξύ των συσκευών ή των εφαρμογών σε ένα δίκτυο και καθιστούν την εν λόγω επικοινωνία αποτελεσματική και αξιόπιστη.
- **Στοίβα**: Μια στοίβα (stack) πρωτοκόλλων, επίσης γνωστή ως στοίβα δικτύου ή στοίβα επικοινωνίας, είναι ένα σύνολο πρωτοκόλλων επικοινωνίας που τοποθετούνται σε επίπεδα (layers) για να επιτρέψουν την επικοινωνία μεταξύ συσκευών κάποιου δικτύου. Κάθε επίπεδο στη στοίβα πρωτοκόλλων είναι υπεύθυνο για μια συγκεκριμένη λειτουργία, όπως ανίχνευση και διόρθωση σφαλμάτων, μετάδοση δεδομένων ή διευθυνσιοδότηση δικτύου. Τα επίπεδα συνεργάζονται μαζί για να παρέχουν ένα αξιόπιστο και αποδοτικό σύστημα επικοινωνίας.

Επίπεδα	Περιεχόμενο	Πρωτόκολλα
Εφαρμογή (Application)	Δεδομένα (Data)	HTTP, FTP, DNS, SSH
Παρουσίαση (Presentation)	Δεδομένα (Data)	JPEG, MPEG, SSL
Συνεδρία (Session)	Δεδομένα (Data)	NetBIOS, RPC, SQL, NFS
Μεταφορά (Transport)	Τμήματα (Segments)	TCP, UDP, SCTP
Δίκτυο (Network)	Πακέτα (Packets)	IP, ICMP
Σύνδεση (Data Link)	Πλαίσια (Frames)	Wi-Fi, Ethernet, Point-to-Point
Φυσικό Επίπεδο (Physical)	Bits	RS-232, Ethernet, USB, Fiber

Σχήμα 2.1. Επίπεδα στοίβας πρωτοκόλλων, μοντέλου OSI.

Κάποια παραδείγματα στοίβας πρωτοκόλλων είναι το μοντέλο OSI (βλ. σχήμα 2.1), η στοίβα Bluetooth, το TCP/IP και πάρα πολλά ακόμη. Ορισμένα από τα παραπάνω θα συναντήσουμε στην συνέχεια της εργασίας και θα μελετήσουμε την λειτουργίας τους.

- **Φυσικό Επίπεδο**: Η προδιαγραφή του φυσικού επιπέδου καθορίζει τις ηλεκτρικές ρυθμίσεις, την τάση και το χρονισμό, μαζί με άλλες ιδιότητες που είναι απαραίτητες για την αποστολή σημάτων μεταξύ συσκευών. Το φυσικό επίπεδο παρέχει τρεις βασικές υπηρεσίες: α. φυσική μετάδοση δεδομένων (αποστολή- λήψη, β. φυσικό συγχρονισμό, (γ.) ενημέρωση κατάστασης και έλεγχο σφαλμάτων.
- **Πρωτόκολλο Ελέγχου Μετάδοσης – TCP:** Είναι ένα πρωτόκολλο δικτύου που λειτουργεί στο επίπεδο μεταφοράς του συνόλου πρωτοκόλλων του Διαδικτύου (IP). Παρέχει αξιόπιστη, ταξινομημένη και ελεγχόμενη αποστολή δεδομένων μεταξύ εφαρμογών που εκτελούνται σε υπολογιστές σε ένα δίκτυο. Το TCP είναι υπεύθυνο για το διαχωρισμό των δεδομένων σε πακέτα, την αποστολή τους και στη συνέχεια την εκ νέου συναρμολόγηση των πακέτων σε αρχικά δεδομένα στην πλευρά του παραλήπτη. Για να εκκινήσει την επικοινωνία μεταξύ δύο συσκευών χρησιμοποιεί έναν **τριεπίπεδο μηχανισμό συγχρονισμού** κατά το οποίο αρχικά ο πελάτης στέλνει το αίτημα συγχρονισμού (SYN) στον διακομιστή, ο διακομιστής στην συνέχεια επιστρέφει το τμήμα συγχρονισμού και αλλά και μια επιβεβαίωση (SYN + ACK) λήψης αιτήματος και τέλος, ο πελάτης επιστρέφει την τελική επιβεβαίωση για την έναρξη της συνομιλίας.
  Χρησιμοποιείται ευρέως για εφαρμογές όπως η αλληλογραφία, η μεταφορά αρχείων και η περιήγηση στο διαδίκτυο, όπου η ακεραιότητα και η αξιοπιστία των δεδομένων είναι σημαντικές. Το εν λόγω πρωτόκολλο θα μας απασχολήσει εκτενώς στην συνέχεια, καθώς πάνω του βασίζονται οι πλέον σύγχρονες επικοινωνίες στην βιομηχανία.
- **User Datagram Πρωτόκολλο – UDP**: Είναι μια εναλλακτική λύση στο πιο περίπλοκο TCP και συχνά χρησιμοποιείται σε καταστάσεις όπου η ταχύτητα είναι πιο σημαντική από την αξιοπιστία. Σε αντίθεση με το TCP, το UDP δεν δημιουργεί σύνδεση πριν από την αποστολή δεδομένων και δεν παρέχει έλεγχο σφάλματος ή επαναλήψεις χαμένων πακέτων. Συνεπώς, το UDP χρησιμοποιείται συχνά για εφαρμογές που απαιτούν μετάδοση δεδομένων πραγματικού χρόνου ή χαμηλή καθυστέρηση επικοινωνίας
- **Σειριακό Πρωτόκολλο Επικοινωνίας:** Ένα σειριακό πρωτόκολλο επικοινωνίας χρησιμοποιείται για τη μετάδοση δεδομένων σειριακά, δηλαδή ένα bit τη φορά. Αυτό σημαίνει ότι τα δεδομένα μεταδίδονται μέσω μιας μονής γραμμής επικοινωνίας, σε αντίθεση με τα παράλληλα πρωτόκολλα που χρησιμοποιούν πολλαπλές γραμμές επικοινωνίας. Αυτό τα καθιστά ιδιαίτερα κατάλληλα για εφαρμογές που απαιτούν μικρό μέγεθος, απλότητα και αξιοπιστία μετάδοσης δεδομένων. Ορισμένα παραδείγματα είναι: RS-485, RS-232, I2C, SPI, Modbus RTU, PROFIBUS, κ.ά.
- **Πύλη TCP/IP (TCP/IP Gateway):** Είναι ένας δρομολογητής δικτύου που χρησιμοποιείται για τη σύνδεση διαφορετικών δικτύων TCP/IP μεταξύ τους. Συνήθως, λειτουργεί ως μεσολαβητής μεταξύ των δικτύων, εκτελώντας τη μετάφραση διευθύνσεων IP και τη μεταφορά δεδομένων ανάμεσα σε διαφορετικά δίκτυα. Επίσης, μία πύλη TCP/IP μπορεί να είναι υπεύθυνη για την επιτήρηση και τον έλεγχο της ασφάλειας του δικτύου και τη διαχείριση της επικοινωνίας μεταξύ των δικτύων.

Έχοντας ορίσει σημαντικές έννοιες για τα βιομηχανικά πρωτόκολλα επικοινωνίας παρακάτω θα μελετηθούν εκτενώς πέντε από αυτά. Η επιλογή αυτή έγινε με κύριο γνώμονα την δημοτικότητά τους σε βιομηχανικές εφαρμογές που αφορούν την παραγωγή και διαχείριση της ηλεκτρικής ενέργειας.

2.2. Πρωτόκολλο επικοινωνίας MODBUS

Ορισμός: Το Modicon Commination Bus, ή απλώς Modbus είναι ένα πρωτόκολλο επικοινωνίας επιπέδου εφαρμογής που δημιουργήθηκε στα τέλη της δεκαετίας του ’70. Ο στόχος ήταν η ανάπτυξη ενός πρωτοκόλλου που θα χρησιμοποιείται ευρέως στα βιομηχανικά συστήματα αυτοματισμού και ελέγχου. Ξεκίνησε ως ένα σειριακό πρωτόκολλο master-slave, που σημαίνει ότι μια **κύρια συσκευή** πρωτοβουλεί, ελέγχει και συντονίζει την επικοινωνία με μία ή περισσότερες άλλες συσκευές χαμηλότεροι επιπέδου (**εξωτερικές μονάδες**).

2.2.1. Μορφές πρωτοκόλλου Modbus

Ενώ αρχικά το πρωτόκολλο εφαρμογής Modbus σχεδιάστηκε αποκλειστικά για **σειριακή επικοινωνία (ως Modbus RTU)** με χρήση σύνδεσης RS-485 ή RS-232, πλέον έχει εξελιχθεί και προσαρμοστεί σε άλλες μορφές φυσικής σύνδεσης. Η πιο διαδεδομένη από αυτές είναι η σύνδεση Ethernet και η λειτουργία του πρωτοκόλλου πάνω στη **στοίβα πρωτοκόλλων TCP/IP**. Έτσι η κοινότητα του Διαδικτύου μπορεί να έχει πρόσβαση στο εξελιγμένο πρωτόκολλο **Modbus TCP**, μέσω μια δεσμευμένης θύρας στη TCP/IP στοίβα. Σε αντίθεση με το σειριακό πρωτόκολλο, η επικοινωνία Modbus TCP λειτουργεί ως **πελάτης-διακομιστής** (client/server), δηλαδή η ανταλλαγή μηνυμάτων δεν απαιτεί αποκλειστικά μία κύρια συσκευή που θα συντονίζει την επικοινωνία αλλά μπορεί να υπάρχουν και περισσότερες (πελάτες). Έτσι επιτυγχάνεται μια μεγαλύτερη ευελιξία στην επικοινωνία μεταξύ των διασυνδεδεμένων συσκευών.

Τα πρωτόκολλα της οικογένειας Modbus είναι ίσως τα πιο διαδεδομένα στον τομέα της βιομηχανικής αυτοματοποίησης καθώς η δομή τους είναι ταιριαστή με την επικοινωνία μεταξύ βιομηχανικών συσκευών, όπως Ελεγκτών Προγραμματιζόμενης Λογικής (PLCs), Συστημάτων Ανθρώπου-Μηχανής (HMIs), διανεμημένες μονάδες εισόδων-εξόδων (Distributed I/O) και συστημάτων απομακρυσμένου ελέγχου (SCADA).

Το Modbus καθορίζει τη μορφή μηνυμάτων, τις μεθόδους επικοινωνίας και τη διάταξη του δικτύου για την ανταλλαγή δεδομένων μεταξύ συσκευών, επιτρέποντας την απομακρυσμένη παρακολούθηση και έλεγχο βιομηχανικών διεργασιών**.** Έχει γίνει δημοφιλής επιλογή για τη βιομηχανική αυτοματοποίηση λόγω της απλότητάς του, της χαμηλής επιβάρυνσης (overhead) στο δίκτυο και της ευρείας υποστήριξης από τους κατασκευαστές. Περισσότερα στοιχεία θα δούμε στην συνέχεια με έμφαση στο πρωτόκολλο TCP/IP.

2.2.2. Δομή πακέτων στο Modbus/TCP

Όπως αναφέρθηκε παραπάνω, υπάρχουν δύο βασικές εκδόσεις του πρωτοκόλλου Modbus, το **Modbus Serial (ή RTU)** και το **Modbus/TCP**. Η **κύρια διαφορά των δύο έγκειται σε επίπεδο σύνδεσης**, με το σειριακό να μεταφέρει τα δεδομένα με τη μορφή πλαισίων που αποτελούνται από bits ενώ το Modbus TCP τα δεδομένα Modbus ενθυλακώνονται στο πρωτόκολλο TCP/IP και μεταφέρονται ως πακέτα IP μέσω του δικτύου. Λόγω της ευρείας αποδοχής του δευτέρου σε περισσότερες βιομηχανικές εφαρμογές, στην παρούσα εργασία θα επικεντρωθούμε στο Modbus/TCP και για το υπόλοιπο της έρευνας, πολλές αναφορές στο Modbus θα σημαίνουν Modbus/TCP.

Το Modbus, λοιπόν, είναι σχεδιασμένο για να επιτρέπει την επικοινωνία βιομηχανικού εξοπλισμού όπως υπολογιστές, αισθητήρες, προγραμματιζόμενοι λογιστικοί ελεγκτές (PLCs) και άλλες φυσικές συσκευές εισόδων/εξόδων μέσω του δικτύου IP/Ethernet. Η επικοινωνία αυτή γίνεται με την μορφή ανταλλαγής πακέτων μηνυμάτων που εμπεριέχουν δεδομένα. Τα πακέτα αυτά εκτός των δεδομένων που ανταλλάσσονται, εμπεριέχουν και άλλες σημαντικές πληροφορίες. Όλα τα στοιχεία εντάσσονται σε μια γενικότερη δομή (πακέτου) που περιλαμβάνει πληροφορίες σχετικά με την ανταλλαγή (πχ. Πρωτόκολλο, λειτουργία, συσκευή που συμμετέχει επικοινωνία, κλπ.) Συνεπώς, **τα επίπεδα TCP/IP του πρωτοκόλλου και το Ethernet σε φυσικό επίπεδο είναι υπεύθυνα για τη μεταφορά μια ολόκληρης δέσμης πληροφοριών στο επίπεδο εφαρμογής**. Αναλυτικότερα στα Modbus μηνύματα, τα δεδομένα πάντα συνοδεύονται με τον σχετικό κώδικα λειτουργίας, ο οποίος καθορίζει τον τύπο της λειτουργίας που εκτελείται, ή καλύτερα που ζητήθηκε από μια συσκευή. Έτσι τα δεδομένα που ανταλλάσσονται δεν είναι απλοί αριθμοί αλλά αποκτούν φυσικό νόημα από τον κώδικα στον οποίο έχουν αντιστοιχηθεί.

Συγκεκριμένα, κάθε συσκευή που υποστηρίζει επικοινωνία με Modbus έχει έναν χάρτη καταχωρητών (registers) που αντιστοιχούν σε θέσεις μνήμης με ψηφιακά δεδομένα και μια σειρά από κώδικες διαφόρων λειτουργιών. Οι λειτουργίες αυτές μπορεί να χρησιμοποιούνται για την παρακολούθηση, τη διαμόρφωση και τον έλεγχο των εισόδων και εξόδων της συσκευής. Στον παρακάτω πίνακα (Σχήμα 2.2) απεικονίζεται η γενική δομή ενός μηνύματος εφαρμογής Modbus, χωρισμένη σε επί μέρους πεδία και είναι γνωστή ως **Application Data Unit (ADU) ή Μονάδα Δεδομένων Εφαρμογής**.

Transaction Identifier	**Protocol Identifier**	**Length Field**	**Unit ID**	**Function Code**	**Data - Payload**
Αναγνωριστικό Συνδιαλλαγής	Modbus (=0)	Μέγεθος Μηνύματος	Ταυτοποίηση Μονάδας	Κώδικας Λειτουργίας	Φορτίο Δεδομένων
2 bytes	2 bytes	2 bytes	1 byte	1 byte	Έως 252 bytes

Κεφαλίδα Εφαρμογής Modbus (MBAP) **Μονάδα Δεδομένων (PDU)**

Σχήμα 2.2. ADU - Μονάδα Δεδομένων Εφαρμογής Modbus.

Η δομή μηνυμάτων Modbus που απεικονίζεται παραπάνω διαιρείται σε δύο βασικά τμήματα. Το πρώτο μέρος είναι η **κεφαλίδα** του Πρωτοκόλλου Εφαρμογής Modbus (MBAP), η οποία αποτελείται από το αναγνωριστικό της συνδιαλλαγής, το αναγνωριστικό του πρωτοκόλλου, το μέγεθος του μηνύματος και το αναγνωριστικό συσκευής (ή μονάδας). Το δεύτερο μέρος είναι η τυπική **μονάδα δεδομένων** πρωτοκόλλου Modbus (PDU) και αποτελείται από δύο τμήματα, τον κώδικα λειτουργίας και τα το φορτίο δεδομένων. Παρακάτω περιγράφεται η σημασία κάθε πεδίου ενός Modbus ADU:

1. **Αναγνωριστικό Συνδιαλλαγής**: Σκοπός του πεδίου είναι να ταυτοποιήσει μια αποστολή αιτήματος ή απάντησης μεταξύ ενός πελάτη και ενός διακομιστή και

να τους συγχρονίσει. Δημιουργείται έτσι ένα μοναδικό αναγνωριστικό (ID) της συνδιαλλαγής στο αίτημα του πελάτη το οποίο στην συνέχεια αντιγράφεται από τον διακομιστή και περιλαμβάνεται στην απάντησή του. Το αναγνωριστικό συνδιαλλαγής είναι ένας ακέραιος αριθμός μεγέθους 2 bytes.

2. **Αναγνωριστικό Πρωτοκόλλου**: Είναι ένας 2-byte ακέραιος αριθμός που χρησιμοποιείται για να διασφαλιστεί ότι η συσκευή λήψης μπορεί να ερμηνεύσει σωστά τα δεδομένα που μεταδίδονται και να εφαρμόσει τους κατάλληλους κανόνες του πρωτοκόλλου Modbus για το χειρισμό του μηνύματος. Το MODBUS προσδιορίζεται από το αναγνωριστικό πρωτοκόλλου με την τιμή "0" ή "0x0000" η οποία περιλαμβάνεται τόσο στα μηνύματα τύπου αιτήματος όσο και στις απαντήσεις.
3. **Πεδίο Μεγέθους**: Το πεδίο αυτό έχει επίσης μέγεθος 2 bytes και καθορίζει τον αριθμό των bytes που ακολουθούν στο υπόλοιπο μήνυμα. Περιλαμβάνει δηλαδή το μέγεθος των επόμενων τμημάτων της κεφαλίδας, καθώς και το μέγεθος των τμημάτων που εμπεριέχουν τα δεδομένα. Ο αριθμός αυτός μπορεί να διαφέρει μεταξύ αιτήματος πελάτη και της αντίστοιχης απάντησης του διακομιστή.
4. **Αναγνωριστικό Μονάδας**: Το μέγεθος του αναγνωριστικού μονάδας είναι 1 byte και αποτελεί έναν μοναδικό αριθμό που προσδιορίζει την εξωτερική μονάδα, στην προκειμένη περίπτωση έναν διακομιστή, που πρόκειται να επικοινωνήσει ο πελάτης. Δηλαδή πρόκειται για την ταυτοποίηση η οποία αντιστοιχεί σε μια μοναδική συσκευή-διακομιστή. Αυτό το πεδίο χρησιμοποιείται επίσης για σκοπούς εσωτερικής δρομολόγησης στο σύστημα και την δημιουργία επικοινωνίας με μια εξωτερική μονάδα που υποστηρίζει άλλη μορφή του Modbus (πχ. MODBUS+ ή MODBUS σειριακής γραμμής). Αυτό πρακτικά μπορεί να γίνει μέσω μιας πύλης (gateway) ανάμεσα στην σειριακή γραμμή και δίκτυο Ethernet TCP-IP. Τέλος, το αναγνωριστικό ορίζεται αποκλειστικά από τον Modbus-πελάτη στο αίτημά του και πρέπει να επιστραφεί με την ίδια τιμή στην απάντηση του διακομιστή.
5. **Κώδικας Λειτουργίας**: Ο κώδικας λειτουργίας υποδηλώνει μια υπηρεσία που υποστηρίζεται από το πρωτόκολλο Modbus η οποία ζητείται να εκτελεστεί από μια Modbus συσκευή. Το Modbus μπορεί να υποστηρίζει έως και 19 διαφορετικές λειτουργίες, συμπεριλαμβανομένων εντολών ανάγνωσης ή εγγραφής coils, διακριτών εισόδων και καταχωρητών. Κάθε κωδικός λειτουργίας έχει μια συγκεκριμένη περιοχή διευθύνσεων και μορφή δεδομένων. Έχει μέγεθος 1 byte και μπορεί να παίρνει τιμές μεταξύ των αριθμών 1 έως 127. Οι συσκευές-πελάτες πρέπει να χρησιμοποιούν τον σωστό κωδικό λειτουργίας για να επικοινωνήσουν αποτελεσματικά με άλλες συσκευές Modbus. Αναλυτικά οι κώδικες λειτουργίας που υποστηρίζονται από το Modbus TCP και οδηγίες χρήσης τους αναφέρονται στο εξής άρθρο [ipc2u.com/articles/knowledge-base/detailed-description-of-the-modbus-tcp-protocol-with-command-examples/]. Οι πιο συχνοί κωδικοί που συναντάμε περιλαμβάνονται στον παρακάτω πίνακα του σχήματος 2.3. Χρησιμοποιώντας αυτούς τους κωδικούς λειτουργίας, οι συσκευές Modbus μπορούν εύκολα να ενσωματωθούν σε μεγαλύτερα συστήματα ελέγχου και να επικοινωνήσουν αποτελεσματικά με άλλες συσκευές του δικτύου.
6. **Φορτίο Δεδομένων**: Το φορτίο του μηνύματος έχει μεταβλητό μέγεθος που περιορίζεται σε 252 bytes και περιλαμβάνει δεδομένα που έχουν συγκεκριμένη ερμηνεία για κάθε κωδικό λειτουργίας. Για έναν κωδικό ανάγνωσης δεδομένων το φορτίο έχει δύο πεδία, έναν αριθμό αναφοράς και έναν αριθμό bit/word. Ο αριθμός αναφοράς καθορίζει την αρχική διεύθυνση μνήμης για τη λειτουργία ανάγνωσης. Το πεδίο μέτρησης των bit/word καθορίζει τον αριθμό των αντικειμένων μνήμης που πρέπει να αναγνωστούν. Τα φορτίο δεδομένων της αντίστοιχης απάντησης έχει δύο ελαφρώς διαφορετικά πεδία, τον αριθμό μέτρησης των byte και τα πραγματικά δεδομένα. Το πεδίο μέτρησης byte

καθορίζει το μήκος των δεδομένων σε bytes, ενώ το πεδίο δεδομένων περιέχει τις τιμές των αντικειμένων μνήμης που αναγνώστηκαν. Αντίθετα, το φορτίο σε ένα μήνυμα αιτήματος για εγγραφή δεδομένων, εκτός από αναφορές μνήμης, εμπεριέχει και τις αντίστοιχες τιμές που πρέπει να εγγραφούν.

7. **Έλεγχος σφάλματος**: Η λειτουργία ελέγχου σφάλματος δεν υποστηρίζεται από το Modbus TCP παρά μόνο στο σειριακό πρωτόκολλο, αλλά είναι άξια αναφοράς από άποψη ασφάλειας. Σε περίπτωση αποτυχίας στην ανταλλαγής πληροφοριών υποδηλώνεται μια διαφορετική απάντηση από την εξωτερική μονάδα της σειριακής επικοινωνίας. Συγκεκριμένα, η συσκευή επιστρέφει μια τιμή σφάλματος που περιλαμβάνει τον κώδικα λειτουργίας του αιτήματος της κύριας συσκευής με το περισσότερο σημαντικό bit ψηφίο να ισούται με «1». Η απουσία αυτού του πεδίου στο Modbus/TCP δεν σημαίνει αναγκαστικά ελλιπή ασφάλεια, διότι το TCP επίπεδο παρέχει τους δικούς του μηχανισμούς ελέγχου (πχ. έλεγχος ροής, ανίχνευση ή διόρθωση σφάλματος) και παρέχει από την μεριά του έναν βαθμό αξιοπιστίας στην επικοινωνία.

Τύπος	F.C. (hex)	Περιγραφή Λειτουργίας
Read Data - Ανάγνωση Δεδομένων	**01**	**Εσωτερικά «Πηνία»:** Η λειτουργία μπορεί να διαβάσει έως 2000 πηνία **(δυαδικά δεδομένα – 1 bit)** από τις αναγραφόμενες στο PDU διευθύνσεις μνήμης μιας απομακρυσμένης συσκευής.
	02	**Διακριτοί Είσοδοι:** Ανάγνωση ψηφιακών εισόδων (1-bit) μιας συσκευής. Το PDU αίτημα καθορίζει την διεύθυνση της πρώτης εισόδου και τον αριθμό των εισόδων προς ανάγνωση.
	03	**Πολλαπλοί Καταχωρητές – μνήμης:** Η λειτουργία διαβάζει το περιεχόμενο ενός συνεχούς τμήματος καταχωρητών στην μνήμη μιας συσκευής. Κάθε καταχωρητής περιλαμβάνει δεδομένα των 16-bit.
	04	**Καταχωρητές Εισόδου:** Χρησιμοποιείται για την ανάγνωση από 1 έως 125 συνεχόμενων καταχωρητών εισόδου (δεδομένων 16-bit) της απομακρυσμένης συσκευής.
Write Data - Εγγραφή Δεδομένων	**05**	**Μοναδικό «Πηνίο»:** Ο κωδικός εγγράφει μια δυαδική τιμή κατάστασης (ON/OFF) σε μια συγκεκριμένη ψηφιακή έξοδο της συσκευής. Η τιμή (FF) ενεργοποιεί την έξοδο ενώ η (00) την απενεργοποιεί. Διαφορετικές τιμές θεωρούνται μη έγκυρες για αυτήν την λειτουργία.
	06	**Μοναδικός Καταχωρητής:** Εδώ εγγράφονται τιμές (16-bit) σε αποκλειστικά έναν καταχωρητή. Το μήνυμα αιτήματος καθορίζει τη διεύθυνση του καταχωρητή που πρόκειται να επεξεργαστεί.
	0F	**Πολλαπλά «Πηνία»:** Η λειτουργία χρησιμοποιείται για να ενεργοποιήσει ή να απενεργοποιήσει κάθε πηνίο σε μια ακολουθία ψηφιακών θέσεων μνήμης. Στο αίτημα αναφέρονται ποια πηνία θα δεχτούν επεξεργασία.
	10	**Πολλαπλοί Καταχωρητές:** Εγγράφει ένα μπλοκ συνεχόμενων καταχωρητών (1 έως 123) στην μνήμη της συσκευής. Οι τιμές που ζητούνται για εγγραφή καθορίζονται στο πεδίο δεδομένων του αιτήματος.

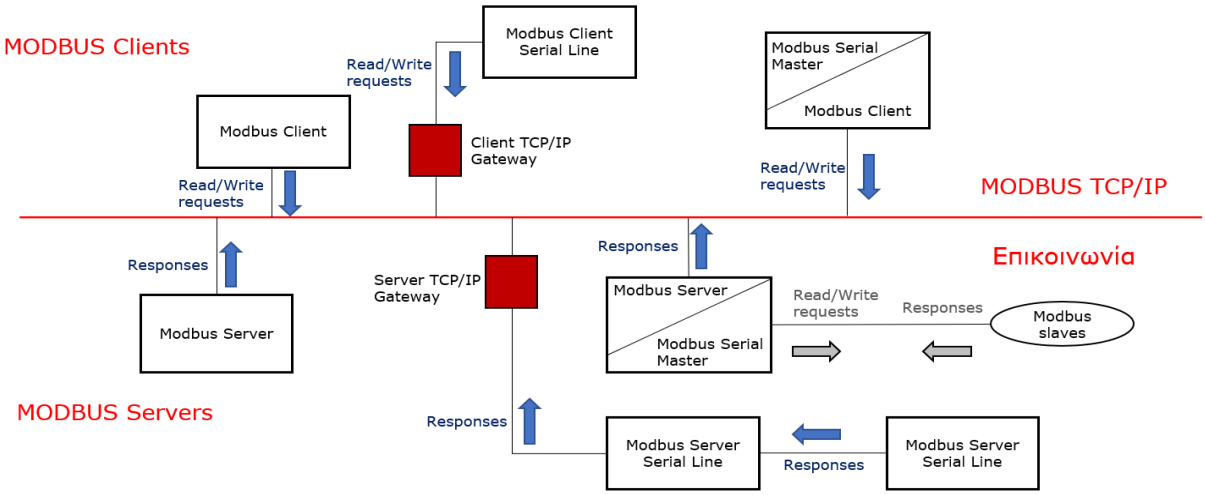
Σχήμα 2.3 – 8 συνηθισμένα Modbus - Function Codes

2.2.3. Διαμόρφωση Δικτύου Modbus και τύποι μηνυμάτων

Πλέον τα περισσότερα συστήματα Modbus όπως αναφέρθηκε εκτενώς χρησιμοποιούν το TCP/IP. Η προδιαγραφή του πρωτοκόλλου καθορίζει μια ενσωμάτωση των πακέτων Modbus στο TCP/IP και έτσι η κοινότητα του Ίντερνετ μπορεί να έχει πρόσβαση στη δεσμευμένη θύρα 502 της TCP/IP στοίβας. Η επικοινωνία τύπου πελάτη-διακομιστή που παρέχει η TCP/IP μορφή του πρωτοκόλλου επιτρέπει μεγάλη ευελιξία στην διαμόρφωση της αρχιτεκτονικής του

επικοινωνιακού δικτύου σε σχέση με μια αρχιτεκτονική σειριακής επικοινωνίας όπου επιτρέπεται μόνο μία κύρια συσκευή ως συντονιστής της επικοινωνίας με συσκευές χαμηλότερου επιπέδου. Αντιθέτως, το Modbus TCP παρέχει δυνατότητα επικοινωνίας μεταξύ διαφορετικών «κύριων» συσκευών-πελάτη και συσκευών-διακομιστή χαμηλότερου επιπέδου σε ένα κοινό δίκτυο. Ακόμη, στο κοινό δίκτυο επικοινωνίας Modbus/TCP μπορεί να συνδέονται και τα σειριακά δίκτυα χρησιμοποιώντας γέφυρες (bridges), δρομολογητές (routers) ή πύλες (Server TCP/IP Gateways). Έτσι το σειριακό Modbus RTU μεταφράζεται εύκολα σε TCP/IP και κύριες σειριακές συσκευές σειριακής επικοινωνίας που μπορούν να υποστηρίξουν και τους δύο τύπους μπορούν να πάρουν την μορφή ενός πελάτη ή διακομιστή στην κοινή επικοινωνία.

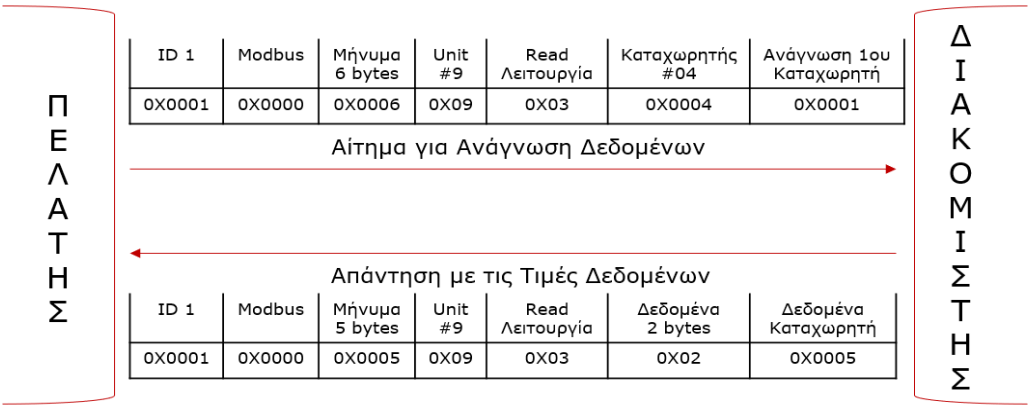
Μια **τυπική αρχιτεκτονική δικτύου** επικοινωνίας Modbus φαίνεται στο παρακάτω Σχήμα 2.4:



Σχήμα 2.4 – Παράδειγμα αρχιτεκτονικής ενός δικτύου Modbus

Στην παραπάνω αρχιτεκτονική μπορούμε να διακρίνουμε ότι οι TCP-IP πύλες από το σειριακό μέρος μπορεί να είναι πάνω από μία σε έναν Modbus δίκτυο. Αυτό πρακτικά σημαίνει ότι το ίδιο πρωτόκολλο, ως προς την δομή και τις βασικές αρχές που το διέπουν, διαφέρει από την σειριακή λογική όπου η επικοινωνία είναι καθετοποιημένη με αυστηρή ιεραρχία και δημιουργεί ένα πλέγμα επικοινωνίας με πολλές διακλαδώσεις. Υπάρχει δηλαδή μεγαλύτερη ευελιξία στην επικοινωνία μεταξύ των διαφόρων συσκευών του συστήματος βελτιστοποιώντας έτσι την διάχυση της πληροφορίας με άμεσο τρόπο σε όλα τα στρατηγικά σημεία του δικτύου επικοινωνίας.

Ωστόσο, για να επιτευχθεί μια εύκολη διασύνδεση σειριακών γραμμών με το TCP/IP επίπεδο, το Modbus σε επίπεδο εφαρμογής διατηρεί τις βασικές του αρχές και την μορφή των μηνυμάτων. Ως ένα **πρωτόκολλο αιτήματος/απάντησης** ο πελάτης θα συντονίζει και θα εκκινεί μια συνομιλία χρησιμοποιώντας τις τεχνικές συνομιλίας που καθορίζονται από το πρωτόκολλο. Το παρακάτω σχήμα 2.5 φωτογραφίζει ένα στιγμιότυπο ανταλλαγής μηνυμάτων μεταξύ δύο τυχαίων συσκευών, όπου ο πελάτης αποστέλλει ένα μήνυμα αιτήματος και ο διακομιστής επιστρέφει την απάντησή του.



Σχήμα 2.5 - Παράδειγμα αιτήματος και απάντησης λειτουργίας READ

Τα μηνύματα αιτήματος μπορεί να είναι είτε **ιδιωτικά** σε κάποιον μεμονωμένο διακομιστή είτε ως μια **εκπομπή του ίδιου αιτήματος** προς όλες τις συσκευές (broadcast messages) με την χρήση του αναγνωριστικού μονάδας «unit ID = 0». Στην συνέχεια ο διακομιστής ή **οι διακομιστές που ερωτήθηκαν οφείλουν να επιστρέψουν με την απάντηση που αντιστοιχεί στο αίτημα**. Σε περιπτώσεις που αυτή η αρχή διαρρηγνύεται (πχ. Οι διακομιστές στέλνουν απαντήσεις χωρίς να έχει προηγηθεί κάποιο αίτημα ή απαντά διαφορετικός διακομιστής από αυτόν που έλαβε αίτημα πελάτη) τότε υπάρχει η πιθανότητα εξωτερικής εισβολής στην επικοινωνία του συστήματος και πρέπει να αναζητηθούν τρόποι επίλυσης ώστε να διασφαλισθεί η ακεραιότητα και η αποτελεσματικότητα της επικοινωνίας. Τέτοιες εισβολές και αντίστοιχους τρόπους ανίχνευσης και επίλυσης θα αναζητήσουμε στα επόμενα κεφάλαια της διπλωματικής εργασίας.

2.2.4. Σημαντικά οφέλη και μειονεκτήματα επικοινωνίας Modbus

Η ανάπτυξη του σειριακού Modbus σε πρωτόκολλο διαδικτύου από μόνη της σημαίνει σημαντική εξέλιξη στην δίκτυο επικοινωνίας μια εφαρμογής. Η αναβάθμιση του πρωτοκόλλου από τα κλασικά συστήματα σειριακών διαύλων σε σύγχρονα συστήματα βασισμένα στο TCP/IP και η ενσωμάτωση του σε ολοένα και περισσότερες βιομηχανικές εφαρμογές συστημάτων ελέγχου δημιουργεί νέες δυνατότητες αλλά και κινδύνους. Επιγραμματικά, η γρήγορη και πολυεπίπεδη μεταφορά δεδομένων καθώς και σημαντική μείωση του κόστους εγκατάστασης του δικτύου, με την χρήση καλωδίων Ethernet της Τεχνολογίας Πληροφορικής και Επικοινωνιών (ICT) αποτελούν τα μεγαλύτερα οφέλη που προσφέρει το εξελιγμένο πρωτόκολλο.

Με την διεξαγωγή μια σύγκρισης μεταξύ Modbus RTU και Modbus/TCP μπορούμε να καταγράψουμε κάποιες ουσιαστικές διαφορές, οι οποίες μπορούν να θεωρηθούν και ως **προτερήματα του εξελιγμένου πρωτοκόλλου έναντι του σειριακού**. Κατόπιν μελέτης των δύο εκδόσεων, τα βασικά οφέλη που προσδίδει στην διαμόρφωση του δικτύου επικοινωνίας η μετάβαση σε Modbus/TCP καταγράφονται παρακάτω:

- **Συνδεσμολογία**: Η φυσική σύνδεση των συσκευών αποτελεί την πιο βασική διαφορά ως προς την εγκατάσταση στο πεδίο. Με το σειριακό πρωτόκολλο η σύνδεση συσκευών γίνεται μέσω ενός ενσύρματου συνδέσμου (RS485 ή RS-232) που ενώνει αλυσιδωτά (ή με δίαυλο) τα μέρη που επικοινωνούν μεταξύ τους. Η παραπάνω συνδεσμολογία μπορεί να είναι περίπλοκη και ευαίσθητη με

αποτέλεσμα την συχνή διακοπή της επικοινωνίας από εξωγενής παράγοντες, όπως η φθορά. Αντίθετα, με το Modbus TCP/IP οι συσκευές συνδέονται εύκολα μεταξύ τους μέσω μια κλασικής συνδεσμολογίας Ethernet. Παραδείγματος χάρη σε ένα switch, κατευθείαν πάνω στο δίκτυο.

- **Ταχύτητα μετάδοσης δεδομένων**: Το Modbus RTU έχει μέγιστη ταχύτητα μετάδοσης δεδομένων 115,2 kbps, ενώ το Modbus TCP/IP μπορεί να μεταδώσει δεδομένα σε πολύ μεγαλύτερες ταχύτητες, έως και 100 Mbps.
- **Επίπεδο εφαρμογής**: Η εξέλιξη του πρωτοκόλλου ανέδειξε νέα πεδία εφαρμογών όπου η επικοινωνία μπορεί να υλοποιηθεί με Modbus. Το Modbus RTU χρησιμοποιείται ευρέως σε ενσωματωμένα συστήματα και βιομηχανικές εφαρμογές, κυρίως στο χαμηλότερο επίπεδο της καθετοποιημένης ιεραρχίας του δικτύου (δηλ. διαμοιρασμένα I/O ή Λογικοί Ελεγκτές με αισθητήρες και ενεργοποιητές). Πλέον το Modbus TCP εμφανίζεται και σε ανώτερα επίπεδα ελέγχου για επικοινωνία μεταξύ των λογικών ελεγκτών, λογικών ελεγκτών με συστήματα SCADA, ή άλλα συστήματα επίβλεψης και ελέγχου.
- **Διάχυση πληροφορίας:** Λόγω της αρχιτεκτονικής πελάτη/διακομιστή που μελετήθηκε στην προηγούμενη υποενότητα, η πληροφορία μεταφέρεται αποτελεσματικά σε περισσότερα σημεία ενός συστήματος και γίνεται άμεσα προσβάσιμη από πολλούς χρήστες σε διαφορετικά επίπεδα της ιεραρχίας του δικτύου.
- **Κόστος:** Η χρήση καλωδίου Ethernet από μόνη της μπορεί να μειώσει σημαντικά το κόστος μια εφαρμογής συγκριτικά με την καλωδίωση που απαιτεί μια σειριακή επικοινωνία. Εκτός αυτού, η υλοποίηση ενός γενικά TCP/IP δικτύου υλοποιείται αποδοτικότερα για την εξοικονόμηση πόρων. Αντιθέτως, μια σειριακή τοπολογία δίνει λιγότερες δυνατότητες βελτιστοποίησης στην εγκατάσταση.

Τα παραπάνω θεωρούνται πέντε πολύ ουσιαστικά πλεονεκτήματα έναντι μιας σειριακής επικοινωνίας. Παρ' όλα αυτά, έχει μεγαλύτερη ουσία να αντιμετωπίσουμε την οικογένεια Modbus ως ένα σύνολο βιομηχανικών πρωτοκόλλων που συνεργάζονται και συμμετέχουν από κοινού στο σύστημα επικοινωνίας. Συνολικά λοιπόν η επικοινωνία Modbus έχει να προσφέρει σημαντικά πλεονεκτήματα στα προηγμένα ενεργειακά συστήματα. Τα πιο σημαντικά από αυτά αναφέρονται παρακάτω.

1. **Τυποποίηση**: Το Modbus αποτελεί ένα - de facto – τυποποιημένο βιομηχανικό πρωτόκολλο και συναντάται στις περισσότερες εφαρμογές ελέγχου παγκοσμίως. Ιδιαίτερα στον τομέα της ενέργειας, το Modbus είναι ευρέως διαδεδομένο και υποστηρίζεται από τους περισσότερους κατασκευαστές συσκευών και εφαρμογών, με εξειδίκευση στα ηλεκτρικά συστήματα ελέγχου.
2. **Απλότητα**: Είναι εύκολο στην σύνδεση και στην διαμόρφωσή του καθώς οι λειτουργίες του είναι απλές και συγκεκριμένες. Ο τύπος των μηνυμάτων που ανταλλάσσονται είναι επίσης απλός, ως προς την δομή τους, και τυποποιημένος. Συνεπώς ενσωματώνεται σχετικά εύκολα σε υπάρχοντα συστήματα. Η υλοποίησή του μπορεί να απαιτεί μόνο λίγες μέρες. Αυτό είναι μεγάλο πλεονέκτημα σε σχέση με τους μήνες εργασίας που μπορεί να απαιτηθούν για την εκμάθηση και την εφαρμογή άλλων πρωτοκόλλων.
3. **Ευελιξία**: Παρέχει ευελιξία για την διαμόρφωση του δικτύου και πολλαπλές επιλογές επικοινωνίας, σειριακή, Ethernet TCP/IP, Wi-Fi και άλλες.
4. **Επεκτασιμότητα**: Το δίκτυο μπορεί να σχεδιαστεί με διαφορετικούς τρόπους (αστέρι, ιεραρχημένη δομή, δακτύλιος) και μοντέλα επικοινωνίας και άρα μπορεί να υποστηρίξει μεγάλο αριθμό διασυνδεδεμένων συσκευών. Το σύστημα διευθυνσιοδότησης του πρωτοκόλλου υποστηρίζει έως και 65.535 διαφορετικές διευθύνσεις συσκευών, επομένως οι Modbus εφαρμογές είναι εύκολα επεκτάσιμες.

5. **Αξιοπιστία**: Η διαχρονικότητα του αποδεικνύει την αξιοπιστία του στα δίκτυα ηλεκτρικής ενέργειας, παρέχοντας σταθερό και αξιόπιστο μέσο επικοινωνίας σε υποδομές, ζωτικής σημασίας για τον άνθρωπο. Οι εφαρμογές Modbus συγκρατούν πολλά αντίγραφα δεδομένων (πχ. αντίγραφα δικτύου, συσκευών, κ.ά) πράγμα που βοηθά στην αντιμετώπιση μεμονωμένων σφαλμάτων επικοινωνίας εξασφαλίζοντας ότι η επικοινωνία παραμένει λειτουργική

Η ανάπτυξη του Modbus που προσφέρει όλα τα παραπάνω οφέλη έχει οδηγήσει πολλούς δημόσιους -και μη- οργανισμούς στην ενσωμάτωση του πρωτοκόλλου σε κρίσιμα συστήματα ελέγχου. Ωστόσο, αυτό δεν σημαίνει ότι η επικοινωνία Modbus παραμένει πάντα ασφαλή και αδιάβλητη. Δυστυχώς, το πρωτόκολλο δεν αναπτύχθηκε με γνώμονα την ασφάλεια της επικοινωνίας και μπορεί να γίνει ευάλωτο σε κακόβουλα λογισμικά.

Το Modbus δεν διαθέτει βασικούς μηχανισμούς ασφαλείας, γεγονός που εμφανίζει πολλαπλές ευπάθειες τόσο στο σχεδιασμό του όσο και στην υλοποίησή του. Η εκμετάλλευση των διάφορων ευπαθειών μπορεί να οδηγήσει ορισμένους τύπους κυβερνοεπιθέσεων (πχ. MITM, παρακολούθησης επικοινωνία, κ.ά) και να επηρεάσει σε μεγάλο βαθμό εταιρείες και τον γενικό πληθυσμό. Για παράδειγμα κακόβουλες ενέργειες μπορούν να στοχεύσουν σε κρίσιμες -για τον άνθρωπο- υποδομές, όπως τα εργοστάσια παραγωγής ηλεκτρικής ενέργειας.

Το πρώτο βήμα για την αντιμετώπιση πιθανών κινδύνων σε ένα κυβερνοσύστημα είναι η **αναφορά των τρωτών σημείων της επικοινωνίας** που χρησιμοποιείται. Παρακάτω καταγράφονται βασικά σημεία του Modbus όπου παρατηρούνται ζητήματα έλλειψης ασφάλειας:

1. **Δομή Μηνύματος**: Ένα Modbus ADU, όπως μελετήθηκε προηγουμένως (βλ. Σχήμα 2.2), δεν πιστοποιεί σε κανένα σημείο την ταυτότητα του αποστολέα ή του παραλήπτη. Δηλαδή δεν παρέχονται κατάλληλοι μηχανισμοί εξουσιοδότησης ώστε να ανιχνεύουν και να απορρίπτουν εγχυμένα πακέτα. Συνεπώς όποιος αποκτά πρόσβαση στο δίκτυο μπορεί ανεμπόδιστα να γράφει, να διαβάζει ή να λαμβάνει δεδομένα από μια συνομιλία. Αυτή η ευπάθεια ονομάζεται **έλλειψη αυθεντικοποίησης**.
2. **Περιεχόμενο Μηνύματος**: Όλα τα μηνύματα Modbus που ανταλλάσσονται στο μέσο μετάδοσης έχουν την μορφή απλού κειμένου, χωρίς κρυπτογράφηση. Αυτό σημαίνει ότι σε περίπτωση παρεμβολής στην επικοινωνία από κάποιον κακόβουλο εξωτερικό παράγοντα, ο εισβολέας μπορεί εύκολα να διαβάσει ή να τροποποιήσει τα δεδομένα. Αναδεικνύονται έτσι σοβαρά **ζητήματα έλλειψης εμπιστευτικότητας και ακεραιότητας**.
3. **Σύνδεση TCP**: Στο Modbus/TCP η επικοινωνία μεταξύ των συσκευών ενσωματώνεται σε μία μόνιμη σύνδεση TCP χρησιμοποιώντας τη δεσμευμένη θύρα 502 για την τοπική ή απομακρυσμένη αποστολή και λήψη μηνυμάτων. Συνεπώς ένας επιτιθέμενος για να εισβάλλει στην επικοινωνία θα πρέπει να «κλέψει», ή να αντικαταστήσει με μια άλλη, την υπάρχουσα TCP σύνδεση. Ωστόσο οι πιο προηγμένοι και σύγχρονοι ελεγκτές για διευκόλυνση της επικοινωνίας διαθέτουν πολλαπλές ταυτόχρονες συνδέσεις στην θύρα 502. Αυτή δυνατότητα μπορεί να λειτουργήσει και ως ευκαιρία για πιθανούς εισβολείς να πετύχουν πιο απλές επιθέσεις, κάνοντας την επικοινωνία ακόμη πιο ευάλωτη.
4. **Εφαρμογές Διαδικτύου:** Με την ενσωμάτωση του Modbus στο IP πρωτόκολλο, τα παραδοσιακά περιβάλλοντα επιχειρησιακών τεχνολογιών δεν είναι πια απομονωμένα. Τα νέα συστήματα απομακρυσμένου ελέγχου εκμεταλλεύονται ολοένα και περισσότερο τις δυνατότητες που προσφέρει η TCP/IP επικοινωνία αναπτύσσοντας εφαρμογές στο Ίντερνετ γεγονός που δημιουργεί νέες

προκλήσεις για την ασφάλεια δεδομένων και επικοινωνίας. Οι Modbus συσκευές σε συστήματα IoT βρίσκονται πολύ **εκτεθειμένες σε επιθέσεις βασιζόμενες στο δίκτυο**, όπως σάρωση θυρών (port scanning) ή επιθέσεις άρνησης υπηρεσίας (DoS).

Περισσότερους τύπους επιθέσεων που εκμεταλλεύονται τις παραπάνω ευπάθειες θα συναντήσουμε αναλυτικότερα στο Κεφάλαιο 3.

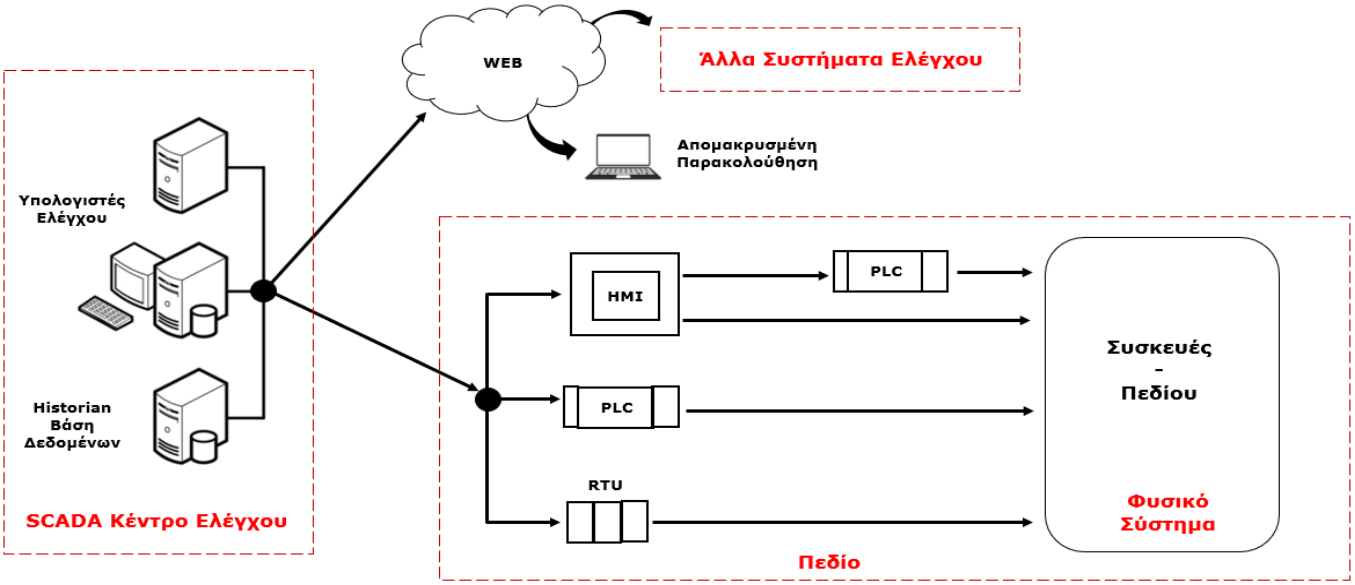
2.2.5. Συστήματα και συσκευές επικοινωνίας Modbus

Σε γενικά πλαίσια, το Modbus χρησιμοποιείται για την επικοινωνία μεταξύ συσκευών στο πλαίσιο ενός βιομηχανικού δικτύου. Η απλότητα της σειριακής επικοινωνίας ως προς τους κανόνες της και το περιεχόμενο των μνημάτων καθιστά το πρωτόκολλο ιδανικό για την διαχείριση ακατέργαστων δεδομένων κατευθείαν από το πεδίο. Οι συσκευές που το υποστηρίζουν μπορεί να είναι αισθητήρες, ελεγκτές, προγραμματιζόμενοι λογικοί ελεγκτές, μετρητές, μονάδες ελέγχου κίνησης και άλλες παρόμοιες συσκευές στο φυσικό περιβάλλον της παραγωγής.

Από την ανάλυση που προηγήθηκε σχετικά με την αναβάθμιση και τις υπηρεσίες που προσφέρει πλέον το Modbus, συμπεραίνουμε ότι η χρήση του δεν μπορεί να περιοριστεί μόνο στον τοπικό έλεγχο της παραγωγής (πχ. Στον Αυτόματο Ρυθμιστή της Τάσης ή τον τοπικό έλεγχο στροφών). Η δομή και η αρχιτεκτονική της επικοινωνίας του **Modbus TCP διευκολύνει σε μεγάλο βαθμό τη μεταφορά της φυσικής πληροφορίας από το πεδίο παραγωγής σε κάποιο απομακρυσμένο κέντρο**. Επεκτάθηκε λοιπόν ως μέσω επικοινωνίας στα ανώτερα επίπεδα παρακολούθησης της μονάδας παραγωγής και σε γενικότερα επιχειρησιακά συστήματα ελέγχου. Συστήματα **Αυτομάτου Ελέγχου Παραγωγής** (AGC), για παράδειγμα, που απαιτούν τηλεμετρία και απομακρυσμένο έλεγχο δεδομένων της παραγωγής, μπορούν να επικοινωνήσουν με τα χαμηλότερα επίπεδα μέσω ενός Modbus δικτύου.

Συγκεκριμένα, το πρωτόκολλο έχει γίνει ένα από τα πιο δημοφιλή πρωτόκολλα επικοινωνίας για την σύνδεση διαφορετικών συστημάτων ελέγχου με το **κεντρικό σύστημα Ανταλλαγής Δεδομένων και Απόκτησης Δεδομένων - SCADA**. Μπορεί επίσης να χρησιμοποιηθεί για την επικοινωνία μεταξύ διαφορετικών συστημάτων SCADA που βασίζονται σε διαφορετικά πρωτόκολλα επικοινωνίας ή για την μεταφορά πληροφοριών από το SCADA στα ανώτερα κέντρα ελέγχου. Οι δυνατότητες που δίνει το πρωτόκολλο στο SCADA, ώστε να **παρακολουθεί σε πραγματικό χρόνο και από μακρινές τοποθεσίες** τις διεργασίες που εκτελούνται στο πεδίο μιας ηλεκτρικής εγκατάστασης αποτελεί και τον βασικό λόγο διάδοσής του σε τέτοιου είδους εφαρμογές.

Σχήμα 2.6 - Διάγραμμα διασύνδεσης συστημάτων και συσκευών Modbus



Σε επίπεδο συσκευών, η διασύνδεση του Modbus μπορεί να γίνει με οποιοδήποτε είδος συσκευής ελέγχου που υποστηρίζει το πρωτόκολλο, συμπεριλαμβανομένων των ελεγκτών PLC, Διεπαφών Χρήστη-Μηχανής (HMIs), απομακρυσμένων μονάδων εισόδων/εξόδων (RTU) και ειδικών εξαρτημάτων, οργάνων μέτρησης και ενεργοποίησης που βρίσκονται στο πεδίο. Σε μια τυπική αρχιτεκτονική δικτύου Modbus διασυνδέονται συσκευές όπως φαίνεται στο παρακάτω Σχήμα *(2.6).*

Τέλος θα πρέπει να αναφέρουμε ότι, η μεγάλη διάδοση του Modbus σε συστήματα ελέγχου στην βιομηχανική αυτοματοποίηση έχει οδηγήσει όλους τους κατασκευαστές που δραστηριοποιούνται στον τομέα να ενσωματώνουν το Modbus στα προϊόντα τους. Ακόμη και ανταγωνιστικά πρωτόκολλα επικοινωνίας στην αγορά, όπως το Profibus ή CC-Link είναι σε μεγάλο βαθμό βασισμένα στην λογική του Modbus και οι περισσότερες συσκευές που τα υποστηρίζουν διαθέτουν ταυτόχρονα και Modbus επικοινωνία, ώστε να παρέχουν δυνατότητες ενσωμάτωσης σε υπάρχοντα συστήματα. Αυτήν την στιγμή το Modbus υποστηρίζεται από τουλάχιστον 2000 κατασκευαστές ανά τον κόσμο.

2.3. Πρωτόκολλο επικοινωνίας DNP3

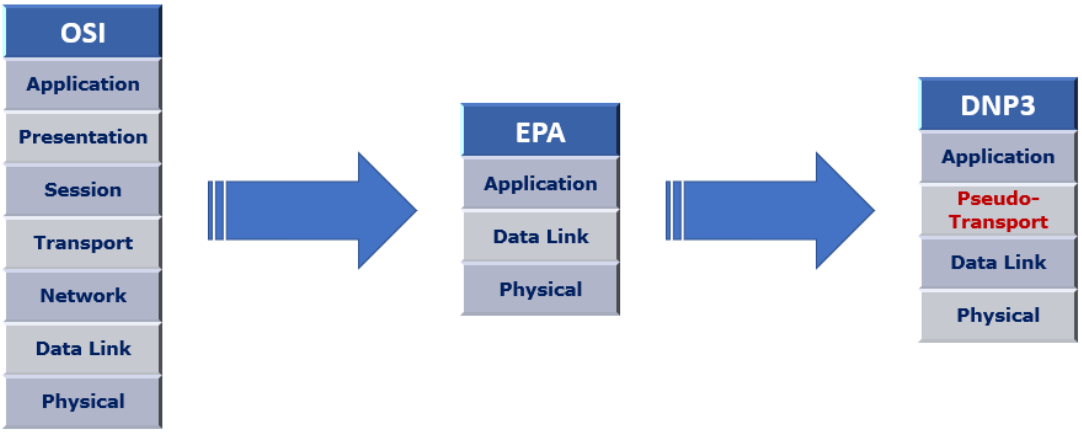
Ορισμός: Το DNP 3.0 (Πρωτόκολλο Κατανεμημένου Δικτύου, 3η Έκδοση), ή απλώς DNP3, είναι ένα σύνολο πρωτοκόλλων επικοινωνίας που χρησιμοποιούνται σε συστήματα αυτοματοποίησης διεργασιών και ιδιαίτερα σε εφαρμογές αυτοματοποίησης συστημάτων ηλεκτρικής ενέργειας. Αναπτύχθηκε για την επικοινωνία μεταξύ διάφορων τύπων εξοπλισμού απόκτησης και ελέγχου δεδομένων, όπως βάσεις δεδομένων και υπολογιστές SCADA, μονάδες απομακρυσμένου τερματισμού (RTUs) και έξυπνες ηλεκτρονικές συσκευές (IEDs). Ανακαλύφθηκε στις αρχές της δεκαετίας του '90 για να καλύψει τις ανάγκες κρίσιμων ηλεκτρικών υποδομών στην Αμερική. Πλέον θεωρείται ως ένα αξιόπιστο και αποδοτικό πρωτόκολλο και χρησιμοποιείται ευρέως σε αμερικάνικες -και όχι μόνο- βιομηχανίες ηλεκτρικής ενέργειας.

2.3.1. Γενικές πληροφορίες για το μοντέλο επικοινωνίας DNP3

Η πρωταρχική ιδέα ήταν η κατασκευή ενός κατάλληλου πρωτοκόλλου επικοινωνίας για τηλεμετρία και συστήματα ανάκτησης δεδομένων, το οποίο θα ανταποκρίνεται στις απαιτήσεις ενός βιομηχανικού περιβάλλοντος. Οι πρώτες αρχιτεκτονικές SCADA, βασίζονταν σε κυκλώματα επικοινωνίας που ήταν αρκετά ευαίσθητα με αποτέλεσμα την συχνή παραμόρφωση των σημάτων επικοινωνίας. Ιδιαίτερα σε εφαρμογές Υψηλής και Μέσης τάσης, όπου ο θόρυβος είναι μεγάλος, η ανάγκη ύπαρξης μιας ανθεκτικής επικοινωνίας ήταν και είναι επιτακτική.

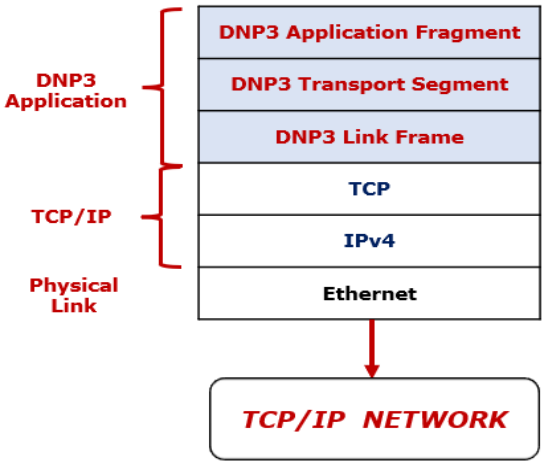
Η Διεθνής Επιτροπή Ηλεκτροτεχνικών Προδιαγραφών (IEC) αρχικά συνέστησε το πρότυπο IEC 870 για εφαρμογές μετάδοσης δεδομένων τηλεμετρίας σε συστήματα βασισμένα στο μοντέλο Open Systems Interconnection (OSI). Τα επίπεδα πρωτοκόλλων που χρησιμοποιεί το μοντέλο φαίνονται στον πρώτο πίνακα του κεφαλαίου (Σχήμα 2.1). Ωστόσο, το OSI είναι ένα γενικό και πολυεπίπεδο μοντέλο που περιλαμβάνει και περιττά επίπεδα, για μια εφαρμογή SCADA. Την παράλειψη των επιπέδων αυτών πετυχαίνει η δημιουργία μιας **Αρχιτεκτονικής Ενισχυμένης Απόδοσης (EPA)** στην επικοινωνία. Το μοντέλο EPA είναι πιο συνοπτικό και περιλαμβάνει μόνο τρία βασικά επίπεδα πρωτοκόλλων: την Εφαρμογή, την Σύνδεση δεδομένων και το Φυσικό επίπεδο. Ωστόσο, το EPA δεν είχε την δυνατότητα να υποστηρίξει τα μηνύματα επιπέδου εφαρμογής που ήταν μεγαλύτερα από το μέγιστο μέγεθος ενός πλαισίου Σύνδεσης Δεδομένων.

Η ανάπτυξη του DNP3 πάτησε πάνω σε αυτόν τον περιορισμό και ενσωμάτωσε στο μοντέλο EPA ένα ψευδο-επίπεδο μεταφοράς για τη δυνατότητα κατάτμησης των μεταφερόμενων μηνυμάτων. Στο σχήμα 2.7 αντιπαραβάλλεται διαγραμματικά η εξέλιξη των επιπέδων στα μοντέλα που ακολουθούσε η επικοινωνία SCADA έως την ανάπτυξη του DNP3.



Σχήμα 2.7 - Μοντέλο επικοινωνίας DNP3

Η επικοινωνία DNP3 μπορεί να υλοποιηθεί μέσω διάφορων φυσικών μέσων, συμπεριλαμβανομένων των σειριακών συνδέσεων (πχ. RS-485). Ωστόσο, τα σύγχρονα συστήματα SCADA χρησιμοποιούν συνήθως το DNP3 βασισμένο στο Ethernet Για την ενσωμάτωση του πρωτόκολλο στην IP στοίβα, η DNP κοινότητα ορίζει ρητά ότι τα τρία βασικά επίπεδα του πρωτοκόλλου (Εφαρμογή, Μεταφορά και Σύνδεση) δεν πρέπει να τροποποιηθούν. Για αυτό το λόγο, τα τρία DNP3 επίπεδα τοποθετούνται απευθείας πάνω από τα στρώματα TCP/IP ή UDP/IP στην ιεραρχία της στοίβας. Παρακάτω σχηματοποιείται ένα παράδειγμα εφαρμογής του DNP3 πάνω στα TCP/IP πρωτόκολλα.



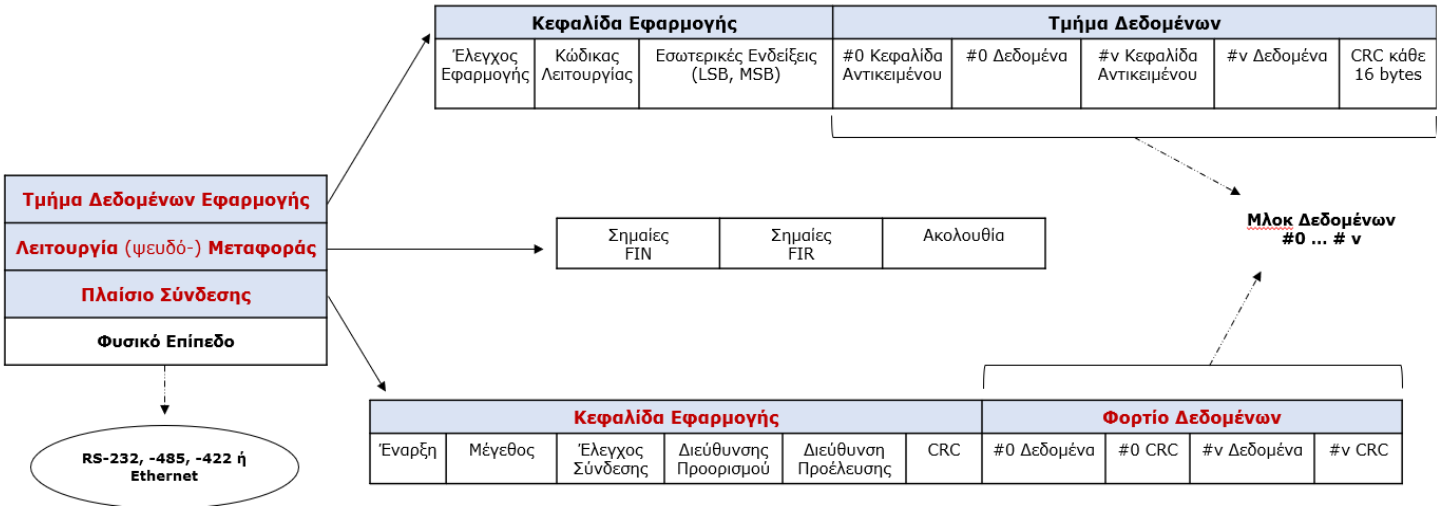
Από τα σχήμα 2.8 γίνεται κατανοητό ότι τα επίπεδα του DNP3 δεν διατηρούν το επίπεδό τους στην νέα στοίβα ούτε τροποποιούνται κατά την ενσωμάτωσή τους στα TCP και IP πρωτόκολλά. Αντιθέτως, διατηρούν την μορφή και την ιεραρχία μεταξύ τους διαμορφώνοντας ένα **κοινό τρι-επίπεδο τμήμα DNP3- Εφαρμογής**.

Η δομή των τριών επιπέδων του DNP3 θα αναλυθεί εκτενώς στην ενότητα που ακολουθεί.

Σχήμα 2.8 – Εφαρμογή DNP3 στην TCP/IP στοίβα.

2.3.2. Η εσωτερική δομή των DNP3 επιπέδων εφαρμογής

Στα πλαίσια του EPA μοντέλου, λοιπόν, το DNP3 προδιαγράφει δύο πρωτόκολλα δύο διαφορετικών επιπέδων και μια πρόσθετη λειτουργία. Αρχικά, προσδιορίζει ένα πρωτόκολλο στο **επίπεδο Σύνδεσης Δεδομένων** (2ο), το οποίο παρέχει υπηρεσίες κατακερματισμού δεδομένων, έλεγχο σφαλμάτων, έλεγχο σύνδεσης, προτεραιοποίηση και υπηρεσίες διευθυνσιοδότησης δεδομένων 2ου επιπέδου. Επίσης δημιουργεί **λειτουργίες μεταφοράς**, οι οποίες είναι παρόμοιες με εκείνες του 4ου επιπέδου στο μοντέλο OSI. Τέλος, το DNP3 θα καθορίσει και το **επίπεδο Εφαρμογής** (7ο επίπεδο), το οποίο περιλαμβάνει λειτουργίες και γενικούς τύπους δεδομένων κατάλληλους για κοινές εφαρμογές SCADA. Ακολουθεί η παρουσίαση των τριών επιπέδων στο σχήμα 2.9 και στις επιμέρους περιγραφές των τμημάτων τους.



Σχήμα 2.9 – Επίπεδα DNP3 και επιμέρους τμήματά

1. **Πλαίσια Σύνδεσης-Δεδομένων**: Το πρωτόκολλο παρέχει μια αξιόπιστη λογική σύνδεσης μεταξύ συσκευών για τη διευκόλυνση της μεταφοράς μηνυμάτων σχηματοποιημένων σε πλαίσια. Έχει μέγιστο μέγεθος 292 bytes (10-byte η κεφαλίδα και 282 bytes το τμήμα δεδομένων). Οι βασικές λειτουργίες που παρέχει η κεφαλίδα είναι ο σχηματισμός πλαισίων μηνυμάτων, οι κώδικες ελέγχου, η επιβεβαίωση σύνδεσης, διευθυνσιοδότηση και η ανίχνευση σφάλματος CRC.
   Το επίπεδο Σύνδεσης Δεδομένων περιλαμβάνει τα παρακάτω πεδία:

- **Πεδίο έναρξης:** Η κεφαλίδα ξεκινά με την τιμή "05 64" (2- bytes), η οποία προσδιορίζει στον παραλήπτη από πού ξεκινάει το πλαίσιο του μηνύματος. Κάθε φορά που εμφανίζεται η συγκεκριμένη ακολουθία, σημαίνει ότι ξεκινά ένα νέο πλαίσιο.
- **Πεδίο μεγέθους**: Η τιμή μεγέθους υποδηλώνει το μέγεθος του υπόλοιπου πλαισίου, εξαιρουμένου του κώδικα CRC.
- **Έλεγχος σύνδεσης:** Σε αυτό το πεδίο εμπεριέχονται δεδομένα που ελέγχουν την ροή του μηνύματος και καθορίζουν την γενική λειτουργία του πλαισίου. Στα πρώτα 4 bit καθορίζονται η κατεύθυνσης του μηνύματος, κύρια συσκευή προς έναν εξωτερικό σταθμό ή αντίστροφα, αν η συνομιλία ξεκινά από πρωτεύουσα ή δευτερεύουσα συσκευή και 2 σημαίες για τον συγχρονισμό επικοινωνίας και έλεγχο ροής. Τα τελευταία 4-bit αποτελούν τον κώδικα λειτουργίας που καθορίζει την λειτουργία του πλαισίου.
- **Πεδία Διευθυνσιοδότησης**: Τα πεδία αυτά είναι πολύ σημαντικά για την DNP3 επικοινωνία καθώς η λειτουργία διευθυνσιοδότησης υλοποιείται αποκλειστικά στο επίπεδο σύνδεσης και όχι στο επίπεδο εφαρμογής. Συγκεκριμένα ορίζει δύο πεδία των 16 bits το τέλος της κεφαλίδας, πριν τον CRC. Το πρώτο πεδίο καθορίζει τον παραλήπτη ή τους παραλήπτες σε περίπτωση αποστολής μηνύματος πολλαπλής εκπομπής (0xFFFF). Το δεύτερο πεδίο υποδηλώνει την διεύθυνση του δημιουργού και αποστολέα του μηνύματος.
- **CRC**: Πρόκειται για έναν κωδικό επαλήθευσης της ακεραιότητας της μετάδοσης και υποδηλώνει το τέλος των στοιχείων της κεφαλίδας.
- **Φορτίο Δεδομένων**: Στο τμήμα που ακολουθεί την κεφαλίδα υπάρχει το πραγματικό φορτίο δεδομένων που μεταδίδονται και μπορεί να έχει μέγεθος έως 282 bytes. Τα συνολικό φορτίο περιλαμβάνει δεδομένα χωρισμένα 16-bit μπλοκς. Στο τέλος κάθε μπλοκ υπάρχει ένας CRC για επιπλέον έλεγχο.

2. **Λειτουργία Μεταφοράς**: Το ψευδό-επίπεδο μεταφοράς (με μέγιστο μέγεθος 250 bytes) χειρίζεται τον κατακερματισμό και την εκ νέου συναρμολόγηση πλαισίων από το επίπεδο σύνδεσης στο επίπεδο εφαρμογής και αντίστροφα. Αποτελείται από δύο σημαίες, FIR και FIN και έναν αριθμός ακολουθίας. Οι σημαίες FIR (first bit) και FIN (final bit) υποδεικνύουν το πρώτο και το τελευταίο πλαίσιο που περιλαμβάνονται σε ένα κατακερματισμένο μήνυμα. Ο αριθμός ακολουθίας, ο οποίος αυξάνεται για κάθε διαδοχικό πλαίσιο, χρησιμοποιείται για την επανασυναρμολόγηση μηνυμάτων ώστε να μπορέσει το επίπεδο εφαρμογής να τα επεξεργαστεί. Αντίστροφα, η λειτουργία μεταφοράς επιτρέπει στα μηνύματα εφαρμογής, τα οποία είναι μεγαλύτερα από ένα πλαίσιο σύνδεσης δεδομένων, τον κατακερματισμό τους σε περισσότερα πλαίσια.

3. **Επίπεδο Δεδομένων Εφαρμογής**: Το επίπεδο της Εφαρμογής αντίστοιχα χωρίζεται σε κεφαλίδα και φορτίο δεδομένων. Η κεφαλίδα καθορίζει αν το μήνυμα είναι αίτημα κύριας συσκευής ή απάντηση εξωτερικού σταθμού, την λειτουργία κάθε μηνύματος καθώς επίσης προσφέρει λειτουργίες συγχρονισμού και γεγονότα με χρονοσήμανση. Στο επίπεδο εφαρμογής επίσης διαχωρίζονται τα μηνύματα που υπερβαίνουν το επιτρεπόμενο μέγεθος, το οποίο

προσδιορίζεται από το μέγεθος της προσωρινής μνήμης (buffer) του δέκτη. Το τυπικό μέγιστο όριο μεγέθους ενός μηνύματος είναι 2048 και 4096 bytes.
Η κεφαλίδα των μνημάτων αναλύεται στα παρακάτω πεδία:

- **Πεδίο Ελέγχου Εφαρμογής:** Το πεδίο ελέγχου εφαρμογής εκτελεί παρόμοιες λειτουργίες με την κεφαλίδα της Σύνδεσης, με την διαφορά ότι βρίσκονται σε ανώτερο επίπεδο. Αρχικά, υπάρχουν δύο σημαίες για να προσδιορίσουν το άνω και κάτω όριο του μηνύματος και τον ακολουθιακό αριθμό για την επανασυναρμολόγηση των πλαισίων σε ένα μήνυμα. του μηνύματος. Υπάρχουν δύο επιπλέον σημαίες (CON & UNS) οι οποίες υποδεικνύουν αντιστοίχως εάν το μήνυμα είναι τύπου «επιβεβαίωσης παραλαβής» και εάν πρόκειται για αυτόκλητη απάντηση.
- **Κώδικας Λειτουργίας:** Η τιμή αυτή ουσιαστικά καθορίζει την συγκεκριμένη λειτουργία κάθε μηνύματος. Αυτό το πεδίο χρησιμοποιείται τόσο σε αιτήματα όσο και σε απαντήσεις, αλλά οι διαθέσιμες λειτουργίες αλλάζουν ανάλογα με τον τύπο του μηνύματος. Κάποιοι γνωστοί κώδικες, μεταξύ άλλων, είναι οι παρακάτω:

F.C. (hex)	Κατηγορία
00	Επιβεβαίωση παραλαβής αιτήματος
01	Ανάγνωση
02	Εγγραφή
03-06	Λειτουργίες Ελέγχου
07-0C	Λειτουργίες Παύσης (μετρητών)
0F-10	Αρχικοποίηση δεδομένων εφαρμογής
14-15	Ενεργοποίηση αυτόκλητων μηνυμάτων
16	Ανάθεση Κλάσης
1F	Εφαρμογή ρυθμίσεων διαμόρφωσης
20-22	Αυθεντικοποίηση

Σχήμα 2.10 – Παραδείγματα Κωδικών Λειτουργίας DNP3

- **Εσωτερικές Ενδείξεις:** Στις κεφαλίδες μηνυμάτων απάντησης περιλαμβάνεται ακόμη ένα πεδίο μεγέθους 2-byte για εσωτερικές ενδείξεις (IIN 1& 2). Το πεδίο αυτό επιστρέφει χρήσιμες πληροφορίες για τον κατάσταση του εξωτερικού σταθμού προς την κύρια συσκευή. Κάθε bit στο πεδίο εσωτερικής ένδειξης έχει μια συγκεκριμένη σημασία που ενημερώνεται σε κάθε μήνυμα απάντησης. Παραδείγματα κωδικών IIN είναι η επανεκκίνηση συσκευής, μη έγκυρες παράμετροι, μη υλοποιημένος κωδικός λειτουργίας, άγνωστα ζητούμενα αντικείμενα, κ.ά.

- **Τμήμα Δεδομένων:** Τέλος ένα μήνυμα εφαρμογής ολοκληρώνεται με ένα τμήμα δεδομένων που περιέχει τα πραγματικά δεδομένα της μετάδοσης, τα οποία όμως διαφέρουν από το φορτίο επιπέδου Σύνδεσης. Στην Εφαρμογή τα δεδομένα έχουν αντικειμενοστραφή λογική εισάγοντας πριν το πραγματικό φορτίο κεφαλίδες αντικειμένων που περιλαμβάνουν τέσσερα πεδία καθοριστικά για τα δεδομένα που ακολουθούν. Πρώτον, η ομάδα αντικειμένων καθορίζει αν τα δεδομένα αναφέρονται σε δυαδικές ή αναλογικές εισόδους και εξόδους,

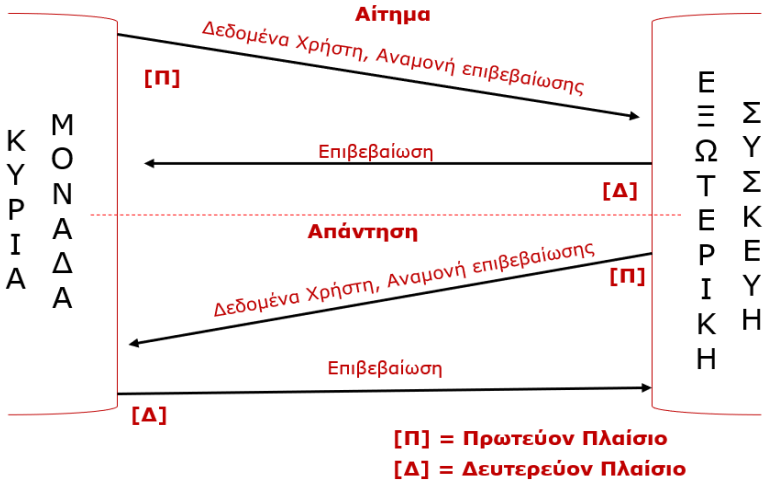
μετρητές κλπ. Δεύτερον η παραλλαγή αντικειμένου καθορίζει τις διάφορες παραλλαγές των αντικειμένων της ομάδας (πχ. Χρονοσήμανση). Τέλος υπάρχουν δύο αλληλεξαρτόμενα πεδία οι κωδικοί ποιοτικοποίησης δεδομένων και το εύρος, που καθορίζουν τον τύπο των δεδομένων.

2.3.3. Αρχή ανταλλαγής μηνυμάτων και αρχιτεκτονικές του δικτύου DNP3

Το DNP3 είναι επίσης ένα πρωτόκολλο (όπως και το Modbus) που αναπτύχθηκε αρχικά για να εφαρμοστεί σε αρχιτεκτονικές σειριακής επικοινωνίας. Για να υποστηρίξει αποδοτικά μια καθετοποιημένη ιεραρχική δομή, τα μηνύματα DNP3 ακολουθούν την αρχή αιτήματος/απάντησης όπου τα αιτήματα αποστέλλονται αποκλειστικά από τις κύριες μονάδες προς τις εξωτερικούς σταθμούς, ενώ οι εξωτερικοί σταθμοί επιστρέφουν απαντήσεις είτε αυτόκλητα είτε επειδή ζητήθηκαν. Για παράδειγμα μια κύρια μονάδα ζητά από μια ή περισσότερες εξωτερικές συσκευές για να ενεργοποιήσουν κάποια φυσική διεργασία, να συλλέξουν και να μεταδώσουν πραγματικά δεδομένα ή να συγχρονίσουν τα εσωτερικά τους ρολόγια.

Πιο συγκεκριμένα οι τύποι των DNP3 μηνυμάτων ταξινομούνται στις παρακάτω τρεις βασικές κατηγορίες. Πρώτον, σε μια **μονοδρομική συνδιαλλαγή (unicast)**, η κύρια μονάδα στέλνει ένα μήνυμα αιτήματος σε μια καθορισμένη εξωτερική συσκευή, η οποία απαντά με ένα μήνυμα απάντησης. Για παράδειγμα, ο master μπορεί να στείλει ένα μήνυμα "ανάγνωσης" όπως ένα αίτημα ανάγνωσης τρέχουσας έντασης ή ένα μήνυμα "εγγραφής" για να εκτελέσει μια ενέργεια ελέγχου όπως να απενεργοποιήσει ένα διακόπτη του κυκλώματος. Η εξωτερική συσκευή πεδίου οφείλει να απαντήσει με το αντίστοιχο μήνυμα (π.χ. αποστολή τιμής της τρέχουσας έντασης, επιβεβαίωση ότι ο διακόπτης κυκλώματος απενεργοποιήθηκε ή ένα μήνυμα σφάλματος). Δεύτερον, Σε μια **συνδιαλλαγή πολλαπλής εκπομπής (broadcast),** ο κεντρικός υπολογιστής στέλνει ένα μήνυμα σε όλες τις συνδεδεμένες εξωτερικές συσκευές ελέγχου στο δίκτυο (π.χ. ένα μήνυμα "εγγραφής" που επαναφέρει αισθητήρες ρεύματος στις προκαθορισμένες ρυθμίσεις). Σε αυτήν την περίπτωση οι εξωτερικές συσκευές δεν επιστρέφουν κάποια απάντηση. Η τρίτη και τελευταία μέθοδος επικοινωνίας περιλαμβάνει **αυτόκλητες απαντήσεις** από τους εξωτερικούς σταθμούς. Αυτές οι απαντήσεις συνήθως χρησιμοποιούνται για την παροχή περιοδικών ενημερώσεων ή ειδοποιήσεων, όπως για παράδειγμα η ανάγνωση έντασης ρεύματος που υπερβαίνει το επιτρεπτό όριο.

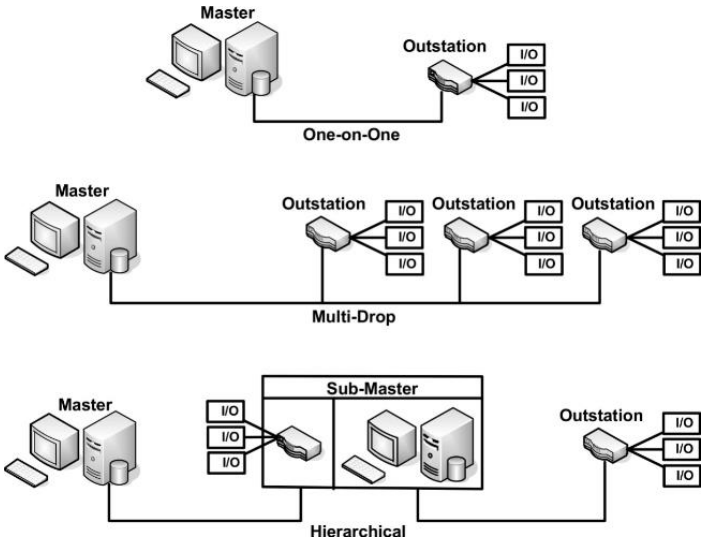
Μια δεύτερη σημαντική κατηγοριοποίηση πλαισίων μηνυμάτων που αναφέρθηκε στην προηγούμενη ενότητα, είναι τα **πρωτεύοντα** και **δευτερεύοντα πλαίσια**. Για κάθε αποστολή μηνύματος αιτήματος ή απάντησης, ακολουθεί ένα μήνυμα επιβεβαίωσης από τον εκάστοτε παραλήπτη προς τον αρχικό αποστολέα. Τα πλαίσια επιβεβαίωσης θεωρούνται δευτερεύοντα ενώ τα πλαίσια που αποτελούν τον πρωταρχικό σκοπό της συνδιαλλαγής θεωρούν πρωτεύοντα. Εισάγεται έτσι μια λογική ελέγχου η οποία υποδηλώνει εάν η διεύθυνση προορισμού παρέλαβε το πρωτεύον μήνυμα επιτυχώς. Αν ένα μήνυμα είναι πρωτεύον [Π] ή δευτερεύον [Δ] δεν καθορίζεται από το εάν ο αποστολέας είναι κύρια ή εξωτερική συσκευή. Ένα σχηματικό παράδειγμα μπορεί να είναι το παρακάτω:



Σχήμα 2.11 – Μηνύματα επιβεβαίωσης παραλαβής μηνύματος

Ως προς την αρχιτεκτονική επικοινωνίας, ένα DNP3 δίκτυο μπορεί να διαμορφωθεί με αντίστοιχους τρόπους όπως και σε ένα Modbus δίκτυο (βλ. ενότητα 2.2). Στο παρακάτω σχήμα (Σχ.2.12) παρουσιάζονται τρεις βασικές αρχιτεκτονικές που μπορεί να υποστηρίξει το πρωτόκολλο.

Σε μια διαμόρφωση "ένα προς ένα", κύρια και εξωτερική μονάδα μοιράζονται μια αποκλειστική σύνδεση, όπως μια τηλεφωνική γραμμή dial-up. Στην δημοφιλή "multi-drop" διαμόρφωση, η κύρια μονάδα επικοινωνεί, συνήθως σειριακά, με περισσότερες συνδεδεμένες συσκευές. Έτσι κάθε εξωτερική μονάδα λαμβάνει κάθε αίτημα από την κύρια, αλλά απαντά μόνο σε μηνύματα που απευθύνονται στην ίδια. Σε μια "ιεραρχική" διαμόρφωση, μια συσκευή μπορεί να συμπεριφέρεται ως εξωτερική μονάδα σε ένα τμήμα ης επικοινωνίας και ταυτόχρονα ως κύρια μονάδα σε ένα άλλο τμήμα. Μια τέτοια διπλή συσκευή ονομάζεται "sub-master".



Σχήμα 2.12 – Αρχιτεκτονικές Δικτύου DNP3

2.3.4. Σχολιασμός επικοινωνίας DNP3 - Σημαντικά οφέλη και μειονεκτήματα

Εστιάζοντας κυρίως σε εφαρμογές απομακρυσμένου ελέγχου και παρακολούθησης μπορούμε εκ πρώτης ανάγνωσης να διαπιστώσουμε ότι το DNP3 διατηρεί βασικές αρχές, που συναντήσαμε στην ενότητα Modbus, τόσο σε λογική ανταλλαγής μηνυμάτων όσο και στην αρχιτεκτονική του δικτύου. Προσφέρεται μια πολυεπίπεδη ανταλλαγή μηνυμάτων αιτήματος και απάντησης που υποστηρίζει εύκολα τόσο επικοινωνία βασισμένη στην TCP/IP στοίβα όσο και την σειριακή για τις συσκευές στην κατώτερη ιεραρχικά βαθμίδα. Εξυπηρετείται δηλαδή ο βασικός στόχος των SCADA συστημάτων που είναι η επικοινωνία των συσκευών πεδίου με τα κέντρα ελέγχου και παρακολούθησης. Παρά τις ομοιότητες που διακρίνουμε στα δύο πρωτόκολλα που αναλύθηκαν έως τώρα, το DNP3 ως ένα πρωτόκολλο που σχεδιάστηκε εξ αρχής για τα συστήματα SCADA εισάγει νέες και προηγμένες λειτουργίες στην επικοινωνία.

Η **προηγμένη λειτουργικότητα** του DNP3 μπορεί να συνοψισθεί στα παρακάτω βασικά οφέλη που προσφέρει στην επικοινωνία:

1. **Αυτόκλητες Αναφορές Δεδομένων**: Οι αυθόρμητες απαντήσεις επιτρέπουν στις συσκευές του πεδίου να στείλουν δεδομένα στο κέντρο ελέγχου χωρίς να απαιτείται η ζήτησή τους. Με την σωστή διαμόρφωση των ρυθμίσεων των συσκευών, δημιουργείται μια αυτόκλητη ανατροφοδότηση και ενημέρωση κατάστασης από το φυσικό περιβάλλον προς το κέντρο ελέγχου. Με αυτόν τον τρόπο δημιουργείται μια πιο **αυτοματοποιημένη και αποδοτική επικοινωνίας ελαττώνοντας ταυτόχρονα την κίνηση στο δίκτυο**, καθώς μπορούν να παραληφθούν περιττά μηνύματα αιτήματος.
2. **Χρονοσημάνσεις Δεδομένων**: Οι λειτουργίες συγχρονισμού σημειώνουν στα δεδομένα ακριβείς «χρονικές ετικέτες», κάνοντας την επεξεργασία τους περισσότερο ουσιαστική. Οι χρήστες μπορούν να αναλύσουν καλύτερα τα δεδομένα που παρακολουθούν γνωρίζοντας τον ακριβή χρόνο που συνέβησαν και να αποδώσουν **καλύτερη ερμηνεία των γεγονότων** που συντελούνται στο πεδίο. Η χρονοσήμανση είναι αντίστοιχα σημαντική και στον τομέα της **κυβερνοασφάλειας** διότι δίνει την δυνατότητα δημιουργίας πραγματικών γραφημάτων και χρονολογιών για τα δεδομένα που λαμβάνονται. Συνεπώς η παρατήρηση «μη-κανονικών» γεγονότων γίνεται πιο ακριβής.
3. **CRC:** Ο ενσωματωμένος μηχανισμός ανίχνευσης και διόρθωσης σφαλμάτων προσδίδει μεγαλύτερη αξιοπιστία στην επικοινωνία συγκριτικά με πρωτόκολλα που διαθέτουν πολύ πιο απλούς μηχανισμούς.
4. **Ανθεκτικότητα:** Είναι Σχεδιασμένο για να λειτουργεί σε ακατάλληλα και θορυβώδη περιβάλλοντα και είναι ικανό να χειρίζεται σφάλματα επικοινωνίας και αποτυχίες δικτύου. Τα 3+1 επίπεδα της αρχιτεκτονικής του παρέχουν υψηλό βαθμό ανοχής σφάλματος και ανθεκτικότητα σε βλάβες.
5. **Τύποι Δεδομένων:** Το DNP3 είναι ένα πρωτόκολλο που μπορεί να προσαρμοστεί ανά εφαρμογή για να ανταποκριθεί σε διαφορετικές απαιτήσεις. Οι κεφαλίδες αντικειμένων διαθέτουν μια ευρεία γκάμα τύπων, (πχ. αναλογικών, δυαδικών, μετρητικών, χρονικών τιμών, τιμών ασφάλειας κ.ά) που προσφέρουν μεγάλη **ευελιξία στην διαχείριση δεδομένων** από τους χρήστες της DNP3 Εφαρμογής.
6. **<u>Αυθεντικοποίηση</u>:** Το επίπεδο εφαρμογής του DNP3 περιλαμβάνει ξεχωριστό πεδίο ταυτοποίησης της επικοινωνίας. Σύμφωνα με τις νέες εκδόσεις του προτύπου IEEE 1815, η λειτουργία αυθεντικοποίησης εξασφαλίζει ότι η (α.) outstation-συσκευή είναι βέβαιη ότι επικοινωνεί με εξουσιοδοτημένο χρήστη της υπηρεσίας και (β.) ο DNP3 master (κέντρο ελέγχου) μπορεί να επιβεβαιώσει ότι

επικοινωνεί με εξουσιοδοτημένο και σωστό εξωτερικό σταθμό. Η λειτουργία χρησιμοποιεί προεπιλεγμένο κλειδί ασφαλείας (pre-shared key), αλλά παρέχει επίσης μεθόδους απομακρυσμένης τροποποίησης του κλειδιού μ συμμετρική είτε ασύμμετρη (public key) κρυπτογραφία. Σχηματικά η Αυθεντικοποίηση μπορεί να υλοποιηθεί με την αρχιτεκτονική του σχήματος 2.13 χρησιμοποιώντας υπηρεσίες καταγραφής ιστορικού.

Σχήμα 2.13 – Αυθεντικοποίηση DNP3

Συνοψίζοντας τον παραπάνω σχολιασμό, διαπιστώνουμε ότι το DNP3 διακρίνεται για τις προηγμένες λειτουργίες του σε σχέση με παραδοσιακά βιομηχανικά πρωτόκολλα και για την εξειδίκευσή του σε συστήματα SCADA. Τα πλεονεκτήματα αυτά από την άλλη μπορούν να αποδειχθούν και μειονέκτημα υπό την εξής σκοπιά:

1. **Πολυπλοκότητα:** Στο πρωτόκολλο περιλαμβάνεται πολλές και λεπτομερείς λειτουργίες που το καθιστούν αρκετά πολύπλοκο. Η διαμόρφωσή του περιλαμβάνει πάνω από εκατό σελίδες ρυθμίσεων της επικοινωνίας με μεγάλο όγκο επιλογών και υπηρεσιών. Συνεπώς, η υλοποίηση, η διαμόρφωση και η υποστήριξή που πρέπει να παρέχεται σε μια επικοινωνία DNP3 απαιτεί εξειδικευμένες γνώσεις από τους χρήστες.
2. **Επιβάρυνση Δικτύου:** Το overhead του συστήματος μπορεί να γίνει μεγάλο χρησιμοποιώντας σημαντικό μέρος του εύρους ζώνης. Αυτό εξηγείται από το μεγάλο και μεταβλητό μέγεθος των μηνυμάτων που ανταλλάσσονται κατά την DNP3 επικοινωνία και την απαραίτητη κωδικοποίηση και επεξεργασία τριών (και όχι ενός) επιπέδων εφαρμογής. Συνεπώς η μη αποτελεσματική αξιοποίηση των δυνατοτήτων του πρωτοκόλλου μπορεί τελικά να οδηγήσει σε σημαντικές επιπτώσεις στην επίδοση, την ταχύτητα και την αποδοτικότητα του SCADA.
3. **Συμβατότητα**: Το DNP3 χρησιμοποιείται ευρέως στην Αμερική και ορισμένες άλλες χώρες, αλλά δεν είναι τόσο δημοφιλές, όσο άλλα πρωτόκολλα SCADA, στην Ευρώπη. Αυτό μπορεί να περιορίσει τις επιλογές και την ευελιξία εάν χρειαστεί μεταφορά και ενσωμάτωση του SCADA (σε DNP3) σε άλλα συστήματα ή περιοχές.
4. **Κυβερνοασφάλεια:** Μπορεί το πρωτόκολλο να εισάγει λειτουργίες αυθεντικοποίησης ωστόσο αυτό δεν σημαίνει ότι εξαλείφονται μια για πάντα οι κίνδυνοι από εξωτερικούς εισβολείς. Αφενός πέραν της αυθεντικοποίησης δεν παρέχονται άλλοι μηχανισμοί προστασίας από κυβερνοεπιθέσεις, αφετέρου η

διαδικασία ταυτοποίησης εξουσιοδοτημένων συσκευών είναι προαιρετική στην διαμόρφωση του πρωτοκόλλου και δεν υιοθετείται ευρέως. Αυτό μπορεί να εκθέσει το σύστημα SCADA σας σε κυβερνοεπιθέσεις, όπως πλαστογράφηση, παρέμβαση ή απόρριψη υπηρεσιών. Το πρότυπο IEC 62351-3 προτείνει κάποιες τεχνικές προστασίας στο επίπεδο μεταφοράς συνιστώντας την χρήση του DNP3 με TLS (Transport Layer Security). Περισσότερες τεχνικές ασφαλείας θα μελετηθούν συνολικά σε παρακάτω Κεφάλαιο (Κ.5.).

2.3.5. Η εφαρμογή του DNP3 σε ηλεκτρικά συστήματα και προκλήσεις

Ένα ανθεκτικό και αποδοτικό πρωτόκολλο επικοινωνίας, σαν το DNP3, αποτελεί μια ελκυστική επιλογή για οργανισμούς που αναζητούν ένα πρωτόκολλο για τον αυτόματο κρίσιμων ενεργειακών υποδομών. Ως ένα πρωτόκολλο που εξειδικεύεται στην επικοινωνία συστημάτων ανάκτησης δεδομένων και παρακολούθησης γεγονότων που συντελούνται στο πεδίο., **το DPN3 έχει ταιριαστή εφαρμογή σε όλα τα SCADA** συστήματα στον τομέα της ηλεκτρική ενέργειας. Συνεπώς μπορούμε εύκολα **να το εμπιστευτούμε σε συστήματα παραγωγής ηλεκτρικής ισχύος** καθώς από άποψη λειτουργικότητας είναι πιο προηγμένο, παραδείγματος χάριν συγκριτικά με το Modbus.

Στην πράξη, το συναντάμε ευρέως σε κυρίως Αγγλόφωνες χώρες με εφαρμογή τόσο στην παραγωγή όσο και σε συστήματα διανομής και μετάδοσης ηλεκτρικής ενέργειας. Ειδικότερα, όμως σε σημεία των συστημάτων που απαιτείται κεντρικό σύστημα SCADA. Για παράδειγμα, η μεγάλη πλειοψηφία (περίπου το 75%) των επιχειρήσεων παραγωγής ηλεκτρικής ενέργειας στην Βόρεια Αμερική χρησιμοποιούν το DNP3 σε διάφορες εφαρμογές βιομηχανικού ελέγχου.

Η έκρηξη της χρήσης του DNP3 οφείλεται κυρίως στην όλο ένα και μεγαλύτερη ανάγκη εύκολης ενσωμάτωσης των συστημάτων απομακρυσμένου ελέγχου στο διαδίκτυο. Το ενσωματωμένο σε TCP/IP DNP3 συνδέει μέσω δρομολογητών δικτύου μια τεράστια γκάμα συσκευών όπως, PLC, RTUs και IEDs απαθείας στο κέντρο ελέγχου. Το κέντρο ελέγχου πλέον έχει τεράστιες δυνατότητες απομακρυσμένου ελέγχου έως και με την χρήση WEB. Από την άλλη βέβαια, αυτό ανοίγει τον «ασκό του Αιόλου» σε ζητήματα κυβερνοασφάλειας.

Η υποβάθμιση της ασφάλειας των συστημάτων SCADA, λόγω Ίντερνετ εφαρμογών, είναι ένα από τα βασικά σημερινά ζητήματα που εγείρουν προβληματισμό στον Ενεργειακό Τομέα. Το τρωτό σημείο βρίσκεται στο γεγονός ότι τα δεδομένα που μεταδίδονται στο Διαδίκτυο μπορούν να αποτελέσουν πια εύκολο στόχο εισβολέων και κακόβουλων λογισμικών. Στον βαθμό που ακόμα και απλοί μηχανισμοί ασφαλείας που παρέχει η προδιαγραφή DNP3 είναι πλέον ξεπερασμένοι, κανένα πρωτόκολλο SCADA δεν παρέχουν τον ίδιο βαθμό ακεραιότητας και εμπιστευτικότητας στο σύστημα επικοινωνίας. Συνεπώς **η μεγάλη πρόκληση** που γεννάται σήμερα δεν είναι άλλη από την ανάπτυξη καινοτόμων τεχνικών προστασίας της επικοινωνίας εξελίσσοντας περεταίρω τα αξιόπιστα πρωτόκολλα (όπως το DNP3) στον τομέα της κυβερνοασφάλειας.

2.4. Πρότυπο πρωτοκόλλων επικοινωνίας IEC 60870-Μέρος 5

Πρότυπα IEC: Το IEC αντιπροσωπεύει τη Διεθνή Ηλεκτροτεχνική Επιτροπή, μια παγκόσμια οργάνωση που αναπτύσσει διεθνή πρότυπα για ηλεκτρικές, ηλεκτρονικές και σχετικές τεχνολογίες. Ένα πρωτόκολλο προτύπου IEC, συνεπώς, είναι ένα πρωτόκολλο επικοινωνίας που έχει αναπτυχθεί και δημοσιευθεί από το IEC ως διεθνές πρότυπο. Αυτά τα πρωτόκολλα σχεδιάζονται και τυποποιούνται για να διευκολύνουν την επικοινωνία μεταξύ διαφορετικών συσκευών και συστημάτων, διασφαλίζοντας την αλληλεπίδραση και τη συμβατότητα σε διάφορους τομείς και εφαρμογές. Ένα πρότυπο προσδιορίζεται από έναν μοναδικό αριθμό και τα μέρη που το απαρτίζουν. Τα μέρη έχουν συνήθως αύξοντα αριθμό και το καθένα περιγράφει και αναλύει συγκεκριμένες πτυχές του συνολικού προτύπου.

IEC 60870: Είναι μια σειρά διεθνών προτύπων που καθορίζει γενικές πληροφορίες σχετικά με το πρότυπο, συνθήκες λειτουργίας, ηλεκτρικές διεπαφές, απαιτήσεις απόδοσης και πρωτόκολλα μετάδοσης δεδομένων. Αναπτύχθηκε περιοδικά και με ιεραρχικό τρόπο μεταξύ των ετών 1988 και 2000 και αποτελείται από έξι μέρη και συνοδευτικά τμήματα. Συγκεκριμένα τα μέρη -5 και -6 του προτύπου περιγράφουν βασικούς άξονες ενός μοντέλου επικοινωνίας, εξειδικευμένο στην απομακρυσμένη επίβλεψη και στον έλεγχο συστημάτων ισχύος.

2.4.1. Η περιγραφή του IEC 60870-5 και συνοδευτικών τμημάτων

Στο IEC 60870 πρότυπο προδιαγράφονται πρωτόκολλα επικοινωνίας, κατάλληλα για συστήματα ηλεκτρικής ενέργειας. Αρχικά ο σκοπός ήταν να δημιουργηθούν πρωτόκολλα ικανά να υποστηρίξουν μια αξιόπιστη επικοινωνία, σε μεγάλες αποστάσεις και σε ακατάλληλα και θορυβώδη περιβάλλοντα. Το μέρος -5 του προτύπου έρχεται να προδιαγράψει ένα πρωτόκολλο μετάδοσης που θα καλύπτει την παραπάνω απαίτηση. Από την άλλη, το μέρος -6 περιγράφει ένα γενικότερο προφίλ της επικοινωνίας επικεντρωμένο στο πεδίο της Εφαρμογής. Στην παρούσα ενότητα (2.4) θα ασχοληθούμε με το πρωτόκολλο προδιαγραφής IEC 60870-5, ενώ το 6^{ο} μέρος του προτύπου θα μελετηθεί στην τελευταία ενότητα του κεφαλαίου λόγω των διαφορετικών του χαρακτηριστικών συγκριτικά με τα υπόλοιπα πρωτόκολλα που μελετάμε.

Συγκεκριμένα, **η IEC 60870-5** παρέχει ένα **προφίλ επικοινωνίας για την αποστολή βασικών μηνυμάτων τηλεελέγχου** μεταξύ δύο συστημάτων, τα οποία χρησιμοποιούν μεταξύ τους μόνιμα και απευθείας συνδεδεμένα κυκλώματα δεδομένων. Το γενικό προφίλ της IEC 60870-5 επικοινωνίας ακολουθεί το μοντέλο EPA και καθορίζεται από τα επιμέρους τμήματα της προδιαγραφής. Τα τμήματα που μας ενδιαφέρουν στην παρούσα ερευνητική εργασία περιγράφονται στον παρακάτω πίνακα (Σχήμα 2.14):

Τμήμα	Περιγραφή
IEC 60870-5-1	Μορφή Πλαισίου Μετάδοσης (EPA – επίπεδο σύνδεσης)
IEC 60870-5-2	Υπηρεσίες Μετάδοσης Σύνδεσης-Δεδομένων (EPA – επίπεδο σύνδεσης)
IEC 60870-5-3	Γενική Δομή των Δεδομένων Εφαρμογής (EPA – επίπεδο εφαρμογής)
IEC 60870-5-4	Ορισμός και Κωδικοποίηση Στοιχείων Πληροφορίας (EPA – επίπεδο εφαρμογής)
IEC 60870-5-5	Βασικές Λειτουργίες Εφαρμογής (επεξεργασία χρήστη)
IEC 60870-5-101	Πρωτόκολλα Μετάδοσης βασικών λειτουργιών τηλεελέγχου.
IEC 60870-5-104	Πρωτόκολλα Μετάδοσης: Πρόσβαση στο Δίκτυο για το IEC 60870-5-101 με χρήση προτύπων μεταφοράς δεδομένων.
IEC TS 60870-5-7	**Επεκτάσεις ασφάλειας** για τα πρωτόκολλα IEC 60870-5-101 και IEC 60870-5-104, με εφαρμογή του IEC 62351.

Σχήμα 2.14 – Τμήματα προτύπου IEC 60870-5

Η ενότητα θα ασχοληθεί φυσικά με τα συνοδευτικά πρότυπα 101 και 104, τα οποία και καθορίζουν τα πρωτόκολλα επικοινωνίας μεταξύ συσκευών ενός συστήματος ισχύος αλλά και μεταξύ διαφορετικών συστημάτων. Τα συνοδευτικά πρότυπα για τη μετάδοση βασικών μηνυμάτων απομακρυσμένου ελέγχου ακολουθούν επίσης το επίπεδο φυσικής σύνδεσης και δεδομένων του μοντέλου OSI υποστηρίζοντας πολλαπλούς τρόπους μεταφοράς δεδομένων, συμπεριλαμβανομένων των ισορροπημένων και μη ισορροπημένων τρόπων.

Παλαιότερα όταν αναφερόμασταν στο IEC 60870 στα πλαίσια εφαρμογών SCADA, συνήθως εννοούταν το συνοδευτικό πρότυπο 60870-5-101. Όταν αυτό κυκλοφόρησε, το 1995, ανέλυε ένα πλήρες πρωτόκολλο μετάδοσης τιμών μεταξύ συσκευών πεδίου, απομακρυσμένων τερματικών μονάδων και κέντρο ελέγχου, που το επέτρεψε να χρησιμοποιηθεί στην παραγωγή. Το 2000 η επόμενη έκδοση του προτύπου, IEC 60870-5-104, επέτρεψε στα πλαίσια μηνυμάτων της πρώτης έκδοσης να μεταδοθούν σε δίκτυα βασισμένα στο IP πρωτόκολλο και το Ethernet.

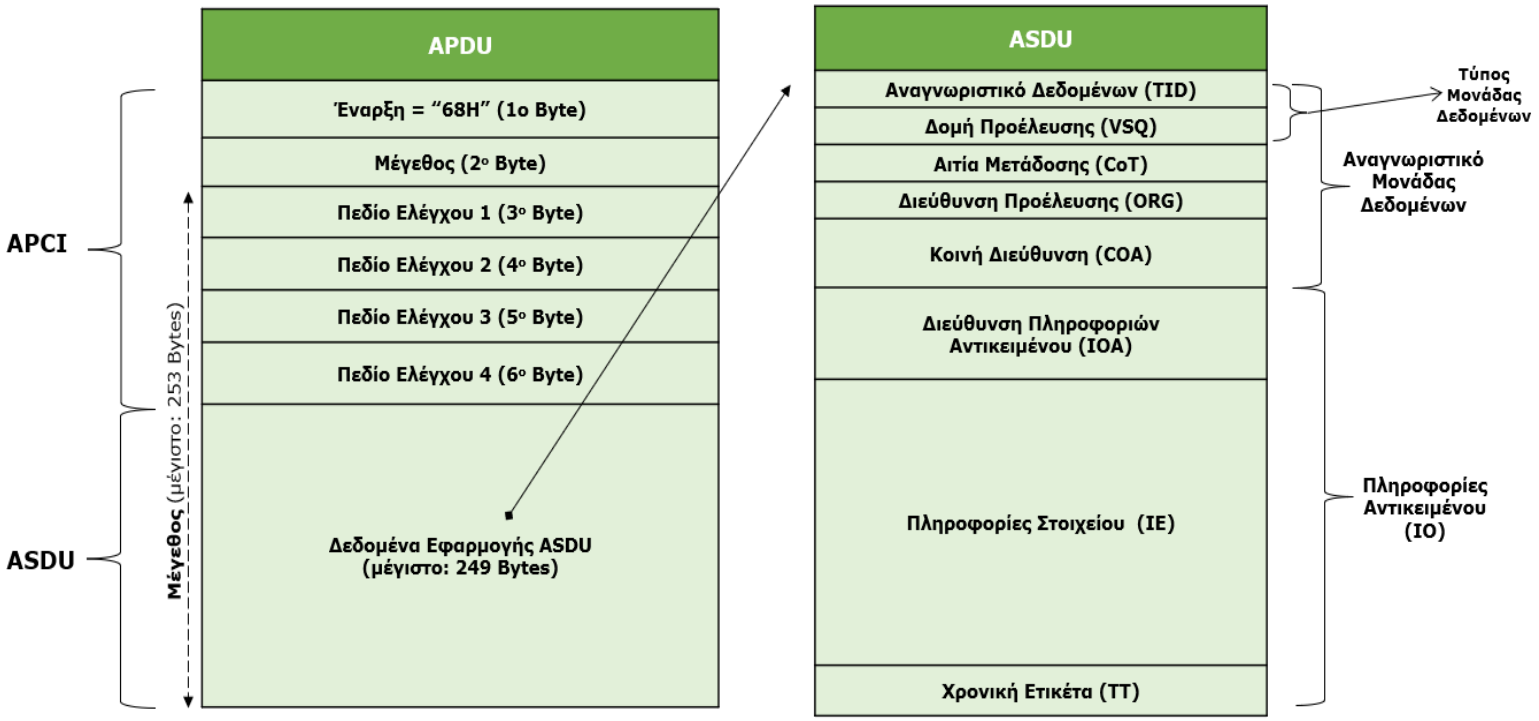
Το **IEC 60870-5-101**, ως η παλαιότερη προδιαγραφή πρωτοκόλλων του γενικού προτύπου, περιγράφει ένα σχετικά απλό πρωτόκολλο με βασικές λειτουργίες. Είναι σχεδιασμένο για χρήση **σειριακών συνδέσεων** και επιτρέπει μόνο μορφές επικοινωνίας **Κύριας μονάδας – εξωτερικού σταθμού**. Συμπεριφέρεται δηλαδή όπως και τα υπόλοιπα σειριακά πρωτόκολλα που έχουμε μελετήσει ως τώρα. Το πρωτόκολλο είναι σχετικά αργό και περιορισμένο στις δυνατότητές του, αλλά είναι επίσης πολύ αξιόπιστο και κατάλληλο για απλές εφαρμογές. Από την άλλη πλευρά, το **IEC 60870-5-104** είναι μια πιο προηγμένη προδιαγραφή που σχεδιάστηκε για την ενσωμάτωση του σειριακού πρωτοκόλλου σε δίκτυα **TCP/IP**. Υποστηρίζει ταχύτερες ρυθμίσεις επικοινωνίας και πιο προηγμένες λειτουργίες, όπως πολλαπλή διευθυνσιοδότηση **πελάτη-εξυπηρετητή**. Ενώ σε γενικές γραμμές είναι πιο πολύπλοκο από το IEC 60870-5-101, προσφέρει μεγαλύτερη ευελιξία και είναι καταλληλότερο για πιο προηγμένες εφαρμογές.

Στην συνέχεια της μελέτης θα σχολιάζουμε την πιο προηγμένη και πλέον διαδεδομένη έκδοση πρωτοκόλλων, η οποία έχει και το μεγαλύτερο ενδιαφέρον από την σκοπιά της ασφάλειας. Η προδιαγραφή πρωτοκόλλων IEC 60870-5-104, θα αναφέρεται εν συντομία ως IEC/104.

2.4.2. Δομή "Μονάδας Δεδομένων" πρωτοκόλλων IEC 60870-5

Τα μηνύματα που ανταλλάσσονται σύμφωνα με τις προδιαγραφές ολόκληρης της σειράς 60870-5 περιλαμβάνουνται μια συγκεκριμένη δομή πακέτων. Το επίπεδο εφαρμογής του προτύπου μεταφέρει κάθε φορά μια **Μονάδα Δεδομένων και Υπηρεσιών Εφαρμογής** (Application Service Data Unit ή απλά **ASDU**), όπως φαίνεται στο σχήμα 2.15. Τα μηνύματα ASDU μεταφέρονται τόσο με το πρωτόκολλο επικοινωνίας του IEC 60870-5-101 όσο και με το IEC/104. Επειδή η προδιαγραφή IEC/104 περιγράφει και επίπεδο μεταφοράς για το πρωτόκολλο εφαρμογής, καθορίζει επίσης μηχανισμούς έναρξης ή λήξης -σε αντίθεση με το IEC/101- για τα δεδομένα ASDU που μεταδίδονται.

Για αυτόν τον ρόλο δημιουργείται, από το IEC/104, ένας επιπλέον τύπος μηνυμάτων που λειτουργούν ως προσθετική κεφαλίδα του αρχικού ASDU. Το νέο πακέτο δεδομένων ονομάζεται **Έλεγχος Πληροφορίας του Πρωτοκόλλου Εφαρμογής** (Application Control Information ή **APCI**) και μπορεί να ανιχνεύει την έναρξη και το τέλος ASDU μηνυμάτων. Τελικά στο IEC/104 , τα δεδομένα ASDU συνδυάζονται με τα μηνύματα ελέγχου APCI και σχηματίζουν ένα ολοκληρωμένο πακέτο δεδομένων, δηλαδή την **Μονάδα Δεδομένων Πρωτοκόλλου Εφαρμογής** (Application Protocol Data Unit ή **APDU**. Η δομή και το μέγεθος ενός APDU πακέτου φαίνεται αναλυτικά στο σχήμα που ακολουθεί.



Σχήμα 2.15 – Μονάδα Δεδομένων Πρωτοκόλλου Εφαρμογής IEC/104

Όπως απεικονίζεται παραπάνω, **τα μηνύματα ελέγχου πληροφορίας APCI αποτελούνται** από τα εξής επί μέρους οκταδικά πεδία, τον **χαρακτήρα έναρξης (68H)**, τα **τέσσερα πεδία ελέγχου** και το **πεδίο μεγέθους** αναφερόμενο στο «μήκος» της συνολικής μονάδας APDU. Το δεύτερο πεδίο ενός APCI ορίζεται ως μέγιστο μέγεθος ενός APDU τα 253 bytes. Στην τιμή αυτή

ουσιαστικά περιλαμβάνονται το μέγεθος των πεδίων ελέγχου που είναι 4 bytes και το μέγεθος των δεδομένων του ASDU που ακολουθεί.

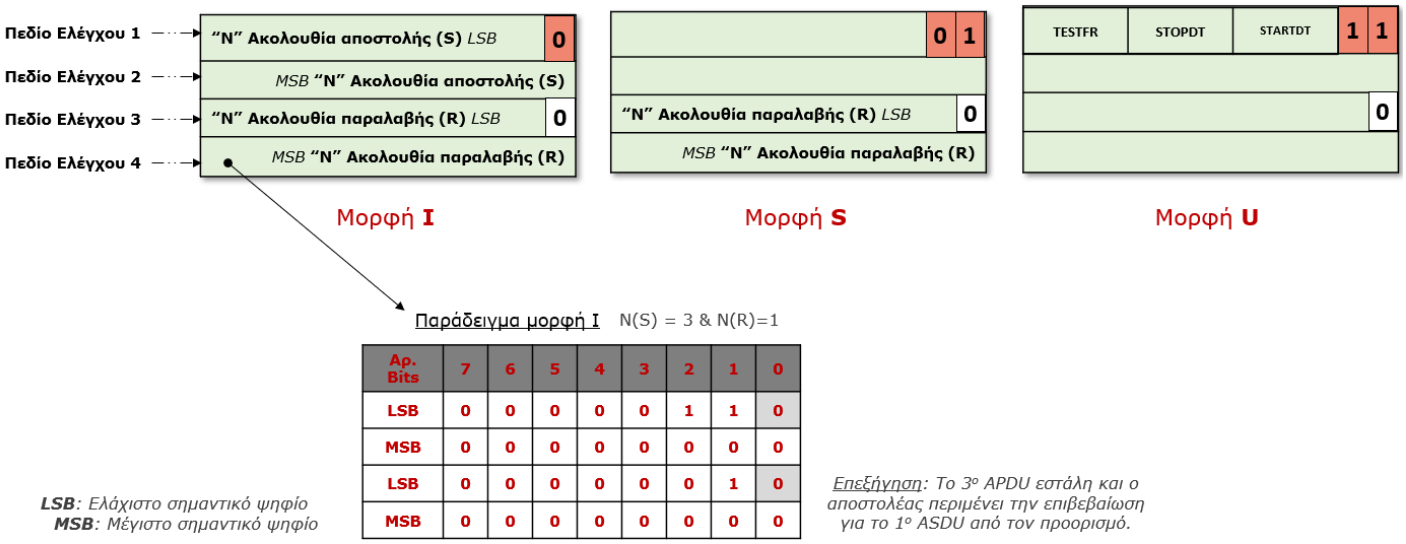
Το γενικό πλαίσιο ενός APCI δεν έχει πάντα την ίδια μορφή, αυτή **καθορίζεται πάντα από τα δύο τελευταία bits του 1ου πεδίου ελέγχου** όπως θα δούμε στο επόμενο παράδειγμα (σχήμα 2.16). Κάθε μορφή υποδεικνύει και έναν άλλο μηχανισμό ελέγχου και διαφορετικές λειτουργίες που περιλαμβάνει το πρότυπο. Συγκεκριμένα Το πρότυπο έχει προδιαγράψει τρεις βασικές μορφές πλαισίου (I, U και S) για τα APCI πεδία ελέγχου.

- **Μορφή I** (Information – 0 bit): Χρησιμοποιείται για την μετάδοση δεδομένων μεταξύ του αποστολέα και του παραλήπτη σε μια συνομιλία. Εμπεριέχει μια ακολουθία αριθμών για να διασφαλίσει την αξιόπιστη και οργανωμένη αποστολή πληροφοριών ελέγχου και δεδομένων (πχ. μετρήσεις αισθητήρων, κ.ά) και πάντα ακολουθείται από πακέτο ASDU το οποίο μεταφέρει το φορτίο των δεδομένων. Στην I-μορφή εκτός από πληροφορίες μεταφέρονται και αναγνωρίσεις δεδομένων. Η λογική είναι ότι ο αποστολέας αυξάνει έναν αριθμό ακολουθίας αποστολής N(S), ενώ ο παραλήπτης αυξάνει έναν αριθμό ακολουθίας παραλαβής N(R). Ο παραλήπτης επιβεβαιώνει κάθε APDU ή έναν αριθμό APDU επιστρέφοντας (με την R ακολουθία) μια τιμή που υποδηλώνει πόσα ASDU έχει αναγνωρίσει. Σε περίπτωση μετάδοσης μεγαλύτερου όγκου δεδομένων μόνο προς μία κατεύθυνση, πρέπει να αποσταλεί ένα μήνυμα S μορφής προς την άλλη κατεύθυνση για να επιβεβαιωθούν οι APDU πριν την υπερχείλιση του buffer.

- **Μορφή S** (Supervisory – 01 bits): Χρησιμοποιείται για την εποπτεία και τον έλεγχο της μετάδοσης δεδομένων. Περιλαμβάνει κυρίως λειτουργίες σχετικές με την αναγνώριση και τον έλεγχο ροής των δεδομένων. Δηλαδή περιέχει πληροφορίες σχετικά με τον έλεγχο και την κατάσταση του συστήματος τηλεχειρισμού. Για παράδειγμα με την S-μορφή έναν μήνυμα μπορεί να ζητήσει επιβεβαίωση παραλαβής δεδομένων, να υποδείξει επαναποστολή των δεδομένων και να διευθύνει την ροή δεδομένων μεταξύ αποστολέα και παραλήπτη.

- **Μορφή U** (Unnumbered – 11 bits): Χρησιμοποιείται για λειτουργίες ελέγχου που δεν απαιτούν αναγνώριση. Για παράδειγμα η U-μορφή ταιριάζει με μηνύματα εντολών, αιτημάτων ή άλλων μηνυμάτων που δεν περιλαμβάνουν μετάδοση δεδομένων. Τέτοιες εντολές μπορεί να είναι μια δοκιμή σύνδεσης αποστολέα-παραλήπτη, η έναρξη ή ο τερματισμός της μετάδοσης δεδομένων μεταξύ τους, κ.ά. Αφού τα μηνύματα τύπου U δεν περιλαμβάνουν δεδομένα, δεν θα πρέπει να περιμένουμε και κάποιο ASDU πακέτο να ακολουθεί.

- **Χαρακτηριστικό παράδειγμα** για κάθε μορφή ελέγχου APCI είναι αυτό της παρακάτω εικόνας.



Αρ. Bits	7	6	5	4	3	2	1	0
LSB	0	0	0	0	0	1	1	0
MSB	0	0	0	0	0	0	0	0
LSB	0	0	0	0	0	0	1	0
MSB	0	0	0	0	0	0	0	0

Σχήμα 2.16 – Μορφές πεδίων ελέγχου APCI και παράδειγμα I-ακολουθίας

Συμπερασματικά το APCI καθορίζει τη δομή της μετάδοσης δεδομένων και τον τρόπο χειρισμού της από τη συσκευή που παραλαμβάνει τα δεδομένα. Δηλαδή διαχειρίζεται την ροή ανταλλαγής ASDU πακέτων -όταν απαιτείται- μεταξύ συσκευών παραλήπτη και αποστολέα.

Το πακέτο δεδομένων και υπηρεσιών ASDU περιέχει τα πραγματικά δεδομένα προς μετάδοση. Στο πακέτο ASDU υπάρχουν πληροφορίες σχετικά με τον τύπο των δεδομένων, την διεύθυνση αποστολέα του πακέτου, την διεύθυνση προορισμού και κώδικες λειτουργίας. Η δομή του ASDU χωρίζεται σε δύο βασικά τμήματα: το τμήμα αναγνώρισης δεδομένων και το τμήμα των πραγματικών δεδομένων, τα οποία επιμερίζονται περεταίρω πεδία , όπως είδαμε στην εικόνα 2.15. Στις παραγράφους που ακολουθούν (A. & B.) περιγράφονται αντιστοίχως οι λειτουργίες των δύο τμημάτων ενός ASDU.

A. Πεδία Αναγνώρισης Μονάδας Δεδομένων

Το πρώτο κατά σειρά τμήμα του ASDU ονομάζεται αναγνωριστικό δεδομένων (data unit identifier) και αποτελείται συνήθως από πέντε πεδία. Το πρώτο byte-πεδίο υποδεικνύει τον γενικό τύπο της πληροφορίας, το δεύτερο ορίζει τον αριθμό των μεταβλητών-αντικειμένων που μεταδίδονται στο ASDU, το τρίτο υποδεικνύει την αιτία μετάδοσης, το τέταρτο προαιρετικό πεδίο έχει την διεύθυνση της συσκευής-αποστολέα. Το πέμπτο και τελευταίο πεδίο του τμήματος αναγνώρισης έχει μέγεθος 2 Bytes και καθορίζει διευθύνσεις προορισμού.

- **Αναγνωριστικό Τύπου Δεδομένων (TID)**: Είναι το πρώτο πεδίο του τμήματος και καθορίζει τον τύπο δεδομένων που περιέχονται στο ASDU. Διάφοροι τύποι μπορεί να είναι: Μετρούμενα μεγέθη, εντολές ελέγχου ή παρακολούθησης, παρακολούθηση και έλεγχος συστήματος. Προσφάτως έχουν εισαχθεί τύποι ασφάλειας για την αυθεντικοποίηση μηνυμάτων. Το πεδίο αυτό προσδιορίζει ολόκληρο το πακέτο ASDU συνεπώς και όλα τα αντικείμενα δεδομένων που μεταφέρει.
- **Δομή Μεταβλητής (VSQ)**: Εδώ ορίζεται η δομή των μεταβλητών του πακέτου. Δηλαδή προσδιορίζεται ο αριθμός των αντικειμένων (IO) που ακολουθεί στο 2ο τμήμα του ASDU και πώς είναι η αλληλουχία τους στο πακέτο. Το πρώτο bit του

πεδίου(SQ) καθορίζει αλληλουχία και τα υπόλοιπα 7bits δηλώνουν αριθμό αντικειμένων ή στοιχείων αντικειμένου. Οι δύο δομές που καθορίζει το 1^{ο} bit είναι οι εξής:
Η τιμή SQ=0, υποδηλώνει μια αλληλουχία ίσων αντικειμένων όπου κάθε αντικείμενο ξεκινά με το πεδίο της διεύθυνσής του.
Η τιμή SQ=1, καθορίζει πακέτο με ένα μοναδικό αντικείμενο και υποδηλώνει μια αλληλουχία στοιχείων εντός του. Το πεδίο διεύθυνσης αντικειμένου καθορίζει την διεύθυνση του πρώτου στοιχείου της αλληλουχίας.

- **Αιτία μετάδοσης (CoT)**: Είναι ο λόγος για τον οποίο ανταλλάσσονται ASDU δεδομένα, δηλαδή παρέχει πληροφορίες σχετικά με την προέλευση και το περιεχόμενο του μηνύματος. Συγκεκριμένα πεδίο CoT περιέχει έναν αριθμητικό κωδικό των 6 bits που αντιπροσωπεύει μια συγκεκριμένη αιτία της μετάδοσης. Το CoT χρησιμοποιείται από τον παραλήπτη για να καθορίσει την κατάλληλη ενέργεια κατά την επεξεργασία του μηνύματος. Για παράδειγμα, εάν το CoT υποδεικνύει μια περιοδική μετάδοση, ο δέκτης μπορεί απλώς να καταγράψει τα δεδομένα και να μην προβεί σε άμεση ενέργεια. Εάν το CoT υποδεικνύει μια μετάδοση που εκκινείται από συμβάν (event), ο παραλήπτης μπορεί να χρειαστεί να λάβει άμεσα μέτρα με βάση το περιεχόμενο του μηνύματος. Συνηθισμένοι κωδικοί μετάδοσης CoT μπορεί να περιλαμβάνουν:
  1. Περιοδική ή κυκλική μετάδοση
  2. Μετάδοση που ξεκίνησε η σάρωση φόντου
  3. Αυθόρμητη μετάδοση
  4. Μετάδοση με εκκίνηση συμβάντων
  5. Αίτημα μετάδοσης
  6. Μετάδοση ενεργοποίησης
  7. Μετάδοση επιβεβαίωσης ενεργοποίησης
  8. Απενεργοποίηση μετάδοσης
  9. Μετάδοση επιβεβαίωσης απενεργοποίησης

  Τα πρώτα 2 bits του πεδίου δηλώνουν αν το μήνυμα είναι για δοκιμή (Test Bit) και εάν υπάρχει θετική ή όχι επιβεβαίωση (P/N bit) της λειτουργίας που εκτελείται.

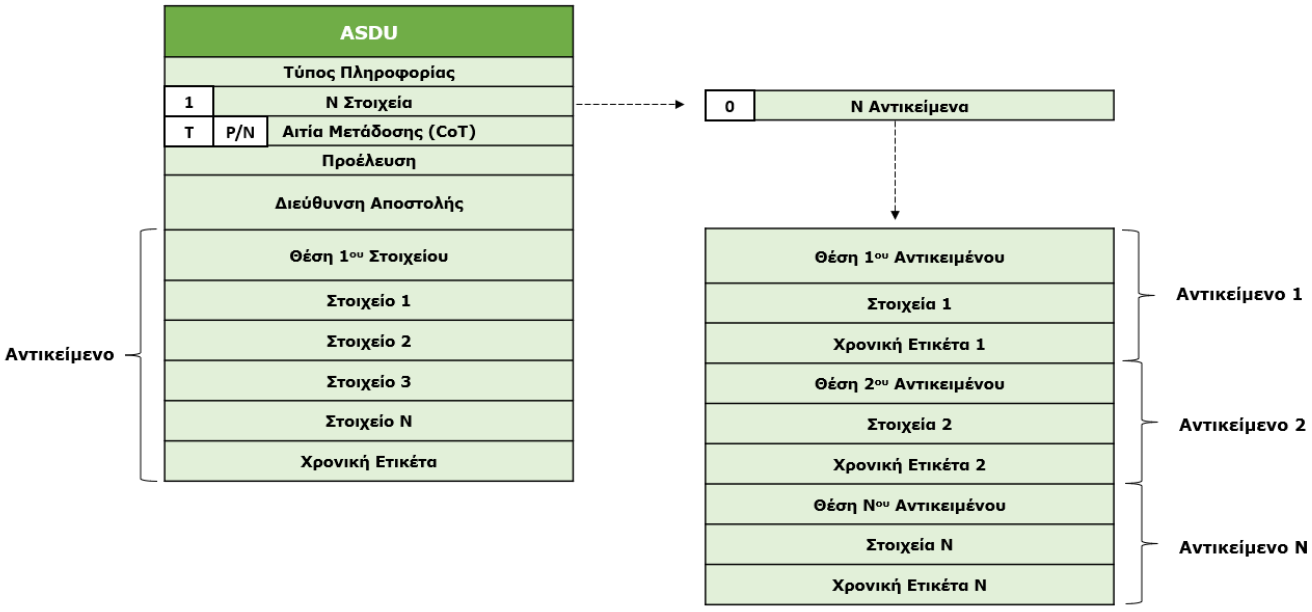
- **Διεύθυνση Προέλευσης (ORG):** Το πεδίο αυτό είναι προαιρετικό για συστήματα με έναν σταθμό ελέγχου και απαραίτητο για συστήματα που απαρτίζονται από περισσότερους. Είναι κυρίως ένας τρόπος αυτοπροσδιορισμού των συσκευών ελέγχου. Για παράδειγμα το πεδίο βοηθά σε μια λειτουργία επίβλεψης μιας συσκευής ώστε να επιστρέφονται επιβεβαιώσεις στον καθορισμένο σταθμό ελέγχου και όχι σε όλο το σύστημα ελέγχου (περίπτωση που δεν χρησιμοποιείται το πεδίο).
- **Κοινή διεύθυνση (Common Address)**: Είναι η κοινή διεύθυνση όπου περιλαμβάνονται τα δεδομένα ASDU και μπορεί να θεωρηθεί ως η διεύθυνση προορισμού του μηνύματος. Περιλαμβάνει 2 Bytes διότι μπορεί να μην αναφέρεται μόνο σε έναν ελεγχόμενο σταθμό αλλά και σε μια υποομάδα σταθμών. Η κοινή διεύθυνση είναι σημαντική για να διασφαλιστεί ότι τα μηνύματα αποστέλλονται στον σωστό προορισμό και ότι τα μηνύματα απάντησης αποστέλλονται πίσω στη σωστή πηγή.

Β. Πεδία Αντικειμένων Πληροφορίας

Το **αντικείμενο πληροφορίας (Information Object ή IO)** ή πληροφορίας περιλαμβάνει ένα σύνολο στοιχείων δεδομένων που αντιπροσωπεύουν συγκεκριμένες πληροφορίες σχετικά με το σύστημα ισχύος, όπως την κατάσταση

μιας συγκεκριμένης συσκευής ή τις τιμές μέτρησης ενός αισθητήρα. Κάθε αντικείμενο έχει έναν μοναδικό αριθμό αναγνώρισης, ο οποίος επιτρέπει στη συσκευή λήψης να ερμηνεύει σωστά τα δεδομένα. Το IO τμήμα του ASDU αποτελείται από τα κάτωθι επί μέρους πεδία:

- **Διεύθυνση αντικειμένου πληροφοριών (IOA):** Είναι ένα πεδίο τριών byte που προσδιορίζει την συγκεκριμένη διεύθυνση δεδομένων, εντός συσκευής, που μεταδίδεται. Περιλαμβάνει τη διεύθυνση της απομακρυσμένης συσκευής και τη διεύθυνση του σημείου δεδομένων εντός της μνήμης της. (πχ. Διεύθυνση/εις αντικειμένου στην εξωτερική μονάδα)
- **Στοιχεία πληροφοριών (IE):** Το πεδίο αυτό είναι μεταβλητού μεγέθους και περιέχει το πραγματικό φορτίο δεδομένων που μεταδίδονται. Η δομή και η μορφή του IE εξαρτώνται από τον τύπο των δεδομένων που μεταδίδονται (bool, integer, real, bitstring).
- **Χρονική Ετικέτα/Time Tag:** Ο χρόνος κατά τον οποίο παρήχθη ή ελήφθη μια μέτρηση, ένα συμβάν ή μια εντολή. Παρέχει έναν τρόπο συγχρονισμού και παραγγελίας των δεδομένων που ανταλλάσσονται μεταξύ διαφορετικών συστημάτων ή συσκευών. Το πεδίο της ετικέτας χρόνου έχει μήκος 4 byte και αναπαρίσταται με τη μορφή του αριθμού των χιλιοστών του δευτερολέπτου. Η χρονική ετικέτα είναι προαιρετική, που σημαίνει ότι μπορεί να συμπεριληφθεί ή να παραλειφθεί ανάλογα με τη συγκεκριμένη εφαρμογή και τα δεδομένα που μεταδίδονται. Όταν περιλαμβάνεται, η χρονική ετικέτα επιτρέπει τον ακριβή χρονισμό και την αλληλουχία των γεγονότων στο σύστημα ισχύος, επιτρέποντας την αποτελεσματική παρακολούθηση, έλεγχο και ανάλυση.



Σχήμα 2.17 – Παράδειγμα: Αντικείμενα και Στοιχεία ASDU

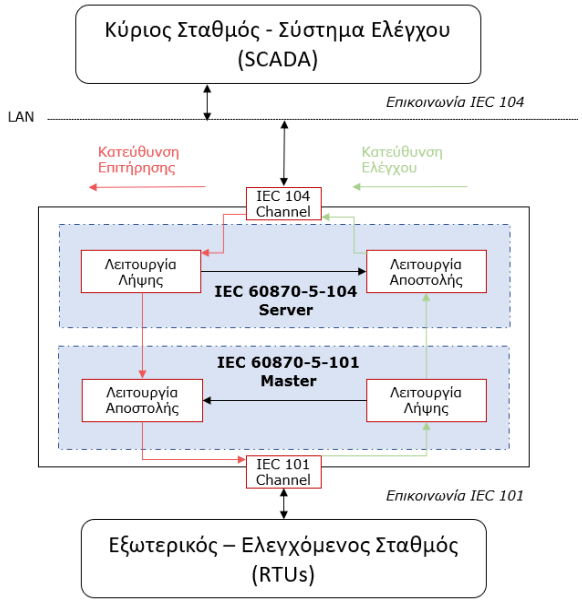
2.4.3. Λειτουργίες επικοινωνίας IEC 60870-5 και τοπολογία δικτύου

Μελετώντας την δομή μηνυμάτων διαπιστώνουμε ότι η προδιαγραφή του προτύπου προσφέρει κάποιες προηγμένες λειτουργίες, σε επίπεδο κανόνων επικοινωνίας, διευθυνσιοδότησης, δεδομένων μηνυμάτων και αρχιτεκτονικής της επικοινωνίας. Αυτές οι δυνατότητες αυξάνουν σε μεγάλο βαθμό την λειτουργικότητα της μετάδοσης πληροφορίας μεταξύ των συσκευών του δικτύου.

Από τα πρώτα πράγματα που εύκολα μπορούμε να διακρίνουμε είναι η **απουσία αναγνωριστικού συναλλαγής** και τα πολλά πεδία διευθύνσεων στα οποία βασίζεται η επικοινωνία. Κάθε αντικείμενο αναφέρεται με την IP διεύθυνση (IEC/104) του ελεγχόμενου σταθμού στο επίπεδο 3 του OSI, τη διεύθυνση του ελεγχόμενου σταθμού στο επίπεδο 7 (κοινή διεύθυνση) και με μια διεύθυνση αντικειμένου (IOA). Ο συνδυασμός των δύο τελευταίων με μια αιτία μετάδοσης (CoT) είναι αυτό που τελικά μπορεί να ταυτοποιήσει μια συναλλαγή χωρίς χρήση αναγνωριστικού. Συνεπώς, η **διευθυνσιοδότηση** παίζει κομβικό ρόλο στην λειτουργία του πρωτοκόλλου καθώς μέσω αυτής ανιχνεύονται πιθανά χαμένα μηνύματα.

Οι λειτουργίες διευθυνσιοδότησης επιτρέπουν επίσης ισορροπημένες και μη μεταδόσεις μηνυμάτων. Στην **μη ισορροπημένη μετάδοση**, ο κύριος σταθμός εκκινεί όλες τις μεταφορές μηνυμάτων ενώ οι ελεγχόμενοι σταθμοί απλώς ανταποκρίνονται σε αυτά τα μηνύματα. Οι υπηρεσίες που εκτελούνται είναι (α.) *Αποστολή - Χωρίς Απάντηση* για γενικά μηνύματα και κυκλικές εντολές (β.) *Αποστολή-με Επιβεβαίωση* για εντολές ελέγχου και (γ.) *Αίτημα – Απάντηση* για ανάγνωση δεδομένων από εξωτερικούς σταθμούς. Αντίθετα στην **ισορροπημένη μετάδοση** μηνυμάτων κάθε σταθμός μπορεί λειτουργήσει ταυτόχρονα ως ελεγχόμενος ή κύριος σταθμός. Η λογική αυτή χρησιμεύει σε συνδέσεις σημείου-προς-σημείο και πολλαπλών σημείων-προς-σημείο. Εδώ οι δύο υπηρεσίες είναι (α.) *Αποστολή-με Επιβεβαίωση* και (β.) *Αποστολή - Χωρίς Απάντηση* για διασύνδεση σημείο-προς-σημείο.

Ακόμα μια σημαντική έννοια που έχει αναφερθεί αλλά πρέπει να αποσαφηνιστεί για να κατανοήσουμε την λογική της επικοινωνίας είναι η διάκριση ανάμεσα σε **κατευθύνσεις ελέγχου και παρακολούθησης**. Επειδή το πρωτόκολλο ακόμα και σε μια ιεραρχική δομή υποθέτει ότι κάθε συσκευή μπορεί να είναι είτε ελεγχόμενη είτε κύρια ορίζει 3 βασικές κατευθύνσεις λειτουργίας για να γίνει ξεκάθαρη η ροή της πληροφορίας.



- **Κατεύθυνση Επιτήρησης**: Είναι η κατεύθυνση μετάδοσης από τον ελεγχόμενο σταθμό (πχ. RTU) προς τον εποπτικό σταθμό (πχ. Η/Υ). Αυτή η κατεύθυνση μεταφέρει κρίσιμα δεδομένα πεδίου προς τα ανώτερα επίπεδα ελέγχου.
- **Κατεύθυνση Ελέγχου:** Εδώ η ροή μετάδοσης γίνεται από τον σταθμό ελέγχου (πχ. SCADA) προς τον εξωτερικό ελεγχόμενο σταθμό. Περιλαμβάνει εντολές ενεργοποίησης ή απενεργοποίησης συσκευών, εγγραφή δεδομένων, κλπ.
- **Αντίστροφη Κατεύθυνση:** Όταν αντιστρέφονται οι ρόλοι και οι εξωτερικοί σταθμοί στέλνουν εντολές ή οι κύριοι σταθμοί στέλνουν δεδομένα στην κατεύθυνση της επιτήρησης.

Σχήμα 2.18 – Τοπολογία δικτύου IEC/104

Χαρακτηριστικό παράδειγμα τοπολογίας δικτύου επικοινωνίας και κατευθύνσεων ροής είναι αυτό του παραπάνω σχήματος (2.18).

2.4.4. Πλεονεκτήματα, μειονεκτήματα και ζητήματα κυβερνοασφάλειας προτύπου IEC 60870-5

Από τα παραπάνω στοιχεία προκύπτουν διάφορα οφέλη που προσδίδει η προδιαγραφή IEC 60870-5 στο σύστημα επικοινωνίας βιομηχανικών εφαρμογών. Τα πιο **βασικά πλεονεκτήματα** που διαπιστώνουμε είναι τα παρακάτω:

1. **Υψηλή Λειτουργικότητα:** Σε συνέχεια της ανάλυσης των λειτουργιών του προτύπου, είναι εμφανής η πιο προηγμένη λειτουργικότητα που έχει συγκριτικά με τα πρωτόκολλα που έχουν μελετηθεί ως τώρα. Οι διάφορες λειτουργίες που προσφέρει το μοντέλο APDU, όπως ο συντονισμένος έλεγχος της ροής μηνυμάτων, το προηγμένο σύστημα διευθυνσιοδότησης και οι τύποι δειγματοληπτικού ελέγχου, καθιστούν το πρωτόκολλο ικανό να ανταπεξέλθει σε μεγαλύτερες εφαρμογές με περισσότερες αρμοδιότητας πέραν της απλής παρακολούθησης και ανάκτησης δεδομένων.
2. **Τύποι Δεδομένων:** Το πρότυπο προδιαγράφει αντικείμενα δεδομένων που μεταφέρουν τα μηνύματα ξεφεύγοντας από την παραδοσιακή προδιαγραφή των πακέτων μηνυμάτων. Έτσι τα μηνύματα δεν μεταφέρουν απλώς ακέραιες 16-bit τιμές καταχωριτών όπως τα παραδοσιακά πρωτόκολλα, αλλά υποστηρίζουν δεδομένα εντολών, αναλογικών μετρήσεων, δυαδικών, κ.ά.
3. **Τυποποίηση:** Η ενότητα σχολιάζει πρωτόκολλα που έχουν κατασκευαστεί και τυποποιηθεί από τον Διεθνή Οργανισμό IEC. Συνεπώς πολύ γρήγορα υιοθετήθηκε στη βιομηχανία ηλεκτρικής ενέργειας. Έτσι οι κατασκευαστές υποχρεώνονται σε συμμόρφωση στις προδιαγραφές του προτύπου διασφαλίζοντας ότι διαφορετικές συσκευές και συστήματα μπορούν να επικοινωνούν μεταξύ τους απρόσκοπτα. Η τυποποίηση αυτή τελικά βελτιώνει την **διαλειτουργικότητα** των συστημάτων που ακολουθούν το πρότυπο στην διαμόρφωση του επικοινωνιακού τους δικτύου.
4. **Αξιοπιστία:** Οι λειτουργίες που προσφέρει το APCI πακέτο, δηλαδή την αριθμητική ακολουθία απεσταλμένων μηνυμάτων διαμορφώνουν ένα πλαίσιο οργανωμένης και συντονισμένης επικοινωνίας, όπου η ροή ανταλλαγής μηνυμάτων καταγράφεται. Τέτοιες δυνατότητες δεν προσφέρονται στα πρωτόκολλα που μελετήσαμε ως τώρα (Modbus, DNP3), γεγονός που προσδίδει μεγάλο βαθμό αξιοπιστίας στο IEC/104.
5. **Χρονοσήμανση:** Η ανάγκη για ακριβή συγχρονισμό των δεδομένων που ανταλλάσσονται μεταξύ των συστημάτων φαίνεται και σε αυτό το πρωτόκολλο επικοινωνίας. Οι χρονικές ετικέτες των ASDU δεδομένων επιτρέπουν τη συγχρονισμένη διαχείριση και επεξεργασία των δεδομένων από διάφορα υποσυστήματα, επιτρέποντας τον ακριβή συγχρονισμό των ενεργειακών διαδικασιών και την αποτελεσματική λειτουργία του συστήματος ελέγχου. Επομένως, η λειτουργία χρονοσήμανσης είναι κρίσιμη για την αξιοπιστία και τη συνοχή των επικοινωνιακών διαδικασιών της επικοινωνίας IEC/104.

Το γεγονός ότι το πρότυπο που μελετάμε ανήκει στην οικογένεια της IEC, η οποία την σημερινή εποχή μελετά στα ζητήματα κυβερνοασφάλειας και προτείνει βελτιώσεις, αυξάνει σε μεγάλο βαθμό την εμπιστοσύνη των χρηστών. Ωστόσο, όπως κάθε βιομηχανικό πρωτόκολλο, έτσι και τα πρωτόκολλα της προδιαγραφής ακόμα παρουσιάζουν κενά στους μηχανισμούς ασφαλείας.

Στην πράξη λοιπόν η ασφάλεια του IEC 104 έχει αποδειχθεί προβληματική, καθώς σε πρόσφατες αναφορές ασφαλείας, έχουν αναφερθεί πολλαπλά προβλήματα ασφαλείας που σχετίζονται με αυτό το πρωτόκολλο. Κατόπιν έρευνας που διεξήχθη σχετικά με τα **ευάλωτα σημεία της επικοινωνίας** του, διαπιστώθηκαν τα εξής θέματα:

1. **Απουσία Checksum:** Η απουσία πεδίου αθροίσματος ελέγχου στο πρωτόκολλο IEC 60870-5-104 σημαίνει ότι εξαρτάται πλήρως από τα κατώτερα επίπεδα επικοινωνίας για την προστασία της ακεραιότητας των δεδομένων. Συνεπώς μεγάλο μέρος της ασφάλειας επαφίεται στο TCP/IP πρωτόκολλο, όπου ναι μεν υπάρχουν μηχανισμοί ελέγχου, αλλά η έκθεση της επικοινωνίας στο Διαδίκτυο προσδίδει μεγάλα επίπεδα αβεβαιότητας.
2. **Μετάδοση μηνυμάτων απλού κειμένου**: Η ανταλλαγή μη κρυπτογραφημένων απλών κειμένων καθιστά την μετάδοση πληροφοριών μεταξύ του κέντρου ελέγχου και των υποσταθμών ευάλωτη σε επιθέσεις παρακολούθησης, παρείσφρησης και παρενόχλησης της επικοινωνίας. Για παράδειγμα, ένας επιτιθέμενος μπορεί να εκτελέσει μια επίθεση Man-in-the-Middle (MITM) και να συλλέξει και να ερμηνεύσει τιμές μέτρησης στο πεδίο και εντολές του απομακρυσμένου κέντρου ελέγχου. Για τα κλεμμένα στοιχεία υπάρχει επίσης ο κίνδυνος να τροποποιηθούν και στη συνέχεια να αποσταλθούν πίσω στην υποδομή επικοινωνιών. Ένα τέτοιο γεγονός απειλεί ευθέως την σταθερότητα και την ασφάλεια του συστήματος ισχύος, σε επίπεδο παραγωγής και ακόμη περισσότερο σε επίπεδο ελέγχου.
3. **Ελλιπής Αυθεντικοποίηση**: Λόγω έλλειψης ταυτοποίησης χρήστη κακόβουλοι εισβολείς θα μπορούσαν να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση στα συστήματα SCADA και να εκτελέσουν εντολές ανάκτησης πληροφοριών και απομακρυσμένου χειρισμού. Εδώ το πρόβλημα γίνεται ακόμη πιο κρίσιμο καθώς απειλείται γενικότερα η ακεραιότητα του συστήματος και η διαθεσιμότητα των πληροφοριών. Η πρόσβαση αγνώστων στο σύστημα μπορεί να οδηγήσει σε καταστροφικές ζημιές και παραβίαση της λειτουργίας και ασφάλειας του συστήματος SCADA. Για παράδειγμα, μια ψευδής εντολή ελέγχου από απόσταση, όπως "ανοίξτε το διακόπτη κυκλώματος", μπορεί να προκαλέσει το σύστημα ισχύος να αποβάλλει φορτίο, επηρεάζοντας την αξιοπιστία του εφοδιασμού ισχύος και απειλώντας την ασφάλεια.
4. **Μέγεθος**: Παρά τις επεκτάσεις ασφαλείας του δημιουργού, το πρωτόκολλο μπορεί, βάσει προδιαγραφής, να μεταδώσει μόνο 255 bytes ταυτόχρονα. Αυτό περιορίζει έμμεσα τον αριθμό των bit ασφαλείας που μπορούν να προστεθούν κατά τη μετάδοση δεδομένων. Συνεπώς η διασφάλιση της ακεραιότητας του επικοινωνιακού συστήματος απαιτεί πιο προηγμένες τεχνικές ανίχνευσης και απόκρουσης επιθέσεων.

Τέλος και πέραν των ζητημάτων ασφάλειας θα μπορούσαμε να θεωρήσουμε ακόμη ένα μειονεκτήματα για το IEC/104 σε σχέση με άλλες επιλογές επικοινωνίας και διαμόρφωσης του δικτύου, σε ένα βιομηχανικό περιβάλλον.

5. **Πολυπλοκότητα:** Από την δομή των APDU μηνυμάτων και τις πολλές δυνατότητες που προσφέρει η προδιαγραφή καταλαβαίνουμε ότι η υλοποίησή του απαιτεί εξειδικευμένες γνώσεις και περισσότερο χρόνο. Αυτά τα δύο επηρεάζουν τόσο την συνθετότητα όσο και το κόστος διαμόρφωσης και συντήρησης του επικοινωνιακού δικτύου. Ειδικά στα βιομηχανικά περιβάλλοντα η απλότητα αποτελεί προτέρημα και έτσι πιο απλά πρωτόκολλα (πχ. Modbus) μπορεί να προτιμηθούν, ακόμη και αν δεν είναι τόσο προηγμένα από σκοπιά προσφερόμενων λειτουργιών στην επικοινωνία και τον χρήστη.

2.4.5. Τα πεδία εφαρμογής του IEC 60870-5

Το πρότυπο IEC 60870-5 έχει πλέον υιοθετηθεί στη βιομηχανία ηλεκτρικής ενέργειας και αποτελεί ένα από τα πιο διαδεδομένα πρότυπα πρωτοκόλλων για συστήματα απομακρυσμένου ελέγχους και απόκτησης δεδομένων. Είναι γεγονός ότι,

η προηγμένη λειτουργικότητά του σε εφαρμογές SCADA και επικοινωνίας με απομακρυσμένα RTUs και άλλες έξυπνες συσκευές, έφερε το πρωτόκολλο σε αρκετά πλεονεκτική θέση έναντι του πιο απλοϊκού Modbus. Σε αντιπαράθεση με το DNP3, το IEC 60870-5 συναντάται κυρίως στην Ευρώπη, αλλά και σε ορισμένες ασιατικές χώρες. Επιπλέον, καθώς τα τρία αυτά πρωτόκολλα ενσωματώνουν εύκολα την TCP/IP στοίβα και το Ethernet μπορούν εξίσου να χρησιμοποιηθούν σε εφαρμογές που απαιτούν πρόσβαση στο διαδίκτυο.

Ως προς τα συστήματα ηλεκτρικής ισχύος, το πρότυπο είναι ικανό να εφαρμοστεί τόσο σε συστήματα μετάδοσης και διανομής όσο και σε εργοστάσια παραγωγής, καθώς προδιαγράφει ένα σύστημα επικοινωνίας ειδικά διαμορφωμένης για τον απομακρυσμένο έλεγχο στον ενεργειακό τομέα. Ειδικότερα, λόγω της μεγαλύτερης αξιοπιστίας του είναι ταιριαστό να προτιμηθεί σε εφαρμογές όπου η μετάδοση μηνυμάτων περιλαμβάνει κρίσιμες πληροφορίες και ξεπερνά τα φυσικά όρια του συστήματος. Για τον λόγο αυτό, είναι ευρέως διαδεδομένο σε **συστήματα παρακολούθησης και ελέγχου έξυπνων υποσυστημάτων και υποσταθμών** μέσω ενός υπερκείμενου κεντρικού σταθμού.

Η αξιοπιστία του IEC 60870-5, μεγαλώνει την προτίμησή του σε εφαρμογές που έχουν να κάνουν με την **ασφάλεια και την προστασία του ηλεκτρικού συστήματος** σε διάφορους τομείς. Για παράδειγμα χρησιμοποιείται για την ανταλλαγή δεδομένων από και προς τον εξοπλισμό ηλεκτρικής προστασίας, όπως ρελέ, διακόπτες και μετασχηματιστές. Επίσης, χρησιμοποιείται αρκετά για δοκιμές και εφαρμογές κυβερνοασφάλειας για τον εξοπλισμό του δικτύου τηλεελέγχου. Αυτό φάνηκε και από το διαθέσιμο βιβλιογραφικό υλικό που υπάρχει για ζητήματα επιθέσεων στην κυβερνοασφάλεια.

2.5. Πρότυπο επικοινωνίας IEC 61850

2.5.1. Γενικά στοιχεία για τα πρωτόκολλα υποσταθμών του IEC 61850

Το σύνολο πρωτοκόλλων που πρόκειται να μελετηθούν στην παρούσα ενότητα **σχεδιάστηκαν και έχουν ευρεία εφαρμογή κυρίως στο υποσταθμούς ηλεκτρικής ενέργειας**. Λόγω της ύψιστης σημασίας που έχουν τα **Συστήματα Αυτοματισμού Υποσταθμών (ΣΑΥ)** στην διαδικασία παραγωγής και μεταφοράς ηλεκτρικής ενέργειας, θεωρήθηκε κομβική η δημιουργία ενός προτύπου που θα τυποποιεί το σύνολο των κανόνων επικοινωνίας μεταξύ των συσκευών που απαρτίζουν τους υποσταθμούς.

Παλαιότερα, τα βιομηχανικά πρωτόκολλα και οι κλασικές αρχιτεκτονικές επικοινωνίας παρείχαν στους υποσταθμούς σχετικά απλές λειτουργίες αυτοματισμού. Η παραδοσιακή επικοινωνία είχε σχεδιαστεί χωρίς να εφαρμόζει προηγμένες τεχνικές διότι βασιζόταν στην τότε διαθέσιμη δικτυακή τεχνολογία. Την τελευταία εικοσαετία ωστόσο συντελείται μια τεράστια εξέλιξη στην τεχνολογία δικτύων που άλλαξε δραματικά το τι είναι πλέον εφικτό για τον αυτοματισμό του ηλεκτρικού συστήματος σε έναν υποσταθμό. Τεχνολογίες όπως οι εφαρμογές στο Ίντερνετ, τα δίκτυα ευρείας περιοχής και υψηλής ταχύτητας, τα υπολογιστικά συστήματα υψηλής απόδοσης σε χαμηλό κόστος παρέχουν δυνατότητες που δύσκολα θα μπορούσαν να φανταστούν κατά την σχεδίαση των παλαιότερων πρωτοκόλλων για τον αυτοματισμό υποσταθμών.

Ορισμός: Το **IEC 61850** είναι ένα νέο και πολύ σημαντικό διεθνές πρότυπο εξειδικευμένο στους υποσταθμούς ηλεκτρικής ενέργειας με ουσιαστική συμβουλή στον τρόπο σχεδιασμού και διαμόρφωσης των Συστημάτων Αυτοματισμού Υποσταθμών. Είναι ένα παγκόσμιο πρότυπο για την δικτύωση και τον αυτοματισμό ηλεκτρικών συστημάτων και αναπτύχθηκε από τη Διεθνή Επιτροπή Ηλεκτροτεχνικού Σχεδιασμού (IEC) το 2004 για να παρέχει ένα κοινό πλαίσιο για την αυτοματοποίηση, την παρακολούθηση και τον έλεγχο των υποσταθμών. Το πρότυπο αναθεωρείται και ενημερώνεται από την IEC κοινότητα έως και σήμερα.

Η ανάπτυξη του IEC 61850 έχει μεγάλο αντίκτυπο στην βιομηχανική αυτοματοποίηση που οφείλεται στην καθιέρωση του **αντικειμενοστραφούς μοντέλου δεδομένων.** Το πρότυπο διαθέτει μια εκτενείς **σουίτα πρωτοκόλλων επικοινωνίας**, που επιτρέπουν την μετάδοση πληροφοριών και δεδομένων ανάμεσα στον εξοπλισμό του υποσταθμού. Ειδικότερα**,** στο πρότυπο περιγράφεται ένα σύνολο κανόνων διαμόρφωσης επικοινωνίας, πρωτοκόλλων και μοντέλων δεδομένων που επιτρέπουν σε έξυπνες ηλεκτρονικές συσκευές (IEDs) στους υποσταθμούς να επικοινωνούν μεταξύ τους και με συστήματα ανώτερων επιπέδων (πχ. κέντρα ελέγχου) χρησιμοποιώντας μια προηγμένη γλώσσα. Το IEC 61850 υποστηρίζει τόσο τις παραδοσιακές μεθόδους ενσύρματης επικοινωνίας όσο και τις νεότερες μεθόδους επικοινωνίας βασισμένες στο Ethernet, παρέχοντας μια ευέλικτη και διαχρονική λύση για την αυτοματοποίηση υποσταθμών.

Όπως συνηθίζεται σε όλα τα πρότυπα IEC, το 61850 χωρίζεται σε μέρη, τα οποία καθορίζουν διαφορετικές πτυχές του συνολικού προτύπου. Αυτά τα μέρη συνεργάζονται μεταξύ τους για να καθορίσουν ένα ολοκληρωμένο σύνολο προδιαγραφών για τον αυτοματισμό συστημάτων υποσταθμών και καθορίζουν την επικοινωνία, τη διαλειτουργικότητα και την ασφάλεια του συστήματος στον κυβερνοχώρο.

Στον παρακάτω πίνακα περιγράφονται τα 10 πρώτα και πιο σημαντικά μέρη του προτύπου IEC 61850:

<table>
<tr><th>Μέρη</th><th colspan="2">Περιγραφή</th></tr>
<tr><td>IEC 61850-1</td><td colspan="2">Εισαγωγή και Επισκόπηση</td></tr>
<tr><td>IEC 61850-2</td><td colspan="2">Γλωσσάριο</td></tr>
<tr><td>IEC 61850-3</td><td colspan="2">Γενικές Απαιτήσεις</td></tr>
<tr><td>IEC 61850-4</td><td colspan="2">Περιέχει διαδικασίες διαχείρισης συστήματος και εργασιών συγκεκριμένα για συστήματα αυτοματισμού ενέργειας στα οποία γίνεται επικοινωνία μεταξύ IED συσκευών.</td></tr>
<tr><td>IEC 61850-5</td><td colspan="2">Περιέχει πληροφορίες σχετικά με τις απαιτήσεις επικοινωνίας των λειτουργιών αυτοματισμού σε υποσταθμούς.</td></tr>
<tr><td>IEC 61850-6</td><td colspan="2">Καθορίζει την γλώσσα προγραμματισμού για τη διαμόρφωση των IEDs στα ΣΑΥ που ονομάζεται Γλώσσα Περιγραφής Συστήματος Διαμόρφωσης (SCL).</td></tr>
<tr><td>IEC 61850-7-1</td><td rowspan="4">Παρουσιάζει λεπτομερή αναφορά του πρωτοκόλλου επιπέδου εφαρμογής ACSI, των Λογικών Κόμβων (LN), των Αντικειμένων Δεδομένων (DO), των Κοινών Κλάσεων Δεδομένων (CDC) και περιγράφει πώς θα επιτευχθεί η διαλειτουργικότητα χρησιμοποιώντας τα παραπάνω υλικά.</td><td rowspan="5">Βασική Δομή Επικοινωνίας για Υποσταθμό και Εξοπλισμός τροφοδοσίας</td></tr>
<tr><td>IEC 61850-7-2</td></tr>
<tr><td>IEC 61850-7-3</td></tr>
<tr><td>IEC 61850-7-4</td></tr>
<tr><td>IEC 61850-7-410</td><td></td></tr>
</table>

IEC 61850-7-420	Εξειδικεύονται στην επικοινωνία για την παρακολούθηση και τον έλεγχο, στις λογικές μοντελοποίησης και οδηγίες συγκεκριμένα σε Υδροηλεκτρικούς σταθμούς. Επίσης περιγράφονται Λογικοί Κόμβοι πόρων διαμοιρασμένης ενέργειας.	
IEC 61850-7-510		
IEC 61850-8-1	Τα τμήματα αυτά καθορίζουν τη δομή του πρωτοκόλλου και την αντιστοίχιση διαφορετικών υπηρεσιών ACSI σε μηνύματα MMS, μηνύματα XML που μεταφέρονται μέσω του πρωτοκόλλου XMPP και του Ethernet.	Χαρτογράφηση ειδικής υπηρεσίας επικοινωνίας - Specific Communication Service Mapping (SCSM)
IEC 61850-8-2		
IEC 61850-9-2		
IEC 61850-9-3	Καθορίζει το προφίλ του πρωτοκόλλου ακρίβειας χρόνου (PTP) της IEEE 1588-2008 σε συμμόρφωση με το IEC61850.	
IEC 61850-10	Καθορίζει την διαδικασία για την δοκιμή συμμόρφωσης.	

Σχήμα 2.19 – Προδιαγραφές προτύπου IEC 61850

Σε σχέση με τον παραπάνω πίνακα, το πρότυπο σήμερα έχει εξελιχθεί ακόμα περισσότερο, έχοντας προσθέσει επιπλέον μέρη στην συλλογή του. Ωστόσο, στην παρούσα εργασία **θα μελετήσουμε κυρίως το IEC 61850-7 όπου αναδεικνύεται ο πυρήνας της λογικής που έχει η επικοινωνία** και περιλαμβάνονται οι διάφορες λειτουργίες των πρωτοκόλλων, η δομή των μηνυμάτων που ανταλλάσσονται και η μορφή των δεδομένων. Οι ξεχωριστές ιδιότητες κάθε πρωτοκόλλου προδιαγραφής IEC 61850 σημαίνουν και διαφορετικές αδυναμίες στο καθένα και τελικά διαφορετικές τεχνικές που θα πρέπει να αναπτυχθούν για την αντιμετώπιση κινδύνων στον κυβερνοχώρο του υποσταθμού.

Πριν προχωρήσουμε στην μελέτη της δομής των μηνυμάτων μετάδοσης του IEC 61850 θα πρέπει να αποσαφηνίσουμε τις βασικές διαφορές του σε σχέση με το IEC 60870, καθώς και τα δύο περιλαμβάνουν πρωτόκολλα για εφαρμογές υποσταθμών. Όπως είδαμε στην προηγούμενη ενότητα, το IEC 60870 είναι ένα πρότυπο που χρησιμοποιείται για τον απομακρυσμένο έλεγχο και την παρακολούθηση των υποσταθμών. Περιλαμβάνει δηλαδή πρωτόκολλα επικοινωνίας πιο ταιριαστά για SCADA εφαρμογής. Από την άλλη, το IEC 61850 είναι ένα πλήρες πρότυπο για την αυτοματοποίηση του ίδιου του Υποσταθμού. Ορισμένες από τις κύριες διαφορές μεταξύ τους συνοψίζονται παρακάτω:

- Στο IEC 60870-5 είδαμε ένα επίπεδο δεδομένων με προκαθορισμένα αντικείμενα πληροφοριών και τύπους δεδομένων, ενώ το IEC 61850 χρησιμοποιεί ένα αφηρημένο και ιεραρχικό μοντέλο δεδομένων με λογικούς κόμβους, λογικές συσκευές και αντικείμενα δεδομένων.
- Το IEC 104 χρησιμοποιεί το πρωτόκολλο TCP ως πρωτόκολλο μεταφοράς, ενώ το IEC 61850 περιλαμβάνει μια ευρεία γκάμα πρωτοκόλλων που χρησιμοποιούν τόσο το TCP/IP, αλλά και άλλα πρωτόκολλα στοίβας UDP, MMS, κ.ά.
- Το IEC 104 έχει ένα χαμηλότερο επίπεδο ασφάλειας από το IEC 61850, το οποίο διαθέτει μια ειδική σειρά προτύπων (IEC 62351) για τεχνολογίες κυβερνοασφάλειας.

2.5.2. Βασική δομή και πρωτόκολλα επικοινωνίας IEC 61850-7

Η επικοινωνία εντός του υποσταθμού επικαθορίζεται από κάποιες συγκεκριμένες αλληλεπιδράσεις μεταξύ των συντελεστών του συστήματος ΣΑΥ. Οι αλληλεπιδράσεις αυτές κατανέμονται κυρίως σε τρεις βασικές κατηγορίες: **α. συλλογή/εγγραφή δεδομένων**, **β. παρακολούθηση/αναφορά δεδομένων**

και **γ. καταγραφή συμβάντων**. Για την πρώτη κατηγορία, όλα τα αιτήματα και οι δραστηριότητες ελέγχου προς τις φυσικές συσκευές μοντελοποιούνται ως την λήψη ή την εγγραφή τιμών σε αντίστοιχα «χαρακτηριστικά» που έχουν τα δεδομένων (data attributes). Για την ιχνηλάτηση και αναφορά δεδομένων στο IEC 61850-7 περιγράφεται ένας αποτελεσματικός τρόπος για την συνεχόμενης παρακολούθησης της κατάστασης του συστήματος, έτσι ώστε οι εντολές ελέγχου να εκτελούνται στον σωστό χρόνο.

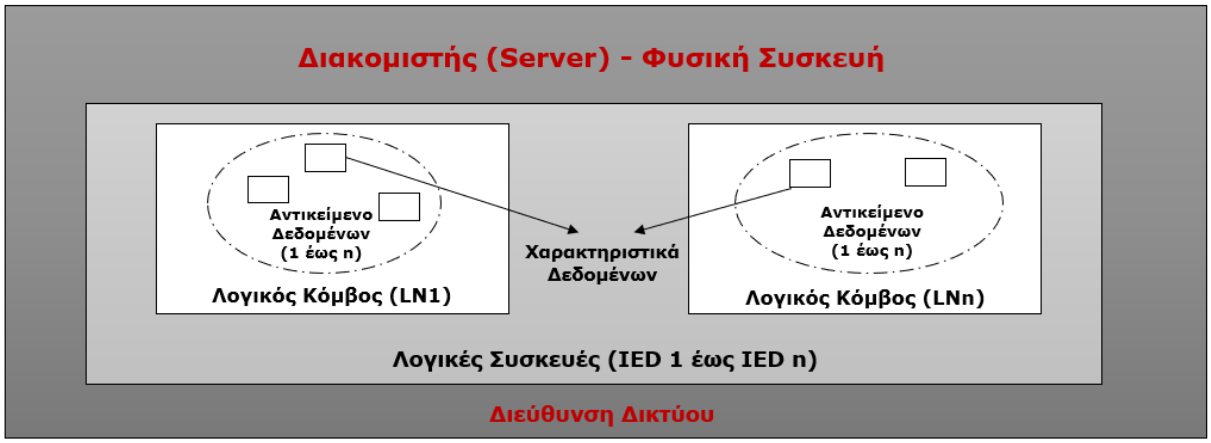
Για να πραγματοποιηθούν οι παραπάνω τύποι αλληλεπιδράσεων, το πρότυπο IEC 61850 καθορίζει μια σχετικά περίπλοκη δομή επικοινωνίας. Συγκεκριμένα πέντε βασικά είδη προφίλ εφαρμογής καθορίζονται στο πρότυπο: το αφηρημένο πρωτόκολλο υπηρεσιών επικοινωνίας (ACSI), το γενικό αντικειμενοστραφές προφίλ γεγονότων υποσταθμού (GOOSE) και το γενικό προφίλ κατάστασης γεγονότων υποσταθμού (GSSE), το πρωτόκολλο πολλαπλής μετάδοσης για δειγματοληψίες και μετρήσεις τιμών (SMV) και τέλος ένα προφίλ συγχρονισμού (TimeSync). Οι υπηρεσίες που προσφέρει το ACSI επιτρέπουν την επικοινωνία μεταξύ εφαρμογών και εξυπηρετητών του συστήματος σε μια διαδραστική αλληλεπίδραση τύπου πελάτη/διακομιστή. Από την άλλη, το GOOSE παρέχει ένα γρήγορο τρόπο ανταλλαγής δεδομένων στο δίαυλο επικοινωνίας του υποσταθμού και το GSSE παρέχει έναν άμεσο τρόπο ανταλλαγής κατάστασης στο επίπεδο υποσταθμού. Το SMV παρέχει έναν αποτελεσματικό τρόπο ανταλλαγή δεδομένων σε ένα δίκτυο διεργασίας.

Στην συνέχεια η εργασία επικεντρώνεται στην ανάλυση των παραπάνω πρωτοκόλλων. Στην πρώτη υποενότητα (Α) θα αναλύσουμε τους τύπους των δεδομένων που ανταλλάσσονται με την αντικειμενοστραφή λογική του ACSI, ενώ στην δεύτερη (Β) θα δοθεί πλήρης περιγραφή των υπολοίπων πρωτοκόλλων. Τέλος (Γ) θα αναφερθούμε σε μια ακόμη σημαντική υπηρεσία, αυτήν της αντιστοίχισης των αντικειμένων στα πρωτόκολλα εφαρμογής.

Α. ACSI και Αντικειμενοστραφή Μοντελοποίηση Δεδομένων:

Το κανάλι επικοινωνίας ACSI αποτελεί πολύ σημαντικό μέρος μιας λογικής σύνδεσης μεταξύ δύο λογικών κόμβων που επικοινωνούν στο δίκτυο. Για την ακρίβεια είναι το κύριο προφίλ επικοινωνίας στο πρότυπο IEC 61850 καθώς επιτρέπει στις εφαρμογές να επικοινωνούν με συσκευές-διακομιστές και καθορίζει τη σημασιολογία των δεδομένων που ανταλλάσσονται μεταξύ τους. **Η επιτροπή προτύπων IEC υιοθέτησε μια αντικειμενοστραφή προσέγγιση στον σχεδιασμό του ACSI**, η οποία περιλαμβάνει έναν ιεραρχικό και περιεκτικό μοντέλο δεδομένων και ένα σύνολο διαθέσιμων υπηρεσιών για κάθε ομαδοποίηση (κλάση) σε αυτό το μοντέλο δεδομένων. Αν και το μοντέλο δεδομένων περιγράφεται συνήθως εκτός του πεδίου εφαρμογής του ACSI, στην πραγματικότητα αποτελεί κομμάτι αυτού. Τα οφέλη της χρήσης μιας επικοινωνίας αντικειμενοστραφούς λογικής έχουν μεγάλη σημασία διότι τα «αντικείμενα» δεδομένων (π.χ. δεδομένα καταχωρητών) μπορούν να αναφέρονται με έναν ευανάγνωστο τρόπο (π.χ. "Relay0/MMXU0.voltage") αντί να χρησιμοποιείται η παραδοσιακή κωδικοποίηση διευθύνσεων (όπως Reg#02432). Αυτή η αναπαράσταση των δεδομένων βοηθά τους προγραμματιστές να κατασκευάσουν πιο αξιόπιστα λογισμικά για τις εφαρμογές ηλεκτρικής ενέργειας και πιο κατανοητά στους μηχανικούς που χειρίζονται την κάθε εφαρμογή.

Παρακάτω παρουσιάζεται μια αναπαράσταση της μοντελοποίησης του προτύπου για να μας βοηθήσει στην κατανόηση των βασικών λογικών στοιχείων που θα περιγράφουν στην συνέχεια.



Σχήμα 2.20 – Τα επίπεδα μοντελοποίησης αντικειμένων του IEC61850

Η γενική ιδέα της μοντελοποίησης είναι ότι κάθε διακομιστής του δικτύου (πχ. μια έξυπνη συσκευή) φιλοξενεί διάφορα αρχεία ή λογικές συσκευές, όπου **κάθε λογική συσκευή καθιστά την λογική αντιστοιχία σε μια φυσική συσκευή**. Οι λειτουργίες που υποστηρίζουν και εμπεριέχονται σε μια λογική συσκευή αναπαρίστανται από μια συλλογή πρωτογενών λειτουργικών μπλοκ που ονομάζονται λογικοί κόμβοι. Το IEC 61850-7 (στο 7-4) τυποποιεί μια συλλογή συμβατών τύπων λογικών κόμβων οι οποίοι καθορίζονται από τον παρακάτω ορισμό.

Ένας **Λογικός Κόμβος (LN)** είναι μια ομάδα δεδομένων και συναφών υπηρεσιών που σχετίζονται λογικά με μια λειτουργία του συστήματος ηλεκτρικής ενέργειας. Για παράδειγμα οι λογικοί κόμβοι για αυτόματο έλεγχο έχουν ονομασίες που όλες ξεκινούν με το γράμμα "A", ενώ εκείνοι για δειγματοληψίες και ηλεκτρικές μετρήσεις, ξεκινούν με το γράμμα "M". Αντίστοιχα, υπάρχουν λογικοί κόμβοι για Εποπτικό Έλεγχο (C), Γενικές Λειτουργίες (G), Διασύνδεση/Αρχειοθέτηση (I), Λογικοί Κόμβοι Συστήματος (L), Προστασία (P), Σχετικά με την Προστασία (R), Αισθητήρες (S), Μετασχηματιστές Μέτρησης (T), Διακόπτες (X), Μετασχηματιστές Ισχύος (Y) και Άλλος Εξοπλισμός (Z). Κάθε λογικός κόμβος έχει έναν αναγνωριστικό αριθμό ως κατάληξη στην ονομασία του. Εκτός από τους κανονικούς λογικούς κόμβους για λειτουργίες, το πρότυπο απαιτεί επίσης από κάθε λογική συσκευή να έχει δύο συγκεκριμένους λογικούς κόμβους: τον Λογικό Κόμβο Μηδέν (LN0) και το LPHD, οι οποίοι αντιστοιχούν στη λογική συσκευή και τη φυσική συσκευή, αντίστοιχα. Εκτός από την αποθήκευση πληροφοριών κατάστασης της λογικής συσκευής, ο LN0 παρέχει επιπλέον λειτουργίες όπως ελέγχους ρυθμίσεων, έλεγχο GSE, έλεγχο τιμών δειγματοληψίας κ.ά. Το παρακάτω παράδειγμα θα συμβάλει στην περαιτέρω κατανόηση της αναπαράστασης τον Λογικών Κόμβων της εφαρμογής:

Τα δεδομένα που ανταλλάσσονται μεταξύ των λογικών κόμβων ορίζονται ως **Αντικείμενα Δεδομένων (Data-Objects)** και ένας λογικός κόμβος συνήθως περιέχει αρκετά από αυτά. Επιπλέον, κάθε αντικείμενο είναι και ένα παράδειγμα μιας συνολικότερης **Κοινής Κλάσης Δεδομένων (Common-Data-Classes)** η οποία απαρτίζεται από αντικείμενα με κοινά, μεταξύ τους, χαρακτηριστικά. Δηλαδή, ένα αντικείμενο αποτελείται από πολλά **Χαρακτηριστικά Δεδομένων (Data-Attributes)**, τα οποία είναι χαρακτηριστικά που ορίζει η αντίστοιχη κοινή κλάση δεδομένων. Τα χαρακτηριστικά δεδομένων έχουν τύπο και περιορισμούς λειτουργικότητας και αντί να ομαδοποιούνται δεδομένων ανά αντικείμενο, παρέχεται ένας αποδοτικότερος τρόπος οργάνωσής τους σύμφωνα με την προκαθορισμένη λειτουργικότητα κάθε λογικού κόμβου.

1ο Παράδειγμα: Υποθέτουμε ότι υπάρχουν δύο είσοδοι τιμών σε μία έξυπνη συσκευή η οποία παρακολουθεί αντίστοιχα δύο τριφασικές τροφοδοσίες. Το καθορισμένο όνομα του λογικού κόμβου για μια μονάδα μέτρησης τριφασικής ισχύος είναι το "MMXU". Για να διαχωρίσουμε τις ξεχωριστές μετρήσεις που λαμβάνει η IED συσκευή για τις δύο τροφοδοσίες, θα αναπαρασταθούν οι λογικοί κόμβοι MMXU1 και MMXU2. Ο λογικός κόμβος μπορεί επίσης να χρησιμοποιήσει ένα προαιρετικό πρόθεμα εφαρμογής LN για να παρέχει περαιτέρω αναγνώριση του σκοπού του.

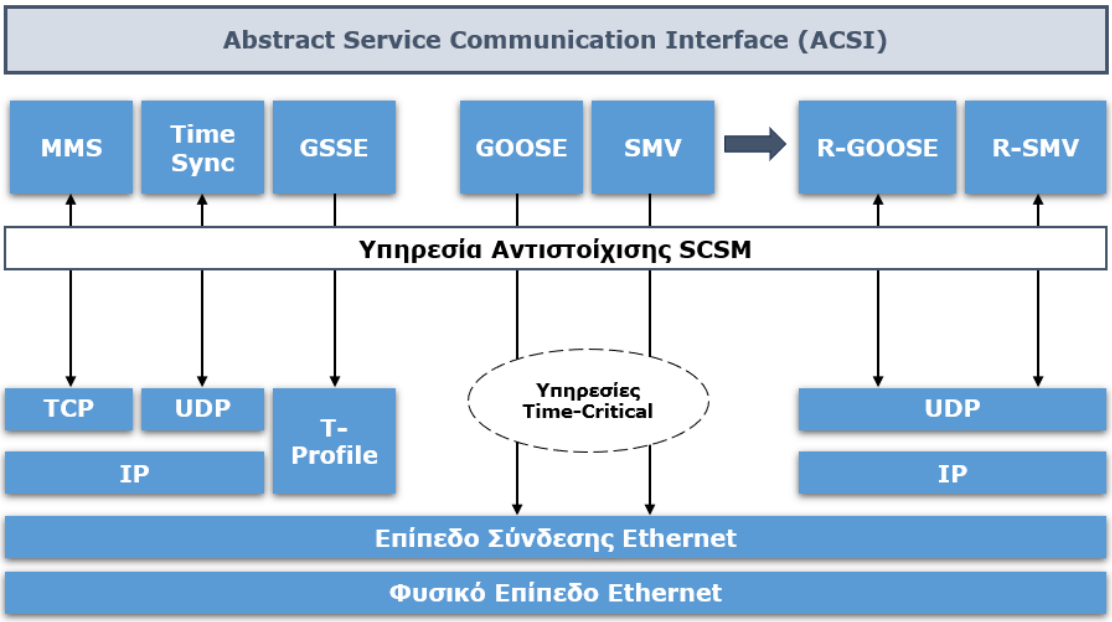
2ο Παράδειγμα: Κάθε στοιχείο δεδομένων έχει ένα μοναδικό όνομα, τα οποία καθορίζονται από το πρότυπο και σχετίζονται λειτουργικά με τον σκοπό του συστήματος ηλεκτρικής ενέργειας. Ένας διακόπτης κυκλώματος που μοντελοποιείται σε έναν αντικείμενο δεδομένων - κλάσης XCBR - περιλαμβάνει μια ποικιλία χαρακτηριστικών-δεδομένων. Βασικά χαρακτηριστικά είναι το "Loc" για τον προσδιορισμό εάν η λειτουργία είναι απομακρυσμένη ή τοπική, το "OpCnt" για έναν μετρητή λειτουργιών, το "Pos" για τη θέση του διακόπτη, το "BlkOpn" για εντολές στον διακόπτη να «ανοίξει» το κύκλωμα, το "BlkCls" για εντολές ενεργοποίησης του διακόπτη και το "CBOpCap" για χαρακτηριστικά λειτουργίας του διακόπτη κυκλώματος.

Μπορούμε να θεωρήσουμε ότι τα χαρακτηριστικά δεδομένων είναι το ίδιο σημαντικά με τα ίδια τα αντικείμενα δεδομένων για δύο βασικούς λόγους. Καταρχήν, τα αντικείμενα δεδομένων αποτελούν απλά λογικές συλλογές των περιεχόμενων τους, ενώ τα (πρωτογενή) χαρακτηριστικά δεδομένων αποτελούν την πραγματική λογική αντιστοίχιση σε φυσικές οντότητες (μονάδες μνήμης, καταχωρητές, θύρες επικοινωνίας, κ.λπ.). Δεύτερον, ο λόγος της δημιουργίας αντικειμένων κατά την μοντελοποίηση είναι η ευκολότερη διαχείριση και ανταλλαγή τιμών μιας ομάδας χαρακτηριστικών δεδομένων που μοιράζονται την ίδια λειτουργία.

Β. Βασικά πρωτόκολλα ανταλλαγής μηνυμάτων

Στο πρότυπο IEC 61850, ολόκληρο το σύστημα υποσταθμού μοντελοποιείται ως ένα κατανεμημένο σύστημα που αποτελείται από μια σειρά αλληλεπιδράσεων μεταξύ λογικών κόμβων, οι οποίοι διασυνδέονται μέσω λογικών συνδέσεων. Η λογική σύνδεση είναι μια λογική έννοια συνδέσεων μεταξύ κόμβων, οι οποίες μπορεί να είναι άμεσες ή έμμεσες ή ακόμη και συνδυασμός διαφορετικών τύπων καναλιών επικοινωνίας. Στην πραγματικότητα, η σύνδεση δύο λογικών κόμβων είναι συνήθως είτε έμμεση με την χρήση πρωτοκόλλων μεταφοράς TCP, UDP είτε άμεση με απευθείας σύνδεση στο Ethernet επίπεδο σύνδεσης-δεδομένων. Περισσότερα στοιχεία για τις λογικές συνδέσεων θα δούμε και στην παράγραφο 2.5.3.

Όπως αναφέρθηκε εισαγωγικά, προδιαγράφονται κάποια βασικά προφίλ πρωτοκόλλων επικοινωνίας που καθορίζουν μορφές μηνυμάτων που μεταδίδονται και είναι ειδικά διαμορφωμένα για συγκεκριμένες δραστηριότητες εντός του ΣΑΥ. Συγκεκριμένα το ACSI βασίζεται στην σουίτα μηνυμάτων MMS που πατάει στην TCP/IP στοίβα, ενώ τα μηνύματα αναφοράς συμβάντων υποσταθμού GOOSE και οι δειγματοληψίες τιμών SMV χρησιμοποιούν άμεση σύνδεση Ethernet. Το παρακάτω σχήμα (*Σχήμα 2.21)* απεικονίζει ένα πλήρες διάγραμμα συνδέσεων για τα προφίλ μηνυμάτων που έχουν αναφερθεί ως τώρα. Στην συνέχεια δίνονται σύντομες περιγραφές των μηνυμάτων και τη δομής τους.

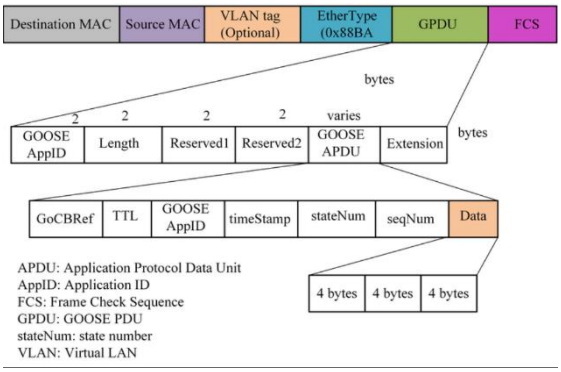


Σχήμα 2.21 – Προφίλ επικοινωνίας ACSI

1. **GSE – Generic Substation Events:** Σημαίνει «Γενικά Συμβάντα Υποσταθμού» και είναι ένας **μηχανισμός πολυκάναλης ανταλλαγής δεδομένων υψηλής ταχύτητας** που χρησιμοποιείται για την ανταλλαγή -χρονικά κρίσιμων- πληροφοριών μεταξύ των έξυπνων ηλεκτρονικών συσκευών. Τα μηνύματα GSE χωρίζονται σε δύο κατηγορίες: τα μηνύματα GOOSE και GSSE, όπου τα πρώτα χρησιμοποιούνται για τη μετάδοση πληροφοριών σχετικά με συμβάντα (events) ενώ τα δεύτερα για να στείλουν πληροφορίες σχετικά με αλλαγές κατάστασης (status) τιμών στον υποσταθμό. Τα μηνύματα αυτά είναι πολύ σημαντικά για τον έλεγχο και την προστασία του συστήματος καθώς προσφέρουν μια πολύ γρήγορη επικοινωνία, γεγονός που οφείλεται τόσο στην μορφή τους όσο και στην στοίβα πρωτοκόλλων που βασίζονται. Δηλαδή, αντί να χρησιμοποιήσουν TCP ή UDP ως επίπεδα μεταφοράς, το GSSE χρησιμοποιεί το δικό του ειδικό επίπεδο μεταφοράς (GSSE-T profile), ενώ τα μηνύματα GOOSE αποστέλλονται απευθείας στο επίπεδο σύνδεσης Ethernet χωρίς να περνούν από κάποιο επίπεδο μεταφοράς ή δικτύου.

   Η δομή κάθε μηνύματος GOOSE αποτελείται από δύο μέρη, την κεφαλίδα του μηνύματος και το πραγματικό φορτίο. Η κεφαλίδα του μηνύματος περιέχει πληροφορίες, όπως MAC διευθύνσεις προέλευσης και προορισμού, το VLAN ID, το επίπεδο προτεραιότητας και το EtherType. Το φορτίο GOOSE περιέχει τα πραγματικά δεδομένα που μεταδίδονται και αποτελείται από αρκετά πεδία που χρησιμοποιούνται για τη μεταφορά δεδομένων που απαιτούν χαμηλή καθυστέρηση. Τα πεδία αυτά είναι το AppID, το οποίο είναι ένα μοναδικό

αναγνωριστικό του μηνύματος, το πεδίο μήκους, που καθορίζει το μέγεθος του φορτίου, το Time Allowed To Live (TTL), το οποίο καθορίζει τον αριθμό των διακλαδώσεων ή δρομολογητών που μπορεί να διασχίσει το μήνυμα πριν απορριφθεί και το DataSet πεδίο περιέχει τα πραγματικά δεδομένα που ανταλλάσσονται. Μεγάλη σημασία για την προτεραιοποίηση των γεγονότων έχει ο αριθμός ακολουθίας "seqNum", ο οποίος καθορίζει την σωστή σειρά επεξεργασίας των μηνυμάτων. Αυτό το πεδίο είναι ιδιαίτερα σημαντικό σε εφαρμογές υψηλού ρυθμού μετάδοσης GOOSE, τόσο για την οργανωμένη επεξεργασία τους όσο και για την διαπίστωση πιθανής απώλειας μηνυμάτων.



Τα μηνύματα GSSE, από την άλλη, δεν περιλαμβάνουν πληθώρα τύπων δεδομένων. Μεταδίδονται αποκλειστικά σε δυαδική μορφή, στηρίζοντας την ιδέα «μικρότερο μέγεθος μηνυμάτων για την υψηλότερη ταχύτητα κωδικοποίησης/αποκωδικοποίησης του μηνύματος». (πχ. Αν κάποιος διακόπτης είναι ανοικτός ή κλειστός). Συγκεκριμένα, ένα GSSE μήνυμα αποτελείται από μια λίστα κατάστασης (σειρά bits) που υποδεικνύει την εμφάνιση συγκεκριμένων γεγονότων. Η λίστα κατάστασης αποτελείται από «λέξεις» των 32-bit λέξεις, που αντιπροσωπεύουν κάποιο διαφορετικό τύπο γεγονότος. Η πρώτη λέξη περιέχει το αναγνωριστικό εφαρμογής, το οποίο αναγνωρίζει την πηγή και τον προορισμό του μηνύματος. Η δεύτερη λέξη περιέχει τον αριθμό κατάστασης, που υποδεικνύει εάν το μήνυμα είναι νέο ή αναμεταδόθηκε. Η τρίτη περιέχει μια σημαία ελέγχου, που υποδεικνύει εάν το μήνυμα προορίζεται για δοκιμαστικούς σκοπούς ή όχι. Η τέταρτη λέξη υποδεικνύει την έκδοση του αρχείου διαμόρφωσης που χρησιμοποιήθηκε για τη δημιουργία του μηνύματος. Τέλος, οι υπόλοιπες λέξεις περιέχουν τα δεδομένα κατάστασης των γεγονότων, τα οποία είναι δυαδικές τιμές και πληροφορούν για την κατάσταση ενός συγκεκριμένου γεγονότος (πχ. κλειστός ή ανοικτός διακόπτης).

2. **SMV - Sampled Measured Values:** Τα μηνύματα SMV χρησιμοποιούνται για τη **μετάδοση δειγματοληπτικών αναλογικών σημάτων**, συνήθως από μετασχηματιστές τάσης ή ρεύματος, μέσω ενός ψηφιακού δικτύου επικοινωνίας. Αυτό το πρωτόκολλο σχεδιάστηκε για να παρέχει ακριβή μετάδοση δεδομένων χαμηλής καθυστέρησης για εφαρμογές προστασίας και ελέγχου στα συστήματα ισχύος. Τα δεδομένα μπορούν να χρησιμοποιηθούν για λειτουργίες όπως ανίχνευση βλαβών και αποσύνδεση φορτίου, μεταξύ άλλων. Σχεδιάστηκε για να υποστηρίζει τόσο την **περιοδική αναφορά** των τιμών μέτρησης όσο **αναφορές με συμβάντα**. Στην πρώτη περίπτωση, το μήνυμα SMV μεταδίδονται σε τακτά χρονικά διαστήματα μεταφέροντας την πιο πρόσφατη τιμή μέτρησης. Στην δεύτερη, αποστέλλονται μηνύματα όταν ανιχνεύεται μια νέα τιμή μέτρησης που υπερβαίνει ένα συγκεκριμένο όριο ή πληροί μια συγκεκριμένη συνθήκη.

   Η δομή μηνυμάτων περιλαμβάνει μια κεφαλίδα και το τμήμα δεδομένων, όπως τα GOOSE, και πεδία που περιέχουν κρίσιμες πληροφορίες μετρήσεων όπως η πραγματική τιμή μέτρησης, χρονική ετικέτα, η ποιότητα της μέτρησης και οι σχετικές μονάδες μέτρησης.

3. **MMS (Manufacturing Message Specification):** Το MMS είναι ένα ευρέως γνωστό -και πολύ σημαντικό- πρωτόκολλο μνημάτων το οποίο συναντάται σε πολλούς τομείς της βιομηχανίας, όπως η αυτοματοποίηση διαδικασιών και η

επιτήρηση των συστημάτων ελέγχου. Ειδικεύεται στην επικοινωνία μεταξύ διαφορετικών συσκευών σε ένα βιομηχανικό περιβάλλον και επιτρέπει σε έξυπνες συσκευές να ανταλλάσσουν πληροφορίες για την κατάστασή τους, τις μετρήσεις και άλλα σημαντικά δεδομένα σε πραγματικό χρόνο. Βρίσκεται στο επίπεδο παρουσίασης του μοντέλου OSI και βασίζεται στην στοίβα TCP/IP. Ουσιαστικά αποτελεί **το βασικό προφίλ επικοινωνίας τύπου πελάτη-διακομιστή στην εφαρμογή του ACSI**.

Τα μηνύματα MMS αποτελούνται από δύο μέρη: τα μηνύματα αιτήματος MMS και τα μηνύματα απάντησης MMS. Η (α.) **υπηρεσία αιτήματος MMS (MSR)** αποτελείται από πεδία που καθορίζουν τις λειτουργίες της υπηρεσίας. Το πεδίο τύπου μηνύματος υποδεικνύει τον τύπο της λειτουργίας που πρέπει να εκτελεστεί, όπως ανάγνωση, εγγραφή ή διαγραφή. Το πεδίο αντικειμένου καθορίζει το αντικείμενο ή το στοιχείο δεδομένων που πρέπει να αποκτηθεί πρόσβαση, και το πεδίο παραμέτρων περιέχει επιπλέον παραμέτρους που απαιτούνται για τη λειτουργία. Η (β.) **υπηρεσία απάντησης MMS (MSRESP)** περιλαμβάνει την απάντηση στο αίτημα που αποστέλλεται από τον πελάτη. Αποτελείται επίσης από αρκετά πεδία, συμπεριλαμβανομένου του τύπου μηνύματος που υποδεικνύει τον τύπο της απάντησης, όπως επιτυχή ολοκλήρωση, αποτυχία ή σφάλμα. Το πεδίο κώδικα απάντησης περιέχει τον κωδικό κατάστασης ενώ το πεδίο δεδομένων μεταφέρει τα πραγματικά δεδομένα που επιστρέφονται από τον διακομιστή, όπως τιμές χαρακτηριστικών αντικειμένων δεδομένων.

4. Τέλος, τα μηνύματα GOOSE και SMV μπορεί επίσης να μεταφερθούν στο επίπεδο 2 μέσω των επιπέδων UDP/IP σχηματίζοντας έτσι τα νέα δρομολογημένα μηνύματα **Routed-GOOSE και Routed-SMV**. Τα R-GOOSE και R-SMV μηνύματα έχουν παρόμοια μορφή με τα GOOSE και SMV αντίστοιχα, με μια επιπλέον προσθήκη, την **κεφαλίδα δρομολόγησης.** Αυτή οποία περιέχει πληροφορίες σχετικά με τις διευθύνσεις του δικτύου. Με αυτόν τον τρόπο τα μηνύματα δεν περιορίζονται στην επικοινωνία του υποσταθμού αλλά επιτρέπουν την επικοινωνία μεταξύ πολλαπλών υποσταθμών ή άλλων τμημάτων δικτύου.

Το IEC 61850 προδιαγράφει και άλλους τύπους μηνυμάτων πέραν όσων αναφέρθηκαν. Επιλέξαμε να αναλύσουμε ενδεικτικά τα πιο σημαντικά και αυτά που καθορίζουν μια διαφορετική δομή στοίβας πρωτοκόλλων για την αντίστοιχη επικοινωνία. Ακριβώς επειδή η ενσωμάτωση (ή όχι) διαφορετικών πρωτοκόλλων (πχ. μεταφοράς) στην μετάδοση κάθε μηνύματος σημαίνει αντικειμενικά και διαφορετικό χρόνο μετάδοσης, το πρότυπο δίνει βαρύνουσα σημασία στον χρόνο. Η διάρκεια μετάδοσης είναι πρακτικά η απόδοση του μηνύματος στις απαιτήσεις του συστήματος, διότι αυτές οι απαιτήσεις καθορίζουν χρονικά βασικές λειτουργίες του υποσταθμού. Συνεπώς το πρότυπο κατηγοριοποιεί τα μηνύματα με αυτό το κριτήριο.

Ο **χρόνος μετάδοσης μηνύματος** ορίζεται από το άθροισμα του χρόνου μετάδοσης κατά μήκος της δικτυακής σύνδεσης μεταξύ δύο έξυπνων συσκευών (t_δ) και τον χρόνο εκτέλεσης του αλγορίθμου επεξεργασίας της επικοινωνίας που υπάρχει σε κάθε συσκευή ($t_{\varepsilon 1,\varepsilon 2}$). Δηλαδή ο συνολικός χρόνος μετάδοσης για κάθε μήνυμα ορίζεται ως εξής:

$$T_{\mu\varepsilon\tau.} = t_{\varepsilon 1} + t_\delta + t_{\varepsilon 2}$$

Παρακάτω αναφέρονται οι χρόνοι απόδοσης για κάθε κατηγορία μηνύματος:

Τύπος	Μηνύματα Εφαρμογής	Κατηγορία	Χρονική Απαίτηση	
1A	**GOOSE, GSSE**	Χρονικά κρίσιμα “trip”	10 ms	**3 ms**
1B	**GOOSE, GSSE**	Χρονικά κρίσιμα “άλλα”	100 ms	20 ms
2	**MMS**	Μέσης ταχύτητας	100 ms	
3	**MMS**	Χαμηλής Ταχύτητας	500 ms	
4	**SMV**	Ανεπεξέργαστα δεδομένα	10 ms	**3 ms**
5	**FTP**	Μεταφορά αρχείων	≥1000 ms	
6	**PTP**	Συγχρονισμός	Ακρίβεια χρόνου	
7	**MMS**	Χαμηλής ταχύτητας με αυθεντικοποίηση	500 ms	

Σχήμα 2.22 – Απόδοση μηνυμάτων IEC 61850

- **Τύπου 1A και 1B:** Τα μηνύματα GOOSE και GSSE αντιστοιχίζονται άμεσα στο επίπεδο Ethernet για να μειωθεί το μέγεθος της στοίβας, καθώς αυτά τα μηνύματα αναφέρουν γεγονότα πεδίου και είναι χρονικά κρίσιμα. Αυτή η κατηγορία μηνυμάτων χρησιμοποιείται σε διατάξεις προστασίας του υποσταθμού και περιέχουν δεδομένα ένδειξης κατάστασης ή εντολής, όπως "τριπ", "κλείσιμο", "εκκίνηση", "διακοπή" ή "αποκλεισμός". Τα μηνύματα που μεταφέρουν την εντολή "τριπ" ονομάζονται Τύπου 1A, ενώ τα υπόλοιπα Τύπου 1B.
- **Τύπου 2:** Τα μηνύματα μέσης ταχύτητας χρησιμοποιούνται για την μετάδοση πληροφοριών κανονικής λειτουργίας του υποσταθμού. Περιέχουν κρίσιμες πληροφορίες συστήματος ως προς την σημασία τους, όχι όμως ως προς τον χρόνο(non-critical). Αυτή η κατηγορία απαιτεί επικοινωνία πελάτη-εξυπηρετητή και περιλαμβάνει μηνύματα της σουίτας MMS, που είτε είναι περιοδικά είτε ενεργοποιούνται από κάποιο γεγονός.
- **Τύπου 3:** Είναι κοινά μηνύματα ελέγχου και εντολών όπως για παράδειγμα ανάγνωση/εγγραφή τιμών, καταγραφή/μετάδοση γεγονότων, λειτουργίες αυτόματου ελέγχου, κ.ά. Δεν είναι χρονικά κρίσιμα διότι συνήθως δεν περιλαμβάνουν δεδομένα ενέργειας αλλά διαφορετικές παραμέτρους (μετρήσεις πίεσης, θερμοκρασίας, κ.λπ.). Έτσι μπορούν να αντιστοιχίζονται στις MMS υπηρεσίες μέσω του TCP πρωτοκόλλου μεταφοράς, όπως και τα μηνύματα τύπου 2.
- **Τύπου 4:** Σε αυτήν την κατηγορία βρίσκονται μηνύματα μη επεξεργασμένων δεδομένων που μετρήθηκαν στο πεδίο. Εδώ περιλαμβάνονται SMV μηνύματα κυκλικής/περιοδικής δειγματοληψίας από τα όργανα μετασχηματιστών τα οποία σχηματίζουν συνεχείς συγχρονισμένες ροές δεδομένων που παράγονται σε ένα ΣΑΥ. Όπως είδαμε και στην ανάλυσή τους τα SMV αντιστοιχίζονται κατευθείαν στο επίπεδο Ethernet χωρίς ενδιάμεσες επεξεργασίες και για αυτό η απόδοση τους είναι μεγάλη.
- **Τύπου 5:** Τα μηνύματα αυτής της κατηγορίας αφορούν το πρωτόκολλο μεταφοράς αρχείων (FTP). Έχουν μεγάλο όγκο δεδομένων που αποτελούνται από εγγεγραμμένα αρχεία, αρχεία πληροφοριών και ρυθμίσεων τα οποία μεταδίδονται κατά περίσταση σε έναν παραλήπτη σε επιλεγμένο χρόνο. Επειδή μπορεί να έχουν μεγάλο όγκο και άρα μεγάλο χρόνο μετάδοσης, τα δεδομένα αυτά κατακερματίζονται σε μικρότερα μπλοκ δεδομένων ώστε να αφήνουν άλλες δραστηριότητες στο δίκτυο να συμβαίνουν ενδιάμεσα της μετάδοσης του αρχείου. Αυτή η ιδιότητα τα καθιστά και τα λιγότερα σημαντικά ως προς την χρονική απαίτηση και χρησιμοποιούν το UDP πρωτόκολλο μεταφοράς.

- **Τύπος 6**: Αυτή η κατηγορία μηνυμάτων περιλαμβάνει τα μηνύματα συγχρονισμού για τα εσωτερικά ρολόγια των συσκευών IED στο ΣΑΥ. Αυτά τα μηνύματα είναι περιοδικά και η περιοδικότητά τους καθορίζεται με βάση την ακρίβεια που απαιτείται για την εφαρμογή. Χρησιμοποιούν το πρωτόκολλο IEEE 1588 Precision Time Protocol (PTP) μέσω του επιπέδου μεταφοράς UDP/IP.
- **Τύπου 7**: Είναι επίσης μηνύματα εντολών (όπως ο τύπος 3) αλλά περιέχουν πρόσθετες λειτουργίες αυθεντικοποίησης. Χρονικά κατατάσσονται επίσης στα μην κρίσιμα μηνύματα.

Επεξήγηση: Για τους τύπους 1 και 4 (GSE και SMV) το πρότυπο ορίζει δύο κλάσεις επίδοσης για αυτό και στον πίνακα (σχήμα 2.22) αναγράφονται δύο διαφορετικές χρονικές απαιτήσεις.

Γ. Αντιστοίχιση αντικειμένων στα πρωτόκολλα μηνυμάτων

Η βασική αρχιτεκτονική που υιοθετείται από το IEC 61850, ακολουθεί μια αφηρημένη λογική για να περιγράψει σε επίπεδο εφαρμογής τα διάφορα στοιχεία του συστήματος ισχύος. Δημιουργεί έτσι αφηρημένα μοντέλα αντικειμένων, δεδομένων και υπηρεσιών - όπως περιεγράφηκε στην παράγραφο 2.5.2/Α – τα οποία είναι ανεξάρτητα από οποιοδήποτε πρωτόκολλο. Τα αφηρημένα μοντέλα της επικοινωνίας ACSI παρέχουν μια σειρά υπηρεσιών και απαντήσεων σε αυτές τις υπηρεσίες που επιτρέπουν σε όλες τις συσκευές να συμπεριφέρονται με έναν κοινό τρόπο στο εσωτερικό του επικοινωνιακού δικτύου.

Παρόλο που η αφηρημένο μοντελοποίηση είναι κρίσιμη για την επίτευξη αυτού του επιπέδου συμβατότητας, η μετάδοση της πληροφορίας θα πρέπει να λειτουργεί στα πλαίσια συγκεκριμένων πρωτοκόλλων, ώστε τα μοντέλα να λειτουργήσουν εντός των καθόλου αφηρημένων υπολογιστικών περιβαλλόντων. Συνεπώς, θα πρέπει να υπάρξει μια συγκεκριμένη **διαδικασία αντιστοίχισης (mapping) των αφηρημένων μοντέλων δεδομένων με βασικά πρωτόκολλα υπηρεσιών επικοινωνίας** (TCP/IP, κ.ά.). Το IEC 61850 προδιαγράφει την υπηρεσία SCSM για να επιτελέσει ακριβώς αυτόν τον ρόλο.

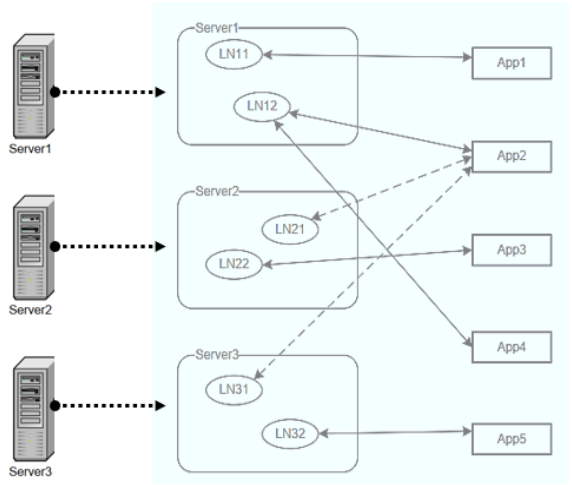
Το SCSM καθορίζει επακριβώς τον τρόπο με τον οποίο οι αφηρημένες υπηρεσίες και μοντέλα δεδομένων που καθορίζονται στο IEC 61850-7-2 αντιστοιχίζονται σε συγκεκριμένα επικοινωνιακά πρωτόκολλα και μορφές δεδομένων. Για παράδειγμα, το IEC 61850-8-1 αντιστοιχεί τα αφηρημένα αντικείμενα και υπηρεσίες στα πρωτόκολλα μηνυμάτων MMS, ενώ για τη μετάδοση δειγματοληπτικών τιμών μέσω του ISO/IEC 8802-3 (Ethernet) η αντιστοίχιση καθορίζεται στο πρότυπο IEC 61850-9-2. Έτσι, η υπηρεσία αντιστοίχισης τελικά **εξασφαλίζει τη διαλειτουργικότητα και τη συμβατότητα** μεταξύ διάφορων συσκευών και εφαρμογών που χρησιμοποιούν το πρότυπο IEC 61850.

2.5.3. Υπηρεσίες ACSI και τοπολογία επικοινωνίας

Στο ιεραρχικό μοντέλο δεδομένων που ορίζεται στο πρότυπο IEC 61850, ο διακομιστής (server) είναι το υψηλότερο επίπεδο της ιεραρχίας και λειτουργεί ως το σημείο «επαφής» φυσικών συσκευών και λογικών αντικειμένων. Θεωρητικά, ένας Ηλεκτρονικός Συσκευαστής (IED) μπορεί να φιλοξενεί έναν ή περισσότερους διακομιστές, αλλά στην πράξη συνήθως λειτουργεί μόνο ένας διακομιστής σε ένα IED. Ο server είναι ουσιαστικά ένα πρόγραμμα που εκτελείται σε ένα IED και μοιράζεται ίδιες έννοιες με άλλους διακομιστές όπως για παράδειγμα ο FTP διακομιστής. Κάθε διακομιστής έχει τουλάχιστον ένα σημεία πρόσβασης (access

points) στο οποίο συνδέεται ένας πελάτης (client) που θέλει να αποκτήσει πρόσβαση σε δεδομένα ή υπηρεσίες του διακομιστή.

Όλες οι υπηρεσίες που προσφέρει το ACSI αιτούνται από εφαρμογές (applications) και απαντώνται από διακομιστές (servers). Για να ζητηθεί λοιπόν μια υπηρεσία από έναν διακομιστή, η αντίστοιχη εφαρμογή πρέπει πρώτα να δημιουργήσει μια έγκυρη διμερή συνεργασία (TPAA) μαζί του. **Η διμερής συνεργασία διατηρεί την κατάσταση της συνεδρίας και παρέχει μια εικονική προβολή του διακομιστή στην εφαρμογή**. Μια τυπική αλληλεπίδραση μεταξύ μιας Εφαρμογής και ενός Διακομιστή είναι ως εξής: (α.) Η Εφαρμογή ζητά μια TCP σύνδεση με τον Διακομιστή, (β.) η Εφαρμογή συνδέεται στον Διακομιστή με την υπηρεσία *"Associate"* παρέχοντας τον σχετικό κωδικό σύνδεσης, και (γ.) όταν ο Διακομιστής εγκρίνει το αίτημα της Εφαρμογής δημιουργεί ένα TPPA αντικείμενο το οποίο φτιάχνει μια εικονική απεικόνιση των δύο. (δ.) Στην συνέχεια συντελείται μια συνεχείς επικοινωνία αποστολής αιτημάτων από την Εφαρμογή, επεξεργασίας τους και επιστροφή απαντήσεων από τον Διακομιστή. Για τον τερματισμό της συνεδρίας, (ε.) η Εφαρμογή καλεί την υπηρεσία *"Release",* (στ.) με τον Διακομιστή να τερματίζει το TPAA που δημιούργησε προηγουμένως. Κάποια παραδείγματα άλλων υπηρεσιών είναι *Λήψη καταλόγου Διακομιστή (GetServerDirectory), Λήψη δεδομένων λογικού κόμβου (GetAllDataValues), Εγγραφή Δεδομένων (SetDataValues), Αποστολή μηνύματος GOOSE (SendGOOSEMessage), Διαγραφή αρχείου (DeleteFile)* και πάρα πολλές ακόμη [31].



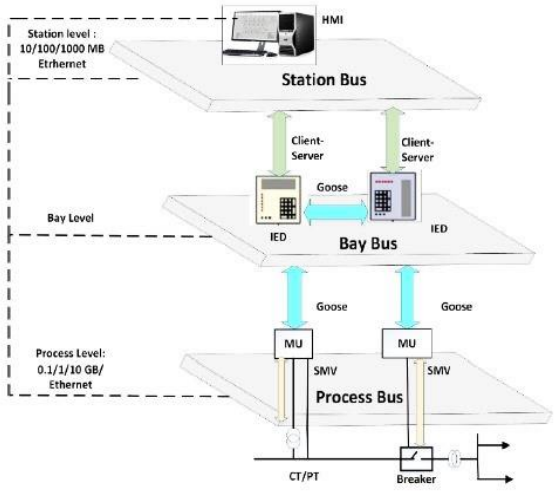
Η ανταλλαγή μηνυμάτων και αιτημάτων υπηρεσιών εγκαθιδρύουν στο ΣΑΥ ένα δίκτυο Εφαρμογής-Διακομιστή. Την ίδια στιγμή οι έξυπνες συσκευές επικοινωνούν μεταξύ τους δημιουργώντας λογικές συνδέσεις μεταξύ λογικών κόμβων - που βρίσκονται νοητά στο εσωτερικός τους. Εάν θεωρήσουμε ότι οι συσκευές αυτές αποτελούν διακομιστές πολλών εφαρμογών τότε μπορούμε αφαιρετικά να θεωρήσουμε ότι το δίκτυο έχει μια μορφή Εφαρμογής – Λογικών Κόμβων.

Σχήμα 2.23 – Δίκτυο Logical Node/Application

Σε επίπεδο τοπολογίας το δίκτυο ακολουθεί μια τυπική αρχιτεκτονική ενός συστήματος αυτοματισμού του υποσταθμού (βλ. Σχήμα 2.25). Το δίκτυο του υποσταθμού συνδέεται με το **εξωτερικό δίκτυο ευρείας περιοχής (WAN)** μέσω μιας ασφαλούς πύλης ώστε οι εξωτερικοί απομακρυσμένοι χειριστές και **τα κέντρα ελέγχου να μπορούν να χρησιμοποιήσουν τις εφαρμογές ACSI**. Έτσι μπορούν «συνομιλήσουν» και να ελέγξουν έξυπνες συσκευές στον υποσταθμό.

Εντός του υποσταθμού, υπάρχει ένας ή περισσότεροι δίαυλοι (υποσταθμού) όπου συνδέονται όλες οι IED - έξυπνες συσκευές. Ο δίαυλος αυτός θεωρείται ως ένα δίκτυο Ethernet με μεσαίο εύρος ζώνης, το οποίο μεταφέρει όλα τα αιτήματα και απαντήσεις του ACSI ή τα μηνύματα γεγονότων GSE. Ιεραρχικά χαμηλότερα στην τοπολογία υπάρχει ακόμη ένας δίαυλος επικοινωνίας, ο οποίος συνδέει τις έξυπνες συσκευές με τις παραδοσιακές συσκευές (μονάδες συγχώνευσης

κλπ.) στο επίπεδο ισχύος. Έτσι οι έξυπνες συσκευές παρακολουθούν τις διεργασίες που συντελούνται στο πεδίο λαμβάνοντας δεδομένα κατάστασης και μετρήσεων. Ο δίαυλος αυτός (διεργασιών) θεωρείται ως ένα δίκτυο Ethernet υψηλού εύρους ζώνης. Ένας υποσταθμός συνήθως έχει μόνο ένα δίαυλο υποσταθμού, αλλά πολλούς διαύλους παρακολούθησης διεργασιών πεδίου. Αυτή η αρχιτεκτονική επιτρέπει την αποτελεσματική ανταλλαγή δεδομένων και ελέγχου μεταξύ των διάφορων συσκευών και εφαρμογών εντός και εκτός του υποσταθμού. Στην διπλανή εικόνα δίνεται μια χαρακτηριστική απεικόνιση της τοπολογίας και των μηνυμάτων που ανταλλάσσονται σε ένα δίκτυο υποσταθμού.



Σχήμα 2.24 – Τοπολογία Επικοινωνίας Υποσταθμούς

Στο χαμηλότερο επίπεδο υπάρχουν κλασικές συσκευές πεδίου (όπως αισθητήρες, ενεργοποιητές, μετασχηματιστές τάσης ή ρεύματος κ.λπ.). Λόγω της ανάγκης για ψηφιοποίηση των βασικών τιμών που μετρούνται στην «πηγή», η μετάδοση των δειγματοληπτικών μετρήσεων στα ανώτερα στρώματα απαιτεί κάποιες **μετρητικές ηλεκτρονικές συσκευές** (merge units). Οι ηλεκτρονικοί μετρητές με την σειρά τους **συνδέονται στον δίαυλο του επιπέδου διεργασιών** όπου μεταφέρονται πλέον ψηφιοποιημένα δεδομένα, σχετικά με την τάση, το ρεύμα και την κατάσταση, και άλλων τιμών που σχετίζονται με την πρωτογενή διαδικασία του συστήματος ισχύος. Το IEC 61850 καθορίζει τη ανταλλαγή αυτών των δεδομένων μέσω δύο διαφορετικών ορισμών πρωτοκόλλου, δηλαδή του Μέρους 9.1 που καθορίζει μια σταθερή σύνδεση «σημείο-σε-σημείο» (point-to-point) που μεταφέρει ένα σταθερό σύνολο δεδομένων και του Μέρους 9.2 που καθορίζει ένα σύνολο δεδομένων που μπορεί να μεταδοθεί με πολλαπλά (multicast) μηνύματα.

Το επίπεδο Bay, αποτελεί μια ομαδοποίηση έξυπνων IED συσκευών σύμφωνα με κάποια κοινή λειτουργία ή εξοπλισμό ελέγχου (Πίνακες παροχής Ισχύος, Διακόπτες Ισχύος, κλπ.). Εκεί συντελούνται πρωτοβάθμιες λειτουργίες ελέγχου και παρακολούθησης για έναν δίαυλο διεργασιών από διάφορες έξυπνες συσκευές όπως μια μονάδα ελέγχου - bay (BCU). Ένας ελεγκτής BCU ουσιαστικά είναι μια κοινή συσκευή που είναι υπεύθυνη για την παρακολούθηση της κατάστασης των συσκευών, την εκτέλεση εντολών για τον έλεγχο της λειτουργίας τους και την επικοινωνία με άλλες BCU και το επίπεδο διεργασίας για την ανταλλαγή πληροφοριών. Η δικτυακή επικοινωνία χρησιμοποιεί το Ethernet σε επίπεδο σύνδεσης των BCU και άλλων συσκευών εντός του υποσταθμού.

Οι έξυπνες συσκευές συνδέονται ταυτόχρονα με **Επίπεδο Υποσταθμού**, όπου συντελούνται δραστηριότητες απομακρυσμένου ελέγχου και παρακολούθησης της απόδοσης του υποσταθμού αλλά και της σύνδεσής του με το σύστημα μεταφοράς ενέργειας. Ουσιαστικά ελέγχει ολόκληρο τον υποσταθμό και αποτελείται από εξοπλισμό ελέγχου και εποπτείας για την ανταλλαγή πληροφοριών μεταξύ των επιμέρους συσκευών στο επίπεδο της διαχείρισης. Ο εξοπλισμός αυτός περιλαμβάνει υπολογιστές, δρομολογητές δικτύου, προγραμματιζόμενους λογικούς ελεγκτές (PLCs) ακόμη και πύλες για διασύνδεση απομακρυσμένων συστημάτων SCADA ή άλλων υποσταθμών.

2.5.4. Σημαντικά οφέλη και προκλήσεις της επικοινωνίας IEC 61850

Στα παλιά σειριακά πρωτόκολλα επικοινωνίας περιορίζονταν ο αριθμός των bytes που χρησιμοποιούνταν από το πρωτόκολλο λόγω των περιορισμένων εύρους ζώνης που υπήρχαν στη διαθέσιμη σειριακή τεχνολογία πριν από 10-15 χρόνια. Ακόμη και με την μετέπειτα ενσωμάτωσή τους σε λογικές Ethernet μέσω TCP/IP, εξακολουθούσαν να σχεδιάζονται για την ελαχιστοποίηση των bytes που μεταδίδονται στο καλώδιο σύνδεσης και δεν εκμεταλλεύονταν την μεγάλη αύξηση στο εύρος ζώνης που προσφέρουν οι σύγχρονες τεχνολογίες δικτύωσης. Αντιθέτως, το IEC 61850 σχεδιάστηκε από το μηδέν για να λειτουργεί σε σύγχρονες τεχνολογίες δικτύωσης παρέχοντας μοναδικές υπηρεσίες και υψηλή λειτουργικότητα. Το πρότυπο επιτρέπει θεμελιώδεις βελτιώσεις στη διαδικασία αυτοματοποίησης του υποσταθμού συγκριτικά με τα παραδοσιακά πρωτόκολλα. Παρακάτω μελετάμε αυτά τα πλεονεκτήματα.

1. **Ευκολία Χρήσης:** Το εικονικό μοντέλο (ACSI) σε επίπεδο εφαρμογής καθορίζει δεδομένα, υπηρεσίες, συμπεριφορές συσκευών και γενικά τον τρόπο μετάδοσης μηνυμάτων στο δίκτυο. Κάθε στοιχείο έχει ένα - σαφές και αντιπροσωπευτικό για τα δεδομένα του – όνομα αντί για έναν «ξερό» αριθμό καταχωρητή. Τα αντικείμενα δεδομένων προσδιορίζονται από τυποποιημένα ονόματα που «φωτογραφίζουν» συγκεκριμένα μεγέθη του πραγματικού ηλεκτρικού συστήματος. Επιπλέον, οι εφαρμογές δεν χρειάζεται πλέον να ρυθμιστούν χειροκίνητα για κάθε σημείο που θέλουν να αποκτήσουν πρόσβαση, καθώς μπορούν να ανακτήσουν τη λίστα δεδομένων απευθείας από τη συσκευή ή να την εισαγάγουν μέσω SCL. Η γλώσσα SCL (Substation Configuration Language) επιτρέπει τον ακριβή καθορισμό μιας συσκευής και του ρόλου της στο ηλεκτρικό σύστημα χρησιμοποιώντας κοινότυπα αρχεία XML. Όλα τα παραπάνω διαμορφώνουν μια εφαρμογή επικοινωνίας πολύ προσιτή για τον χρήστη.
2. **Χαμηλό κόστος υλοποίησης:** Οι συσκευές ανταλλάσσουν γρήγορα δεδομένα χρησιμοποιώντας τα GOOSE μέσω του δικτύου LAN του υποσταθμού χωρίς την ανάγκη να εγκατασταθούν ξεχωριστά καλώδια για κάθε ρελέ. Αυτό μειώνει σημαντικά το κόστος καλωδίωσης, εκμεταλλευόμενο πλήρως την χωρητικότητα του δικτύου LAN του υποσταθμού για αυτά τα σήματα. Επίσης ελαχιστοποιεί το κόστος κατασκευής μειώνοντας την ανάγκη για σκάψιμο, σωληνώσεις, κανάλια κ.λπ.
3. **Διαλειτουργικότητα και Νέες Δυνατότητες:** Η προσθήκη συσκευών και εφαρμογών σε ένα υπάρχον σύστημα IEC 61850 μπορεί να γίνει με ελάχιστη επίπτωση. Οι καινούργιες επεκτάσεις μπορούν εύκολα να προστεθούν στο υποσταθμό χωρίς να χρειάζεται διαμόρφωση των συσκευών για την απόκτηση που προηγουμένως δεν ήταν προσβάσιμα. Επιπλέων, οι προηγμένες υπηρεσίες του IEC 61850 επιτρέπουν νέες λειτουργίες που δεν ήταν δυνατές με τα πρωτόκολλα προηγούμενης γενιάς, όπως επεκτάσεις προστασίας ευρείας περιοχής.
4. **Χρόνος μετάδοσης:** Όπως αναλύθηκε το πρότυπο ασχολήθηκε με τους χρόνους μετάδοσης δεδομένων και σχεδίασε μια επικοινωνία που εκμεταλλεύεται αποδοτικά το εύρος ζώνης που επιτρέπει η αρχιτεκτονική του δικτύου και οι δίαυλοι των δύο επιπέδων. Παρέχει ευρεία γκάμα μηνυμάτων διαφορετικών ταχυτήτων που ανταποκρίνονται στις εκάστοτε χρονικές απαιτήσεις του υποσταθμού
5. **Υπηρεσίες Καταγραφής/Αναφοράς:** Το πρότυπο IEC 61850 παρέχει ένα αποτελεσματικό μηχανισμό που ονομάζεται "αναφορές" (reporting) για τις εφαρμογές προκειμένου να παρακολουθούν τις αλλαγές στα αντικείμενα του συστήματος στα οποία έχουν εγγραφεί. Η καταγραφή (logging) είναι ένας επιπλέον μηχανισμός για την καταγραφή των γεγονότων όπου τα αρχεία

καταγραφής (logs) αποθηκεύονται στον αντίστοιχο server. Αυτές οι δύο υπηρεσίες είναι πολύ σημαντικές για την ανάπτυξη μηχανισμών ασφαλείας καθώς κάθε λογική συσκευή αποθηκεύει και αναφέρει τις ενέργειες που εκτελεί βοηθώντας την ανίχνευση πιθανής ύποπτης δραστηριότητας.

6. **Ασφάλεια:** Παρέχει υπηρεσίες αυθεντικοποίησης δεδομένων, χρησιμοποιώντας κρυπτογραφικές τεχνικές, όπως ψηφιακές υπογραφές, κρυπτογράφηση και διαχείριση κλειδιών ασφαλείας. Αυτό αυξάνει σε μεγάλο βαθμό την ακεραιότητα και εμπιστευτικότητα του συστήματος συγκριτικά με την χρήση άλλων πρωτοκόλλων επικοινωνίας.

Είναι γεγονός ότι το πρότυπο διακρίνεται για την προηγμένη λειτουργία του και στην αξιοποίηση των δυνατοτήτων του δικτύου. Ωστόσο η επικοινωνία IEC 61850 δεν σημαίνει ότι δεν έχει αδυναμίες.

1. **Πολυπλοκότητα**: Οι πολλές λειτουργίες και τα επίπεδα ασφάλειας που διαθέτει απαιτούν προσεκτική παραμετροποίηση και διαχείριση των δεδομένων. Αυτό αυξάνει σε μεγάλο βαθμό τον κίνδυνο των σφαλμάτων στην διαμόρφωση με αποτέλεσμα να υπάρχουν τρωτά σημεία και από την σκοπιά της κυβερνοασφάλειας.
2. **Μείωση απόδοσης και περιορισμοί**: Οι πρόσθετοι μηχανισμοί ασφαλείας προσθέτουν επιπλέον φορτίο στο δίκτυο (overhead). Δεδομένου ότι, τα κανάλια που χρησιμοποιούνται για την επικοινωνία έχουν περιορισμούς χωρητικότητας μια πιθανή συμφόρηση στο δίκτυο μπορεί να καταλήξει σε απώλεια πακέτων ή μεγάλες καθυστερήσεις. Επομένως, για ένα σύστημα αυτοματισμού που διαχειρίζεται μεγάλο όγκο δεδομένων και έχει πολύπλοκη δικτύωση επικοινωνίας η απόδοση του μειώνεται σημαντικά.
3. **Ανοιχτή επικοινωνία**: Παρά την παρουσία μηχανισμών αυθεντικοποίησης σε ορισμένους τύπους μηνυμάτων, πολλά σημεία του συστήματος συμμετέχουν σε ανοιχτή επικοινωνία. Αυτό διατηρεί τον κίνδυνο ανεπιθύμητης πρόσβασης ή ανατροπής του συστήματος.
4. **Απομακρυσμένη Επικοινωνία**: Με την διεύρυνση της επικοινωνίας IEC 61850 από τους υποσταθμούς σε εξωτερικά συστήματα, η έννοια της ασφάλειας αποκτά ακόμη μεγαλύτερη σημασία. Η χρήση δικτύων WAN ή Ίντερνετ για την μεταφορά ευαίσθητων πληροφοριών (πχ. συναλλαγές στην αγορά ηλεκτρικής ενέργειας) θέτει το σύστημα ενέργειας έκθετο απέναντι σε κυβερνοεπιθέσεις.

Απαιτείται λοιπόν μια ολοκληρωμένη ανανέωση της κυβερνοασφάλειας βασισμένη στους νέους κινδύνους της περιόδου. Οι απαιτήσεις ασφαλείας για διάφορα μηνύματα IEC 61850 καθορίζονται από το πρότυπο **IEC 62351** και θα μελετηθούν σε επόμενο κεφάλαιο.

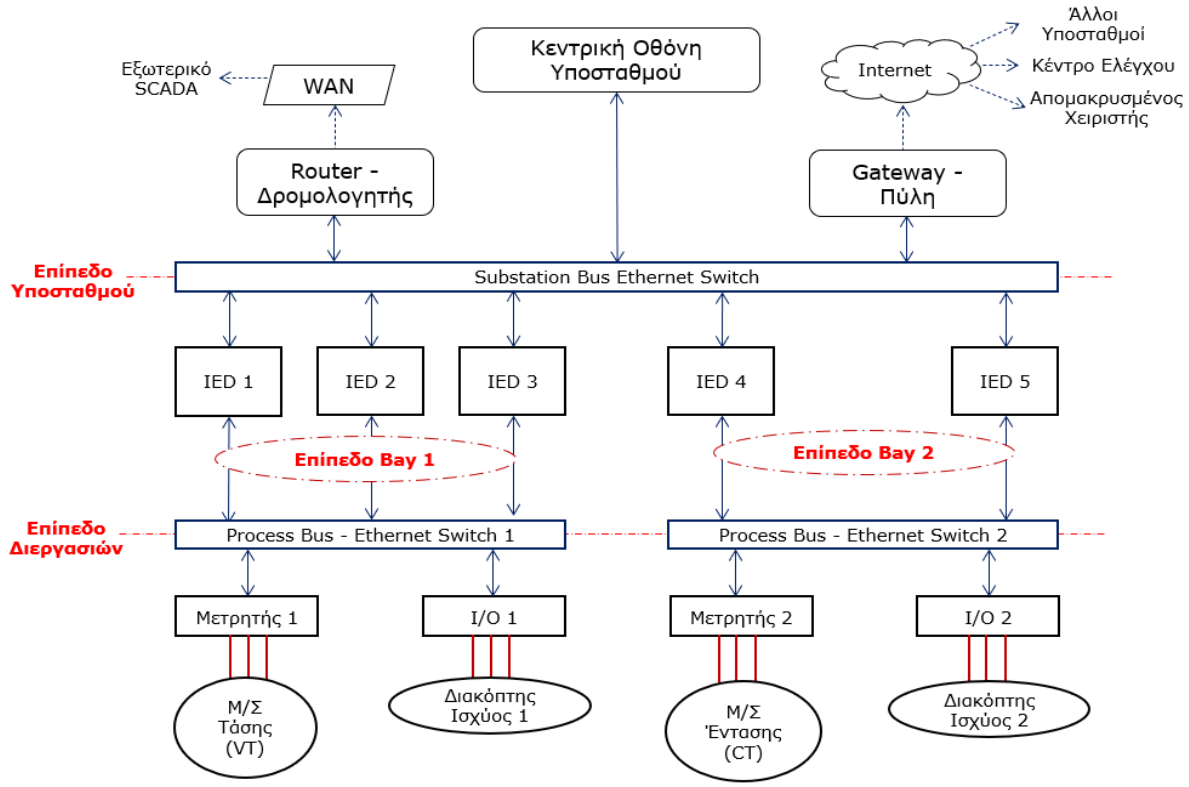
2.5.5. Το IEC 61850 στους Υποσταθμούς Ηλεκτρικής Ενέργειας

Η μεγάλη αναγνωσιμότητά που έχει το IEC 61850 εμφανώς οφείλεται στις προηγμένες δυνατότητες που προσφέρει για την διαμόρφωση έξυπνων δικτύων επικοινωνίας διαφόρων υποδομών. Σήμερα, το πρότυπο αποκτά ολοένα και περισσότερους χρήστες ανά τον κόσμο. Κατά την έρευνα που διενήργησε το Ευρωπαϊκό Δίκτυο Επιχειρησιακών Υπευθύνων Μετάδοσης Ηλεκτρικής Ενέργειας (ENTSO-E) διαπιστώθηκε ότι το IEC 61850 ήταν το πιο διαδεδομένο πρότυπο επικοινωνίας για την αυτοματοποίηση υποσταθμών.

Η επικοινωνία IEC 61850 γενικότερα χρησιμοποιείται στα συστήματα ηλεκτρικής ενέργειας που απαιτούν σύνδεση σε δίκτυα ευρείας ζώνης. Για

παράδειγμα σε ένα σύστημα παραγωγής ηλεκτρικής ενέργειας, ο αυτόματος έλεγχος της παραγωγής θα χρησιμοποιήσει το πρότυπο για λειτουργίες ανάκτησης δεδομένων από το πεδίο παραγωγής. Το ίδιο ισχύει και για συστήματα μετάδοσης και διανομής μέσω της παρακολούθησης που κάνουν οι υποσταθμοί. Έτσι ο υποσταθμός λαμβάνει μετρήσεις και ειδοποιήσεις γεγονότων σε όλες τις διαδικασίες ισχύος και μοιράζεται τις πληροφορίες με απομακρυσμένα εποπτικά συστήματα ή έναν κεντρικό σταθμό ελέγχου.

Σχήμα 2.25– Αρχιτεκτονική ΣΑΥ και συσκευές



Ειδικότερα στους υποσταθμούς το πρότυπο χρησιμοποιείται για την επικοινωνία έξυπνου εξοπλισμού που συμμετέχει στο σύστημα αυτοματισμού το οποίο ακολουθεί την παραπάνω αρχιτεκτονική. Συγκεκριμένα, το **Σύστημα Αυτοματισμού Υποσταθμού (ΣΑΥ ή SAS) είναι ένα είδος συστήματος SCADA**, **ειδικά σχεδιασμένο για την απομακρυσμένο έλεγχο ηλεκτρικών υποσταθμών**. Ενώ οι εφαρμογές SCADA είναι συστήματα αυτοματισμού γενικού σκοπού που χρησιμοποιούνται για την παρακολούθηση διαφόρων βιομηχανικών διαδικασιών, το ΣΑΥ είναι περισσότερο εξειδικευμένο σύστημα που προσαρμόζεται στις μοναδικές ανάγκες της αυτοματοποίησης των υποσταθμών. Για την κατανόηση του ΣΑΥ παρακάτω σημειώνονται κάποιες **κύριες διαφορές** μεταξύ των δύο:

- **Σκοπός**: Το SCADA χρησιμοποιείται για την παρακολούθηση και έλεγχο ολόκληρων βιομηχανικών διαδικασιών, ενώ το ΣΑΥ είναι ειδικά σχεδιασμένο για ηλεκτρικούς υποσταθμούς.
- **Έλεγχος**: Το ΣΑΥ συνήθως παρέχει πιο λεπτομερή έλεγχο πάνω σε κάθε μεμονωμένη συσκευή του υποσταθμού, όπως διακόπτες και ρελέ, ενώ το SCADA επικεντρώνεται περισσότερο στην συνολική εποπτεία και τη βελτιστοποίηση του συστήματος.

- **Πρωτόκολλα επικοινωνίας**: Στα ΣΑΥ χρησιμοποιούνται κυρίως εξειδικευμένα πρωτόκολλα επικοινωνίας (IEC 61850), ενώ το SCADA χρησιμοποιεί πιο γενικού σκοπού βιομηχανικά πρωτόκολλα, όπως το Modbus, το DNP3 ή του IEC/104.
- **Εξοπλισμός**: Στους υποσταθμούς χρησιμοποιούνται πιο εξειδικευμένα υλικά, όπως έξυπνες συσκευές (μετρητές/αναλυτές ή έξυπνοι αισθητήρες), ικανές να λειτουργήσουν σε υψηλές ταχύτητες και γενικότερα βελτιστοποιημένες στην επικοινωνία πραγματικού χρόνου και στον έλεγχο. Ο εξοπλισμός των SCADA μπορεί να είναι πιο γενικού τύπου και περιλαμβάνει οπωσδήποτε διεπαφές ανθρώπου-μηχανής ή κεντρικό υπολογιστή.

Σε επίπεδο εξοπλισμού λοιπόν, τα **ΣΑΥ έχουν ως δομικό στοιχείο μια συλλογή έξυπνων ηλεκτρονικών συσκευών (IEDs)**, εφαρμογών ACSI και συστημάτων επικοινωνίας που συνεργάζονται για την απομακρυσμένη παρακολούθηση και τον έλεγχο του εξοπλισμού ηλεκτρικών υποσταθμών. Ο όρος «έξυπνη ηλεκτρονική συσκευή» αναφέρεται σε ελεγκτές με μικροεπεξεργαστή σε ένα συστήματος ισχύος, οι οποίοι είναι ικανοί να λαμβάνουν ή να αποστέλλουν δεδομένα από ή προς εξωτερική πηγή. Μια IED συσκευή μπορεί να είναι εξοπλισμένη με έναν ή περισσότερους μικροεπεξεργαστές, μνήμες, πιθανώς ένα σκληρό δίσκο και μια συλλογή διεπαφών επικοινωνίας (π.χ. θύρες USB, σειριακές θύρες, διεπαφές Ethernet). Δηλαδή πρόκειται για κανονικούς υπολογιστές με την διαφορά ότι παρέχουν μια δική τους, ειδική ψηφιακή λογική. Συχνά παραδείγματα IED συσκευών είναι έξυπνα ρελέ, ρυθμιστές τάσης ή ελεγκτές διακοπτών ισχύος.

2.6. Πρωτόκολλο επικοινωνίας κέντρων ελέγχου ICCP

Ορισμός: Το ICCP (Inter-Control Center Communications) είναι ένα πρότυπο πρωτόκολλο που χρησιμοποιείται για την ανταλλαγή δεδομένων πραγματικού χρόνου και ιστορικών πληροφοριών του ηλεκτρικού συστήματος, μεταξύ των κέντρων ελέγχου στη βιομηχανία ηλεκτρικής ενέργειας. Ο βασικός σκοπός ανάπτυξής του ήταν η ασφαλής και αξιόπιστη ανταλλαγή πληροφοριών που σχετίζονται με τη διαχείριση ενέργειας, τον έλεγχο του ηλεκτρικού συστήματος και τον συντονισμό μεταξύ διαφορετικών κέντρων ελέγχου. Το ICCP χρησιμοποιείται ευρέως στα συστήματα ηλεκτρικής ενέργειας για εφαρμογές SCADA και EMS, διότι καθιστά δυνατή την αλληλεπίδραση διαφορετικών συστημάτων ελέγχου και εφαρμογών ανάμεσα σε πολλούς οργανισμούς που εμπλέκονται στη λειτουργία του ηλεκτρικού συστήματος. Το πρωτόκολλο καθορίζεται από το 6^{ο} μέρους του προτύπου IEC 60870-6.

2.6.1. Γενικά στοιχεία επικοινωνίας προτύπου IEC 60870-6/TASE.2

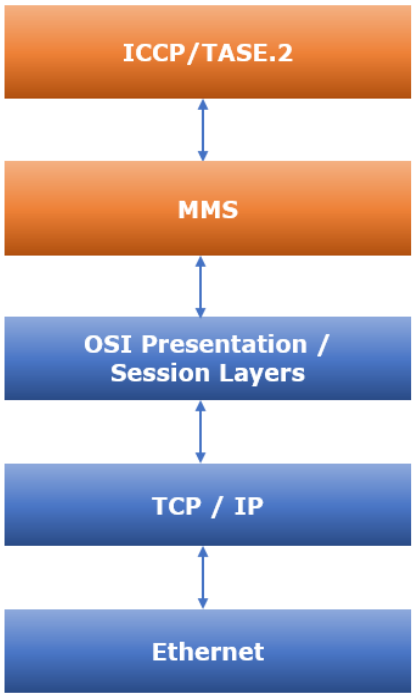
Ως συνέχεια του μέρους 5, το πρότυπο IEC 60870 ορίζει στο μέρος 6 μια δεύτερη προδιαγραφή επικοινωνίας στα συστήματα ηλεκτρικής ενέργειας. Συγκεκριμένα, τα συνοδευτικά του IEC 60870-6/TASE.2 καθορίζουν το πρωτόκολλο και τους κανόνες επικοινωνίας μεταξύ των κέντρων ελέγχου. Επιτρέπει στις δημόσιες υπηρεσίες ηλεκτρικής ενέργειας και στα κέντρα ελέγχου να ενσωματώνουν διάφορα στοιχεία σε ένα ενιαίο και αποδοτικό σύστημα διαχείρισης ενέργειας. Οι συνοδευτικοί παράγραφοι του IEC 60870-6 οι οποίες περιγράφουν την επικοινωνία στα κέντρα ελέγχου είναι οι παρακάτω και από αυτές αντλούμε πληροφορίες για την ανάλυση που γίνεται στην συνέχεια του κεφαλαίου.

- IEC 60870–6-503: TASE.2 - Υπηρεσίες και πρωτόκολλο
- IEC 60870–6–602: Προφίλ μεταφοράς TASE
- IEC 60870–6–702: Λειτουργικό προφίλ για την παροχή της υπηρεσίας εφαρμογής TASE.2 σε τερματικά συστήματα
- IEC 60870–6–802: TASE.2 Μοντέλα αντικειμένων

Από αυτές τις τέσσερις προδιαγραφές καθορίζονται η μορφή του πρωτόκολλου εφαρμογής ICCP και ένα γενικότερο προφίλ της TASE.2 επικοινωνίας. Το μοντέλο αντικειμένων και υπηρεσιών του TASE.2 ορίζεται στο επίπεδο εφαρμογής με το ICCP και χρησιμοποιεί πρόσθετα πρωτόκολλα της οικογένειας ISO στα χαμηλότερα επίπεδα της στοίβας. Στην εφαρμογή ICCP λοιπόν προσδιορίζονται μορφές των μηνυμάτων, τύποι δεδομένων και υπηρεσίες για την ανταλλαγή τους, καθώς και η αντιστοίχιση των μηνυμάτων σε διάφορα δίκτυα επικοινωνίας. Περισσότερες λεπτομέρειες σχετικά με τα παραπάνω αναλύονται στις επόμενες παραγράφους.

2.6.2. Μηνύματα και Αντικείμενα εφαρμογής ICCP

Το πρωτόκολλο εφαρμογής ICCP - και συνολικά επικοινωνίας TASE2. - **βασίζεται στην επικοινωνία ανταλλαγής MMS μηνυμάτων** βάσει ενός κοινού πλαισίου επικοινωνίας διαμορφωμένο για όλες τις ενεργειακές επιχειρήσεις, γνωστό ως Αρχιτεκτονική Επικοινωνίας Υπηρεσιών Δημοφιλούς Χρήσης (UCA). Όπως είδαμε και στην ενότητα του IEC 61850, το MMS είναι ειδικά σχεδιασμένο για τη μεταφορά δεδομένων διεργασίας σε πραγματικό χρόνο και εποπτείας μεταξύ λογικών κόμβων δικτύου. Ο κύριος στόχος του ήταν και είναι να καθορίσει ένα κοινό μηχανισμό επικοινωνίας για συσκευές και εφαρμογές υπολογιστών που θα πετυχαίνει υψηλό επίπεδο διαλειτουργικότητας. Το MMS έχει σχεδιαστεί ώστε να χρησιμοποιεί όλα τα επίπεδα του μοντέλου OSI, ως εκ τούτου το ICCP ακολουθεί αντίστοιχη στοίβα πρωτοκόλλων η οποία έχει την μορφή του σχήματος 2.26.



Σχήμα 2.26 – Πρωτόκολλα εφαρμογής κέντρου ελέγχου ICCP

Το MMS καθορίζει μια ποικιλία αντικειμένων που βρίσκονται σε πολλές τυπικές συσκευές και εφαρμογές που απαιτούν επικοινωνία πραγματικού χρόνου συνθέτοντας ένα **μοντέλο αντικειμένων, υπηρεσιών και συμπεριφοράς** που ονομάζεται Εικονική Συσκευή Κατασκευής ή **μοντέλο VMD**. Το μοντέλο VMD χρησιμοποιεί μια αντικειμενοστραφή προσέγγιση για να αναπαραστήσει διάφορες φυσικές βιομηχανικές συσκευές με γενικό τρόπο. Ουσιαστικά το VMD ορίζεται ως ένα σύνολο ταξινομημένων δεδομένων που αναπαριστούν τους πόρους της πραγματικής συσκευής και ένα σύνολο ταξινομημένων μεθόδων που αναπαριστούν τις υπηρεσίες του MMS που επεξεργάζονται αυτά τα δεδομένα.

Από την άλλη το TASE.2 προδιαγράφει μια αφηρημένη αντικειμενοστραφής μοντελοποίηση, η οποία ορίζει μια σειρά κλάσεων αντικειμένων. Κάθε αντικείμενο είναι μια παράδειγμα μιας κλάσης και αντιστοιχεί σε ένα αφηρημένο στοιχείο που εκδηλώνει συγκεκριμένα χαρακτηριστικά και μπορεί να επηρεαστεί από συγκεκριμένες υπηρεσίες και λειτουργίες του TASE.2. Το κέντρο ελέγχου μοντελοποιείται με έναν ή περισσότερους εικονικούς χειριστές (VCC) που αναπαριστούν τη συνολική συλλογή των πραγματικών αντικειμένων ως ένα εικονικό μοντέλο που μπορεί να παρέχει υπηρεσίες για ένα άλλο κέντρο ελέγχου.

Επιστρέφοντας, στα VMD μπορεί να θεωρηθεί ως ένα αντικείμενο στο οποίο υποτάσσονται όλα τα άλλα αντικείμενα MMS. Αποτελεί το τμήμα μιας εργασίας επεξεργασίας πληροφοριών που παρέχει ένα σύνολο πόρων και λειτουργικοτήτων που σχετίζονται με μια πραγματική συσκευή. Με την αντιστοίχιση ενός TASE.2 VCC σε ένα MMS VMD, το TASE.2 VCC εκτελεί την ίδια λειτουργία για ένα κέντρο ελέγχου που το MMS VMD κάνει για μια πραγματική συσκευή.

Όλες οι υπηρεσίες ICCP παρέχονται μέσω αντικειμένων που μπορούν να θεωρηθούν ως κλασικά αντικείμενα με χαρακτηριστικά δεδομένων (data attributes) και μεθόδους, όπως ορίζονται στην γενική μεθοδολογία σχεδιασμού αντικειμενοστραφών συστημάτων και προδιαγράφονται επακριβώς στο πρότυπο TASE2. Τα αντίστοιχα αντικείμενα MMS με τις υπηρεσίες τους αναφέρονται στα πρότυπα MMS. Εμείς θα επικεντρωθούμε στα αντικείμενα και λειτουργίες του ICCP πρωτοκόλλου όπως αυτά καθορίζονται από το πρότυπο. Σε ένα από τα μέρη του προτύπου προσδιορίζονται επακριβώς σύνολα υποστηριζόμενων λειτουργιών και δυνατοτήτων, στα οποία θα πρέπει να συμμορφώνονται τα διασυνδεδεμένα συστήματα και συσκευές. Αυτές οι προδιαγραφές είναι ιδιαίτερα σημαντικές για τις ICCP επικοινωνίες, οι οποίες συνδέουν μεταξύ τους διαφορετικά συστήματα, καθώς έτσι διασφαλίζεται η διαλειτουργικότητα του συστήματος επικοινωνίας. Τα κύρια **μπλοκ συμμόρφωσης** είναι εννέα και περιγράφονται στην συνέχεια:

- **Μπλοκ 1 – Περιοδικά Δεδομένα Συστήματος**: Το ICCP καθορίζει αρχικά τα αντικείμενα και σύνολα δεδομένων που χρησιμοποιούνται στην εφαρμογή και μεταδίδονται περιοδικά μεταξύ των διασυνδεδεμένων κέντρων ελέγχου. Αυτά τα δεδομένα περιλαμβάνουν για παράδειγμα: αντικείμενα συσχετισμού (association objects) για την έναρξη και λήξη μιας συνεδρίας, σημεία δεδομένων (data points), σύνολα δεδομένων (data sets), σύνολα μεταφοράς (transfer sets) κ.ά.

- **Μπλοκ 2 - Εκτεταμένη Παρακολούθηση Συνόλων Δεδομένων:** Αφορά την μη περιοδική μεταφορά δεδομένων, όπως η ανίχνευση αλλαγών στο σύστημα. Δηλαδή υπάρχει η δυνατότητα δημιουργίας αναφορών κατάστασης για συγκεκριμένα δεδομένα μόνο σε περιπτώσεις εξαίρεσης (RBE). Τις συνθήκες αυτές - για το σύνολο δεδομένων προς παρακολούθηση - ορίζουν οι χρήστες θέτοντας τα επιτρεπτά όρια κατάστασης στο GUI-γραφικό περιβάλλον της ICCP εφαρμογής.

- **Μπλοκ 3 - Μεταφορά Δεδομένων**: Είναι ένας μηχανισμός πιο αποδοτικής μεταφοράς των παραπάνω δεδομένων. Δηλαδή το ICCP παρέχει τη δυνατότητα μεταφοράς των δεδομένων του Μπλοκ 1 και Μπλοκ 2 ως σύνολα αντί ενός για κάθε φορά. Αυτό μπορεί να μειώσει το εύρος ζώνης που απαιτείται για την ανταλλαγή δεδομένων μεταξύ των ενεργειακών υπηρεσιών.

- **Μπλοκ 4 - Μήνυμα Πληροφοριών:** Πρόκειται για μηχανισμό μεταφοράς κειμένου ή δυαδικού μηνύματος. Το GUI της εφαρμογής δίνει την δυνατότητα στον χρήστη να ανταλλάσσει απλά κείμενα με ένα άλλο κέντρο ελέγχου ή σε περισσότερα πολλαπλές εκπομπές (broadcast) τέτοιων μνημάτων. Το λογισμικό

ICCP εμφανίζει τα μηνύματα που λαμβάνονται από τα κέντρα ελέγχου με βάση την προτεραιότητά τους και δύναται να εκπέμπει σημαντικές ειδοποιήσεις (κειμένου) στον χειριστή.

- **Μπλοκ 5 - Έλεγχος Συσκευής:** Το TASE.2 αναπαριστά την πραγματική συσκευή με ένα αντικείμενο ελέγχου της συσκευής όπως ορίζεται στο MMS πρωτόκολλο. Υπάρχουν δύο τύποι αντικειμένων ελέγχου συσκευών: Άμεσος Έλεγχος (Direct Control) και Επιλογή πριν την Εκτέλεση (Select-Before-Operate, SBO). Τα αντικείμενα συσκευών άμεσου ελέγχου μπορούν να λειτουργούν από τον client ανά πάσα στιγμή ενώ τα SBO απαιτούν να επιλεγεί η συσκευή από τον TASE.2-πελάτη πριν από την απόπειρα ελέγχου της συσκευής.

- **Μπλοκ 6 - Έλεγχος Προγράμματος:** Αυτό το μπλοκ επιτρέπει σε έναν πελάτη ICCP να ελέγχει απομακρυσμένα τα προγράμματα που εκτελούνται σε ένα διακομιστή ICCP. Το αντικείμενο προγράμματος αναπαρίσταται ως μια κλήση προγράμματος όπως ορίζεται στο MMS πρωτόκολλο.

- **Μπλοκ 7 - Αναφορά Συμβάντων**: Είναι ένας μηχανισμός αναφοράς συμβάντων συστήματος. Με την δημιουργία κάποιου νέου γεγονότος οι ICCP-πελάτες μπορούν να «εγγραφούν» στο νέο γεγονός ώστε να λαμβάνουν ειδοποιήσεις από το σύστημα ICCP.

- **Μπλοκ 8 - Πρόσθετο Αντικείμενο Χρήστη:** Αυτό το μπλοκ παρέχει τη δυνατότητα ανταλλαγής πληροφοριών προγραμματισμού, λογιστικής και άλλων γενικών πληροφοριών του εργοστασίου ενέργειας μεταξύ των κέντρων ελέγχου.

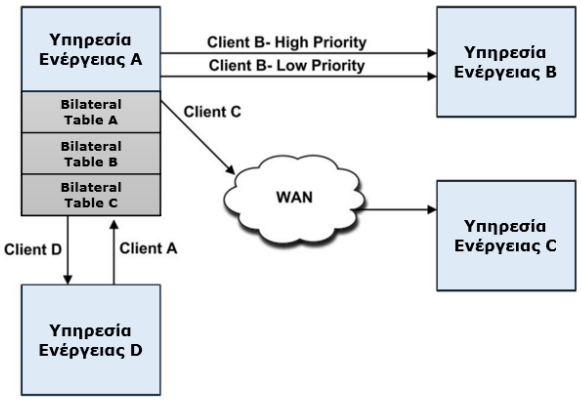
- **Μπλοκ 9 - Δεδομένα Χρονοσειράς:** Η μεταφορά δεδομένων χρονοσειράς επιτρέπει σε έναν πελάτη να ζητήσει αναφορές ιστορικών δεδομένων από έναν διακομιστή για ένα καθορισμένο χρονικό διάστημα. Αυτές οι πληροφορίες είναι πολύ χρήσιμες για τη λήψη αποφάσεων και την ανάλυση σφαλμάτων που έχουν συμβεί σε μια συγκεκριμένη χρονική περίοδο.

2.6.3. Αρχή επικοινωνίας και αρχιτεκτονική δικτύου ICCP/TASE.2

Το ICCP βασίζεται στις αρχές επικοινωνίας πελάτη/διακομιστή που σημαίνει ότι όλες οι μεταφορές δεδομένων ξεκινούν με ένα αίτημα από ένα κέντρο ελέγχου προς ένα άλλο κέντρο ελέγχου που είναι ο διαχειριστής των δεδομένων. Ένα κέντρο ελέγχου μπορεί να είναι ταυτόχρονα πελάτης και εξυπηρετητής. Οι τύποι αιτημάτων μπορεί να είναι μονά αιτήματα, αιτήματα για περιοδικές μεταφορές ή αιτήματα μόνο για την ανανέωση των αλλαγών (βλ. μπλοκ συμμόρφωσης ICCP). Ο διακομιστής ελέγχει κάθε αίτημα του πελάτη για να βεβαιωθεί ότι ο συγκεκριμένος πελάτης έχει δικαιώματα πρόσβασης στα δεδομένα ή στις δυνατότητες που ζητήθηκαν. **Ο έλεγχος πρόσβασης παρέχεται μέσω Πινάκων Διμερών Συσχετίσεων (Bilateral Tables)** που καθορίζονται για κάθε συνεργασία πελάτη/διακομιστή και περιέχουν τις παρακάτω πληροφορίες:

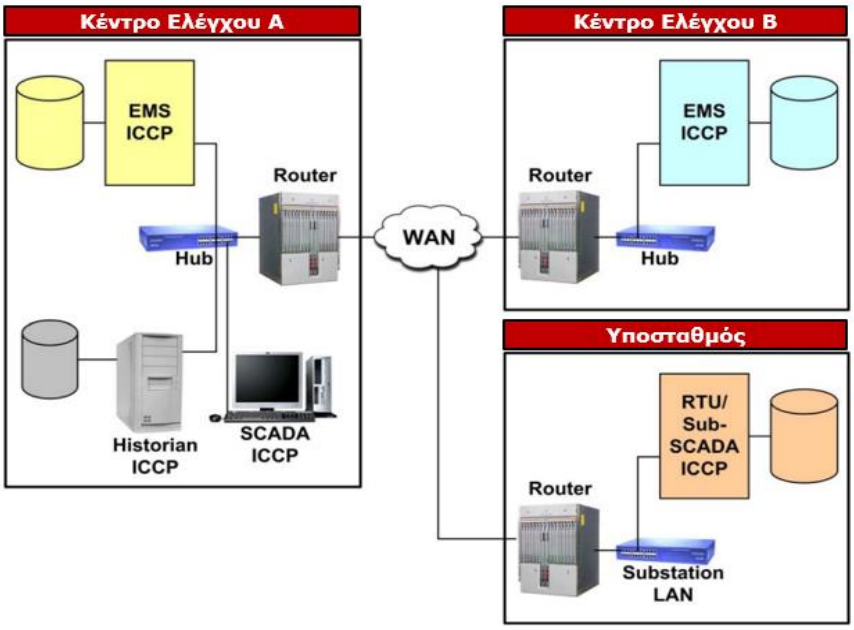
- **Σύνολα δεδομένων:** Τα σύνολα τιμών δεδομένων που μπορούν να μεταφερθούν ως μια μονάδα.
- **Σύνολο μεταφοράς:** Ένα υποσύνολο ενός συνόλου δεδομένων που καθορίζει τη συχνότητα και την κατεύθυνση της μεταφοράς δεδομένων.
- **Λίστα ελέγχου πρόσβασης:** Μια λίστα χρηστών ή εφαρμογών που έχουν άδεια πρόσβασης σε ένα σύνολο δεδομένων ή ένα σύνολο μεταφοράς.
- **Παράμετροι ασφαλείας:** Παράμετροι που καθορίζουν τις μεθόδους πιστοποίησης και κρυπτογράφησης για τη μεταφορά δεδομένων.

Οι λογικές συνδέσεις ή «συσχετίσεις» μεταξύ των κέντρων ελέγχου που επικοινωνούν είναι εντελώς γενικές. Ένας πελάτης μπορεί να δημιουργήσει συσχετίσεις με περισσότερους από έναν διακομιστές αλλά επίσης ένας πελάτης μπορεί να δημιουργήσει περισσότερες από μία συσχετίσεις με τον ίδιο διακομιστή. Οι διαφορετικές συσχετίσεις με τον ίδιο διακομιστή γίνεται σε πολλά επίπεδα και είδη υπηρεσιών, έτσι ώστε τα δεδομένα σε πραγματικό χρόνο υψηλής προτεραιότητας (high-priority) να μην καθυστερούν από μεταφορές δεδομένων χαμηλότερης προτεραιότητας (low-priority). Παρακάτω δίνεται σχετικό διάγραμμα συσχετίσεων ενός ICCP-πελάτη.



Σχήμα 2.27 – Συσχετίσεις ICCP πελάτη

Το σύστημα ICCP περιλαμβάνει οποιεσδήποτε φυσικές διεπαφές (physical interfaces), υπηρεσίες μεταφοράς και δικτύου που ταιριάζουν στο OSI μοντέλο, με το TCP/IP μέσω Ethernet (802.3) να είναι το πιο συνηθισμένο. **Η κοινή αρχιτεκτονική υλοποίησης του ICCP** χρησιμοποιεί λοιπόν συνδέσεις Ethernet και μπορεί να δημιουργήσει μια ενιαία σύνδεση σημείου-προς-σημείο, μεταξύ δύο κέντρων ελέγχου. Ωστόσο, η πιο γενική περίπτωση διαμόρφωσης του δικτύου είναι για πολλά κέντρα ελέγχου δημιουργώντας ένα δρομολογημένο **δίκτυο ευρείας περιοχής (WAN)**.



Σχήμα 2.28 – Αρχιτεκτονική Δικτύου ICCP

Όπως φαίνεται και στο παραπάνω διάγραμμα διαφορετικά συστήματα και τοπικά δίκτυα μπορούν μέσω ICCP πρωτοκόλλου και χρήσης δρομολογητών να δημιουργήσουν ένα κοινό δίκτυο ευρείας περιοχής. Στο από WAN δίκτυο, οι κεντρικοί εξοπλισμοί ελέγχου του κάθε συστήματος (Κεντρικοί Υπολογιστές Κέντρου Ελέγχου, ICCP Servers και Ιστορικό, SCADA διαφόρων επιπέδων, κλπ.) ανταλλάσσουν μεταξύ τους κρίσιμες πληροφορίες για τον συνολικό έλεγχο και συντονισμό.

2.6.4. Σημαντικές δυνατότητες και ευάλωτα σημεία του ICCP

Συμπερασματικά από τα παραπάνω, το ICCP καθιστά ένα πρωτόκολλο εφαρμογής ειδικά διαμορφωμένο να εξυπηρετεί λειτουργίες και ανάγκες συστημάτων στις ανώτερες βαθμίδες του βιομηχανικού ελέγχου. Κατά την ανάπτυξή του, η ικανοποίηση ζητημάτων όπως η διαχείριση και η διάθεση μεγάλου όγκου δεδομένων, η διαλειτουργικότητα με άλλα πρωτόκολλα επικοινωνίας σε συστήματα χαμηλότερου επιπέδου (ιεραρχικά) ή η ευκολία χρήσης της εφαρμογής του από το ανθρώπινο δυναμικό ήταν σε βασική προτεραιότητα. Συνεπώς δεν έχει μεγάλη ουσία η σύγκρισή του με τα υπόλοιπα πρωτόκολλα που μελετήθηκαν καθώς οι ίδιες οι λειτουργίες του αποτελούν και τα πλεονεκτήματά του για το πεδίο χρήσης του πρωτοκόλλου. Παρακάτω αναφέρονται κάποιες πολύ σημαντικές.

1. **Αντικειμενοστράφεια**: Τα δεδομένα μοντελοποιούνται με τη μορφή αντικειμένων, συγκεντρώνοντας όλα τα σχετικά δεδομένα σε ένα μόνο αντικείμενο. Αυτό καθιστά το πρωτόκολλο εύκολο στην διαμόρφωσή και την βελτίωσή του από τους προγραμματιστές.
2. **Πραγματικός Χρόνος:** Ο σχεδιασμός του στοχεύει στην ανταλλαγή δεδομένων σε πραγματικό χρόνο, και προσφέρει ταχύτερη λήψη αποφάσεων και απόκριση στις μεταβαλλόμενες συνθήκες στο σύστημα ισχύος. Επιτρέπει αυτόματη περιοδική ή εκδηλωτική λήψη δεδομένων (event driven) αλλά και την απόρριψη παλαιών δεδομένων βάσει ενός χρονικού διαστήματος ζωής που τους επιτρέπεται. Επίσης επιτρέπει την άμεση αποστολή δεδομένων που άλλαξαν κατάσταση βελτιώνοντας την κίνηση στο δίκτυο.
3. **Έλεγχος Συμφόρησης:** Παρέχονται πρόσθετοι μηχανισμοί ανίχνευσης της κυκλοφοριακής συμφόρησης και λαμβάνονται αυτόματα διορθωτικά μέτρα για την βελτίωσης της κυκλοφορίας στο δίκτυο.
4. **Προτεραιοποίηση Μηνυμάτων**: Καθορίζονται τέσσερα επίπεδα προτεραιότητας στο επίπεδο μεταφοράς και δικτύου για τον έλεγχο, την αναφορά εξαιρέσεων, την περιοδική αναφορά και τη μεταφορά αρχείων.
5. **Τυποποίηση**: Το ICCP ακολουθεί τα διεθνή πρότυπα, διασφαλίζοντας ότι οι συσκευές και τα συστήματα από διαφορετικούς προμηθευτές μπορούν να επικοινωνούν μεταξύ τους.
6. **Διαλειτουργικότητα**: Μια υλοποίηση δεν χρειάζεται να υποστηρίζει όλα τα τμήματα συμμόρφωσης για να ισχυριστεί συμμόρφωση με το πρότυπο. Χρειάζεται μόνο η υλοποίηση εκείνων των τμημάτων που απαιτούνται για να επιτευχθεί η απαιτούμενη λειτουργικότητα, πχ η ελάχιστη υλοποίηση απαιτεί μόνο το Μπλοκ 1. Δεν είναι επίσης απαραίτητο να υποστηρίζονται όλα τα αντικείμενα που ορίζονται στο πρότυπο για οποιοδήποτε μπλοκ.
7. **Επεκτασιμότητα:** Υποστηρίζει μεγάλα και πολύπλοκα συστήματα, επιτρέποντας την ενσωμάτωση νέων συσκευών και εφαρμογών που απαιτούνται. Μπορεί να διαμορφωθεί για να ανταποκρίνεται στις συγκεκριμένες ανάγκες διαφορετικών εφαρμογών και συστημάτων, καθιστώντας το ένα ευέλικτο πρωτόκολλο για ένα ευρύ φάσμα περιπτώσεων χρήσης. Η συμμόρφωση στα μοντέλα OSI & UCA επιτρέπει επίσης στο ICCP μελλοντικές βελτιώσεις.

8. **Εμπιστευτικότητα:** Εξασφαλίζεται η αυθεντικοποίηση των συνδεόμενων εφαρμογών. Η πρόσβαση σε δεδομένα και λειτουργίες ελέγχεται μέσω Διμερών Πινάκων (Bilateral Tables) που είδαμε στην προηγούμενη ενότητα.
9. **Ακεραιότητα:** Προσφέρονται δυνατότητες κρυπτογράφησης των δεδομένων ενισχύοντας την προστασία κρίσιμων πληροφοριών από πιθανές απόπειρες υποκλοπής τους.
10. **Ασφάλεια:** Το ICCP αρχικά ήταν ένα σχετικά μη προστατευμένο πρωτόκολλο και, ως εκ τούτου ευάλωτο σε παραβιάσεις ακεραιότητας, παρεμβολής ή αλλοίωσης, παραποίησης και παρακολούθησης. Λόγω αυτών των ευπαθειών της ICCP επικοινωνίας, πλέον έχουν εισαχθεί ασφαλτικές βελτιώσεις, γνωστές ως **Secure ICCP**, και περιλαμβάνονται στα νέα προϊόντα ICCP. Αυτές οι βελτιώσεις δημιούργησαν ένα προϊόν του οποίου η επικοινωνία μπορεί να κρυπτογραφηθεί και να εισάγει εργαλεία για να λύσει βασικά ζητήματα ασφάλειας που αντιμετωπίζουν όλα τα βιομηχανικά πρωτόκολλα.

Παρά τις διατάξεις ασφαλείας του ICCP ο εντοπισμός και η καταγραφή πιθανών ευπαθειών του πρωτοκόλλου έχει βαρύνουσα σημασία, καθώς μιλάμε για πρωτόκολλο επικοινωνίας κέντρων ελέγχου. Αυτό σημαίνει ότι ανταλλάσσονται απόρρητες πληροφορίες ολόκληρου του συστήματος ενέργειας και μια πιθανή παραβίαση και υποκλοπή δεδομένων θα έθετε σε μεγάλο κίνδυνο τον συνολικό έλεγχο της παραγωγικής μονάδας. Σημαντικά πεδία που απαιτούν ιδιαίτερη προσοχή στην επικοινωνία ICCP είναι τα παρακάτω:

1. **Ευπάθειες στο Software:** Το λογισμικό που χρησιμοποιείται στα συστήματα ICCP μπορεί να περιέχει ευπάθειες που μπορούν να εκμεταλλευτούν οι εισβολείς για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση ή να διαταράξουν το σύστημα.

2. **Ευπάθεια στην διαμόρφωση:** Τα κακώς διαμορφωμένα συστήματα ICCP μπορεί να είναι ευάλωτα σε επιθέσεις, καθώς μπορεί να έχουν ανοιχτές θύρες ή αδύναμους κωδικούς πρόσβασης που μπορούν εύκολα να αξιοποιηθούν.

3. **Επικοινωνίας WAN:** Το πρωτόκολλο ICCP εφαρμόζεται κατά κύριο λόγο σε ευρείας ζώνης δίκτυα όπου η πληροφορία διανύει μεγάλες αποστάσεις, από ένα κέντρο ελέγχου σε ένα άλλο ή σε υποσταθμούς. Η τοπολογία αυτή λοιπόν, από μόνη της, καθιστά την επικοινωνία ιδιαίτερα ευάλωτη καθώς η ανάπτυξη αμυντικών μηχανισμών είναι δυσκολότερη εκτός των φυσικών συνόρων του συστήματος.

4. **Εσωτερικές απειλές:** Συχνά οι κίνδυνοι προέρχονται εκ των έσω και από το ανθρώπινο δυναμικό που χειρίζεται την εφαρμογή ICCP. Εργαζόμενοι ή εργολάβοι με προνομιακή πρόσβαση πολλές φορές κάνουν κατάχρηση των προνομίων τους με αποτέλεσμα να κακοδιαχειρίζονται και να προκαλούν βλάβες στο σύστημα.

Στο επόμενο κεφάλαιο θα συναντήσουμε περιπτώσεις και παραδείγματα επιθέσεων και σε επίπεδο εφαρμογής όπου θα αναδειχθούν περισσότερα τα ευπαθή πεδία του ICCP αλλά και τον υπολοίπων πρωτοκόλλων επικοινωνίας. Έτσι θα μπορέσουμε να καταλάβουμε καλύτερα τι επιπτώσεις μπορεί να υπάρξουν στα συστήματα ισχύος που χρησιμοποιούν τις επικοινωνίες που μελετήθηκαν αλλά και να επικεντρωθούμε πιο στοχευμένα σε τεχνικές ανίχνευσης και επίλυσης των κινδύνων.

2.6.5. Πεδία Εφαρμογών ICCP

Το Πρωτόκολλο Επικοινωνίας Κέντρων Ελέγχου μεταξύ Παραγωγών Ενέργειας, αναπτύχθηκε για να επιτρέψει την ανταλλαγή δεδομένων μέσω δικτύων ευρείας περιοχής (WAN) μεταξύ οντοτήτων του ηλεκτρικού συστήματος, συμπεριλαμβανομένων των υπηρεσιών κέντρων ελέγχου, ανεξάρτητων φορέων ελέγχου του συστήματος (ISOs), περιφερειακών φορέων μεταφοράς (RTOs) και ανεξάρτητων παραγωγών ενέργειας (IPP) γνωστών επίσης ως μη-δημόσιων παραγωγών (NUG).

Γενικότερα το πλαίσιο του προτύπου - σε αντίθεση με το IEC 60870-5 που καθορίζει τα πρωτόκολλα μετάδοσης για τα βασικά μηνύματα τηλεελέγχου - πρόκειται για μια προκαθορισμένη και τυποποιημένη διεπαφή για την ανταλλαγή πληροφοριών μεταξύ SCADA συστημάτων και εφαρμογών κέντρου ελέγχου. Κάποια πολύ γνωστά πεδία εφαρμογής που χρησιμοποιούν το ICCP κατά το πρότυπο IEC 60870-6 παρατίθενται συνοπτικά παρακάτω:

- **Συστήματα Διαχείρισης Ενέργειας (Energy Management Systems, EMS):** Το ICCP χρησιμοποιείται για την ανταλλαγή δεδομένων πραγματικού χρόνου μεταξύ διαφορετικών συστημάτων EMS, όπως συστήματα SCADA, για την παρακολούθηση και έλεγχο του ηλεκτρικού δικτύου.
- **Αυτόματος Έλεγχος Παραγωγής (Automatic Generation Control, AGC):** Το ICCP χρησιμοποιείται για την ανταλλαγή πληροφοριών μεταξύ διαφορετικών συστημάτων AGC για τη διατήρηση της ισορροπίας μεταξύ παραγωγής και ζήτησης στο δίκτυο ισχύος.
- **Συστήματα Διαχείρισης Διανομής (Distribution Management Systems, DMS):** Το ICCP χρησιμοποιείται για την ανταλλαγή πληροφοριών μεταξύ διαφορετικών συστημάτων DMS, όπως τα συστήματα διαχείρισης διακοπών ρεύματος, για τη βελτίωση της αξιοπιστίας και της αποδοτικότητας του δικτύου διανομής ισχύος.
- **Συστήματα Διαχείρισης Αγοράς:** Το πρωτόκολλο χρησιμοποιείται για την ανταλλαγή δεδομένων μεταξύ διαφορετικών συστημάτων διαχείρισης αγοράς, όπως πλατφόρμες εμπορίας ενέργειας, για τη διευκόλυνση των συναλλαγών ενέργειας μεταξύ διαφορετικών συμμετεχόντων στην αγορά.
- **Διαπεριφερειακός Συντονισμός:** Το ICCP χρησιμοποιείται για τον διαπεριφερειακό συντονισμό και την ανταλλαγή δεδομένων μεταξύ διαφορετικών κέντρων ελέγχου του συστήματος ηλεκτρικής ενέργειας, για την υποστήριξη της ενσωμάτωσης ανανεώσιμων πηγών ενέργειας και τη βελτίωση της ανθεκτικότητας του δικτύου ηλεκτρικής ενέργειας

3. Κυβερνοεπιθέσεις στα πρωτόκολλα επικοινωνίας

3.1. Εισαγωγή στις κυβερνοεπιθέσεις

Σε αυτό το κεφάλαιο μελετώνται κάποιες από τις υφιστάμενες δημοσιεύσεις που σχετίζονται με κυβερνοεπιθέσεις κατά δικτύων επικοινωνίας, τα οποία χρησιμοποιούν τα πρωτόκολλα επικοινωνίας που αναλύθηκαν προηγουμένως. Αυτή η μελέτη είναι κομβική για την παρούσα διπλωματική εργασία καθώς μας βοηθά **(α.) να κατανοήσουμε στην πράξη τις αδυναμίες που αναφέρθηκαν** για κάθε βιομηχανικό πρωτόκολλο, **(β.) να αναγνωρίσουμε βασικούς τρόπους επιθέσεων** στο κυβερνοσύστημα μιας ενεργειακής υποδομής, **(γ.) να**

εκτιμήσουμε τις πιθανές επιπτώσεις τους τόσο στο δίκτυο επικοινωνίας όσο και στο φυσικό σύστημα παραγωγής ενέργειας και τέλος, **(δ.) να αναδείξουμε την ανάγκη για ανάπτυξη αποτελεσματικών μηχανισμών κυβερνοασφάλειας** σε υπάρχοντα και στα υπό διαμόρφωση ηλεκτρικά συστήματα.

Σε γενικές γραμμές ως κυβερνοεπίθεση στο ενεργειακό κυβερνοσύστημα θεωρούμε τις περιπτώσεις όπου κάποια εξωτερική οντότητα επιχειρεί να εισβάλει, να διαταράξει ή να υποκλέψει την κίνηση αυθεντικών μηνυμάτων που ανταλλάσσονται μεταξύ των συσκευών και εφαρμογών που απαρτίζουν το σύστημα. Για να επιτευχθεί μια κυβερνοεπίθεση, οι εισβολείς εφαρμόζουν συγκεκριμένες τεχνικές (ή συνδυασμό τεχνικών) επιθέσεων ανάλογα με τον βασικό τους σκοπό, την εμπειρία ή τις ικανότητες που διαθέτουν. Για τις τεχνικές που θα αναπτυχθούν, μεγάλο ρόλο παίζουν και τα αντίστοιχα τρωτά σημεία που αναγνωρίζουν οι επιτιθέμενοι στο πρωτόκολλο που χρησιμοποιείται, στις φυσικές συσκευές ή εφαρμογές και στη συνολική αρχιτεκτονική του δικτύου. Οι δύο πιο αναγνωρίσιμες καταστάσεις κυβερνοεπίθεσης είναι η άρνηση - ή απόρριψη - υπηρεσίας (Denial of Service) και η ενδιάμεση εισβολή (Man in the Middle). Όταν λοιπόν κάποιος επιτιθέμενος επιθυμεί να εφαρμόσει τις παραπάνω επιθέσεις, θα πρέπει αρχικά να κατέχει τα απαραίτητα λογισμικά εργαλεία αλλά και την γνώση τεχνικών που επιτρέπουν: την παρακολούθηση της κίνησης πακέτων, την αναγνώριση αυθεντικών διευθύνσεων των συσκευών ή τον κατακλυσμό του δικτύου από πλαστά μηνύματα. Τέτοιες τεχνικές επιθέσεων θα μελετήσουμε στις επόμενες ενότητες, τόσο σε θεωρητικό όσο και σε πειραματικό επίπεδο.

Το παρόν κεφάλαιο οργανώνεται σύμφωνα με την δομή του 2^{ου} κεφαλαίου, όπου σε κάθε ενότητα γίνεται μελέτη επιθέσεων σε επικοινωνίες που αφορούν το αντίστοιχο πρωτόκολλο. Για τα πρωτόκολλα Modbus, DNP3 και IEC/104, αρχικά έγινε η προσπάθεια ταξινόμησης των πιθανών κυβερνοεπιθέσεων, καθώς τα παραδείγματα που είναι διαθέσιμα στην βιβλιογραφία είναι εκτεταμένα. Αντιθέτως, οι διαθέσιμες δημοσιεύσεις για τα πρωτόκολλα επικοινωνίας IEC 61850 και ICCP ήταν αρκετά περιορισμένες. Για τον λόγο αυτό, τα πρωτόκολλα αυτά αναλύονται συνδυαστικά με συγκεκριμένα παραδείγματα κυβερνοεπιθέσεων σε Φυσικά Συστήματα, δηλαδή σε εφαρμογές παραγωγής ενέργεια από Φωτοβολταϊκά και Αιολικά Πάρκα, αντιστοίχως. Στην παρακάτω μελέτη, εκτός της θεωρητικές αναλύσεις των διαφόρων κυβερνοαπειλών, γίνεται αναφορά σε πραγματικές πειραματικές δοκιμές επιθέσεων που έχουν διεξαχθεί από ερευνητές. Τέλος, σχολιάζονται τα αποτελέσματα των πειραμάτων αυτών και γίνεται προσπάθεια εκτίμησης των πιθανών επιπτώσεων τόσο στο δικτυακό όσο και στο ηλεκτρικό-φυσικό σύστημα.

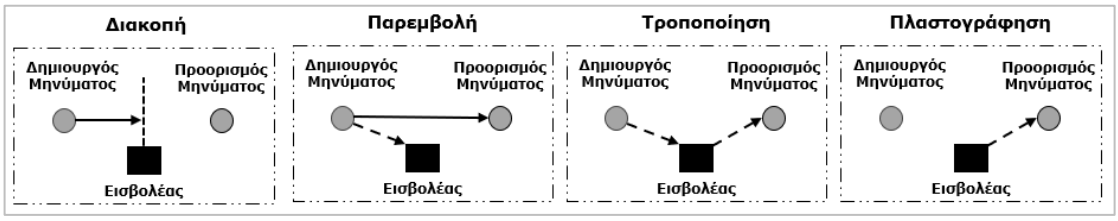
3.2. Κυβερνοεπιθέσεις σε επικοινωνία Modbus

Αρχικά θα μελετηθούν εκτενώς γνωστές επιθέσεις απέναντι σε επικοινωνίες που χρησιμοποιούν πρωτόκολλο Modbus, καθώς είναι το πιο διαδεδομένο πρωτόκολλο στην βιομηχανία, και άρα οι πιθανές επιθέσεις αφορούν και επιφέρουν μεγάλες επιπτώσεις σε πολλά ενεργειακά κυβερνοσυστήματα. Παραδείγματα τέτοιων επιπτώσεων μπορεί να είναι από ασύνηθες και ασταθείς διακοπές των συσκευών πεδίου (πχ. αισθητήρων, ενεργοποιητών, κλπ.) μέχρι μαζικές διακοπές λειτουργίας ή ακόμη και απώλεια ελέγχου σε περίπτωση εισβολής πλαστογραφημένου κεντρικού σταθμού. Βάσει της βιβλιογραφίας, οι έρευνες έχουν ομαδοποιήσει τις επιθέσεις σε επικοινωνίες Modbus σε τρεις βασικές κατηγορίες. Η πρώτη κατηγορία περιλαμβάνει επιθέσεις που εκμεταλλεύονται τις προδιαγραφές του πρωτοκόλλου. Η δεύτερη κατηγορία περιλαμβάνει επιθέσεις που εκμεταλλεύονται τις υλοποιήσεις των πρωτοκόλλων Modbus από τους κατασκευαστές. Τέλος, οι επιθέσεις στην τρίτη

κατηγορία στοχεύουν την υποδομή υποστήριξης, η οποία περιλαμβάνει τα μέσα πληροφορικής, δικτύωσης και τηλεπικοινωνίας. Η παρούσα μελέτη εξετάζει επιθέσεις που είναι αντιπροσωπευτικές για όλες τις εφαρμογές Modbus και συμμορφώνονται με τις προδιαγραφές του πρωτοκόλλου. Στο πρώτο τμήμα της ενότητας παρουσιάζεται μια προτεινόμενη ταξινόμηση διαφόρων επιθέσεων πάνω στις δύο βασικές εκδόσεις Modbus. Στην συνέχεια σχολιάζονται συγκεκριμένες εφαρμογές πειραματικών επιθέσεων που έχουν εκτελεστεί σε TCP/IP επικοινωνίες, δηλαδή στο Modbus/TCP, καθώς αυτές είναι οι περισσότερο ευάλωτες από εξωτερικές απειλές.

3.2.1. Ταξινόμηση κυβερνοεπιθέσεων στο Modbus

Η μέθοδος ταξινόμησης που προτείνεται διαχωρίζει τα δύο βασικά Modbus πρωτόκολλα (σειριακό και TCP) και ταξινομεί τις επιθέσεις αντίστοιχα με αυτόν τον διαχωρισμό. Οι κύριοι στόχοι των κυβερνοεπιθέσεων περιλαμβάνουν τον κεντρικό σταθμό, τις συσκευές πεδίου, τις σειριακές συνδέσεις επικοινωνίας (Modbus Serial) ή τις διαδρομές επικοινωνίας δικτύου TCP (Modbus TCP). Κριτήρια της ταξινόμησης αποτελούν τέσσερα βασικά χαρακτηριστικά απειλών: **παρεμβολή, διακοπή, τροποποίηση και παραποίηση**. Βασική προϋπόθεση διεξαγωγής των επιθέσεων είναι η διαθεσιμότητα ενός παρακολουθητή ανταλλαγής μηνυμάτων (Modbus sniffer) και ενός εισβολέα (packet injector) με τη δυνατότητα να παρεμβάλλεται και να καταγράφει, να αποκλείει, να τροποποιεί ή να πλαστογραφεί αυθαίρετα πακέτα Modbus και ακολουθίες μηνυμάτων.



Για το πρωτόκολλο Modbus Serial οι πιθανές επιθέσεις είναι σχετικά συγκεκριμένες και περιλαμβάνουν συνήθως την αποστολή ενός ή περισσότερων πλαστογραφημένων μηνυμάτων Modbus με ειδικούς κώδικες λειτουργίας και τιμές παραμετροποίησης. Η πρώτη περίπτωση είναι, το σύστημα ελέγχου να στην εκτέλεση πλαστών εντολών ανάγνωσης, σύμφωνα με τον εσφαλμένο κώδικα λειτουργία, επηρεάζοντας τους πόρους και την **εμπιστευτικότητα** της επικοινωνίας. Οι επιθέσεις αυτές, πιο συγκεκριμένα, μπορεί να περιλαμβάνουν ανάγνωση μηνυμάτων Modbus, απόκτηση δεδομένων διαμόρφωσης από εξωτερικούς σταθμούς, κ.λπ. Άλλες επιθέσεις, απειλούν και την **ακεραιότητα** της επικοινωνίας καθώς περιλαμβάνουν εισαγωγή πλαστών δεδομένων εντολών ή εσφαλμένη αναδιαμόρφωση των εξωτερικών σταθμών. Οι πιο καταστροφικές για το φυσικό σύστημα είναι οι επιθέσεις που επηρεάζουν την **διαθεσιμότητα δεδομένων**. Αυτές συνήθως επιφέρουν στις συσκευές απώλεια κύριων λειτουργιών (π.χ. η ικανότητα ανάγνωσης ή παραγωγής μηνυμάτων Modbus), την επανεκκίνηση ή την αναστολή λειτουργίας τους. Παρακάτω περιγράφονται ενδεικτικά τρία παραδείγματα μόνο για το σειριακό Modbus:

- **Εκκαθάριση διαγνωστικού καταχωρητή (Diagnostic Register Reset):** Αυτή η επίθεση εισάγει πλαστά μηνύματα σειριακού Modbus με κώδικα λειτουργίας “08” και παράμετρο “0A”, το οποίο εκκαθαρίζει όλους τους μετρητές και τον διαγνωστικό καταχωρητή της συσκευής-στόχου. Ο επιτιθέμενος με αυτόν τον τρόπο αναδιαμορφώνει παραμέτρους της συσκευής που επηρεάζουν τις λειτουργίες διάγνωσης. Σύμφωνα με τα κριτήρια ταξινόμησης που αναφέραμε,

εντάσσεται στις κυβερνοεπιθέσεις τροποποίησης και πρόκειται για ευθεία απειλή στην ακεραιότητα της επικοινωνίας.

- **Απομακρυσμένη επανεκκίνηση (Remote Restart):** Η επίθεση χρησιμοποιεί τον ίδιο κώδικα διαγνωστικού καταχωρητή αλλά η παράμετρο λειτουργίας έχει τιμή "01" προκαλώντας επανεκκίνηση στην εξωτερική συσκευή. Κατά την διάρκεια της επίθεσης και του χρόνου που απαιτείται για επανεκκίνηση, η συσκευή ουσιαστικά αχρηστεύται, όντας ανίκανη να εκτελέσει προγραμματισμένες λειτουργίες. Με την τροποποίηση της παραμέτρου αυτής, λοιπόν, διακόπτεται η διαθεσιμότητα της συσκευής από το σύστημα επικοινωνίας και συνιστά τόσο επίθεση τροποποίησης όσο και διακοπής.
- **Αναγνώριση εξωτερικού-σταθμού (Slave Reconnaissance):** Είναι μια επίθεση πλαστών εντολών ανάγνωσης χρησιμοποιώντας των κώδικα λειτουργίας "17". Ο εισβολέας δηλαδή παρεμβάλλεται στην αυθεντική επικοινωνία της συσκευής-στόχου και ζητά πληροφορίες κατάστασής της, πλήττοντας την εμπιστευτικότητα του συστήματος.

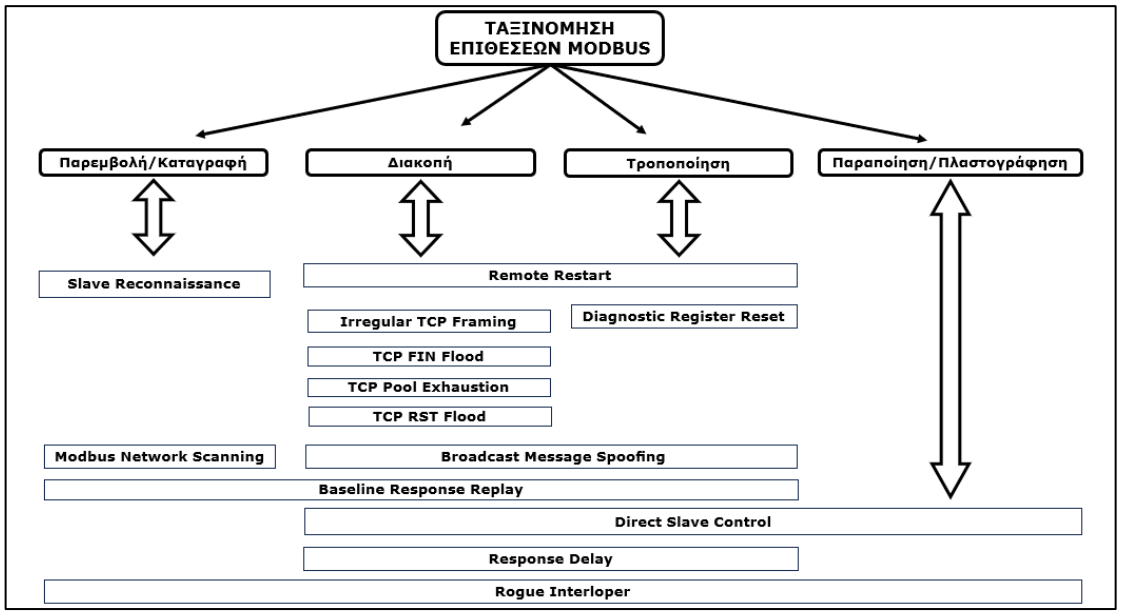
Οι επιθέσεις που αφορούν αποκλειστικά το Modbus TCP μπορεί να έχουν μεγαλύτερη επιτυχία καθώς το πρωτόκολλο είναι περισσότερο ευάλωτο και δίνει στον εισβολέα μεγαλύτερο πεδίο εφαρμογής (πχ. επίπεδο μεταφοράς). Στην έρευνα συναντήσαμε περιπτώσεις επιθέσεων που περιλαμβάνουν μέχρι και πλαστογράφηση ολοκλήρων μονάδων ελέγχου και συσκευών πεδίου, καθώς οι επιτιθέμενοι κατείχαν τις IP διευθύνσεις των αντίστοιχων στόχων. Ωστόσο, οι πιο συνηθισμένες επιθέσεις που αφορούν το Modbus/TCP προκαλούν την **διακοπή συνδέσεων** TCP/IP ή την **ολική απώλεια λειτουργικότητας** της μονάδας ελέγχου και τον ακαριαίο τερματισμό της. Σε αυτές τις περιπτώσεις, η **διαθεσιμότητα** κρίσιμων πληροφοριών και ολόκληρων μονάδων του επικοινωνιακού συστήματος αντιμετωπίζει σοβαρά ζητήματα. Παραδείγματα τέτοιων επιθέσεων που προκαλούν διακοπή της ομαλή επικοινωνίας είναι οι παρακάτω:

- **Αντικανονική πλαισίωση TCP (Irregular TCP Framing):** Πολλά μηνύματα Modbus δεν μπορούν να χωρέσουν σε ένα μόνο πλαίσιο TCP. Έτσι οι επιτιθέμενοι εκμεταλλεύονται αυτή την αδυναμία του πρωτοκόλλου προσπαθώντας είτε να εισάγουν εσφαλμένα (αλλοιωμένα) πλαίσια μηνυμάτων είτε να τροποποιήσουν τα πλαίσια αυθεντικών μηνυμάτων. Το αποτέλεσμα των επιθέσεων αυτού του τύπου είναι ο τερματισμό της σύνδεσης είτε από τη συσκευή ελέγχου είτε από μια συσκευή του πεδίου.
- **Υπερχείλιση σημαίας FIN (TCP FIN Flood):** Η σημαία FIN αφορά κρίσιμες λειτουργίες του πρωτοκόλλου μεταφοράς. Ο κατακλυσμός ενός διακομιστή ή πελάτη Modbus με ψευδή πακέτα TCP μπορεί να οδηγήσει στην υπερχείλιση της σημαίας και να προκαλέσει τερματισμό της TCP σύνδεσης της αντίστοιχης συσκευής.
- **Εξάντληση TCP συνδέσεων (TCP Pool Exhaustion):** Η προδιαγραφή του Modbus TCP εμπεριέχει δύο τύπους συνδέσεων: προτεραιότητας και μη προτεραιότητας. Η επίθεση αυτή σκοπεύει να ανοίξει έναν μεγάλο αριθμό συνδέσεων TCP με μια συσκευή γεμίζοντας τους πίνακες συνδέσεων. Έτσι, τα δύο γκρουπ πινάκων εξαντλούνται και η συσκευή-στόχος δεν μπορεί να αποδεχθεί και να εγκαθιδρύσει καινούργιες συνομιλίες. Το αποτέλεσμα είναι να χαθεί η διαθεσιμότητα της συσκευή αυτής από το σύστημα επικοινωνίας.
- **Υπερχείλιση (TCP RST Flood):** Αντιστοίχως με το πρώτο παράδειγμα, αυτή η επίθεση πλημμυρίζει τον στόχο με πακέτα που περιλαμβάνουν την σημαία RST, προκαλώντας επίσης την διακοπή της TCP σύνδεσης.

Παρά τις διαφορές στα χαρακτηριστικά των επιθέσεων για τις δύο εκδοχές του Modbus, οι περισσότερες επιθέσεις που εντοπίστηκαν και ταξινομήθηκαν έχουν

πεδίο εφαρμογής και τα δύο πρωτόκολλα, **Modbus Serial και Modbus/TCP.** Εδώ η γκάμα των πιθανών κυβερνοεπιθέσεων είναι πλατιά και τα παραδείγματα που αναφέρονται στην συνέχεια περιλαμβάνουν όλα τα κριτήρια ταξινόμησης σύμφωνα με τον τύπο της επίθεσης (βλ. σχήμα 3.1):

- **Εκπομπή πλαστών μηνυμάτων (Broadcast Message Spoofing):** Ο επιτιθέμενος εκπέμπει πλαστά μηνύματα σε όλες τις εξωτερικές συσκευές, τα οποία μπορούν να τροποποιούν δεδομένα και παραμέτρους, όπως είδαμε σε επιθέσεις σειριακού Modbus. Αυτές οι επιθέσεις είναι πολύ επικίνδυνες αφού, διότι για τέτοιου είδους μηνύματα οι συσκευές δεν επιστρέφουν απαντήσεις στην μονάδα ελέγχου. Συνεπώς, μια τέτοια περίπτωση είναι πολύ δύσκολα ανιχνεύσιμη από τους μηχανισμούς ασφαλείας.
- **Αναπαραγωγή απάντησης (Baseline Response Replay):** Αυτή η επίθεση είναι πιο σύνθετη καθώς αντιγράφει μηνύματα απαντήσεων από την αυθεντική κίνηση δικτύου και την επανάληψη επιλεγμένων - από τα καταγεγραμμένα - πακέτων προς τη μονάδα ελέγχου. Θα συναντήσουμε περισσότερες πληροφορίες παρακάτω, στις επιθέσεις Smod.
- **Άμεσος έλεγχος εξωτερικού σταθμού (Direct Slave Control**): Εδώ μιλάμε για μια πιο σοβαρή περίπτωση κυβερνοεπίθεσης κατά την ο οποία ο εισβολέας αρχικά αποκλείει την κύρια μονάδα από την επικοινωνία με εξωτερικές συσκευές και στην συνέχεια αναλαμβάνει τον ρόλο του ελέγχου. Μια τέτοια επίθεση μπορεί να στέλνει κακόβουλα (αλλά νόμιμα για τον στόχο) μηνύματα, ακυρώνοντας έτσι τόσο την ακεραιότητα και αξιοπιστία όσο και την διαθεσιμότητα του συστήματος
- **Έλεγχος Δικτύου (Modbus Network Scanning):** Η επίθεση αυτή περιλαμβάνει αποστολές ακίνδυνων μηνυμάτων σε όλες τις πιθανές διευθύνσεις ενός δικτύου Modbus. Ο σκοπός δεν είναι τόσο να διακόψει ή να τροποποιήσει δεδομένα επικοινωνίας, αλλά να καταγράψει εμπιστευτικές πληροφορίες σχετικά με τις διευθύνσεις συσκευών. Αρχικά, μπορεί να φαίνεται ως μια ακίνδυνη επίθεση για την σταθερότητα του συστήματος, ωστόσο απειλεί ευθέως την αρχή της εμπιστευτικότητας και συνήθως αποτελεί το πρώτο βήμα για μια σειρά νέων επιθέσεων.
- **Καθυστέρηση απαντήσεων (Response Delay):** Στα συστήματα επικοινωνίας η διάθεση της πληροφορίας δεν έχει ουσία εάν δεν συντελείται στον σωστό χρόνο. Δηλαδή, εάν τα δεδομένα που ζητώνται από μονάδες ελέγχου δεν αφορούν εκείνη την χρονική στιγμή αλλά μια παλαιότερη, τότε δημιουργούνται πολλά ζητήματα στην ομαλή λειτουργία του ελέγχου. Η προϋπόθεση αυτή διαρρηγνύεται από κυβερνοεπιθέσεις που στοχεύουν να εισάγουν καθυστερήσεις σε μηνύματα απαντήσεων.
- **Κακόβουλη Εισβολή (Rogue Interloper):** Αρχή όλων των επιθέσεων μπορεί να θεωρηθεί η συνθήκη κατά την οποία ένας εισβολές καταφέρνει να συνδεθεί φυσικά (με θύρα Ethernet ή με κατάλληλο προσαρμογέα σειριακής σύνδεσης) σε έναν απροστάτευτο σύνδεσμο επικοινωνίας. Το σύστημα επικοινωνίας εισέρχεται σε κατάσταση «ενδιάμεση εισβολής» (man-in-the-middle) κατά την οποία ο επιτιθέμενος μπορεί να καταγράφει, να τροποποιεί, να διακόπτει και να παραποιεί πακέτα Modbus όπως επιθυμεί. Η πραγματοποίηση μιας τέτοιας εισβολής θα διαταράξει το σύστημα επικοινωνίας και οι επιπτώσεις θα είναι καταστροφικές.



Σχήμα 3.1 – Ταξινόμηση επιθέσεων σε επικοινωνία Modbus

Στην συνέχεια θα συναντήσουμε ξανά κάποιες από τις παραπάνω, ή παρόμοιες, επιθέσεις δίνοντας έμφαση σε συγκεκριμένες εφαρμογές και εργαλεία επιθέσεων που έχουν εφαρμοστεί σε πειραματικά περιβάλλονται για δοκιμές ασφαλείας του πρωτοκόλλου Modbus.

3.2.2. Κυβερνοεπιθέσεις SMOD στο Modbus/TCP

Όπως διαπιστώθηκε στην ανάλυσή μας στο 2ο κεφάλαιο, το Modbus δεν περιλαμβάνει ελέγχους αυθεντικοποίησης και ασφαλούς πρόσβασης, επιτρέποντας έτσι σε δυνητικούς επιτιθέμενους μια πληθώρα επιλογών που βασίζονται σε γνωστές καταστάσεις επιθέσεων όπως η Απόρριψης Υπηρεσίας (DoS), ο Ενδιάμεσος Εισβολέας (MitM) ή γενικά επιθέσεις που βασίζονται στην μη εξουσιοδοτημένη πρόσβασης στην επικοινωνία. Συνεπώς έχει ιδιαίτερη σημασία να διεξάγονται διαγνωστικές δοκιμές του πρωτοκόλλου, ώστε να υπάρχει μια πλήρη εικόνα για τα επίπεδα ασφάλειας του επικοινωνιακού συστήματος. **Το Smod είναι ένα γνωστό εργαλείο ελέγχου ασφάλειας σχετικά με το πρωτόκολλο Modbus/TCP** και συγκεντρώνει ένα σύνολο λειτουργιών διάγνωσης και δοκιμών επιθέσεων. Ουσιαστικά αποτελεί ένα πλαίσιο δοκιμών διείσδυσης Modbus που μπορεί να χρησιμοποιηθεί για να ελεγχθεί τόσο η ασφάλεια, όσο και η λειτουργικότητα του πρωτοκόλλου. Οι δοκιμές αυτές περιλαμβάνουν διάφορους τύπους επιθέσεων και διαγνωστικών ενεργειών, όπως το fuzzing, η σάρωση, η απόρριψη υπηρεσίας και η πλαστογράφηση ARP πακέτων. Παρακάτω δίνεται η λίστα των επιθέσεων:

Επίθεση	Τύπος	Περιγραφή
modbus/dos/arp	DoS	Επίθεση DoS με «δηλητηρίαση» πακέτων ARP
modbus/dos/galilRIO	DoS	Επίθεση DoS στο PLC σειράς Galil RIO-47100
modbus/dos/writeAllRegister	DoS	DoS επίθεση με εγγραφές σε καταχωρητές
modbus/dos/writeSingleCoils	DoS	DoS επίθεση με εγγραφές σε coil στοιχεία
modbus/function/fuzzing	Fuzzing	Λειτουργία modbus fuzzling
modbus/function/readCoils	Unauthorised Access	Ανάγνωση συγκεκριμένου coil στοιχείου
modbus/function/readDiscreteInput	Unauthorised Access	Ανάγνωση κατάστασης διακριτών εισόδων
modbus/function/readExceptionStatus	Unauthorised Access	Ανάγνωση κατάστασης - εξαίρεσης
modbus/function/readHoldingRegister	Unauthorised Access	Ανάγνωση αριθμού εσωτερικών καταχωρητών
modbus/function/readInputRegister	Unauthorised Access	Ανάγνωση καταχωρητών εισόδου
modbus/function/writeSingleCoils	Unauthorised Access	Εγγραφή είτε 0 είτε 1 σε ένα coil δεδομένο
modbus/function/writeSingleRegister	Unauthorised Access	Εγγραφή συγκεκριμένης τιμής σε καταχωρητή
modbus/scanner/arpWatcher	Reconnaissance Attack	Παρατηρητής ARP
modbus/scanner/discover	Reconnaissance Attack	Προσδιορίζει μια υπηρεσία Modbus που εκτελείται σε μια συσκευή πεδίου
modbus/scanner/getfunc	Reconnaissance Attack	Απαριθμεί κώδικες λειτουργίας που υποστηρίζονται από μια συσκευή πεδίου
modbus/scanner/uid	Reconnaissance Attack	Αναγνωρίζει τις συσκευές και τις διευθύνσεις τους που είναι συνδεδεμένες στο δίκτυο Modbus
modbus/sniff/arp	MiTM	Δηλητηρίαση με ARP πακέτα

Σχήμα 3.2 – Κυβερνοεπιθέσεις SMOD

1. Επίθεση Modbus Teardrop

Η επίθεση Teardrop είναι μια επίθεση τύπου DoS (άρνηση υπηρεσίας) που μεταδίδει αλληλεπικαλυπτόμενα αποσπασμένα πακέτα Modbus/TCP και στοχεύει στην διακοπή της επικοινωνίας του στόχου με άλλες συσκευές του συστήματος. Τα πακέτα που στέλνει ο επιτιθέμενος αποτελούνται από τα αρχικά του πλαίσια ωστόσο αυτά είτε βρίσκονται σε ανακατεμένες θέσεις είτε είναι αλληλεπικαλυπτόμενα. Συνεπώς, οι διαδικασίες διάσπασης και επανασυναρμολόγησης του επιπέδου μεταφοράς δεν μπορούν να λειτουργήσουν με αποτέλεσμα πράγμα που επιφέρει τελικά τον τερματισμός της TCP σύνδεσης. Ο αλγόριθμος 1 παρουσιάζει την λογική σχετικά με την υλοποίηση αυτής της επίθεσης.

Algorithm 1 Teardrop Attack

```
1: procedure TEARDROP                ▷ The execution of the attack
2:     while k < numberOfPackets do
3:         p ← CreateModbusPacket(fc, targetIP)
4:         fragments ← Fragment(p, fragmentSize)
5:         for fragment ∈ Fragments do
6:             send(fragment)
7:         k ← k + 1
```

2. Επίθεση Flag Flood

Η Flag Flood είναι επίσης μια DoS επίθεση και είναι η γενική κατηγορία επιθέσεων υπερχείλισης σημαίας που ασχοληθήκαμε προηγουμένως. Αποστέλλεται συνεχόμενα μια πληθώρα πακέτων TCP με συγκεκριμένες σημαίες (ACK, FIN, SYN και RST) και έχει στόχο την διακοπή της TCP επικοινωνίας. Ο αντίστοιχος αλγόριθμος (Ν. 2) υλοποίησης είναι ο διπλανός.

Algorithm 2 Flag Flood Attack

```
procedure FLAGFLOOD
    while x < numberOfPackets do
        p ← CreatePacket(IP, TCP)
        if Flag == F then
            c ← connectToTarget(targetIP, port)
            c.closeConnection()
        else
            c.send(p)
            attempts ← attempts + 1
    x ← x + 1
```

3. Επίθεση Port Pool Exhaustion

Algorithm 3 Port Pool Exhaustion Attack

```
procedure PORT POOL EXHAUSTION
    while i < numberOfThreads do
        c ← connectToTarget(targetIP)
        attempts ← 0
        startTime ← getTime()
        if c.Connected() && attempts < 3 then
            while elapsedTime < attackTime do
                c.send(KeepAlive)
                elapsedTime ← getTime() − startTime
        else
            c ← connectToTarget(targetIP)
            attempts ← attempts + 1
    i ← i + 1
```

Η επίθεση Port Pool Exhaustion στοχεύει στην εξάντληση του διαθέσιμου εύρους ζώνης του στόχου. Όταν εφαρμόζεται μια τέτοια επίθεση, αλλεπάλληλά νήματα συνδέσεων στην αντίστοιχη θύρα ενός στόχου με γνωστή IP. Η χρονική διάρκεια μιας τέτοιας επίθεσης καθορίζει και το διάστημα κατά το οποίο οι συνδέσεις έχουν εξαντληθεί και άρα ο στόχος δεν μπορεί να επικοινωνεί με το σύστημα (βλ. αλγόριθμο 3).

4. Επίθεση Baseline Response Replay

Συνεχίζοντας όσα αναφέρθηκαν παραπάνω για αυτή την επίθεση, η συνεχομένη αναπαραγωγή απαντήσεων πίσω στην κεντρική μονάδα καταφέρνει να προκαλεί σύγχυση ή έως και διακοπή της επικοινωνίας μεταξύ δύο συνομιλητών στο δίκτυο. Για την καταγραφή πακέτων που απαιτείται, ο επιτιθέμενος εκτελεί μια επίθεση ARP-poisoning για να υποκλέψει την κίνηση δίκτυο. Στη συνέχεια, ορισμένα από τα πακέτα αναπαράγονται επαναλαμβανόμενα στον προορισμό σύμφωνα με τον παρακάτω αλγόριθμο.

Algorithm 4 Baseline Response Replay

```
procedure BRREPLAY
    while x < DurationOfAttack do
        sniff(filter, interface, prn = storePkt)
        send(packetList)
        x ← x + 1
    while attacking == True do
        poisionTarget()
    restoreTarget()
```

5. Επίθεση Response Delay

Η επίθεση καθυστέρησης απόκρισης (response delay attack) ανήκει στην κατηγορία των επαναλαμβανόμενων επιθέσεων (replay attacks). Αρχικά, ο εισβολέας χρησιμοποιεί την τεχνική ARP-poisoning για να παρεμβληθεί ο μεταξύ δύο σημείων που επικοινωνούν και να αποκτήσει τα πακέτα που ανταλλάσσονται. Οι απαντήσεις που θα επιστραφούν από τον εισβολέα θα περιλαμβάνουν χρονικές καθυστερήσεις, τέτοιες ώστε να επιφέρουν σημαντικές επιπτώσεις στο φυσικό περιβάλλον. Η υλοποίηση της επίθεσης βασίστηκε στο iptables και στην ουρά netfilter όπως φαίνεται στον αλγόριθμο 5. Συγκεκριμένα η επίθεση αποτελείται από τρία νήματα. Το πρώτο νήμα αποστέλλει περιοδικά πλαστά πακέτα ARP. Το δεύτερο νήμα αναμένει για ένα συγκεκριμένο χρονικό διάστημα και στη συνέχεια προωθεί όλα τα πακέτα στην ουρά. Τέλος, το κύριο νήμα λαμβάνει τα πακέτα που εισάγονται στην ουρά.

Algorithm 5 Response Delay

```
procedure RECEIVEPACKETS(packet)
    if packet destined for HMI_IP then
        packets_queue.append(packet)
    else
        packet.accept()
procedure FORWARDPACKETS(delay)
    while True do
        sleep(delay)
        for p ∈ packets_queue do
            p.accept()
procedure EXPLOIT(HMI_IP, RTU_IP, queue_id, delay)
    thread_1 ← ARPPoison(HMI_IP, RTU_IP)
    thread_2 ← ForwardPackets(delay)
    thread_1.start()
    thread_2.start()
    nfqueue ← NetfilterQueue(queue_id)
    nfqueue.run()
```

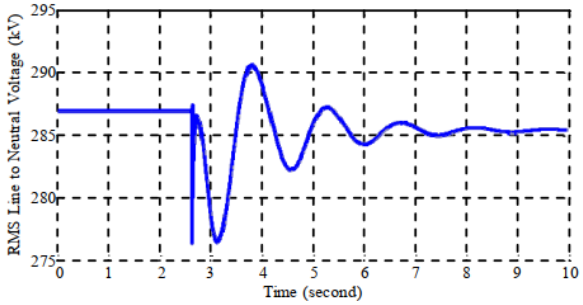
3.2.3. Επίθεση Man-In-The-Middle στο Modbus/TCP

Μεγάλο ενδιαφέρον έχουν οι αναφορές στην βιβλιογραφία των ηλεκτρολόγων μηχανικών του πανεπιστημίου του Τέξας [44], οι οποίοι περιγράφουν την διεξαγωγή χρήσιμών πειραμάτων κυβερνοεπιθέσεων. Οι ερευνητές αναφέρονται στην δημιουργία ενός συστήματος δοκιμών πραγματικού χρόνου, με στόχο να δοκιμαστούν οι ευπάθειες της επικοινωνίας απέναντι σε ορισμένους κινδύνους για το κυβερνοσύστημα. Για την ανάδειξη μιας αποτελεσματικής πλατφόρμας δοκιμαστικών κυβερνοεπιθέσεων, χρησιμοποιήθηκε ως πρωτόκολλο αναφοράς το Modbus/TCP, καθώς είναι και το πιο γνωστό στα συστήματα ισχύος και ταυτόχρονα εύκολο στην υλοποίηση. Η βασική απειλή που δοκιμάστηκε στο δίκτυο επικοινωνίας της πειραματικής διάταξης είναι η εισβολή ενδιαμέσως της επικοινωνίας συσκευών του συστήματος, δηλαδή επιθέσεων Man-in-the-Middle.

Η επίθεση MITM (Man-in-the-Middle) συμβαίνει όταν ένα μη έμπιστο υπολογιστικό σύστημα αποκτά πρόσβαση στην επικοινωνία μεταξύ δύο συσκευών χωρίς εκείνες να είναι ενήμερες για την εξέλιξη αυτής της επίθεσης. Για την επιτυχή πραγματοποίηση της επίθεσης, ο επιτιθέμενος πρέπει να βρίσκεται στο ίδιο υποδίκτυο με τον στόχο και να είναι σε θέση να δηλητηριάσει τους πίνακες ανάλυσης διευθύνσεων ARP των θυμάτων. Ο επιτιθέμενος μπορεί να λαμβάνει την κίνηση από τους δύο στόχους και να λειτουργεί ως δρομολογητής, προωθώντας τη ληφθείσα κίνηση Modbus πακέτων. Ακριβώς αυτό πέτυχε και η εν λόγω δοκιμή χρησιμοποιώντας εξειδικευμένα εργαλεία (Ettercap) για τέτοιες επιθέσεις. Μέσω του Wireshark οι ερευνητές έβλεπαν όλη την κίνηση στο δίκτυο επικοινωνίας και αφού ο επιτιθέμενος είχε γνώση των διευθύνσεων IP του εξυπηρετητή και του ομάδας Modbus, προσομοίωσε επιτυχώς έναν modbus/client, ο οποίος έστελνε εντολές απενεργοποίησης σε IED έξυπνες συσκευές. Η βασική συσκευή-στόχος του

πειράματος ήταν μια μονάδα ενεργοποίησης διακόπτη ισχύος του φυσικού συστήματος. Η αρχική κατάσταση του διακόπτη ήταν στην θέση «1», δηλαδή κλειστός. Τα πλαστά Modbus πακέτα του εισβολέα-πελάτη περιλάμβαναν την διεύθυνση του ενεργοποιητή, την διεύθυνση του καταχωρητή εγγραφής κατάστασης για τον διακόπτη και την τιμή «0» στο φορτίο δεδομένων. Το αποτέλεσμα ήταν προφανώς η αλλαγή κατάστασης του διακόπτη (από 1 σε 0) με αποτέλεσμα το άνοιγμα του ηλεκτρικού κυκλώματος.

Στο σχήμα (3.3) φαίνονται οι μεταβολές της τάσης RMS στον ζυγό από την στιγμή της επίθεσης. Στα 2,5 δευτερόλεπτα, η ισχύς που διέρχονταν μέσω του διακόπτη σταμάτησε, με αποτέλεσμα μια απότομη πτώση στην τάση του δικτύου. Στη συνέχεια, η ροή ισχύος εξομαλύνθηκε σιγά σιγά με την προσαρμογή της ισχύος εξόδου των δύο γεννητριών που συμμετείχαν στο σύστημα ισχύος. για να πλησιάσουν μια νέα σταθερή κατάσταση.



Σχήμα 3.3 – Πτώση τάσης μετά από MitM κυβερνοεπίθεση

3.2.4. Επιθέσεις υπερχείλισης από κατακλυσμό Modbus μηνυμάτων

Η επίθεση Modbus flooding (κατακλυσμός από μηνύματα με στόχο την υπερχείλιση του στόχου) ορίζεται η επίθεση στην οποία ο επιτιθέμενος είναι σε θέση να εισχωρήσει πακέτα στο τοπικό δίκτυο που συνδέει τη συσκευή ελέγχου (PLC, HMI, κλπ.) και το σύστημα ελέγχου και να αναταράξει την κανονική λειτουργία του. Ο επιτιθέμενος δεν προσπαθεί να εμποδίσει τα μηνύματα να φτάσουν στο σύστημα ελέγχου, αλλά αποστέλλει έναν μεγαλύτερο από το συνηθισμένο αριθμό μηνυμάτων με επιλεγμένους κώδικες λειτουργίας με στόχο να ελέγξει το σύστημα μέσω αυτού του κατακλυσμού μηνυμάτων και να αποκρούσει αποτελεσματικά τις νόμιμες εντολές της συσκευής-πελάτη. Το Modbus TCP είναι ιδιαίτερα ευάλωτο σε αυτόν τον τύπο επίθεσης επειδή τα μηνύματα Modbus, εκτός από μηχανισμούς αυθεντικοποίησης που να απορρίπτει παραποιημένα πακέτα, δεν διαθέτει επίσης κανέναν ενσωματωμένο έλεγχο αθροίσματος (checksum) ή ακεραιότητας. Το γεγονός αυτό διευκολύνει τον επιτιθέμενο να πλημμυρίσει το τοπικό δίκτυο με το σύστημα ελέγχου να αποδέχεται τα παραποιημένα μηνύματα Modbus ως εν δυνάμει αυθεντικά.

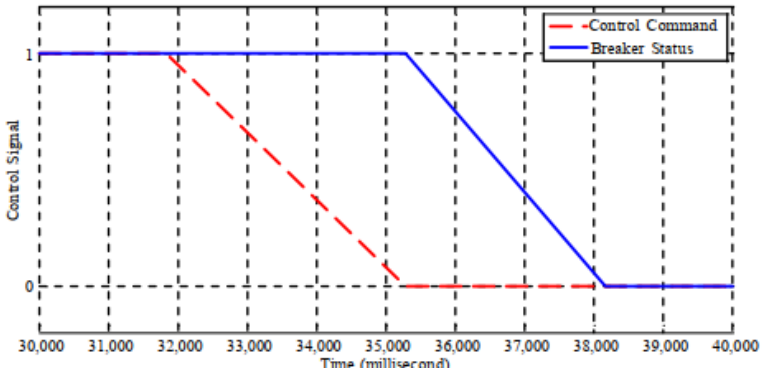
Αξίζει να αναφέρουμε δύο χρήσιμα πειράματα διεξαγωγής επιθέσεων με στόχο την υπερχείλιση της συσκευής ελέγχου, με κατακλυσμό από απεσταλμένα «ψεύτικα» μηνύματα.

1. Επίθεση υπερχείλισης TCP SYN - DoS

Σε συνέχεια του προηγούμενου παραδείγματος και την ίδια πειραματική διάταξη, οι ερευνητές διεξάγουν μια νέα επίθεση τύπου DoS για να ελεγχθεί η ευαισθησία του πρωτοκόλλου Modbus/TCP σε πιθανές καθυστερήσεις στην επικοινωνία. Χρησιμοποιώντας την επίθεση "TCP SYN Flood" ο επιτιθέμενος εκμεταλλεύεται το τριεπίπεδο μηχανισμό συγχρονισμού βημάτων του πρωτοκόλλου TCP για να εγκαθιδρύσει μια αξιόπιστη σύνδεση μεταξύ ενός αποστολέα και ενός παραλήπτη. Η επίθεση TCP SYN flood, συγκεκριμένα, πλημμυρίζει το δίκτυο με αιτήματα σύνδεσης TCP από πιθανούς modbus/πελάτες με παραπλανητικές διευθύνσεις προέλευσης IP και τυχαίες θύρες προορισμού προς τον master. Για την

δημιουργία και την επαναλαμβανόμενη αποστολή των παραπλανητικών αιτημάτων TCP SYN χρησιμοποιήθηκε το εργαλείο Hping.

Στην πειραματική εφαρμογή της επίθεσης, ο επιτιθέμενος έστειλε περίπου για περίπου 55 ms πλαστά SYN πακέτα με ρυθμό 120 πακέτα ανά δευτερόλεπτο. Κατά την διάρκεια της επίθεσης το κέντρο ελέγχου επιχείρησε να εκτελέσει κανονικά λειτουργίες ελέγχου πάνω στο διακόπτη του πειράματος, ζητώντας την κατάστασή του. Το αποτέλεσμα ήταν η λήψη της κατάστασής του από το κέντρο ελέγχου με μια καθυστέρηση των 3 δευτερολέπτων, διότι ο διακομιστής ήταν απασχολημένος με τα πλαστά αιτήματα TCP SYN των επιτιθέμενων.



Σχήμα 3.4 – Καθυστέρηση απάντησης κατά την διάρκεια TCP SYN Flood επίθεσης

Εδώ το συμπέρασμα είναι ότι κατά την διάρκεια της παραπάνω DoS επίθεσης το κέντρο ελέγχου θα λαμβάνει καθυστερημένες πληροφορίες από τις συσκευές IED. Έτσι οι μετρήσεις θα εμποδίζονται από την επίθεση και το κέντρο ελέγχου δεν θα έχει μια ακριβή εικόνα του συστήματος. Συνεπώς, **οι εφαρμογές έξυπνων δικτύων στο κέντρο ελέγχου - που εξαρτώνται από τις πληροφορίες που παρέχουν έξυπνες συσκευές - θα λειτουργούν εσφαλμένα**.

2. Επίθεση με λογισμικό “TCP Modbus Hacker”

Μια δεύτερη απλή εφαρμογή επιθέσεων υπερχείλισης -γραμμένη σε Java- ονομάζεται **"TCP Modbus Hacker" και προγραμματίστηκε πειραματικά για την διεξαγωγή κυβερνοεπιθέσεων σε ένα δίκτυο ελέγχου Modbus**. Η Java έχει εφαρμογή δύο κύριες λειτουργίες: (α.) ανάγνωση και (β.) εγγραφή καταχωρητών στο σύστημα ελέγχου. Αρχικά, το λογισμικό έχει τη δυνατότητα να αναζητήσει όλους τους πιθανούς καταχωρητές του συστήματος, οι οποίοι αντιπροσωπεύουν ενεργοποιητές του συστήματος δοκιμών (πχ. αισθητήρων), προσδιορίζοντας ποιοι από αυτούς είναι ενεργοί. Αυτή η αρχική σάρωση είναι σημαντική για το πείραμα, ώστε οι επιτιθέμενοι να γνωρίζουν ποιοι καταχωρητές χρησιμοποιούνται από το σύστημα ελέγχου και να εκτελούν επιτυχημένες επιθέσεις. Ο "TCP Modbus Hacker" λοιπόν επιτρέπει σε έναν επιτιθέμενο να εγγράψει ένα μεμονωμένο coil στοιχείο ή ταυτόχρονα πολλούς καταχωρητές, χρησιμοποιώντας τις καθορισμένες Modbus λειτουργίες. Επιπλέον, έχει τη δυνατότητα να αλλάξει την ταχύτητα των εντολών που στέλνονται στο στόχο, εισάγοντας ένα χρονικό διάστημα παύσης που μπορεί να διαμορφωθεί σε χιλιοστά του δευτερολέπτου μεταξύ κάθε εντολής που στέλνεται.

Στο πείραμα ο εισβολέας κινείται εναντίον ενός στόχου που είναι μια PLC συσκευή, η οποία αρχικά λαμβάνει σωστές εντολές από έναν προσομοιωτή HMI. Αφού ο "TCP Modbus Hacker" έχει εισαχθεί στο TCP/IP δίκτυο των παραπάνω συσκευών ελέγχου έχει την δυνατότητα να στέλνει στο PLC εντολές γρηγορότερα

από τον HMI-πελάτη. Ως εκ τούτου ενώ το σύστημα ελέγχου προσπαθεί ακόμα να εκτελέσει όλες τις εντολές που λαμβάνει, αναπόφευκτα τελικά ανταποκρίνεται μόνο στις εντολές που δημιουργεί ο εισβολέας. Στην συνέχεια ο εισβολέας προσπάθησε να διαταράξει τον έλεγχο ενός ελεγκτή πεδίου εκτελώντας επιθέσεις υπερχείλισης εναντίον του PLC, κατά τις οποίες πλημμύριζε το PLC με τιμές κατάστασης του ελεγκτή πεδίου, αντίθετες από τις πραγματικές. Όταν η συσκευή πεδίου ήταν ενεργοποιημένη (61-90 δευτερόλεπτα) ο επιτιθέμενος πλημμύριζε το PLC με καταστάσεις «0», ενώ όταν η κατάσταση του ελεγκτή άλλαξε σε «0» (στα 91 δευτερόλεπτα), η κατάσταση του επιτιθέμενου αλλάζει αρχίζοντας την αποστολή πακέτων κατάστασης «1».

Τα ευρήματά του πειράματος έδειξαν ότι οι επιθέσεις υπερχείλισης που εκτελέστηκαν σε βάρος του PLC ήταν επιτυχημένες. Στην χρονική περίοδο 61 - 90 δευτερολέπτων η συσκευή πεδίου απενεργοποιήθηκε με επιτυχία καθώς ο επιτιθέμενος πλημμύριζε τον στόχο με εντολές κατάστασης 0 ενώ το HMI εξακολουθούσε να εμφανίζει την συσκευή ως λειτουργούσα . Κατά την περίοδο από 91 έως 120 δευτερόλεπτα, ο ελεγκτής έκλεισε την συσκευή αλλάζοντας την κατάσταση της σε 0. Ωστόσο, ο επιτιθέμενος αντέστρεψε την κατάσταση της επίθεσης σε 1 πετυχαίνοντας την εκ νέου ενεργοποίηση της συσκευής, ενώ το HMI έδειχνε το αντίθετο. Αξίζει επίσης να σημειωθεί ότι, ο χρόνος απόκρισης της συσκευής στις πλαστές εντολές αλλαγής κατάστασης κυμάνθηκε από 1 έως το πολύ 2 δευτερόλεπτα.

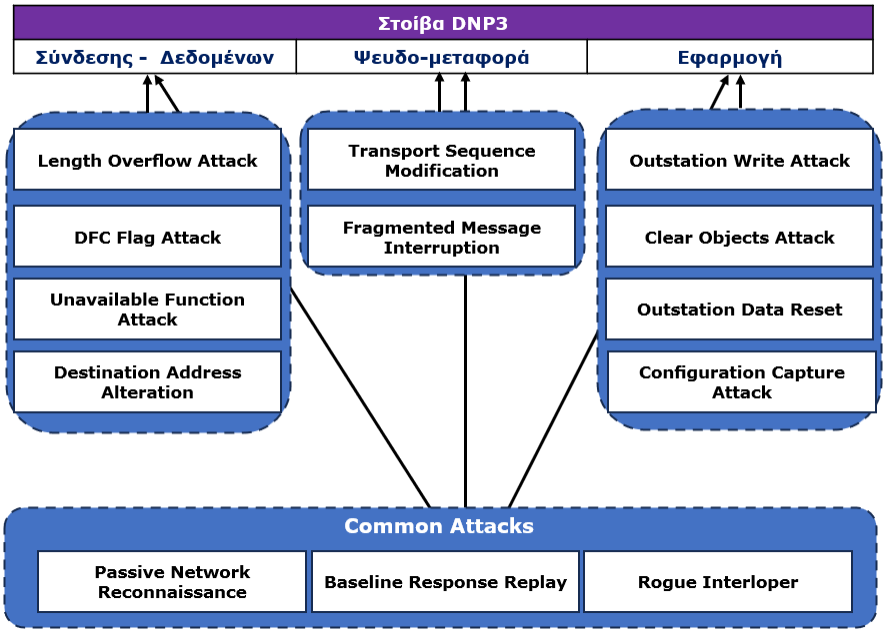
3.3. Κυβερνοεπιθέσεις σε επικοινωνία DNP3

Όπως για το προηγούμενο πρωτόκολλο επικοινωνίας, έτσι και για τα συστήματα DNP3 επικοινωνίας, αρχικά επικεντρωνόμαστε στις επιθέσεις που εκμεταλλεύονται τις προδιαγραφές του πρωτοκόλλου και στοχεύουν όλα εκείνα τα συστήματα SCADA τα οποία συμμορφώνονται με το πρότυπο. **Οι κύριοι στόχοι** αυτών των επιθέσεων μπορεί να είναι ο **κεντρικός DNP3 ελεγκτής**, οι **εξωτερικοί σταθμοί-συσκευές** ή τα **μονοπάτια επικοινωνίας του δικτύου**. Στην ταξινόμηση που θα αναλυθεί στην συνέχεια, οι εντοπισμένες επιθέσεις κατατάσσονται με βάση τις προαναφερθείσες κατηγορίες απειλών και τον αντίστοιχο στόχο. Κάθε επίθεση μπορεί να έχει διάφορες εκδηλώσεις ή "παραδείγματα". Για παράδειγμα, μια επίθεση “Outstation Data Reset” έχει στόχο μια συσκευή πεδίου στην οποία επαναφέρει τα αντικείμενα δεδομένων δίνοντας τιμές ασυνεπείς με την πραγματική κατάσταση του συστήματος. Έτσι επηρεάζει την ίδια την λειτουργία της συγκεκριμένης συσκευής. Συνεπώς, υπάρχουν δύο ταυτόχρονες εκδηλώσεις της επίθεσης σε επίπεδο εφαρμογής, δηλαδή την τροποποίηση και την διακοπή ενός outstation.

3.3.1. Ταξινόμηση κυβερνοεπιθέσεων στο DNP3

Η ταξινόμηση των επιθέσεων στο DNP3 υποστηρίζει τις επίσημες στρατηγικές ανάλυσης κινδύνου και μπορεί να χρησιμοποιηθεί για μια πιο συστηματική εξέταση διαφόρων τεχνικών αντιμετώπισης κυβερνο-κινδύνων, την αξιολόγηση των επιπτώσεων και της σοβαρότητας κάθε απειλής. Στην συγκεκριμένη περίπτωση και λόγω της ιδιαιτερότητας της στοίβας του πρωτοκόλλου, επιλέγουμε να δώσουμε έμφαση στα ευάλωτα σημεία των επιπέδων: **διασύνδεση δεδομένων**, **ψευδο-μεταφορά** και **εφαρμογή**. Συνεπώς, η ταξινόμηση που προτείνεται ακολουθεί μια αντίστοιχη κατηγοριοποίηση επιθέσεων, ανάλογα με το επίπεδο της DNP3-στοίβας που στοχεύει να εκμεταλλευτεί ο επιτιθέμενος. Οι επιθέσεις που εντοπίστηκαν κατά την ανάπτυξη της ταξινόμησης είναι συνολικά 28. Ωστόσο, εμείς θα παρουσιάσουμε ενδεικτικά κάποιες αντιπροσωπευτικές για κάθε επίπεδο και ακόμη τρεις που αναφέρονται σε όλα τα επίπεδα πρωτοκόλλων του DNP3. Αυτές οι ταξινομίες

επιθέσεων μας βοηθούν ουσιαστικά για να αντιληφθούμε τόσο την φύση της επίθεσης όσο και το εύρος των απειλών κατά της ασφαλείας των DNP3 συστημάτων.



Σχήμα 3.5 – Ταξινόμηση επιθέσεων στην DNP3 στοίβα

Οι περιπτώσεις που συναντάμε, φυσικά, εξαρτώνται από τη δυνατότητα διακοπής, παρεμβολής, τροποποίησης ή πλαστογράφησης μηνυμάτων. Το DNP3 επιτρέπει αυτές τις δυνατότητες στους πιθανούς επιτιθέμενους, διότι σε πολλές SCADA εφαρμογές του DNP3 δεν χρησιμοποιούνται μηχανισμοί κρυπτογράφησης, αυθεντικοποίησης και εξουσιοδότησης. Αντιθέτως, τα συστήματα DNP3 συχνά υποθέτουν ότι όλα τα μηνύματα είναι έγκυρα. Οι βασικές επιθέσεις που αξιοποιούν αυτές τις αδυναμίες είναι τρεις και, λόγω της ευελιξίας τους, εκμεταλλεύονται και τα τρία επίπεδα DNP3 που αναφέραμε. **Οι τρεις κοινές επιθέσεις είναι ανάμεσα στις πιο καταστροφικές επιθέσεις** για την επικοινωνία, και παρουσιάζονται παρακάτω:

1. **Παθητική Αναγνώριση Δικτύου (Passive Network Reconnaissance):** Σε γενικές γραμμές, ο επιτιθέμενος, με την κατάλληλη πρόσβαση στο δίκτυο, μπορεί να καταγράφει και αναλύει τα μηνύματα DNP3 που ανταλλάσσονται στο δίκτυο. Έτσι παρέχονται στον επιτιθέμενο εμπιστευτικές πληροφορίες σχετικά με την τοπολογία του δικτύου, τη λειτουργικότητα των συσκευών, τις διευθύνσεις μνήμης και άλλα δεδομένα. Πρόκειται για επίθεση παρεμβολής με πιθανούς στόχους και τους τρεις που αναφέρθηκαν στην εισαγωγή της ενότητας.
2. **Επανάληψη Απάντησης (Baseline Response Replay):** Είναι η αντίστοιχη επίθεση που συναντήσαμε και στο Modbus, όπου ο επιτιθέμενος προσομοιώνει απαντήσεις προς την κύρια συσκευή αποστέλλοντας ταυτόχρονα πλαστογραφημένα μηνύματα προς τις εξωτερικές-συσκευές. Τέτοιες επιθέσεις μπορεί να εκδηλώσουν ολοκληρωτική διακοπή, τροποποιήσεις και πλαστογραφήσεις μηνυμάτων και στους δύο DNP3 συνομιλητές (κύρια - εξωτερική συσκευή).
3. **Κακόβουλη Εισβολή (Rogue Interloper):** Η ίδια επίθεση που εντοπίστηκε στην ταξινόμηση επιθέσεων Modbus, η οποία μπορεί να διαβάζει, τροποποιεί και πλαστογραφεί μηνύματα DNP3 αλλά και την δικτυακή κίνηση. Τα πειράματα σε DNP3 επικοινωνίες έδειξαν πως αυτή η επίθεση είναι και η πιο επικίνδυνη καθώς οδήγησαν στα εξής αποτελέσματα: (α.) ανάκτηση δεδομένων κεντρικού σταθμού συσκευών, και δικτυακής κίνησης, (β.) διακοπή του κεντρικού σταθμού, των συσκευών και δικτύου, καθώς επίσης (γ.) τροποποίηση και (δ.)

πλαστογράφηση των παραπάνω στόχων. Δηλαδή εκδήλωσε κάθε κατηγορία επίθεσης.

Στην συνέχεια παραθέτουμε σημαντικές επιθέσεις που καταγράφηκαν και ταξινομούνται αποκλειστικά στο **επίπεδο Σύνδεσης-Δεδομένων** του DNP3. Ορισμένες από αυτές επηρεάζουν την εμπιστευτικότητα της επικοινωνίας καθώς έχουν την ικανότητα να διαβάζουν δεδομένα ρύθμισης και πληροφορίες τοπολογίας δικτύου. Άλλες στοχεύουν απευθείας στην ακεραιότητα του συστήματος με την εισαγωγή εσφαλμένων δεδομένων ή την αναδιαμόρφωση σημαντικών συσκευών. Τέλος, παρουσιάζονται και απειλές ως προς την διαθεσιμότητα της πληροφορίας με επιθέσεις που διακόπτουν τις επικοινωνίες με τον κεντρικό ελεγκτή.

1. **Υπερχείλιση Μεγέθους (Length Overflow Attack):** Αυτή η επίθεση εισάγει μια εσφαλμένη τιμή στο πεδίο μεγέθους γεγονός που επηρεάζει την ομαλή επεξεργασία του αρχικού μηνύματος. Η επίθεση αυτή μπορεί να οδηγήσει σε καταστροφή πραγματικών δεδομένων, τα οποία ενδεχομένως υπερβαίνουν το πλαστογραφημένο πεδίο μεγέθους. Δημιουργεί δηλαδή σοβαρά ζητήματα ακεραιότητας τους συστήματος αλλά και στην διάθεση των δεδομένων.
2. **Σημαία DFC (DFC Flag Attack):** Η σημαία DFC χρησιμοποιείται για να υποδείξει ότι μια εξωτερική συσκευή είναι απασχολημένη και άρα ένα μήνυμα αιτήματος θα πρέπει να αποσταλεί εκ νέου σε μεταγενέστερο χρόνο. Η εν λόγω επίθεση τροποποιεί στην συσκευή τη σημαία DFC, προσδιορίζοντάς την ψευδώς απασχολημένη. Συνεπώς η μονάδα ελέγχου λαμβάνει συνεχώς μηνύματα μη-διαθεσιμότητας για την συσκευή-στόχο, η οποία τελικά διακόπτεται από την επικοινωνία έως ότου η επίθεση τερματιστεί.
3. **Μη Διαθέσιμη Λειτουργία (Unavailable Function Attack):** Πρόκειται για αποστολή μηνύματος με κώδικα λειτουργίας τιμής "14" ή "15" και υποδεικνύει ότι μια υπηρεσία ενός εξωτερικού σταθμού δε λειτουργεί ή δεν υποστηρίζεται. Έτσι η συσκευή ελέγχου διακόπτει την επικοινωνία με τον εξωτερικό σταθμό, καθώς υποθέτει ότι η υπηρεσία δεν είναι διαθέσιμη.
4. **Τροποποίηση Διεύθυνσης Προορισμού (Destination Address Alteration):** Αλλάζοντας το πεδίο της διεύθυνσης προορισμού, ένας επιτιθέμενος μπορεί να ανακατευθύνει αιτήματα ή απαντήσεις προς άλλες συσκευές, προκαλώντας μεγάλη σύγχυση στην ανταλλαγή των σωστών δεδομένων και δημιουργώντας απρόβλεπτα αποτελέσματα για το σύστημα.

Για το Ψευδο-επίπεδο Μεταφοράς, όπως είδαμε στην ανάλυση του πρωτοκόλλου, οι λειτουργίες που περιλαμβάνονται είναι πολύ συγκεκριμένες και λιγότερες από τα άλλα επίπεδα. Συνεπώς, εντοπίζονται και λιγότερες επιθέσεις σχετικά με αυτό το επίπεδο. Εκτός των τριών κοινών επιθέσεων που αναφέρθηκαν αρχική, η ψευδομεταφορά του DNP3 ενδέχεται να αντιμετωπίσει τις παρακάτω δύο επιθέσεις:

1. **Διακοπή Κατακερματισμένου Μηνύματος (Fragmented Message Interruption**): Η επίθεση δημιουργεί μηνύματα με FIR και FIN σημαίες οι οποίες υποδεικνύουν τα όρια ενός κατακερματισμένου μηνύματος. Όταν αποστέλλεται ένα μήνυμα με σημαία FIR, η διαδικασία μεταφοράς απορρίπτει όλα τα προηγουμένως ληφθέντα κατακερματισμένα τμήματα διαταράσσοντας την ορθή επανασυναρμολόγηση ενός έγκυρου μηνύματος. Από την άλλη, πλαστά μηνύματα με σημαίες FIN θα τερματίζουν πρόωρα την διαδικασία συναρμολόγησης, δημιουργώντας σφάλμα κατά την επεξεργασία του μερικώς ολοκληρωμένου μηνύματος.
2. **Τροποποίηση Ακολουθίας Μεταφοράς (Transport Sequence Modification):** Το πεδίο ακολουθίας χρησιμοποιείται για να εξασφαλίσει την

παράδοση των κατακερματισμένων μηνυμάτων με ορθή σειρά. Η τιμή του πεδίου αυξάνεται με κάθε απεσταλμένο τμήμα του υπό επεξεργασία μηνύματος. Ένας επιτιθέμενος που εισάγει πλαστά μηνύματα σε μια ακολουθία κατακερματισμένων τμημάτων μπορεί να εισάγει λανθασμένα δεδομένα και να προκαλέσει σημαντικά και απρόβλεπτα σφάλματα κατά την επεξεργασία.

Από τα τρία επίπεδα στα οποία ταξινομούνται οι κυβερνοεπιθέσεις στο DNP3, **το Επίπεδο Εφαρμογής** παρέχει και τη μεγαλύτερη λειτουργικότητα, συνεπώς αντιμετωπίζει και περισσότερους κινδύνους. Η ταξινόμηση επιθέσεων -αποκλειστικά- στο επίπεδο εφαρμογής καταγράφει συνολικά 14 επιθέσεις, από τις οποίες επιλέχθηκαν 5 βασικές:

1. **Εγγραφή Δεδομένων σε εξωτερικό-σταθμού (Outstation Write Attack):** Με την χρήση του κώδικα λειτουργίας ”2” τα πλαστά μηνύματα διαφθείρουν τις πληροφορίες που αποθηκεύονται στη μνήμη της συσκευής, προκαλώντας σφάλμα ή υπερχείλιση μνήμης. Εδώ ο στόχος είναι αποκλειστικά ο εξωτερικός σταθμός και η επίθεση είτε οδηγεί σε διακοπή επικοινωνίας από την συσκευή ή τροποποίηση της κατάστασής της.
2. **Εκκαθάριση Αντικειμένων (Clear Objects Attack):** Με τον κώδικα λειτουργίας ”9” ή “10”, η επίθεση κάνει εκκαθάριση των αντικειμένων δεδομένων ενός εξωτερικού σταθμού. Με αυτό τον τρόπο ο εισβολέας διαγράφει κρίσιμα δεδομένα με σκοπό να προκαλέσει δυσλειτουργία ή ολικό σφάλμα στην αντίστοιχη συσκευή-στόχο.
3. **Επαναφορά Δεδομένων εξωτερικού-σταθμού (Outstation Data Reset):** Αυτή η επίθεση στέλνει ένα μήνυμα με κώδικα λειτουργίας “15”. Η επίθεση προκαλεί την επαναφορά των αντικειμένων δεδομένων του αποστάτη με τιμές αναντιστοιχίες με την κατάσταση του συστήματος.
4. **Τερματισμός Εφαρμογής στον εξωτερικό-σταθμό (Outstation Application Termination):** Η επίθεση με κώδικα ”18” χρησιμοποιείται για τη λήξη των εφαρμογών που τρέχουν στους εξωτερικούς σταθμούς. Ένα μήνυμα με αυτόν τον κώδικα λειτουργίας καθιστά μια συσκευή ανίκανη να αποκριθεί σε απλά αιτήματα της συσκευής ελέγχου. Αυτή η επίθεση επιπέδου εφαρμογής όπως και οι προηγούμενες τρεις στοχεύουν σε outstations και θεωρούνται επιθέσεις διακοπής και τροποποίησης.
5. **Καταγραφή Διαμόρφωσης (Configuration Capture Attack):** Στέλνει μήνυμα με ειδικά διαμορφωμένο το πεδίο IIN ώστε να εξαπατήσει την κύρια συσκευή υποδεικνύοντάς της ότι το αρχείο διαμόρφωσης της εξωτερικής-συσκευής έχει καταστραφεί. Η επίθεση αναγκάζει τον κεντρικό σταθμό να μεταδώσει ένα νέο αρχείο, στο οποίο παρεμβάλλεται ο εισβολέας, το τροποποιεί και το φορτώνει στον στόχο. Ουσιαστικά πρόκειται για επίθεση παρεμβολής στον εξωτερικό σταθμό.

3.3.2. Υπερχείλιση μνήμης σε διατάξεις SCADA με πρωτόκολλο DNP3

Η ταξινόμηση των επιθέσεων που προηγήθηκε αποτελεί την απόδειξη πως μια απλή εφαρμογή επικοινωνίας DNP3, χωρίς διατάξεις και μηχανισμούς ασφαλείας, είναι ιδιαίτερα ευάλωτη απέναντι σε απλές κυβερνοεπιθέσεις. Οι εισβολείς μπορούν εύκολα να εκμεταλλευτούν τις αδυναμίες του πρωτοκόλλου και να εισάγουν κακόβουλα πακέτα δεδομένων που θέτουν σε κίνδυνο την λειτουργία του συστήματος. **Για παράδειγμα ας υποθέσουμε ότι,** σε μια απλή διάταξη SCADA υπάρχουν συσκευές αποθήκευσης προσωρινών δεδομένων πεδίου μέχρι την απόκτησής τους από το κέντρο ελέγχου. Σε αυτήν την συνηθισμένη πρακτική αρχιτεκτονικής ένας εισβολέας που εισβάλει στο δίκτυο μπορεί απλώς να

πλημμυρίσει τις συσκευές που υποθέσαμε με πολλαπλά δεδομένα γεγονότων (data events), για να εμποδίσει το κέντρο ελέγχου να ενημερώνεται για την κατάσταση του ηλεκτρικού συστήματος. Η επίθεση δηλαδή γεμίζει τον προσωρινό αποθηκευτικό χώρο γεγονότων των συσκευών και έτσι απαγορεύει την αποθήκευση νέων κρίσιμων ειδοποιήσεων. Μια αντίστοιχη **επίθεση υπερχείλισης στην προσωρινή μνήμη (buffer flooding)** θα μελετήσουμε στην συνέχεια, σύμφωνα με τα ευρήματα που προέκυψαν από τα πειράματα που συναντάμε στην βιβλιογραφία. Ο βασικός λόγος για την διεξαγωγή των πειραμάτων μιας τόσο απλής επίθεσης ήταν οι εξής δύο διαπιστώσεις. Πολλοί εμπορικοί DNP3-συλλέκτες δεδομένων έχουν κοινόχρηστη προσωρινή «μνήμη γεγονότων» και η επικοινωνία μεταξύ ενός κέντρου ελέγχου και ενός συλλέκτη δεδομένων είναι ασύγχρονη σε σχέση με την επικοινωνία μεταξύ του συσσωρευτή δεδομένων και των ρελέ. Μεγάλο ρόλο έπαιξε επίσης το γεγονός ότι, πολλές τεχνικές άμυνας για επιθέσεις DoS, ενδέχεται να μην λειτουργούν κατάλληλα καθώς τα δίκτυα SCADA συνήθως έχουν περιορισμένους πόρους και υψηλές απαιτήσεις για επικοινωνία σε πραγματικό χρόνο.

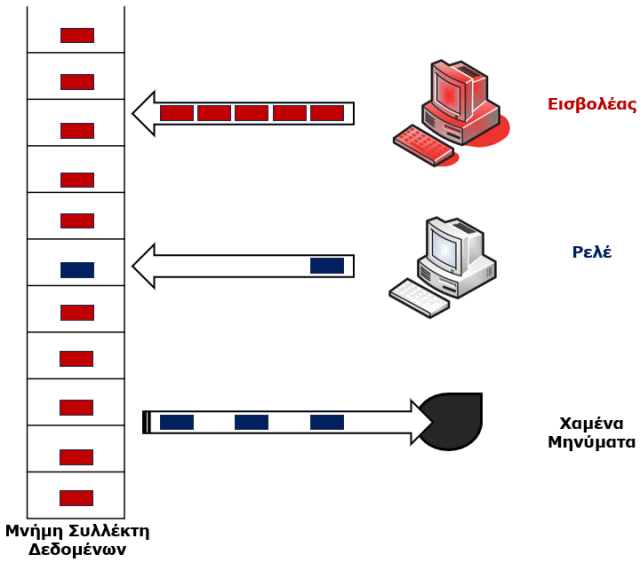
Πιο συγκεκριμένα οι επιθέσεις “buffer flooding” αποκτώντας πρόσβαση στο δίκτυο επικοινωνίας του συστήματος **ο πρώτος στόχος είναι η πλαστογράφηση μιας συσκευής πεδίου** (ρελέ, διακόπτες, κλπ.) οι οποίες ενημερώνουν για την κατάστασή τους τα ανώτερα επίπεδα ελέγχου. Χωρίς να απαιτείται δηλαδή η ολική απόκτηση του ελέγχου του συλλέκτη δεδομένων, πλαστογραφώντας ένα ρελέ πεδίου και δημιουργώντας μια σύνδεση επικοινωνίας με τον συλλέκτη, ο επιτιθέμενος μπορεί να πλημμυρίσει το δίκτυο με μηνύματα γεγονότων. Η πλαστογράφηση αυτή επιτυγχάνεται με διάφορες τεχνικές που εκμεταλλεύονται την έλλειψη αυθεντικοποίησης στο DNP3, είτε μέσω “ARP spoofing” επιθέσεις στο ρελέ, είτε με τεχνικές κρυφού μεσάζοντα (MitM) στην επικοινωνία μεταξύ των δύο συσκευών. Η απόκτηση του ελέγχου μιας συσκευής πεδίου μπορεί να γίνει ακόμη πιο εύκολη για τους εισβολής σε περιπτώσεις κακών πρακτικών ρύθμισης των κωδικών πρόσβασης. Σε πολλά συστήματα SCADA έχει παρατηρηθεί ότι οι χρήστες διατηρούν τους προκαθορισμένους κωδικούς από τον κατασκευαστή, που σημαίνει ότι είναι διαθέσιμοι με μια απλή περιήγηση στο διαδίκτυο.

Για την πειραματικές δοκιμές που έλαβαν μέρος, χρησιμοποιείται ένας δοκιμαστικός συλλέκτης δεδομένων που υποστηρίζει και τους τρεις κλασικούς τύπους δεδομένων: δυαδικά, αναλογικά και μετρητές. Για τον κάθε τύπο δεδομένων διαθέτει μια ξεχωριστή προσωρινή μνήμη - buffer. Εκτός του συλλέκτη, η DNP3 πειραματική διάταξη περιλαμβάνει δύο ρελέ (“1” και “2”) ως outstations και έναν κεντρικό Υπολογιστή ως master που παίζει τον ρόλο του κέντρου ελέγχου. Ο συλλέκτης βρίσκεται στην ενδιάμεση βαθμίδα της ιεραρχικής τοπολογίας, λειτουργώντας ως σταθμός για τον υπολογιστή και ως κύρια συσκευή για τα ρελέ. Οι αρχικές δοκιμές υπερχείλισης έγιναν έχοντας ορίσει μικρά μεγέθη στις μνήμες του συλλέκτη ώστε σε πρώτη φάση να κατανοηθεί ο μηχανισμός γεμίσματος και αδειάσματος. Διεξάγοντας λοιπόν αποστολές αυθεντικών και πλαστών μηνυμάτων γεγονότων παρατηρήθηκαν τα εξής:

- **Η μνήμη** του συλλέκτη είναι ένας προσωρινός αποθηκευτικός χώρος, ο οποίος γεμίζει από τις απαντήσεις (γεγονότα) των ρελέ πεδίου και αδειάζει από ένα αίτημα του σταθμού ελέγχου.
- Οι μνήμες των τριών τύπων δεδομένων χρησιμοποιούν τον μηχανισμό **«Πρώτα έρχεται - Πρώτα εξυπηρετείται» (FCFS),** κατά την First In First Out (FIFO) λογική.
- Οι **μνήμες μετρητών και δυαδικών γεγονότων** χρησιμοποιούν τη **λειτουργία "διαδοχικών γεγονότων"** κατά την οποία κάθε νέο γεγονός καταλαμβάνει νέο χώρο στην μνήμη. Εάν αυτή είναι γεμάτη, τότε το όλα τα

ληφθέντα γεγονότα απορρίπτονται και μια επίθεση υπερχείλισης μνήμης μπορεί να είναι επιτυχημένη. Σε αυτήν την περίπτωση το bit επισήμανσης υπερχείλισης στην αρχή του DNP3 μηνύματος γίνεται αληθές.

- Η **μνήμη των αναλογικών γεγονότων** χρησιμοποιεί τη λειτουργία **"πιο πρόσφατο γεγονός"** κατά την οποία φυλάσσεται χώρος για κάθε μεμονωμένο σημείο δεδομένων που μπορεί να αποκτηθεί από τον συλλέκτη. Όταν ένα νέο γεγονός φτάνει, τότε όλες οι θέσεις μνήμης που σχετίζονται με τα δεδομένα που μεταφέρει αντικαθίστανται, ανεξαρτήτως εάν οι τρέχουσες τιμές τους έχουν πρώτα διαβαστεί από ένα αίτημα του σταθμού ελέγχου. Αυτό σημαίνει ότι οι μνήμες αναλογικών γεγονότων είναι ανθεκτικές σε buffer flooding, καθώς η επίθεση επιδρά μόνο στον χώρο της μνήμης που επιτίθεται ο εισβολέας.



Σχήμα 3.6 – Διάγραμμα μνήμης γεγονότων μετά από επίθεση

Στην συνέχεια τα πειράματα περιλάμβαναν πιο **συντονισμένες επιθέσεις υπερχείλισης μνήμης**. Συγκεκριμένα, ο συλλέκτης δεδομένων «ανακρίνει» τα ρελέ, κάθε 10 δευτερόλεπτα λαμβάνοντας πάντα 3 γεγονότα σε κάθε αίτημα. Η μνήμη γεγονότων λειτουργεί με «διαδοχικά γεγονότα» επιτρέποντας έως 50 γεγονότα για αποθήκευση, τα οποία ο υπολογιστής ελέγχου αιτείται επίσης ανά 10 δευτερόλεπτα. Ωστόσο, ο ρυθμός αποστολής ανεπιθύμητων μηνυμάτων από τα «πλαστά» ρελέ μπορεί να είναι έως 20 γεγονότα ανά δευτερόλεπτο με αποτέλεσμα να καταλαμβάνουν θέσεις μνήμης ταχύτερα από τα αυθεντικά μηνύματα γεγονότων. Κάθε πείραμα διενήργησε συνολικά 100.000 επιθέσεις γεγονότων και το παρακάτω σχήμα (3.7) δείχνει μια διαγραμματική απεικόνιση των επιθέσεων αυτών. Τα αποτελέσματα έδειξαν ότι με έναν ρυθμό αποστολής 5 πλαστών γεγονότων ανά δευτερόλεπτο η μνήμη φτάνει στα όρια της με αποτέλεσμα την απώλεια αυθεντικών πακέτων. Το ποσοστό απώλειας αυξάνεται καθώς αυξάνεται ο ρυθμός αποστολής του επιτιθέμενου και φθάνει σχεδόν στο 80% για ρυθμό επίθεσης 20 γεγονότων/δευτερόλεπτο.

3.3.3. Υποκλοπή και τροποποίηση DNP3 μηνυμάτων

Η έλλειψη αυθεντικοποίησης του DNP3 έχει κεντρίσει το ενδιαφέρον και άλλων ερευνητών ανά τον κόσμο. Στο Ινστιτούτου Μηχανικών Πληροφορικής και Επικοινωνίας στο Τόκυο, Ιαπωνίας [37] οι ερευνητές για την μελέτη της ασφάλειας του πρωτοκόλλου, διενήργησαν πειραματικές επιθέσεις υποκλοπής και

τροποποίησης μηνυμάτων. Χρησιμοποιώντας ένα ανοικτού τύπου λογισμικό για επιθέσεις "Man in the Middle" σε τοπικά LAN δίκτυα, οι μηχανικοί εκχωρούσαν ARP πακέτα στον στόχο. Μετά την έκχυση δηλητηριασμένων πακέτων το Wireshark του εργαστηρίου ανέλυε τα ανιχνευμένα πακέτα.

Ο στόχος του επιτιθέμενου ήταν να τροποποιήσει διάφορα πακέτα DNP3 στο δίκτυο με τον εξής τρόπο. Όταν το εργαλείο επίθεσης λαμβάνει ανιχνευμένα πακέτα, τα διαιρεί σε όλα τα επίπεδα: Ethernet, IP, TCP, DNP3-Data Link, DNP3-Transport και DNP3-Application και στην συνέχεια αναλύει τα αντικείμενα δεδομένων. Το εργαλείο τα τροποποιεί ανασκευάζοντας τα πακέτα με αντίστροφη σειρά, υπολογίζει ξανά τις τιμές του ελέγχου αθροίσματος και τα προωθεί στην αρχική τους θέση. Χρησιμοποιώντας αυτό το εργαλείο, ο επιτιθέμενος ταυτόχρονα μπορεί να αλλάζει κατά το δοκούν το μήνυμα απάντησης των εξωτερικών σταθμών της διάταξης. Παρ' όλα αυτά, τα τροποποιημένα πακέτα εμφανίζουν πάντα ασφαλές τιμές κατάστασης των συσκευών πεδίου στο κέντρο ελέγχου, εξαπατώντας το για τις πραγματικές συνθήκες στο φυσικό σύστημα.

Η εφαρμογή των επιθέσεων διεξήχθη σε μια **πειραματική διάταξη υδροηλεκτρικού σταθμού** και **τα αποτελέσματα ήταν τα ακόλουθα**:

- Λόγω έλλειψης μηχανισμού κρυπτογράφησης της επικοινωνίας, το Wireshark εμφάνισε τα κλεμμένα DNP3 αντικείμενα δεδομένων που ανταλλάχθηκαν, παρ' ότι η επικοινωνία χρησιμοποιούσε πρόσθετα εργαλεία ασφαλείας (DNP3 SA). Η τόσο εύκολη ανίχνευση αντικειμένων με τη MAC διεύθυνση, εγείρει σημαντικούς προβληματισμούς για τα επίπεδα ασφάλειας στην επικοινωνία.
- Για τις βάνες του συστήματος, η τροποποίηση πακέτων λειτούργησε εξίσου αποτελεσματικά. Ο κεντρικός και οι εξωτερικοί σταθμοί εμφάνισαν εντελώς διαφορετικά αποτελέσματα. Συγκεκριμένα, ο κεντρικός σταθμός ελέγχου έδειξε ότι και οι τέσσερις οι πύλες της εφαρμογής έχουν ανοίξει σύμφωνα με το αίτημα του χειριστή (80%, 60%, 80%, 80%). Από την άλλη, οι συσκευές λειτουργούν με τις πλαστογραφημένες τιμές (40%, 30%, 40%, 40%), χωρίς την εμφάνιση σφάλματος από τον κεντρικό ελεγκτή.
- Οι αισθητήρες από την άλλη ενημέρωναν ότι η στάθμη του νερού στις δεξαμενές αποθήκευσης είναι πάνω από το 90%, ωστόσο η κεντρική συσκευή ελέγχου διάβαζε χαμηλότερα επιτρεπτά όρια. Σε αυτήν την περίπτωση, ενώ οι δεξαμενές είναι σε κατάσταση υπερχείλισης, οι διαχειριστές δεν μπορούν να πάρουν ανάλογες αποφάσεις για την αποκατάσταση του προβλήματος.
- Βλέπουμε λοιπόν ότι, λόγω των επιθέσεων τροποποίησης των τιμών πεδίου, **οι διαχειριστές του SCADA δεν μπορούν να αντιληφθούν ότι το σύστημα έχει δεχθεί επίθεση** και είναι σε κατάσταση σφάλματος. Αυτό θα το ανακύψουν μόνο όταν λειτουργήσουν μηχανικές διατάξεις προειδοποίησης, όπου η κρισιακή κατάσταση θα έχει ήδη επιδεινωθεί.

3.4. Κυβερνοεπιθέσεις στο IEC 60870-5-104

Οι επικοινωνίες προτύπου IEC 60870-5-104 όπως ξέρουμε βασίζονται στην στοίβα TCP/IP, γεγονός που καθορίζει συγκεκριμένα ζητήματα ασφάλειας όπως είδαμε στα προηγούμενα πρωτόκολλα. Παρόλο που ο οργανισμός IEC εκδίδει νέες λύσεις και κατευθυντήριες γραμμές (πρότυπο IEC 62351) που ενισχύουν την ασφάλεια του IEC/104, η φύση των βιομηχανικών συστημάτων SCADA δυσκολεύει την άμεση και εύκολη αναβάθμισή των πρωτοκόλλων αυτών. Εκτός των γνωστών αδυναμιών του TCP/IP, ζητήματα όπως έλλειψη κρυπτογράφησης των δεδομένων εφαρμογής και μηχανισμών αυθεντικοποίησης σε διάφορες εντολές, όπως αναλύθηκαν στο 2ο κεφάλαιο, επιτρέπουν σε πιθανούς εισβολείς να εκτελέσουν

απλές επιθέσεις. Η μη εξουσιοδοτημένη είσοδος στην επικοινωνία και δυνατότητα ανάλυσης της κίνησης πακέτων στο δίκτυο καθιστούν επιθέσεις που χρησιμοποιούν κοινές τεχνικές (πχ. επιθέσεις ενδιαμέσου - MiTM) ιδιαίτερα αποτελεσματικές. Αυτή η ευπάθεια είναι αρκετά κρίσιμη και χρειάζεται περαιτέρω διερεύνηση, καθώς και στις IEC-104 επικοινωνίες οι επιτιθέμενοι μπορούν να καταγράψουν την αυθεντική επικοινωνία αλλά και να εισάγουν κακόβουλα δεδομένα.

Για παράδειγμα, ένας εισβολέας μπορεί να αλλάξει διάφορες τιμές ελέγχου σε ένα μήνυμα προκαλώντας την δυσλειτουργία κρίσιμων συσκευών του ηλεκτρικού συστήματος. Μπορεί επίσης να τροποποιήσει τιμές ορίων ειδοποίησης συναγερμού (alarm set points) που αποθηκεύονται στους καταχωρητές του κεντρικού PLC ή άλλων ελεγκτικών συσκευών. Έτσι πετυχαίνει την απενεργοποίηση συναγερμών που θα έπρεπε να είναι ανοικτοί ή αλλάζει τα επίπεδα στα οποία εκείνοι θα πρέπει να ενεργοποιηθούν. Ακόμη, ένας επιτιθέμενος μπορεί να παραποιεί τιμές ανάγνωσης στο κέντρο ελέγχου για να εξαπατήσει τους χειριστές του συστήματος και να επιτρέψει στην επίθεση να περάσει απαρατήρητη.

Στην συνέχεια θα μελετήσουμε διάφορες πειραματικές δοκιμές επιθέσεων στο πρωτόκολλο IEC/104 για να βγάλουμε κάποια ασφαλή συμπεράσματα για τα επίπεδα ασφάλειας που παρέχει το πρωτόκολλο σε εφαρμογές του.

3.4.1. Δοκιμές γενικών τύπων επιθέσεων σε διάταξη επικοινωνίας IEC/104

Η αρχική μελέτη που παραθέτουμε σχετίζεται με τις δοκιμές ασφαλείας που διεξήχθησαν από ερευνητές του Πανεπιστημίου Δυτ. Μακεδονίας. Οι έρευνες αυτές επικεντρώνονται κυρίως σε επιθέσεις που εκμεταλλεύονται τις ευπάθειες συστήματος επικοινωνίας IEC/104. Βασικός σκοπός των δοκιμών ήταν η καταγραφή και ανάλυση της συμπεριφοράς της επικοινωνίας - χρησιμοποιώντας το εργαλείο μαθηματικής μοντελοποίησης CPN – κατά την εμφάνιση γνωστών κυβερνο-απειλών. Αρχικά, ταξινομούν τις πιθανές επιθέσεις που πρόκειται να εμφανιστούν αναγνωρίζοντας τέσσερις πιθανές κατηγορίες κατά του IEC/104:

α. Μη εξουσιοδοτημένη πρόσβαση

β. Επιθέσεις ενδιαμέσου (MitM),

γ. Επιθέσεις άρνησης υπηρεσίας (DoS)

δ. Επιθέσεις ανάλυσης κίνησης δικτύου (Traffic Analysis).

Οι δοκιμές προσομοιώνουν μια απλή διάταξη επικοινωνίας IEC/104 η οποία περιλαμβάνει έναν λογικό ελεγκτή (PLC) και έναν τερματικό σταθμό (MTU) που επικοινωνεί με το PLC και είναι υπεύθυνο να παρακολουθεί και προλαμβάνει πιθανές ανωμαλίες του βιομηχανικού περιβάλλοντος. Τα εργαλεία προσομοίωσης περιλαμβάνουν ενδείξεις σχετικά με την επικοινωνία των δύο παραπάνω συσκευών (σφάλματα, νέες συνδέσεις, αποσυνδέσεις, κλπ.) και πληροφορίες σχετικά με τα πραγματικά IEC/104 μηνύματα (διευθύνσεις αντικειμένων, CoT, σημαίες κλπ.). Ο επιτιθέμενος προσομοιωτής έχει φυσική πρόσβαση στον δρομολογητή του τοπικού δικτύου και χρησιμοποιεί κοινά εργαλεία επιθέσεων, όπως το Ettercap και το hping. Τέλος, μια ακόμη συσκευή, συνδεδεμένη μέσω δικτύου SPAN, αναλαμβάνει την παρακολούθηση και την προστασία της διάταξης.

Οι επιθέσεις που πραγματοποιήθηκαν κατά της επικοινωνίας IEC/104 ήταν οι εξής τέσσερις:

1. **Κατακλυσμός από IEC-104 Πακέτα:** Αποτελεί επίθεση τύπου DoS η οποία επιχείρησε να πλημμυρίσει το MTU με συγκεκριμένα IEC-104 πακέτα εντολών. Ο σκοπός ήταν να προκαλέσει με αυτό τρόπο γενική δυσλειτουργία στο MTU ή ακόμα την οριστική διακοπή της λειτουργίας του. Για την προσομοίωση αυτής της επίθεσης, το PLC προγραμματίστηκε με τρόπο ώστε να μεταδίδει στο MTU μια συγκεκριμένη πληροφορία (ενός bit κατάστασης ή εντολής) ανά δευτερόλεπτο. Η επίθεση, δεν στέφθηκε με επιτυχία και η λειτουργικότητα του MTU δεν επηρεάστηκε. Ωστόσο, εάν υπήρχαν στην διάταξη περισσότερα PLCs που διεξάγουν ταυτόχρονες επιθέσεις, θα ήταν πιθανό να εμφανιστεί κατάσταση υπερχείλισης στο MTU. Είναι επίσης σημαντικό να σημειωθεί ότι η συσκευή παρακολούθησης και ελέγχου δεν εντόπισε την επίθεση, καθώς αυτή η ενέργεια δεν παραβίασε κανόνες ασφαλείας.
2. **Επίθεση Υπερχείλισης TCP SYN:** Στην λογική που έχει περιγράφει στα προηγούμενα πρωτόκολλα, ο κακόβουλος εισβολέας εκμεταλλεύεται το επίπεδο TCP στέλνοντας διαρκώς στο PLC πακέτα SYN χωρίς να λαμβάνει τις αντίστοιχες απαντήσεις (SYN+ACK). Για την προσομοίωση αυτής της επίθεσης, χρησιμοποιήσαμε το εγκατεστημένο εργαλείο hping του Kali Linux. Κατά τη διάρκεια της συγκεκριμένης επίθεσης, παρατηρήθηκε ότι το ποσοστό χρήσης της κεντρικής μονάδας επεξεργασίας (CPU) αυξήθηκε κατά 23%, ενώ το ποσοστό χρήσης της μνήμης αυξήθηκε κατά 12%. Αντιστοίχως, το ποσοστό χρήσης του δικτύου αυξήθηκε κατά 4,81%. Αυτή η επίδραση δεν ήταν αρκετή ώστε να διακόψει την επικοινωνία μεταξύ του PLC και του MTU, ωστόσο σε ένα πραγματικό περιβάλλον με ένα πιο επιφορτισμένο PLC από περιορισμένους υπολογιστικούς πόρους, η επίθεση θα είχε σοβαρή επίδραση. Επιπλέον, εάν υπήρχαν περισσότεροι επιτιθέμενοι, η επίπτωση της επίθεσης θα ήταν προφανώς διαφορετική. Σε αυτήν την περίπτωση η συσκευή παρακολούθησης ανιχνεύει κανονικά την κυβερνοεπίθεση.
3. **Μη εξουσιοδοτημένη πρόσβαση**: Υπό κανονικές προϋποθέσεις, ένας μη εξουσιοδοτημένος χρήστης δεν θα έπρεπε να επικοινωνεί με το PLC. Ωστόσο, η έλλειψη αυθεντικοποίησης και η σωστή τροποποίηση της IP διεύθυνσης του επιτιθέμενου, ώστε να θεωρηθεί μέλος του δικτύου, μπορεί να επιτρέψει την είσοδο ξένων στοιχείων στο σύστημα. Με αυτό τον τρόπο μπορούν στην συνέχεια να διεξαχθούν μια σειρά από επιθέσεις που θα επηρεάσουν την αξιοπιστία της επικοινωνίας, όπως εντολές ανάγνωσης, επαναφοράς λειτουργίας και ανακρίσεων μετρητή. Το εργαλείο ανίχνευσης του πειράματος εντόπισε αρκετές επιθέσεις με αυτά τα χαρακτηριστικά.
4. **Επίθεση απομόνωσης δικτύου IEC/104**: Εδώ η προϋπόθεση είναι μια επίθεση MiTM, όπου ο εισβολέας έχει στόχο να απομονώσει και να απορρίψει την κίνηση δικτύου μεταξύ του PLC και του MTU. Με το λογισμικό Ettercap διεξήχθη αρχικά επίθεση ARP-poisoning. Έπειτα ενεργοποιήθηκε ειδικό φίλτρο του λογισμικού, με το οποίο τα πακέτα που ανταλλάσσονταν απομονώθηκαν και απορρίφθηκαν επιτυχώς.

Επιθέσεις	**Ευπάθεια IEC/104**
Άρνηση Υπηρεσίας - DoS	Ανάθεση Πόρων χωρίς Όρια ή Περιορισμούς
Ανάλυσης Κίνησης	Αποστολή μη-κρυπτογραφημένων ευαίσθητων πληροφοριών
Ενδιαμέσου - MitM	Ελλιπής κρυπτογράφηση ευαίσθητων δεδομένων
Μη-εξουσιοδοτημένη πρόσβαση	Ανεπαρκής έλεγχος πρόσβασης

Σχήμα 3.7 – Συσχέτιση επιθέσεων με ευπάθειες του πρωτοκόλλου IEC/104

Το τελικό στάδιο των δοκιμών ακολουθείται από μια αξιολόγηση του κινδύνου των τεσσάρων τύπων επιθέσεων(βλ. Σχήμα 3.7) που αναφέρθηκαν. Το μοντέλο αξιολόγησης που προκρίνεται από τους ερευνητές ακολουθεί τον παρακάτω μαθηματικό τύπο:

Κίνδυνος = (αξία πόρων × προτεραιότητα συμβάντος × αξιοπιστία συμβάντος) /25

Ως πόρους για το παραπάνω παράδειγμα θεωρούμε τις δύο συσκευές (PLC & MTU) και αξία τους προσδιορίζεται σε ένα εύρος τιμών με μέγιστη τιμή το «5» για το καθένα. Η αξία κάθε πόρου προφανώς αξιολογείται για κάθε εφαρμογή διαφορετικά και σύμφωνα με την σημασία τους για το εκάστοτε σύστημα SCADA. Η προτεραιότητα συμβάντος (επίσης από 0 έως 5) καθορίζεται από την αναμενόμενη επίδραση της απειλής, ενώ η αξιοπιστία συμβάντος (κυμαίνεται από 0 έως 10) καθορίζεται από την πιθανότητα εμφάνισης της απειλής. Σύμφωνα λοιπόν με το παραπάνω μοντέλο ανάλυσης ρίσκου, η αξιολόγηση έδειξε ότι οι επιθέσεις μη εξουσιοδοτημένης πρόσβασης και άρνησης υπηρεσίας εισάγουν τα υψηλότερα επίπεδα κινδύνου συγκριτικά με κυβερνοαπειλές ενδιαμέσου ή ανάλυσης κίνησης. Αυτό επιβεβαιώνει την εκτίμηση ότι η πρόσβαση και η διακοπή αποτελούν τους υψηλότερους κινδύνους για κρίσιμες SCADA υποδομές.

3.4.2. Ενδιάμεσος εισβολέας και αναπαραγωγή δεδομένων

Οι επιθέσεις ενδιαμέσου Man-in-the-Middle, γενικότερα μπορεί να αποδειχθούν περισσότερο σοβαρές στα βιομηχανικά περιβάλλοντα, ανάλογα με τις επιδιώξεις του κακόβουλου εισβολέα. Τέτοια παραδείγματα έχουμε όταν τα διάφορα μηνύματα που διαβάζονται από τα κέντρα ελέγχου δεν μεταβιβάζονται με σωστό περιεχόμενο ή στον επιθυμητό χρόνο. Όταν κρίσιμα δεδομένα είναι παραποιημένα και οι διάφορες εντολές δεν παραδίδονται έγκαιρα ή καθόλου, τότε οι δυνητικές συνέπειες για το ηλεκτρικό σύστημα μπορεί να γίνουν εξαιρετικά απρόβλεπτες και καταστροφικές. Η εισβολή κάποιου στην IEC/104 παίζοντας τον ρόλο του διαμεσολαβητή των μηνυμάτων που ανταλλάσσονται μπορεί να έχει πολλές διαφορετικές εκφάνσεις, λειτουργίες και άρα διαφορετική επικινδυνότητα για το σύστημα. Η πιο απλή εφαρμογή επίθεσης ενδιαμέσου εισβολέα είναι με τις γνωστές **επιθέσεις επανάληψης πακέτων (replay attacks).** Αρχικά ο ενδιάμεσος εισβολές υλοποιεί καταγραφή των αυθεντικών πακέτων και στη συνέχεια επαναλαμβάνει τα δεδομένα είτε αυτούσια είτε τροποποιημένα. Στην πρώτη περίπτωση, οι αναγνώσεις που αποστέλλονται στο σταθμό παρακολούθησης ή οι εντολές προς το σύστημα ελέγχου πολλαπλασιάζονται. Αυτό μπορεί να προκαλέσει ισχυρές διαταραχές σε επιφορτισμένο δίκτυο και ίσως φυσικές ζημιές ως επακόλουθο. Αυτές οι επιθέσεις συνήθως πραγματοποιούνται από άπειρους επιτιθέμενους ή άτομα που πειραματίζονται χωρίς να κατανοούν πλήρως το σύστημα και συνεπώς το επίπεδο απειλής θεωρείται μέτριο. Από την άλλη, αντίστοιχες επιθέσεις ενδιαμέσου εισβολέα οι οποίες τροποποιούν τα δεδομένα που αναμεταδίδουν είναι πολύ πιο ανησυχητικές. Τις κατηγοριοποιούμε σε **επιθέσεις έγχυσης δεδομένων (injection attacks)** και - σύμφωνα με το σχετικό ερευνητικό άρθρο [69] – στοχεύουν στην τροποποίηση παραμέτρων ενός πακέτου πριν φτάσει στον προορισμό του. Παρακάτω παραθέτουμε σχετικά πειράματα επιθέσεων εστιάζοντας εμφανώς στην δεύτερη περίπτωση ως επικινδυνότερη.

Α. Επίθεση Απλής Επανάληψης

Στο πρώτο πείραμα που μελετήσαμε υλοποιούνται δοκιμαστικές επιθέσεις επανάληψης πακέτων σε μια απλή πειραματική διάταξη υποσταθμού, όπου στο κοινό IEC/104 δίκτυο είναι συνδεδεμένοι οι εξής: δύο λογισμικά αναπαράστασης των master και slave και η πλατφόρμα επιθέσεων Kali Linux. Όλα τα πακέτα

καταγράφονται από εξομοιωτές λογισμικού. Όπως αναφέραμε προηγουμένως πρόκειται για ένα απλό είδος επίθεσης, επομένως είναι πιθανότερο να πραγματοποιηθεί από έναν άπειρο ή μη εξοικειωμένο με το σύστημα επιτιθέμενο. Ο σκοπός της επίθεσης είναι να «ανακατέψει» το δίκτυο, καταγράφοντας 104-πακέτα και αναπαράγοντάς τα εναντίον του προκαθορισμένου στόχου. Ο εξομοιωτής της master-συσκευής επιτρέπει την ανάκτηση και προβολή δεδομένων από το σύστημα υποσταθμού. Η slave-συσκευή προσομοιώνεται χρησιμοποιώντας τον προσομοιωτή πακέτων WinPP104, ο οποίος δημιουργεί πακέτα με μετρούμενες τιμές από το υποτιθέμενο πεδίο, στέλνει απαντήσεις προς τον master και επαληθεύει την λήψη τους. Τέλος, η πλατφόρμα επίθεσης-Kali είναι αυτή από όπου επαναλαμβάνονται τα πακέτα το οποία παρατηρούνται από τους ερευνητές μέσω ενός IDS Snort (σχετικά με αυτό θα δούμε περισσότερα στο επόμενο κεφάλαιο).

Το αποτέλεσμα της επίθεσης ωστόσο δεν είχε τόσο μεγάλο αντίκτυπο στο σύστημα διότι τα επαναλαμβανόμενα πακέτα απορρίπτονται από την TCP/IP στοίβα και δεν γίνονται αποδεκτά στο επίπεδο της εφαρμογής. Αυτό συμβαίνει διότι οι τιμές SYN και ACK στα πακέτα, δεν τροποποιήθηκαν πριν από την επαναληπτική αναπαραγωγή τους. Συνεπώς, τα επαναληφθέντα πακέτα δεν θα γίνονται αποδεκτά στο επίπεδο εφαρμογής των περισσότερων εφαρμογών και η επίθεση δεν θα επηρεάζει απευθείας τη λειτουργία του συστήματος αυτοματισμού. Παρ' όλα αυτά, η επίθεση πιθανότατα δεν θα ανιχνεύεται από τους τείχους προστασίας του δικτύου, καθώς θα φαίνεται ως μια έγκυρη κίνηση πακέτων. Σε ένα δίκτυο χαμηλού εύρους ζώνης ή ένα δίκτυο που έχει μεγάλο φορτίο, μια τέτοια επίθεση μπορεί να προκαλέσει ακόμη πτώση του δικτύου αυξάνοντας την πιθανότητα αποσυνδέσεων συσκευών λόγω χρονικού περιορισμού (time-out).

Τελικά, η επίθεση μπορεί να μην έχει μεγάλο βαθμό επικινδυνότητας σε κάποιες εφαρμογές αλλά σε κάθε περίπτωση **η στρατηγική ασφάλειας θα πρέπει να ανιχνεύει την κακόβουλη δραστηριότητα** που εξετάστηκε παραπάνω.

Β. Επίθεση με αναπαραγωγή τροποποιημένων δεδομένων

Στην ίδια διάταξη **οι επόμενες MitM επιθέσεις** δοκίμασαν να τροποποιήσουν τα επιστρεπτέα πακέτα, **πλαστογραφώντας την αιτία μετάδοσης του μηνύματος (πεδίο CoT).** Η τιμή του CoT χρησιμοποιείται ουσιαστικά για να κατευθύνει το ASDU στο σωστό πρόγραμμα ή επεξεργασία. Για τους σκοπούς αυτού του πειράματος, ο προσομοιωτής slave RTU έχει ειδικά διαμορφωθεί ώστε να μεταδίδει αυθόρμητα πακέτα τύπου ID = 30, με χρονικές ετικέτες για κάθε τριάντα δευτερόλεπτα. Όταν ο Snort-παρακολουθητής της κίνησης δικτύου ανιχνεύσει ένα κατάλληλο πακέτο, το αρχικό πακέτο θα πεταχτεί από τον ενδιάμεσο εισβολέας ο οποίος ένα νέο με τροποποιημένο CoT. Κατά την διεξαγωγή της δοκιμής, ο επιτιθέμενος κατάφερε επιτυχώς να τροποποιήσει την τιμή CoT από “3” σε “42”, όπως φάνηκε από τις καταγραφές του Snort. Εδώ πρέπει να επισημανθεί ότι, όταν **το Snort** ανίχνευσε τα εν λόγω πακέτα, **ενεργοποιήσει ένα συναγερμό για το "Ύποπτη Τιμή Πεδίου CoT"**, λόγω των κανόνων Snort που είχαν ήδη αναπτυχθεί από τους ερευνητές.

Στην συνέχεια επιχειρήθηκε η τροποποίηση πληροφοριών εντός του ASDU. Στο νέο πείραμα, προσομοιώνεται ένα σύστημα διανομής ηλεκτρικής ενέργειας και το πειραματικό σενάριο περιλαμβάνει μια I/O θύρα ενός RTU, η οποία ενεργοποιείται ή απενεργοποιείται σε τακτά διαστήματα για τους δοκιμαστικούς σκοπούς. Έτσι επιτυγχάνεται η αναπαράσταση των επικοινωνιών που μπορεί να συμβούν σε μια πραγματική κατάσταση για κάποιο ηλεκτρικό σφάλμα στο φυσικό ηλεκτρικό σύστημα. Τότε, θα μεταδοθεί ένα μήνυμα από τη θέση της βλάβης στον αντίστοιχο διακομιστή SCADA, ο οποίος με την σειρά του θα υποδείξει στον SCADA-

πελάτη ότι έχει ληφθεί ένα σήμα βλάβης. Ο στόχος αυτής της επίθεσης ήταν να παρεμβληθεί ο επιτιθέμενος σε μια αποστολή τιμής "1" (ένδειξη βλάβης) επιστρέφοντας μια τιμή "0" (όχι σφάλμα) από τον διακομιστή. Δηλαδή, επιχειρεί να κύψει την πραγματική κατάσταση του φυσικού συστήματος από τους χρήστες στο κέντρο ελέγχου.

Σε επίπεδο πρωτοκόλλου, όλα αυτά τα δεδομένα αποθηκεύονται εντός του στοιχείου πληροφοριών ενώ τα πακέτα ASDU μπορεί να έχουν μηδέν ή περισσότερα αντικείμενα πληροφοριών ανάλογα με τον τύπο των δεδομένων που μεταφέρουν. Για να αναγνωριστεί το σωστό στοιχείο πληροφοριών απαιτείται μια βαθιά κατανόηση της δικτυακής διαμόρφωσης, όπως αυτή παρουσιάστηκε στο 2^{ο} κεφάλαιο και την ανάλυσή μας για το IEC/104. Κάποιος άπειρος επιτιθέμενος για να αποκτήσει τέτοιες γνώσεις οφείλει να χρησιμοποιήσει πολλαπλές καταγραφές πακέτων σε όλο το δίκτυο, για να τις αναλύσει σε βάθος πριν διεξάγει επιθέσεις. Αυτό οπωσδήποτε απαιτεί χρόνο και δεξιότητες ώστε ο εισβολές να παραμείνει ανενόχλητος για μεγάλο χρονικό διάστημα από πιθανούς εγκατεστημένους μηχανισμούς ασφαλείας.

Η πρώτη φάση της επίθεσης είναι να πραγματοποιηθεί ARP-poisoning κατά δύο στόχων, της πύλης «PRECYSE CONTROL» και του διακομιστή SCADA. Χρησιμοποιείται και εδώ η τεχνική που συναντήσαμε σε προηγούμενα πειράματα ώστε επιτιθέμενος να γίνει «ενδιάμεσος εισβολές» στην επικοινωνία των συσκευών της δοκιμής. Στην επόμενη φάση παρακολουθούνται ASDU τύπου «M_SP_TB_1» που περιέχουν ένα στοιχείο πληροφοριών με το πεδίο SPI (SIQ) να είναι ρυθμισμένο σε “1”. Μόλις βρεθεί ένα τέτοιο ASDU, το πακέτο θα απορριφθεί και θα σταλεί ένα νέο πακέτο, με την τιμή SPI ρυθμισμένη σε “0”. Αποτέλεσμα αυτού είναι ότι τα κέντρα ελέγχου θα βλέπουν μόνο πακέτα με την τιμή SPI να είναι μηδέν. Οι χειριστές του συστήματος θα βλέπουν για παράδειγμα κάποιον διακόπτη υψηλής τάσης απενεργοποιημένο ενώ συμβαίνει το αντίθετο. Αυτό μπορεί να τους οδηγήσει στην ενεργοποίηση του εφεδρικού κυκλώματος, με αποτέλεσμα να δημιουργηθεί μια πιθανή κακόβουλη φυσική κατάσταση του δικτύου ηλεκτρικής ενέργειας.

3.5. Κυβερνοεπιθέσεις στο IEC 61850

Με την ενσωμάτωση έξυπνων ηλεκτρονικών συσκευών (IEDs) στα σύγχρονα Συστήματα Αυτοματισμού Υποσταθμών, η βιβλιογραφία ασχολείται ολοένα και περισσότερο με τα ζητήματα κυβερνοασφάλειας του συστήματος επικοινωνίας, των συσκευών που το απαρτίζουν και των πρωτοκόλλων επικοινωνίας που χρησιμοποιεί. Για το IEC 61850, ως το πρωτόκολλο που χρησιμοποιείται κατά κόρον στους υποσταθμούς, υπάρχουν πολλοί τύποι κυβερνοεπιθέσεων που μπορούν να χρησιμοποιηθούν για να διαταράξουν τη λειτουργία του ευφυούς δικτύου που έχει εγκατασταθεί. Αρχικά θα αναφερθούμε σε πιθανές επιθέσεις για συστήματα που βασίζονται στο IEC 61850 οι οποίες ταξινομούνται κυρίως σε δύο κατηγορίες: (α.) επιθέσεις στο δίκτυο επικοινωνίας και (β.) επιθέσεις στα μηνύματα του πρωτοκόλλου. Στην συνέχεια μελετάμε κυβερνοεπιθέσεις που εκμεταλλεύονται τις αδυναμίες των IED-συσκευών του υποσταθμού και του πρωτοκόλλου IEC 61850 με έμφαση στις επιθέσεις DoS και MitM. Τέλος, θα αναφερθούμε σε πειραματικές δοκιμές κυβερνοεπιθέσεων σε εφαρμογή συστήματος φωτοβολταϊκών.

3.5.1. Ανάλυση επιθέσεων στο πρωτόκολλο IEC 61850

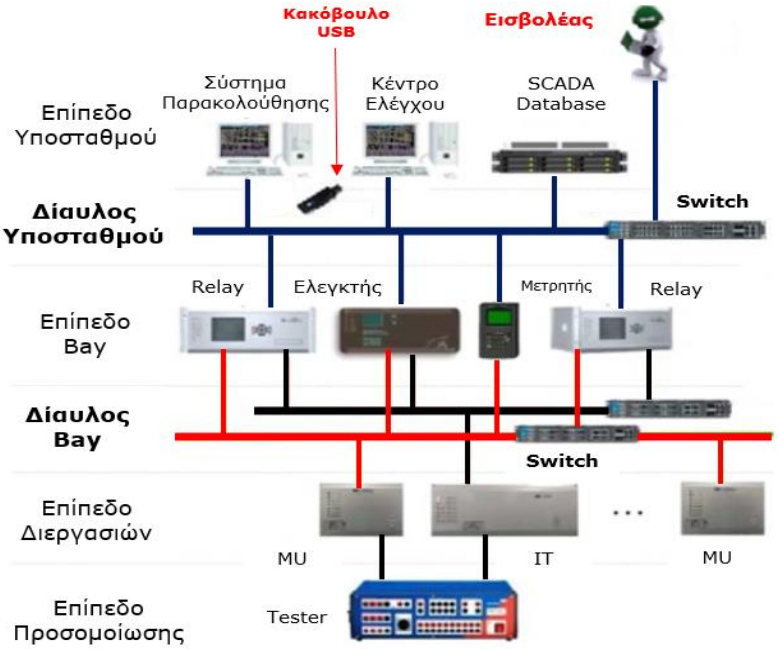
Η βαθιά εξάρτηση των «έξυπνων» δικτύων στους υποσταθμούς από τις έξυπνες συσκευές καθιστά την ασφάλειά τους εξαιρετικά κρίσιμη. Όπως είδαμε και για τα προηγούμενα πρωτόκολλα επικοινωνίας, έτσι και για το IEC 61850 οι κυβερνοεπιθέσεις μπορεί να προκαλέσουν σημαντικές τεχνικές και οικονομικές ζημιές στο φυσικό σύστημα. Ως πρώτο βήμα για την αντιμετώπιση πιθανών

κυβερνοαπειλών είναι σημαντικό να κατηγοριοποιήσουμε τις επιθέσεις στην επικοινωνία των υποσταθμών με βάση την στόχευση που έχουν. Ο παρακάτω πίνακας παρουσιάζει συχνές και σημαντικές απειλές σε δύο κατηγορίες, εκείνες που επιτίθονται στο δίκτυο και τις έξυπνες συσκευές και εκείνες που εκμεταλλεύονται τα μηνύματα του πρωτοκόλλου επικοινωνίας.

Επιθέσεις	Τύπος Επίθεσης	Περιεχόμενο Επίθεσης	Επίπτωση στο ΣΑΥ
Επιθέσεις στο δίκτυο - IEC 61850	Μη εξουσιοδοτημένη πρόσβαση	Επιτρέπει στον εισβολέα να έχει πρόσβαση σε κάποια IED	Η IED έχει επεξεργαστεί ώστε να δίνει λανθασμένες εντολές, να έχει λάθος προεπιλεγμένες ρυθμίσεις ή να δίνει πρόσβαση σε ευαίσθητα δεδομένα
	Σκαλοπάτι (Stepping Stone)	Μια συσκευή δέχεται επίθεση από μια άλλη IED	Αφού ο επιτιθέμενος απέκτησε πρόσβαση σε μια συσκευή μπορεί να υλοποιεί επιθέσεις και στις υπόλοιπες εντός του ΣΑΥ
	Δύσμορφα πακέτα (malformed packets)	Αποστολή δύσμορφων πακέτων σε IED	Αποτυχία επικοινωνίας μεταξύ των IED
	Άρνηση Υπηρεσίας (DoS)	Κατακλύζει την IED-στόχο με ψευδή μηνύματα	Κατανάλωση εύρους ζώνης και αύξηση του ρυθμού χρήσης της CPU
	Εξαπάτηση με ARP πακέτα	Παραπλανά τον παραλήπτη ώστε να πιστεύει ότι λαμβάνει μηνύματα από αξιόπιστο αποστολέα	Η IED θα επικοινωνεί με τον υπολογιστή του επιτιθέμενου αντί για το SCADA
	Ενδιαμέσου εισβολέα (MitM)	Ανακατευθύνει την επικοινωνία μεταξύ IED και SCADA σε ένα κακόβουλο υπολογιστή	Απομακρυσμένη αποστολή κακόβουλων εντολών ελέγχου και αλλαγή ρυθμίσεων προστασίας των IED
	Παρεμβολή στην ρύθμιση παραμέτρων (Configuration Tampering)	Τροποποιεί το αρχείο περιγραφής (CID) που έχει ρυθμιστεί στο IED	Διαταραχή των πρωτοκόλλων επικοινωνίας και του συστήματος παρακολούθησης
Επιθέσεις στα μηνύματα - IEC 61850	Τροποποίηση μηνυμάτων	Τροποποιεί το περιεχόμενο των καταγεγραμμένων πακέτων του δικτύου	Ο εισβολέας αποκτά πρόσβαση στις IED και πράττει κακόβουλες ενέργειες
	Άρνηση υπηρεσιών μηνυμάτων	Αποστολή μεγάλου αριθμού πακέτων μηνυμάτων στο δίκτυο	Αποτυχία των IED να ανταποκριθούν σε εξουσιοδοτημένους χρήστες
	Επανάληψη μηνυμάτων	Καταγράφει τα πακέτα δικτύου που μεταδίδονται μεταξύ των κόμβων και τα επαναλαμβάνει χωρίς αλλαγές	Απενεργοποιεί (εσφαλμένα) διακόπτες και μπορεί να οδηγήσει σε καταστροφικές καταστάσεις

Σχήμα 3.8 – Κυβερνοεπιθέσεις σε δίκτυα IEC 61850

Για τις παραπάνω επιθέσεις πρέπει να σημειωθεί ότι υπάρχουν δύο μέθοδοι - βάσει δύο διαφορετικών τοποθεσιών - για να εκτελεστούν αυτές οι επιθέσεις. Η απευθείας παρέμβαση στο IED από το εσωτερικό του τοπικού δικτύου (LAN) ή μέσω δικτύου ευρείας περιοχής (WAN). Σε αυτές τις δύο περιπτώσεις, ένας κακόβουλος χρήστης του δίκτυο μπορεί να επιχειρήσει αυτοβούλως επιθέσεις ή ο ίδιος να χρησιμοποιηθεί ως «γέφυρα» από έναν εξωτερικό εισβολέα. Στο σχήμα που ακολουθεί απεικονίζονται **σενάρια εισβολής στην δικτυακή τοπολογία ενός έξυπνου υποσταθμού**.



Σχήμα 3.9 – Τρόποι εισβολής σε τυπική τοπολογία ΣΑΥ

Υπάρχουν τρία πιθανά σενάρια επίθεσης (βλ. συνδέσεις με κόκκινο χρώμα σχήματος 3.9) που μπορούν να εφαρμοστούν σε ένα τοπικό δίκτυο IEC 61850 και είναι τα εξής:

1. Μη εξουσιοδοτημένη πρόσβαση μέσω σύνδεσης σε εγκατεστημένο δρομολογητή του δικτύου ή με άμεση φυσική σύνδεση σε κάποια έξυπνη-IED συσκευή.
2. Κακόβουλος USB-driver σε κεντρικό υπολογιστή παρακολούθησης και ελέγχου του υποσταθμού.
3. Ένας πελάτης/εισβολέας δημιουργεί μια γέφυρα και συνδέεται στις υπηρεσίες του εγκατεστημένου δικτύου, είτε σε επίπεδο υποσταθμού είτε σε επίπεδο bay.

Τα πρώτα δύο σενάρια εισβολών μπορούν να αποτραπούν με τη χρήση παραδοσιακών μεθόδων προστασίας, όπως κάμερες ασφαλείας, «τείχη προστασίας» ή λογισμικά ασφαλείας. Το τρίτο σενάριο ωστόσο αποτελεί την μεγαλύτερη πρόκληση και αντικείμενο της έρευνας, καθώς σε αυτήν την περίπτωση η χρησιμοποιούμενη συσκευή εισβολής έχει εξουσιοδοτηθεί ώστε να αποκτήσει πρόσβαση στα δεδομένα του δικτύου επικοινωνίας του υποσταθμού.

Οι τύποι επιθέσεων που αναφέρθηκαν προηγουμένως έχουν τις περισσότερες φορές σοβαρές επιπτώσεις στο σύστημα αυτοματισμού και ως εκ τούτου επιφέρουν σοβαρές ζημιές στο φυσικό ηλεκτρικό σύστημα του υποσταθμού. Οι πιο **συνηθισμένες επιπτώσεις** που προκαλούνται από τις διάφορες κυβερνοεπιθέσεις αναφέρονται στην συνέχεια:

- Άρνηση υπηρεσιών απ' το κεντρικό σύστημα ελέγχου.
- Διακοπή επικοινωνίας ηλεκτρικών διατάξεων προστασίας.
- Διακοπή συστήματος απομακρυσμένης παρακολούθησης.
- Γενική κατάρρευση του δικτύου.
- Γενικός αποκλεισμός της ηλεκτρικής προστασίας.
- Αποτυχία αποκοπής (tripping failure).
- Ανεπιθύμητη λειτουργία ηλεκτρικών διατάξεων προστασίας.
- Εσφαλμένη ανάλυση μετά από γεγονότα πεδίου.

Τα παραπάνω αποτελούν σοβαρό κίνδυνο τόσο για το δίκτυο επικοινωνίας όσο και για το φυσικό σύστημα και την ανθρώπινη ζωή. Δηλαδή, ακόμα κι αν αυτές οι επιθέσεις συμβαίνουν σπάνια σε ένα τοπικό δίκτυο, η επίδρασή τους είναι τόσο σημαντική και πρέπει να λαμβάνεται υπόψη ώστε να εφαρμόζονται ενδεδειγμένοι μηχανισμοί πρόληψης και ασφάλειας. Στην συνέχεια της ενότητας - για δίκτυα IEC 61850 και συστήματα υποσταθμών- θα μελετήσουμε βασικές κυβερνοεπιθέσεις που επιφέρουν κάποιες από της παραπάνω επιπτώσεις.

3.5.2. Απόρριψη Υπηρεσίας - DoS σε Σύστημα Αυτοματισμού Υποσταθμού

Η Απόρριψη Υπηρεσίας (DoS) κατατάσσεται ως μια κυβερνοεπίθεση όπου **οι επιτιθέμενοι εμποδίζουν τους νόμιμους χρήστες ή τη μηχανή μιας υπηρεσίας να έχουν πρόσβαση** σε αυτήν την συγκεκριμένη υπηρεσία. Όπως συναντήσαμε ξανά, η επίθεση αυτή διενεργείται με την συνεχή μετάδοση πολλαπλών πλαστών αιτημάτων προς τον εξυπηρετητή ή την υπηρεσία. Η υπερφόρτωση που δημιουργείται στην στοχευμένη υπηρεσία προκαλεί σημαντικές δυσκολίες στην έγκαιρη ανταπόκριση σε αιτήματα εξουσιοδοτημένων χρηστών, τα οποία τελικά απορρίπτονται από το σύστημα. Μια αναβάθμιση αυτού του τύπου επίθεσης θεωρούνται οι περιπτώσεις όπου οι εισβολείς χρησιμοποιούν περισσότερες μηχανές και συνδέσεις επικοινωνίας για να αυξήσουν την αποτελεσματικότητά τους ή να ελαττώσουν τον χρόνο επιτυχίας της επίθεσης. Ο τύπος αυτός ονομάζεται **Κατανεμημένη Επίθεση Απόρριψης Υπηρεσίας (DDoS)** που συνήθως εγκυμονεί και τους σοβαρότερους κινδύνους για το συστήματα και τα πιθανά συστήματα ανίχνευσης.

Στη βιβλιογραφία [41], [51], [54], [70], [71] έχουν αναφερθεί αρκετές περιπτώσεις επιθέσεων DoS οι οποίες επικεντρώνονται σε υποσταθμούς που χρησιμοποιούν το πρότυπο IEC 61850. Παρακάτω παρουσιάζονται κάποια παραδείγματα:

- **Επιθέσεις DoS σε υπηρεσίες IED:** Οι επιθέσεις DoS σε υπηρεσίες των IED, όπως το Πρωτόκολλο Μεταφοράς Αρχείων (FTP), έχουν ως αποτέλεσμα την πλήρη αδρανοποίηση της επικοινωνίας της έξυπνης συσκευής.
- **Επιθέσεις υπερχείλισης μνήμης με SYN Flood:** Οι γνωστές πλέον επιθέσεις υπερχείλισης είναι τύπου DoS και εκμεταλλεύονται – όπως και στα υπόλοιπα πρωτόκολλα - τις ευπάθειες της TCP υπηρεσίας, τριπλής χειραψίας (SYN, SYN-ACK, ACK). Ο επιτιθέμενος αποστέλλει συναζόμενα πακέτα SYN σε πολλές θύρες ενός εξυπηρετητή χρησιμοποιώντας πλαστές διευθύνσεις IP. Η λαμβάνουσα συσκευή πιστεύει ότι δέχεται νόμιμα αιτήματα σύνδεσης και, συνεπώς, προσπαθεί να απαντήσει σε κάθε αίτημα στέλνοντας πίσω πακέτα SYN-ACK από κάθε στοχευμένη θύρα. Ο κακόβουλος αποστολέας έχοντας πλαστή IP δεν θα επιστρέψει μήνυμα ACK, όμως η λαμβάνουσα συσκευή πριν προλάβει να τερματίσει την σύνδεση λαμβάνει εκ νέου αίτημα SYN προκαλώντας πολλές ταυτόχρονες ανεκπλήρωτες συνδέσεις. Όταν ο αριθμός των ανοικτών

συνδέσεων υπερβαίνει την χωρητικότητα του εξυπηρετητή, αυτός θα αρνηθεί κάθε επόμενη, συμπεριλαμβανομένων των νόμιμων αιτημάτων.

- **Πολλαπλή ρίψη μηνυμάτων:** Εκμεταλλευόμενος τα κοινά μηνύματα GOOSE και SMV του πρωτοκόλλου, ο επιτιθέμενος κατακλύζει τον στόχο με αυτόν τον τύπο μηνυμάτων. Σε αυτό το σενάριο επίθεσης, τα IED αρχίζουν να συμπεριφέρονται ύποπτα λόγω του μεγάλου αριθμού μηνυμάτων που δέχονται, προκαλώντας βλάβη στην κανονική λειτουργία που επιτελούν και προβλήματα διαθεσιμότητας στα δεδομένα.
- **Δηλητηρίαση μηνυμάτων GOOSE:** Μια άλλη μορφή DoS είναι η επίθεση δηλητηρίασης GOOSE μηνυμάτων, όπου τα εξουσιοδοτημένα μηνύματα GOOSE απορρίπτονται από τα στοχευμένα IED, λόγω της εισαγωγής ψευδών μηνυμάτων GOOSE από τους επιτιθέμενους. Οι επιτιθέμενοι για να το επιτύχουν χρησιμοποιούν επιθέσεις πλημμύρας μεγάλου ρυθμού ροής.

Το πείραμα προσομοίωσης που επιλέξαμε να αναφερθούμε [41], αποτελείται από μια διάταξη **τριών ζυγών μεταφοράς** (11kV, 132kV, 22kV) μεταξύ της γεννήτριας και των **δύο επιπέδων μετασχηματισμού τάσης**. Στην είσοδο και την έξοδο κάθε μετασχηματιστή καθώς και στα πειραματικά φορτία υπάρχουν διακόπτες ισχύος που είναι και το αντικείμενο του πειράματος. Οι διακόπτες αυτοί συνδέονται με αντίστοιχα IED έξυπνες συσκευές που βρίσκονται στο bay-επίπεδο του συστήματος του υποσταθμού. Όλες οι συσκευές που προσομοιώνονται επικοινωνούν μεταξύ τους μέσω δρομολογητών όπου εκτός από τις έξυπνες συσκευές, τους προσομοιωτές διακοπτών, μετρητών, κλπ. είναι διασυνδεδεμένοι: ο κεντρικός server του συστήματος, η HMI οθόνη παρακολούθησης και ένας κακόβουλος εισβολέας.

1ο Σενάριο: Ο επιτιθέμενος επιλέγει ως στόχο τον server του δικτύου με τον οποίο μοιράζονται κοινό switch-δρομολογητή. Σε μια τέτοια κατάσταση, εκτελείται μια επίθεση απ' τη θύρα που συνδέεται ο εισβολές, πλημμυρίζοντας τις τις υπόλοιπες με πλαστά δεδομένα. **Η επίθεση αυτή είναι τύπου SYN-flood** και επιτυγχάνεται παραπλανώντας τη διεύθυνση IP προέλευσης και εκμεταλλεύοντας τις υπηρεσίες TCP. Το βασικό εύρημα αυτού του σεναρίου επίθεσης είναι η μεγάλη καθυστέρηση που προκύπτει στο Ethernet δίκτυο, η οποία φτάνει τα 2,5 msec. έως την κατάρρευση του διακομιστή-στόχου. Εάν σκεφτούμε ότι η χρονική απαίτηση ενός GOOSE μηνύματος κυμαίνεται στα 3 – 10 msec. γίνεται αντιληπτή και η επιρροή της επίθεσης στο δίκτυο. Η επίθεση σχεδόν τετραπλασίασε τον αριθμό των πακέτων που λαμβάνει ο server ανά δευτερόλεπτο με αποτέλεσμα την πλήρη κάλυψης της CPU του, σε διάρκεια 1 λεπτού συνεχόμενης ρίψης πακέτων. Η επίθεση **τελικά καταφέρνει να περιορίσει σοβαρά την ικανότητά του server να εγκαθιδρύσει νέες συνδέσεις με νόμιμους πελάτες**, προκαλώντας έτσι κατάσταση άρνησης υπηρεσιών - DoS.

2ο Σενάριο: Εδώ επιχειρείται αντίστοιχη επίθεση σε **νέο καθορισμένο στόχο**, **την κεντρική οθόνη παρακολούθησης κατάστασης** του πειραματικού υποσταθμού. Ο σκοπός της επίθεσης είναι να αποτραπούν οι χρήστες από την εκτέλεση λειτουργιών ελέγχου και παρακολούθησης, λόγω μιας κατάρρευσης του HMI σταθμού. Η συσκευή αυτή καθώς χρησιμοποιεί μικρότερη χωρητικότητα μνήμης για να εκτελέσει τις εργασίες της, φτάνει το μέγιστο της χωρητικότητάς της μετά από 15 λεπτά διεξαγωγής DoS επίθεσης. Η διαφορά στην καθυστέρηση του Ethernet μεταξύ των δύο σεναρίων είναι περίπου 0,7 msec. και η καθυστέρηση αυτή βρίσκεται εντός του αποδεκτού ορίου. Ο λόγος για τη μικρή αύξηση της καθυστέρησης μπορεί να αποδοθεί στο γεγονός ότι ο αριθμός των αιτημάτων που λαμβάνει η σταθμός HMI είναι σημαντικά μικρότερος από αυτόν που λαμβάνει ο

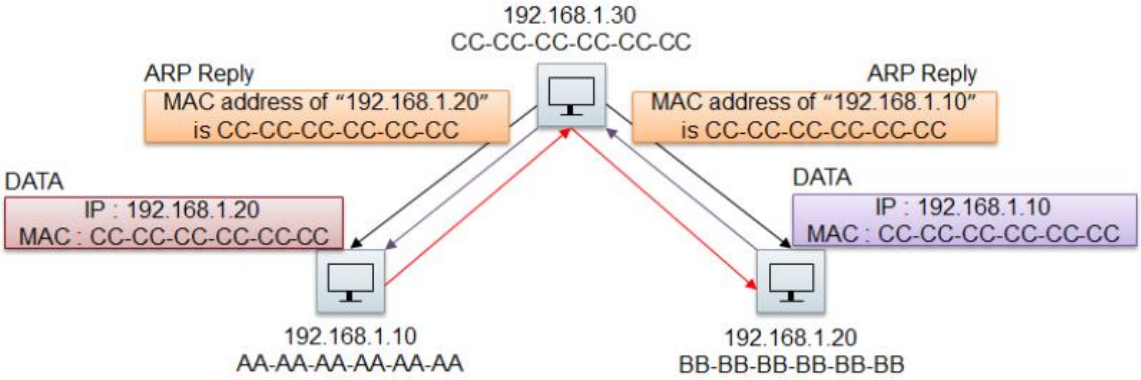
διακομιστής του προηγούμενου σεναρίου. Οι υπόλοιπες IED συσκευές λειτουργούν χωρίς καμία δυσλειτουργία, επομένως οι λειτουργικές συνθήκες είναι σωστές.

3ο Σενάριο: Σε αυτό το σενάριο, πραγματοποιείται μια επίθεση DoS σε δύο IED συσκευές οι οποίες είναι έμμεσα συνδεδεμένες στο δίκτυο μέσω δεύτερου δρομολογητή. Εδώ ο εισβολέας μπορεί να πλαστογραφήσει τα δεδομένα που εισάγονται στα IED, να υπερφορτώσουν τις μονάδες επεξεργασίας της CPU και να καταναλώσουν το διαθέσιμο εύρος ζώνης της σύνδεσης. Τα αποτελέσματα είναι αποθαρρυντικά για το δίκτυο, καθώς οι μνήμες των IED γεμίζουν πλήρως και περνούν σε κατάσταση DoS μετά από μόλις 10 δευτερόλεπτα επίθεσης.

Οι παραπάνω επιθέσεις προσομοίωσης σκοπεύουν να δώσουν μια σαφή εικόνα των κυβερνοαπειλών τύπου DoS στις κρίσιμες συσκευές ενός ΣΑΥ. Τα αποτελέσματα είναι ιδιαίτερα χρήσιμα για μια αρχική κατανόηση των επιπτώσεων στην απόδοση ενός ψηφιακού-έξυπνου υποσταθμού. Μπορούμε να συμπεράνουμε ότι μια επίθεση σε διακομιστή οδηγεί σε μεγαλύτερες καθυστερήσεις σε σύγκριση με μια επίθεση στο HMI ή τα IED του συστήματος. Τα πειράματα έδειξαν επίσης ότι το χρονικό διάστημα μεταξύ των επιθέσεων παίζει σημαντικό ρόλο στις καθυστερήσεις και τη χρήση της CPU στο σύστημα. Δηλαδή ένα γρηγορότερο διάστημα μεταξύ των επιθέσεων θα επιφέρει την μέγιστη χρήση της CPU σε μικρότερο χρόνο. Έτσι **τα βασικά μηνύματα πρωτοκόλλου επικοινωνίας IEC 61850 - GOOSE και SMV - αποτρέπονται από την επιτυχημένη μετάδοσή τους** στον προορισμό λόγω της επίθεσης. Στην συνέχεια διευρύνεται η έρευνα μας για την συμπεριφορά των μηνυμάτων του πρωτοκόλλου απέναντι σε άλλες γνωστές κυβερνοαπειλές.

3.5.3. Επιθέσεις ενδιάμεσου εισβολέα σε επικοινωνία IEC 61850

Σε αυτήν την ενότητα θα μελετήσουμε επιθέσεις ενδιάμεσου εισβολέα σε συστήματα SCADA υποσταθμών και έξυπνες συσκευές ενέργειας. Η βάση των απειλών που θα περιγράφουν είναι επιθέσεις MitM, και θα έχουν ως προκαθορισμένο στόχο συσκευές και συστήματα που χρησιμοποιούν MMS-μηνύματα επικοινωνίας IEC 61850. Στις πειραματικές διαδικασίες υπάρχουν τρεις βασικές υποθέσεις: (α.) τουλάχιστον ένας από τους υπολογιστές στο δίκτυο έχει ήδη παραβιαστεί από έναν επιτιθέμενο, (β.) οι στόχοι των επιθέσεων είναι συνδεδεμένοι στο ίδιο δίκτυο και (γ.) ο επιτιθέμενος μπορεί να παρακολουθεί την κίνηση των δεδομένων και να αναγνωρίζει διευθύνσεις IP και αριθμούς θύρας των στόχων. Το κύριο αντικείμενο των δοκιμών είναι η παραποίηση δεδομένων στο επίπεδο εφαρμογής μέσω διάφορων βοηθητικών τεχνικών επιθέσεων στο επίπεδο σύνδεσης δεδομένων, όπως την δηλητηρίαση με ARP πακέτα.



Σχήμα 3.10 – Δηλητηρίαση με ARP πακέτα

Το **πρωτόκολλο ανάλυσης διευθύνσεων (ARP)**, στο οποίο έχουμε αναφερθεί και σε προηγούμενα MitM παραδείγματα, χρησιμοποιείται για τη μετατροπή των διευθύνσεων IP σε διευθύνσεις MAC. Για να επιτευχθεί η μετατροπή αυτή, αποστέλλεται ένα αίτημα ARP στο LAN και ο χρήστης με τη διεύθυνση IP απαντά με τη διεύθυνση MAC της μέσω μιας απάντησης ARP. Το ARP πρωτόκολλο δεν διαθέτει μηχανισμό αυθεντικοποίησης της αρχικής προέλευσης του μηνύματος και αυτό επιτρέπει την δηλητηρίαση των δύο στόχων με πλαστά πακέτα (σχήμα 3.10). Η διεύθυνση MAC του επιτιθέμενου καταχωρείται ως διεύθυνση IP του θύματος με αποστολή πλαστοπροσωποιημένων απαντήσεων ARP στο LAN. Έτσι, οποιαδήποτε κίνηση προορίζεται για εκείνη την IP διεύθυνση θα αποστέλλεται στον επιτιθέμενο αντί στον στόχο. Ο εισβολέας επαναπροωθεί τα πακέτα στον νόμιμο προορισμό ώστε να εξαπατήσεις το θύμα ότι το μήνυμα παραδόθηκε σωστά. Η παραπάνω τεχνική αποτελεί βασικό στάδιο δημιουργίας κατάστασης ενδιάμεσου εισβολέα στο σύστημα επικοινωνίας.

Όπως είδαμε στην ανάλυση του IEC 61850, το MMS είναι από τις πιο διαδεδομένες υπηρεσίες επικοινωνίας που παρέχει το πρότυπο και βασίζεται πάνω στο πρωτόκολλο IP. Συνεπώς, **η τεχνική του ARP spoofing** που είδαμε προηγουμένως **μπορεί να εκτελεστεί στις MMS επικοινωνίες των συσκευών IEC 61850**, ενώ οι τύποι των MitM επιθέσεων που ενδέχεται να αντιμετωπίσει το σύστημα ποικίλουν. Η παρούσα εργασία δίνει βάση στις τέσσερις πολύ σημαντικές: (α.) «ακρόαση» συνομιλιών, (β.) τροποποίηση μηνυμάτων, (γ.) εισαγωγή πακέτων ή (δ.) επιθέσεις DoS.

1. Όταν επιτευχθεί η τροποποίηση των IP διευθύνσεων και η εισβολή του επιτιθέμενου στην επικοινωνία ως ενδιάμεσος κόμβος, τότε ο εισβολέας μπορεί να συγκεντρώσει χρήσιμες πληροφορίες για τις συσκευές-στόχους που συνομιλούν μεταξύ τους. Η συνομιλία των συσκευών καταγράφεται και **ο επιτιθέμενος μπορεί να παρακολουθεί όλη την κίνηση πακέτων συλλέγοντας και αποκωδικοποιώντας τα μηνύματα MMS** πριν προχωρήσει σε οποιαδήποτε επιπλέον κακόβουλη ενέργεια. Αυτό του επιτρέπει την υλοποίηση επιθέσεων στο επίπεδο εφαρμογής.
2. Στην συνέχεια, **ο επιτιθέμενος έχει την δυνατότητα να τροποποιεί και να μεταδίδει νέα κακόβουλα μηνύματα στον αρχικό προορισμό**. Αυτές οι επιθέσεις τροποποίησης μπορούν να χρησιμοποιηθούν για να κρύψουν ή να παραποιήσουν μετρήσεις σχετικά με τις συσκευές και, κατά συνέπεια, το υποκείμενο φυσικό σύστημα ή για να αποστείλουν μη επιθυμητές εντολές στις συσκευές. Μετά την τροποποίηση, θα πρέπει να υπολογιστούν εκ νέου τα πεδία αθροίσματος ελέγχου του TCP (checksum) στο μήνυμα πριν εκείνα προωθηθούν. Εάν η μήκος του μηνύματος αλλάξει, θα πρέπει επίσης να προσαρμοστούν τα πεδία αναγνώρισης ακολουθίας (sequence) και επιβεβαίωσης (acknowledgement) των μηνυμάτων για να διατηρηθεί η «ομαλή» επικοινωνία μεταξύ των συσκευών.
3. **Μετά την ολοκλήρωση της εισαγωγής κακόβουλων μηνυμάτων** στην επικοινωνία, ο επιτιθέμενος θα πρέπει να διαχειριστεί τα εξής επακόλουθα. Πρώτον, οφείλει να απορρίψει ή να τροποποιήσει πιθανές απαντήσεις του στόχου λόγω των εισαχθέντων μηνυμάτων προς αυτόν. Δεύτερον, οποιαδήποτε πληροφορία αναγνώρισης ακολουθίας θα πρέπει να διορθωθεί κατά τη διάρκεια της υπόλοιπης όπως τα πεδία αναγνώρισης ακολουθίας στην επικεφαλίδα TCP και το πεδίο αναγνώρισης invoke-ID στα μηνύματα MMS. Χωρίς αυτήν την προσαρμογή, η επικοινωνία μεταξύ των συσκευών θα τερματιστεί.
4. Υπάρχουν **παραδείγματα επιθέσεων «Άρνησης Υπηρεσίας – DoS» που μπορούν να εφαρμοστούν σε μια κατάσταση MitM**. Για παράδειγμα, ο εισβολέας μπορεί να παραλείψει την επαναποστολή πλαστών ή μη πακέτων,

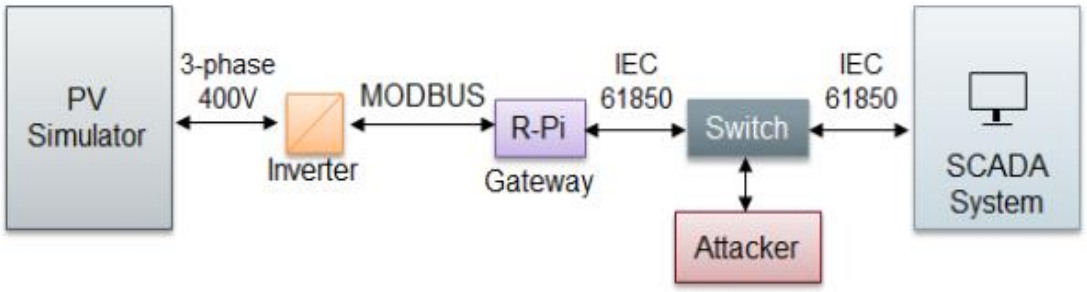
αποκλείοντας αποτελεσματικά όλα τα μηνύματα προς τον αρχικό προορισμό. Θα μπορούσε ακόμη να τροποποιήσει όλα τα δεδομένα στα μηνύματα, ώστε να αχρηστευτούν καθολικά οι συσκευές-στόχοι. Τέλος, ο επιτιθέμενος μπορεί απλώς να εισάγει εντολές τερματισμού για όλες τις συσκευές.

3.5.4. Επίθεση ενδιάμεσου εισβολέα σε Σύστημα Φωτοβολταϊκών

Η διεξαγωγή δοκιμαστικών κυβερνοεπιθέσεων, εκτός από την ανίχνευση βασικών αδυναμιών της εγκατεστημένης επικοινωνίας, έχουν ιδιαίτερη σημασία για την κατανόηση των δυνητικών επιπτώσεων στο φυσικό ηλεκτρικό σύστημα. Μια ακόμα ενδιαφέρουσα περίπτωση δοκιμών, για να εξετάσει αυτές τις επιπτώσεις, υλοποιείται σε ένα πειραματικό περιβάλλον που προσομοιώνει ένα φωτοβολταϊκό πάρκο [43]. Το σύστημα αυτό περιλαμβάνει αντιστροφείς/ρυθμιστές τάσης (inverters) και θα μπορούσε να εφαρμοστεί στα πλαίσια μιας εφαρμογής κατανεμημένων πηγών ενέργειας (DERs). Το δίκτυο επικοινωνίας της πειραματικής διάταξης **βασίζεται στο πρότυπο IEC 61850 και δοκιμάζεται απέναντι σε πειράματα επιθέσεων τύπου MitM.**

Μια τυπική εφαρμογή SCADA σε μονάδες DER υλοποιείται συνήθως για σκοπούς βέλτιστης παροχής ισχύος. Αυτό είναι απαραίτητο σε περιπτώσεις που η παραγωγή ενέργειας είναι σημαντικά υψηλότερη ή το φορτίο ισχύος είναι σημαντικά χαμηλότερο από τον αρχικό σχεδιασμό. Για την επίτευξη αυτής της ρύθμισης ισχύος χρησιμοποιούνται συνήθως ρυθμιστές ισχύος Φ/Β (PV Inverter). Ο inverter πρόκειται για μια έξυπνη ηλεκτρονική συσκευή ισχύος που μπορεί να μετατρέπει DC σε AC τάση. Ανιχνεύοντας τα μέγιστα επιτρεπτά όρια ισχύος (MPPT), ρυθμίζει αναλόγως την ισχύ εξόδου από το ηλιακό πάνελ. Οι συσκευές αυτές δηλαδή μπορούν θα θεωρηθούν τμήμα του αυτόματου ελέγχου ενός κατανεμημένου δικτύου ενέργειας, όπως το σύστημα Φ/Β στο εν λόγω πείραμα.

Στο επίπεδο της επικοινωνίας του πειραματικού συστήματος, ο PV Inverter ανταλλάσσει μηνύματα με το κεντρικό SCADA μέσω επικοινωνίας IEC 61850. Με την βοήθεια ενός R-Pi (βλ. σχήμα 3.11), το πρωτόκολλο IEC 61850 που χρησιμοποιεί το SCADA μεταφράζεται σε Modbus ώστε να επιτελεστεί η επικοινωνία με τον ρυθμιστή-αντιστροφέα.



Σχήμα 3.11 – Εργαστηριακή διάταξη εφαρμογής SCADA σε σύστημα Φ/Β

Για την πειραματική υλοποίηση της παραπάνω διαδικασίας χρησιμοποιείται το πρόγραμμα Ettercap μαζί με ένα προσαρμοσμένο πρόσθετο που έχει σχεδιαστεί για συγκεκριμένες επιθέσεις εναντίων επικοινωνιών MMS του πρωτοκόλλου IEC 61850. Το πρόσθετο εργαλείο αφού εφαρμόσει τις επιθέσεις που αναφέρθηκαν μπορεί να αποκωδικοποιήσει τα πακέτα MMS χρησιμοποιώντας κανόνες κωδικοποίησης ASN.1 (Abstract Syntax Notation One) και Basic Encoding Rules (BER) για να αντλήσει

λεπτομερείς πληροφορίες από τους στόχους. Μπορεί επίσης να τροποποιεί μηνύματα πριν τα προωθήσει, να απορρίπτει πακέτα ή να εισάγει πλαστά δεδομένα.

Για το πείραμα αρχικά ισχύει η προϋπόθεση ότι κάποιος υπολογιστής, ο οποίος είναι συνδεδεμένος στο τοπικό δίκτυο, έχει παραβιαστεί και εντοπίσει τις διευθύνσεις IP του PV Inverter (10..111) και του κεντρικού SCADA ελεγκτή (10..121). Έτσι ο κακόβουλος υπολογιστής ικανοποιεί τις συνθήκες που παρουσιάστηκαν στο 3.5.3 και φέρνει το σύστημα σε κατάσταση MITM. Η διπλανή εικόνα δείχνει τις **καταγραφές των πακέτων** που προέκυψαν από το Wireshark **στην πλευρά του SCADA-πελάτη**. Τα μηνύματα της συνομιλίας που απέσπασε ο εισβολέας περιλαμβάνουν πληροφορίες "αριθμός ακολουθίας", “διεύθυνση IP αποστολέα" και " διεύθυνση IP προορισμού", πρωτόκολλο μεταφοράς, μέγεθος πακέτου και μια σύντομη περιγραφή για το πακέτο. Τα πρώτα επτά πακέτα της καταγραφής είναι πακέτα αρχικοποίησης για μια νέα σύνδεση MMS όπου ο χειριστής έκανε επτά αιτήματα επιβεβαίωσης και έλαβε επτά απαντήσεις. Τα επόμενα καταγεγραμμένα μηνύματα ακολουθούν την εξής αλληλουχία ενεργειών:

No.	Source	Destination	Protocol	Length	Info
505	10..121	10..111	TCP	66	49481→102 [SYN] Seq=0 Win=8192 L
506	10..111	10..121	TCP	66	102→49481 [SYN, ACK] Seq=0 Ack=1
507	10..121	10..111	TCP	54	49481→102 [ACK] Seq=1 Ack=1 Win=
508	10..121	10..111	COTP	76	CR TPDU src-ref: 0x0002 dst-ref:
509	10..111	10..121	COTP	76	CC TPDU src-ref: 0x0002 dst-ref:
510	10..121	10..111	MMS	245	initiate-RequestPDU
511	10..111	10..121	MMS	201	initiate-ResponsePDU
526	10..121	10..111	TCP	54	49481→102 [ACK] Seq=214 Ack=170
1060	10..121	10..111	MMS	133	confirmed-RequestPDU
1061	10..111	10..121	MMS	94	confirmed-ResponsePDU
1062	10..121	10..111	MMS	146	confirmed-RequestPDU
1063	10..111	10..121	MMS	83	confirmed-ResponsePDU
1082	10..121	10..111	TCP	54	49481→102 [ACK] Seq=385 Ack=239
1335	10..121	10..111	MMS	139	confirmed-RequestPDU
1336	10..111	10..121	MMS	90	confirmed-ResponsePDU
1346	10..121	10..111	TCP	54	49481→102 [ACK] Seq=470 Ack=275
1699	10..121	10..111	MMS	133	confirmed-RequestPDU
1700	10..111	10..121	MMS	94	confirmed-ResponsePDU
1701	10..121	10..111	MMS	146	confirmed-RequestPDU
1703	10..111	10..121	MMS	83	confirmed-ResponsePDU
1713	10..121	10..111	TCP	54	49481→102 [ACK] Seq=641 Ack=344
1986	10..121	10..111	MMS	139	confirmed-RequestPDU
1987	10..111	10..121	MMS	90	confirmed-ResponsePDU
1999	10..121	10..111	TCP	54	49481→102 [ACK] Seq=726 Ack=380
2806	10..121	10..111	MMS	139	confirmed-RequestPDU
2807	10..111	10..121	MMS	90	confirmed-ResponsePDU
2822	10..121	10..111	TCP	54	49481→102 [ACK] Seq=811 Ack=416

- Το πρώτο επιβεβαιωμένο αίτημα (#1060) είναι ένα το 'getVariableAccessAttributes' που ζητά την λήψη χαρακτηριστικών για συγκεκριμένα δεδομένα, ενώ το δεύτερο (#1062) είναι ένα αίτημα εγγραφής για να αλλάξει την τιμή του 'MaxWLim' σε «100». Η δεύτερη εντολή πρακτικά ορίζει τον περιορισμό ισχύος του inverter στο 100%. Το αίτημα ανάγνωσης (#1335) επιβεβαιώνει τη τιμή του 'MaxWLim' όπως ορίστηκε από το προηγούμενο αίτημα εγγραφής (100%).
- Στην συνέχεια, ένα αίτημα εγγραφής (#1701) αλλάζει την τιμή του 'MaxWLim' σε «60», δηλαδή ορίζει τον μέγιστο περιορισμό ισχύος στο 60% της πιθανής παραγωγής ισχύος. Ο χειριστής επίσης επιβεβαίωσε την τιμή αυτή στέλνοντας ένα αίτημα ανάγνωσης (#1986).
- Από το αίτημα ανάγνωσης (#2806), ο περιορισμός ισχύος φαίνεται να έχει αλλάξει σε «10». Ωστόσο, δεν έχει προηγηθεί κανένα αίτημα εγγραφής μεταξύ των δύο αιτημάτων ανάγνωσης (#1986 και #2806). Αυτό σημαίνει ότι χωρίς καμία ενέργεια από τον χειριστή, ο περιορισμός ισχύος έχει αλλάξει σε 10%, γεγονός που υποδεικνύει μια πιθανή κυβερνοεισβολή που έδωσε παράτυπες εντολές.

Από την άλλη, στην εικόνα που ακολουθεί φαίνονται οι καταγραφές πακέτων στην πλευρά του διακομιστή (R-Pi), όπου τα πρώτα έξι ζεύγη αιτημάτων-απαντήσεων είναι τα ίδια πακέτα που είδαμε στις καταγραφές στην πλευρά του πελάτη. Ωστόσο, δύο επιβεβαιωμένα αιτήματα (#2099 και #2705) και δύο επιβεβαιωμένες απαντήσεις (#2100 και #2706) δεν μπορούν να βρεθούν στις καταγραφές πακέτων στην πλευρά του πελάτη. Ταυτόχρονα όμως αυτά τα πακέτα δεν έχουν διαφορετικές IP διευθύνσεις και φωτογραφίζουν μια κανονική επικοινωνία μεταξύ Inverter-SCADA. Αυτά τα πακέτα είναι σημειωμένα σε κόκκινο ορθογώνιο (σχήμα 3.12). Τα δύο νέα επιβεβαιωμένα αιτήματα (#2099, #2705) είναι αιτήματα εγγραφής για την αλλαγή χαρακτηριστικών δεδομένων 'MaxWLim' σε

'0x0842200000' και '0x0841200000' αντίστοιχα. Η τελευταία τιμή είναι και η τιμή που εμφανίστηκε στην τελευταία απάντηση ανάγνωσης στις καταγραφές πακέτων στην πλευρά του πελάτη και σημαίνει εγγραφή τιμής 10% στον περιορισμό ισχύος.

Σχήμα 3.12 – Καταγραφές πακέτων στην πλευρά του PV Inverter - διακομιστή

Γίνεται εύκολα αντιληπτό ότι, αυτά τα δύο αιτήματα έχουν εισαχθεί από τον επιτιθέμενο και οι αντίστοιχες απαντήσεις έχουν απορριφθεί ώστε να μην αποσταλούν στον νόμιμο πελάτη, δηλαδή τον χειριστή του SCADA. Ο επιτιθέμενος κατάφερε να μπει ενδιάμεσα στην επικοινωνία πελάτη-διακομιστή, να αναγνώσει τα μηνύματα μετάδοσης και να εισάγει τροποποιημένες τιμές χωρίς να δημιουργήσει εμφανές σφάλμα στην επικοινωνία. Έτσι, ο εισβολέας όριζε κατά το δοκούν τον περιορισμό ισχύος του Inverter ενώ το σύστημα ελέγχου δεν είχε καμία ενημέρωση σχετικά με αυτήν την εντολή.

3.6. Κυβερνοεπιθέσεις στο δίκτυο επικοινωνίας αιολικού πάρκου

Καθότι αδύνατο να εντοπίσουμε μεγάλη γκάμα δοκιμαστικών επιθέσεων αποκλειστικά για το IEC 60870–6/ TASE.2 πρότυπο, **η παρούσα ενότητα θα εξετάσει τα τρωτά κυβερνοφυσικά σημεία ενός δικτυακού συστήματος WAN που περιλαμβάνει ICCP επικοινωνία**. Το δίκτυο αυτό χρησιμοποιείται για τις ανάγκες επικοινωνίας σε τμήματα του συστήματος SCADA και του Συστήματος Διαχείρισης Ενέργειας (EMS) με εφαρμογή σε αιολικά πάρκα. Η επιλογή του συγκεκριμένου παραδείγματος προκύπτει από το γεγονός ότι το δίκτυο ισχύος γίνεται όλο και περισσότερο εξαρτημένο από την παραγωγή αιολικής ενέργειας και άρα η απόδοση του συνολικού συστήματος ισχύος επηρεάζεται αναπόφευκτα από τις λειτουργίες των αιολικών πάρκων.

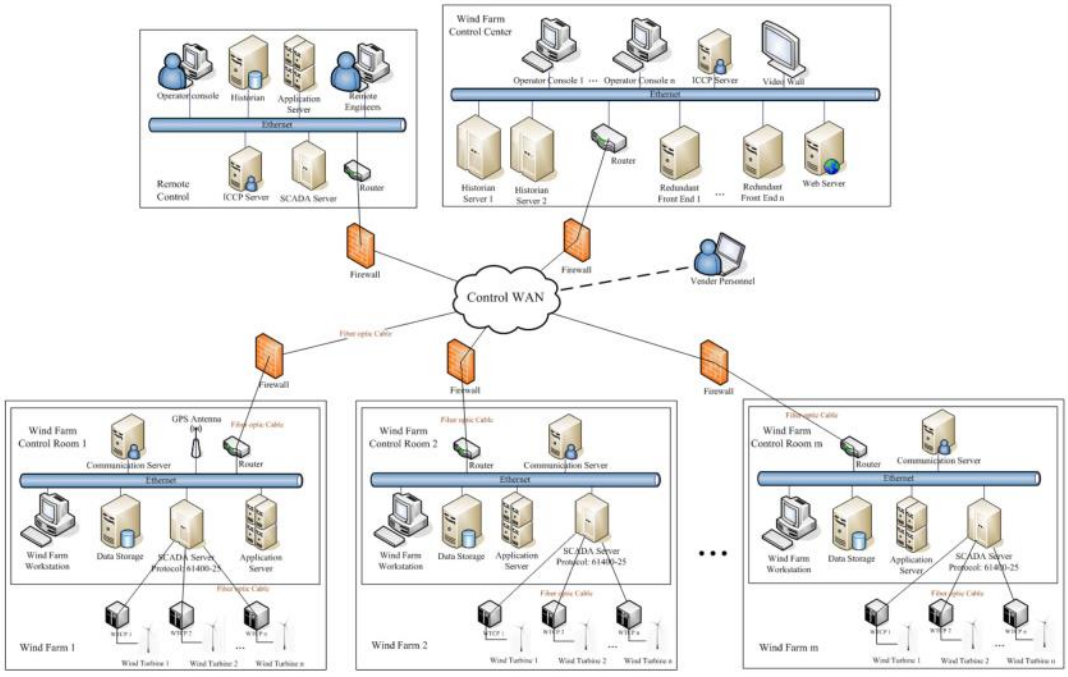
3.6.1. Περιγραφή συστήματος επικοινωνίας στα συστήματα διαχείρισης αιολικών πάρκων

Στην σύγχρονη εποχή, η πληροφορική και η τεχνολογία επικοινωνιών είναι κομβική για τον συντονισμό μεταξύ διαφόρων αιολικών. Το EMS και SCADA σύστημα είναι κρίσιμα για την παρακολούθηση, λειτουργία και προστασία των γεννητριών του πάρκου αλλά και συνολικά του συστήματος ισχύος. Τα SCADA αιολικών πάρκων χρησιμοποιούνται ευρέως για τη διαμόρφωση και την τροποποίηση παραμέτρων είτε μιας συγκεκριμένης μονάδας είτε ολόκληρου αιολικού πάρκου. Μπορεί επίσης να βελτιστοποιήσει το χρονοδιάγραμμα και τις συνθήκες λειτουργίας των μηχανών (πχ.

η λειτουργία σε χαμηλή ισχύ). Επιπλέον, οι φορείς και οργανισμοί αιολικής ενέργειας, οι οποίοι μπορεί να ελέγχουν πολλά αιολικά πάρκα, έχουν την δυνατότητα να συγκεντρώσουν την διαχείρισή τους σε ένα κεντρικό σύστημα διαχείρισης. Αυτό επιτυγχάνεται με την ενσωμάτωσή τους σε ένα EMS όπου ο κύριος έλεγχος εφαρμόζεται από το κέντρο ελέγχου μέσω ενός δικτύου ευρείς περιοχής - WAN.

Το δίκτυο επικοινωνίας του συστήματος ισχύος είναι πλέον ελκυστικός στόχος διάφορων κακόβουλων ομάδων και ατόμων, συνεπώς για τα SCADA/EMS υπάρχει ιδιαίτερη ανησυχία σχετικά με την επάρκεια ασφάλειας στο κυβερνο-σύστημα. Στο υποκείμενο παράδειγμα λοιπόν, οι κυβερνοεπιθέσεις στα συστήματα SCADA/EMS αιολικών πάρκων μπορεί να έχουν ως αποτέλεσμα ευρείες διακοπές στα ηλεκτρικά συστήματα ισχύος επηρεάζοντας την κανονική λειτουργία των ανεμογεννητριών. Λαμβάνοντας υπόψη την ταχεία αύξηση της διείσδυσης της αιολικής ενέργειας, είναι ζωτικής σημασίας να μελετηθούν κυβερνοεπιθέσεις κατά των αιολικών πάρκων και των συστημάτων διαχείρισής τους. Δυστυχώς, το ερευνητικό έργο που σχετίζεται με αυτό το κρίσιμο θέμα είναι αρκετά περιορισμένο έως και σήμερα.

Οι προκλήσεις που έχουν εξεταστεί έως τώρα σε ερευνητικό επίπεδο, αφορούν τα συστήματα SCADA/EMS του προαναφερθείς αιολικού πάρκου και περιγράφουν πέντε βασικά σενάρια κυβερνοεπίθεσης στο δίκτυο επικοινωνίας του. Η αρχιτεκτονική του δικτύου επικοινωνίας ακολουθεί το παρακάτω σχηματικό διάγραμμα.



Σχήμα 3.13 – Αρχιτεκτονική SCADA/EMS δικτύου επικοινωνίας σε αιολικό πάρκο

Το παραπάνω σχήμα απεικονίζει την αντιπροσωπευτική αρχιτεκτονική του συστήματος SCADA/EMS του αιολικού πάρκου, το οποίο χρησιμοποιείται για τον έλεγχο και την παρακολούθηση της παραγωγής και διανομής της αιολικής ενέργειας. Βλέπουμε ότι, το δίκτυο επικοινωνίας του συστήματος διαιρείται σε βασικά

υποδίκτυα: (α.) τα **LAN τοπικά δίκτυα ελέγχου** του αιολικού πάρκου, (β.) το **κεντρικό δίκτυο ελέγχου LAN**, (γ.) ένα **εφεδρικό κέντρο απομακρυσμένου ελέγχου**, και (δ.) οι σύνδεσμοι επικοινωνίας που συνδέουν τα επιμέρους τοπικά δίκτυα μέσω του **κεντρικού δικτύου ελέγχου WAN**.

Στην παρούσα μελέτη θεωρούμε ότι, το τοπικό δίκτυο ελέγχου στο αιολικό πάρκο είναι ένα αυτόνομο δίκτυο SCADA, που χρησιμοποιείται για την παροχή λειτουργιών παρακολούθησης και ελέγχου για τις ανεμογεννήτριες για ένα συγκεκριμένο πάρκο. Στο συγκεκριμένο παράδειγμα τα LAN δίκτυα χρησιμοποιούν ένα διαφορετικό πρωτόκολλο επικοινωνίας (το IEC 61400-25), το οποίο παρέχει τη δυνατότητα στον τοπικό SCADA server να επικοινωνεί με τις ανεμογεννήτριες. Οι πραγματικές εντολές και πληροφορίες μέτρησης παρουσιάζονται στον υπολογιστή του κέντρου, ενώ τα δεδομένα μεγάλης χρονικής διάρκειας που λαμβάνονται από τα μετρητικά στοιχεία αποθηκεύονται σε βάσεις δεδομένων ιστορικού. Το σύστημα SCADA εκτελεί λειτουργίες απόκτησης δεδομένων από το αιολικό πάρκο, δηλαδή διάφορες μετρούμενες ηλεκτρικές τιμές στις ανεμογεννήτριες. Για παράδειγμα, μια λειτουργία METEO που είναι εγκατεστημένη στο SCADA χρησιμοποιείται για τη συλλογή μετεωρολογικών δεδομένων, σημαντικών για την παραγωγή ισχύος, όπως η ταχύτητα του ανέμου και η εξωτερική θερμοκρασία. Τα δεδομένα που συλλέγονται στην συνέχεια επεξεργάζονται κατάλληλα από τον SCADA-διακομιστή και μεταδίδονται σε διακομιστές εφαρμογών του συστήματος. Μέσω του υπολογιστή, οι χειριστές μπορούν να παρακολουθούν ηλεκτρικά γεγονότα και καταστάσεις στο πεδίο και να τροποποιούν παραμέτρους των φυσικών στοιχείων στο αιολικό πάρκο. Αντιλαμβανόμαστε λοιπόν τι μπορεί να συμβεί εάν κάποιος μη-εξουσιοδοτημένος χρήστης διεισδύσει στο τοπικό δίκτυο ελέγχου και ελέγξει τον κεντρικό υπολογιστή. Τότε ο κίνδυνος να αποσταλούν κακόβουλες εντολές για να απενεργοποιηθούν οι ανεμογεννήτριες ή να αλλάξουν οι παράμετροι του κεντρικού ελεγκτή θα ήταν πολύ μεγάλος.

Στο ανώτατο κέντρο ελέγχου του αιολικού πάρκου, υπάρχουν πολλές μονάδες redundant front ends (RFEs), τα οποία χρησιμοποιούνται για τη λήψη και την παράδοση πληροφοριών από ή προς τα αιολικά πάρκα. Οι πληροφορίες κάθε αιολικού πάρκου αποθηκεύονται προσωρινά στους διακομιστές των αντίστοιχων RFE και ενημερώνονται με σταθερή συχνότητα. Αυτά τα RFE βρίσκονται σε λειτουργία hot standby που σημαίνει ότι παρακολουθούνται συνεχώς μεταξύ τους, ώστε σε περίπτωση αποτυχίας του ενός να αναλαμβάνει δράση το άλλο. Έτσι επιτυγχάνεται η υψηλή διαθεσιμότητα για κρίσιμες εφαρμογές, όπως η διαχείριση του αιολικού πάρκου. Στην προτεινόμενη αρχιτεκτονική χρησιμοποιούνται επίσης δύο historian servers για την αποθήκευση ιστορικών δεδομένων που λαμβάνονται από τις front-end μονάδες ή τα αιολικά πάρκα. Οι δύο διακομιστές όντας σε κοινό τοπικό δίκτυο με τα RFE μπορούν εύκολα να τα προσπελάσουν ώστε η διαθεσιμότητα των ιστορικών δεδομένων και απόκτησή τους να βελτιστοποιείται. Ακόμη, στην επικοινωνία συμμετέχει ένας WEB-server για την αποθήκευση δεδομένων πραγματικού χρόνου και την διάθεση πληροφοριών σε απομακρυσμένους πελάτες. Τέλος, ένας ICCP-διακομιστής είναι συνδεδεμένος στο τοπικό δίκτυο για να απαντά σε αιτήματα για ανταλλαγή δεδομένων από ICCP-πελάτες που βρίσκονται στα backup-απομακρυσμένα κέντρα ελέγχου.

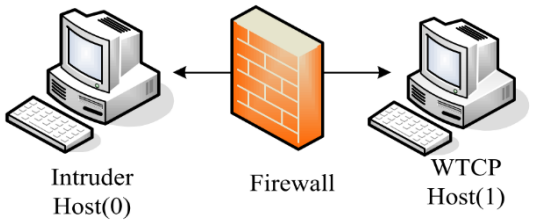
Τα πολλά αυτόνομα αιολικά πάρκα ενσωματώνονται και παρακολουθούνται από το κεντρικό σύστημα EMS που είναι εγκατεστημένο στο κέντρο ελέγχου του αιολικού πάρκου, ώστε να υπάρχει συνολική εποπτεία και κεντρική διαχείριση της ενέργειας που παράγεται. Το EMS του αιολικού πάρκου είναι σε θέση να ρυθμίζει την τάση των ανεμογεννητριών, να συντονίζει την κάθε έξοδο των αιολικών πάρκων και να παρέχει υποστήριξη άεργου ισχύος για το σύστημα. Το δίκτυο του backup-

απομακρυσμένο κέντρο ελέγχου θεωρείται ως το αντίγραφο ασφαλείας του LAN του βασικού κέντρου ελέγχου και είναι σε θέση να ελέγξει το απομακρυσμένα τα σύστημα SCADA των αιολικών πάρκων.

Για την επίτευξη των παραπάνω διασυνδέσεων είναι **απαραίτητη η ανάπτυξη ενός WAN-δικτύου ευρείας περιοχής** όπως φαίνεται στην αρχιτεκτονική του σχήματος 3.11. Επίσης, μια αποτελεσματική διαχείριση μεγάλου αριθμού αιολικών πάρκων από ένα κέντρο ελέγχου απαιτεί χρήση των κατάλληλων βιομηχανικών πρωτοκόλλων επικοινωνίας. Καθώς αναφερόμαστε κυρίως στα κέντρα ελέγχου, το παράδειγμά μας χρησιμοποιεί τρία πρωτόκολλα επικοινωνίας: IEC 61400-25, IEC 61850 και το ICCP. Με αυτά τα πρωτόκολλα, μπορεί να υλοποιηθεί μια κοινή αρχιτεκτονική επικοινωνίας τόσο για την παρακολούθηση των υποσταθμών όσο και για τον έλεγχο των αιολικών πάρκων. Τα πρωτόκολλα αυτά εμφανώς χρησιμοποιούνται σε επίπεδο επικοινωνίας μεταξύ των διαφόρων σημείων ελέγχου (κεντρικός έλεγχος, τοπικά κέντρα, υποσταθμοί, απομακρυσμένος έλεγχος, διαδίκτυο, κλπ.). Αντιθέτως οι συσκευές χαμηλότερων επιπέδων, όπως για παράδειγμα μετρητές ενέργειας, χρησιμοποιούν συνήθως σειριακά πρωτόκολλα (πχ. IEC 60870-5-102), το οποίο θα πρέπει να συνδεθεί με το σύστημα SCADA/EMS του αιολικού πάρκου, μέσω προσαρμογέα σειριακού πρωτοκόλλου σε πρωτόκολλο βασισμένο στο Ethernet.

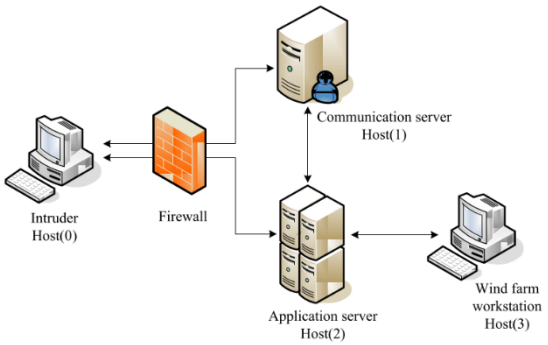
3.6.2. Σενάρια κυβερνοεπιθέσεων στα δίκτυα ελέγχου του αιολικού πάρκου

Όπως συναντήσαμε και στις προηγούμενες περιπτώσεις, πιθανός στόχος μιας κυβερνοεπίθεσης σε έναν σύστημα ηλεκτρικής ενέργειας μπορεί να είναι κρίσιμα υλικά προστασίας του ηλεκτρικού κυκλώματος, όπως οι διακόπτες ισχύος. Η επιτυχία τέτοιων επιθέσεων (πχ. με ψευδείς εντολές trip σε κρίσιμα σημεία) μπορεί να προκαλέσει την απενεργοποίηση ανεμογεννητριών του αιολικού πάρκου. Κάτι τέτοιο θα κλόνιζε σε μεγάλο βαθμό την αξιοποίηση της αιολικής ενέργειας και ανάλογα με τον βαθμό εξάρτησης, την αξιοπιστία του συνολικού συστήματος ηλεκτροδότησης.. Στη συνέχεια, αναφέρονται **πέντε σενάρια απειλών στο κυβερνοσύστημα ελέγχου του αιολικού πάρκου** και συζητούνται δυνητικές επιπτώσεις τους στο αιολικό σύστημα.



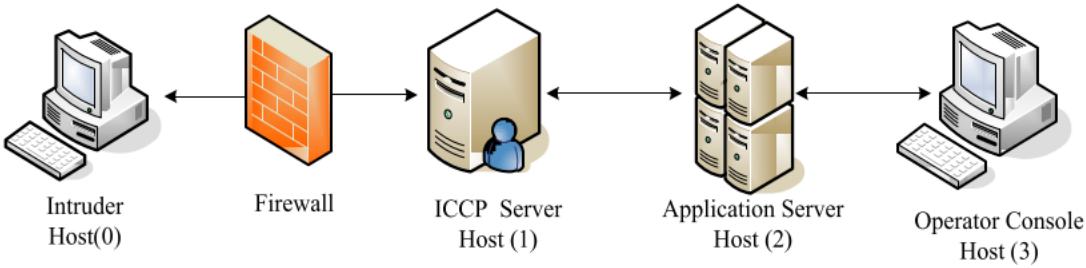
1. **Επίθεση στον πίνακα ελέγχου ανεμογεννήτριας:** Ο ΠΕ μιας ανεμογεννήτριας (ή αλλιώς WTCP) είναι ουσιαστικά η μονάδα ελέγχου και παρακολούθησής της και αποτελείται από μια οθόνη/ες και λειτουργικά πλήκτρα. Μέσω του ΠΕ, εκτός από τον ανάκτηση δεδομένων της στιγμιαίας κατάστασης και των μετρητικών τιμών της ανεμογεννήτριας, μπορούν επίσης να πραγματοποιηθούν σημαντικές λειτουργίες ρύθμισης στη συνδεδεμένη ανεμογεννήτρια. Επειδή ο ΠΕ είναι συνήθως είναι εύκολα προσβάσιμος, είναι ακόμα εύκολο να προσεγγιστεί από μη-εξουσιοδοτημένους επιτιθέμενους. Μπορούμε να θεωρήσουμε ότι πρόκειται για τον ευκολότερο στόχο για κάποιον επιτιθέμενο εφόσον καταφέρει να παρακάμψει τον προστατευτικό τοίχο (firewall). Ο επιτιθέμενος μπορεί να συνδέσει μια συσκευή διείσδυσης στον ΠΕ και στη συνέχεια να αποκτήσει τον πλήρη έλεγχο του ΠΕ εξαπολύοντας γνωστές κυβερνοεπιθέσεις, όπως buffer overflow ή εισάγοντας κακόβουλες εντολές.
2. **Επίθεση στον τοπικό έλεγχο LAN ενός αιολικού πάρκου:** Επίσης πιθανές, είναι οι επιθέσεις στα διάφορα δίκτυα LAN του συστήματος SCADA/EMS, στα

οποία ο επιτιθέμενος έχει καταφέρει να αποκτήσει πρόσβαση και να στέλνει κακόβουλες εντολές. Η πρόσβαση στο τοπικό δίκτυο, ωστόσο, δεν σημαίνει απαραίτητα μια τοπική εισβολή. Έμπειροι εξωτερικοί επιτιθέμενοι μπορούν να εκμεταλλευτούν ευπάθειες συσκευών που επικοινωνούν με βάση το Ethernet, χρησιμοποιώντας τες ως γέφυρες εισόδου στην τοπική επικοινωνία. Έτσι, κάποιος επιτιθέμενος μπορεί να διεισδύσει σε διάφορα εσωτερικά LAN του συστήματος SCADA/EMS, εκμεταλλευόμενος τα ευάλωτα σημεία των υπηρεσιών που εκτελούνται στο ενδιάμεσο στοιχείο. Η διείσδυση αυτή ουσιαστικά επιτρέπει στον εισβολέα να διεξάγει επιθέσεις σε όλα τα διασυνδεδεμένα στοιχεία του τοπικού LAN, να αποκτά έλεγχο σε νέους στόχους με απώτερο σκοπό να φτάσει εφαρμογές ελέγχου της ανεμογεννήτριας..



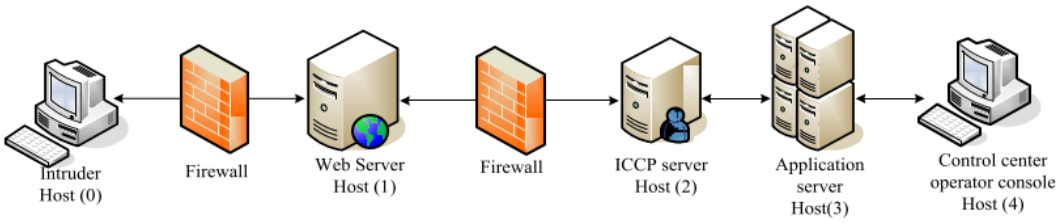
Περισσότερο πολύπλοκές αλλά ιδιαίτερα επικίνδυνες είναι οι περιπτώσεις όπου ο καθορισμένος στόχος τους εισβολέα είναι ο κεντρικός έλεγχος του συνολικού συστήματος διαχείρισης του αιολικού πάρκου. Σε αυτήν την περίπτωση θα πρέπει να παρακαμφθεί το προστατευτικό τείχος (firewall) ώστε να διεισδύσει είτε στον εξυπηρετητή επικοινωνίας, είτε στον εξυπηρετητή εφαρμογών. Ο εξυπηρετητής επικοινωνίας, που είναι παρόμοιος με τον εξυπηρετητή ICCP, χρησιμοποιείται για την επεξεργασία των πληροφοριών που ανακτήθηκαν ή αποστέλλονται στο κέντρο ελέγχου και δεν επιτρέπεται η άμεση επικοινωνία με το περιβάλλον εργασίας του πάρκου (workstation). Από την άλλη, ο εξυπηρετητής εφαρμογών αποθηκεύει δεδομένα μέτρησης στην πραγματική βάση δεδομένων και μεταδίδει άμεσα εντολές ελέγχου στο περιβάλλον εργασίας. Συνεπώς, εάν ο επιτιθέμενος αποκτήσει δικαιώματα ελέγχου στα παραπάνω περιβάλλοντα εργασίας, οι ανεμογεννήτριες του πάρκου δύναται να λαμβάνουν ψευδείς εντολές διακοπής της λειτουργίας τους.

3. **Επίθεση στο εφεδρικό κέντρο απομακρυσμένου ελέγχου:** Το εξωτερικό κέντρο ελέγχου χρησιμοποιείται τόσο ως εφεδρεία όσο και για τον συντονισμό του κεντρικού κέντρου ελέγχου, ώστε να μπορεί να επιτελέσει αποτελεσματικά τον εποπτικό έλεγχο, εξ αποστάσεως. Εκμεταλλευόμενος τα τρωτά σημεία του διακομιστή εφαρμογής που συνδέεται άμεσα με τον ICCP-server, ο επιτιθέμενος αποκτά πλήρη πρόσβαση στην εφαρμογή. Με αυτόν τον τρόπο ο εισβολέας διαθέτει μια καμουφλαρισμένη ταυτότητά χρήστη, η οποία του δίνει δυνατότητα πρόσβασης στην κονσόλα του χειριστή. Τα βήματα επίθεσης στο εφεδρικό δίκτυο ελέγχου αντιγράφου ασφαλείας φαίνεται παρακάτω.



4. **Επίθεση στο τοπικό δίκτυο του κέντρου ελέγχου**: Σε αυτό το σενάριο ο επιτιθέμενος στοχεύει αρχικά σε εισβολή στον εξυπηρετητή-ιστού (web server), ο οποίος μπορεί να είναι εγκατεστημένος στην «αποστρατευτική» ζώνη - DMZ του δικτύου. Εάν ο επιτιθέμενος έχει παρακάμψει και το δεύτερο προστατευτικό τείχος που χωρίζει τη DMZ και το δίκτυο ελέγχου του κέντρου, μπορεί να φτάσει επιτυχώς στον εξυπηρετητή ICCP, που χρησιμοποιείται όπως είδαμε για επικοινωνίες αντιγράφων ασφαλείας του κέντρου ελέγχου. Οι υπόλοιπες ενέργειες είναι παρόμοιες με τις επιθέσεις που είδαμε για το εφεδρικό δίκτυο ελέγχου. Σχολιάζοντας τις δύο περιπτώσεις επιθέσεων, πρέπει να σημειωθεί ότι ο επιτιθέμενος έχει την δυνατότητα να εκμεταλλευτεί διαφορετικά ευπαθή στο δίκτυο ελέγχου του αιολικού πάρκου. Το γεγονός αυτό αναδεικνύει και τις τεράστιες προκλήσεις για την ανάπτυξη μηχανισμών προστασίας. Στο διάγραμμα που ακολουθεί παρουσιάζεται η διάταξη και η αντίστοιχη επίθεση στο δίκτυο ελέγχου του αιολικού πάρκου.

5. **Επίθεση στις συνδέσεις επικοινωνίας των αιολικών πάρκων**: Οι πιθανές συνδέσεις επικοινωνίας που μπορούν να υποστούν επίθεση στο SCADA/EMS



είναι αυτές μεταξύ του δικτύου κέντρου ελέγχου και του τοπικού δικτύου των επιμέρους πάρκων, καθώς και οι συνδέσεις μεταξύ των Πινάκων Ελέγχου και των ανεμογεννητριών. Για παράδειγμα μια επίθεση ενδιαμέσου εισβολέα (MITM) είναι εφικτό να εφαρμοστεί σε αυτές τις συνδέσεις επικοινωνίας, για τις οποίες το κύριο υλικό που χρησιμοποιείται είναι η οπτική ίνα. Μια αποτελεσματική τακτική θα ήταν να εγκατασταθούν ειδικές κρυφές συσκευές παρακολούθησης στο καλώδιο των οπτικών ινών, όπου ο επιτιθέμενος θα μπορούσε να αποκτήσει σημαντικές πληροφορίες ή να εισάγει πλαστογραφημένα δεδομένα στις συνδέσεις.

3.6.3. Επιπτώσεις και επιβεβαιωμένα συμβάντα κυβερνοεπιθέσεων στα αιολικά πάρκα

Σε όλα τα παραπάνω σενάρια επιθέσεων, μετά την απόκτηση των επιθυμητών προνομίων πρόσβασης, ο επιτιθέμενος μπορεί να πραγματοποιεί κυβερνοεπιθέσεις με ποικίλους τρόπους, όπως να υποκλέπτει πληροφορίες, να αποκλείει ανεμογεννήτριες από την παραγωγή, να διαταράσσει την τάση στο δίκτυο ή να διακόπτει πλήρως την λειτουργία του συστήματος ηλεκτροδότησης. Σε ορισμένες ακραίες περιπτώσεις, η ανεμογεννήτρια θα μπορούσε να υποστεί φυσικές βλάβες, αν και αυτό είναι μια αρκετά δύσκολη εργασία λαμβάνοντας υπόψη τις σχετικές λειτουργίες παρακολούθησης και προστασίας. Σε κάθε περίπτωση όμως εάν μια ανεμογεννήτρια τελικά τερματιστεί, τότε θα προκληθεί **μείωση της συνολικής δυνατότητας παραγωγής** και αυτό μπορεί να οδηγήσει σε **σημαντική απώλεια φορτίου**. Αυτός είναι και ένας αρκετά επιζήμιος τρόπος με τον οποίο οι ανεμογεννήτριες επηρεάζουν αρνητικά τη λειτουργία την ηλεκτροδότηση σε σχέση με την απώλεια πληροφοριών. Εκτός από την άμεση τερματισμό των ανεμογεννητριών, οι επιτιθέμενοι με προηγμένες δεξιότητες μπορούν να ελέγχουν τις ανεμογεννήτριες και να διαταράσσουν κατά το δοκούν τη συχνότητα ή την τάση.

Αν και σε γενικές γραμμές οι ανεμογεννήτριες λειτουργούν με ανωμαλίες, εφόσον η λειτουργία τους παρακολουθείται διαρκώς από το κέντρο ελέγχου, οι υπεύθυνοι του συστήματος ηλεκτροδότησης οφείλουν να εξετάσουν σοβαρά την ανάπτυξη μέτρων κυβερνοασφάλειας.

Την παραπάνω ανάγκη επιβεβαιώνουν δημοσιεύματα τον Απρίλιο του 2022, σύμφωνα με τα οποία, **υπηρεσία αιολικών πάρκων** (Deutsche Windtechnik) **υπέστη «στοχευμένη και επαγγελματική» κυβερνοαπειλή** και εντάχθηκε στην μεγάλη λίστα γερμανικών παρόχων ηλεκτρικής ενέργειας οι οποίες τα τελευταία χρόνια αντιμετώπισαν διαταραχές ύστερα από συμβάντα κυβερνοεπίθεσης. Η επίσημη ανακοίνωση της εταιρίας αναφέρει, μεταξύ άλλων, ότι αναγκάστηκε να απενεργοποιήσει τις ανεμογεννήτριες και διακόψει τις συνδέσεις του απομακρυσμένου συστήματος παρακολούθησης για λόγους ασφάλειας. Μάλιστα ο έλεγχος και η αποκατάσταση των επικοινωνιακών συνδέσεων στα αιολικά πάρκα διήρκησαν αρκετές ημέρες. Παραμένει ανεπιβεβαίωτο έως και σήμερα, εάν τα κακόβουλα λογισμικά της επίθεσης κατάφεραν να υποκλέψουν σημαντικές πληροφορίες για την παραγωγή (πράγμα που φαντάζει αρκετά πιθανό), ωστόσο οι ήδη φανερές επιπτώσεις έχουν ιδιαίτερη σημασία. Αφενός η απώλεια παραγωγής ενέργειας για το διάστημα των δύο ημερών προκάλεσε ανισορροπίες στο δίκτυο και αφετέρου, τις μέρες που ακολούθησαν, η αδυναμία επικοινωνίας με κομβικά στοιχεία του συστήματος οδήγησαν σε απώλεια αρκετών πληροφοριών σχετικά με την παραγωγή. Σύμφωνα με άλλες αναφορές στην Γερμανία έχουν προηγηθεί περισσότερες περιπτώσεις κυβερνοεπιθέσεων. Για παράδειγμα, κατασκευαστής ανεμογεννητριών υποχρεώθηκε να απενεργοποιήσει όλα τα IT συστήματά του σε πολλές τοποθεσίες και τμήματα επιχειρήσεων μετά από συμβάν κυβερνοεπίθεσης την ίδια χρονιά. Στην συνέχεια ακολούθησε σημαντική επίθεση κατά γνωστής εταιρείας επικοινωνιών μέσω δορυφόρου, η οποία προκάλεσε δυσλειτουργία σε τουλάχιστον 5.800 ανεμογεννήτριες της Enercon. Ακόμη μια επιβεβαιωμένη και σημαντική επίθεση κατά γνωστής κατασκευάστριας εταιρίας ανεμογεννητριών, ήταν η περίπτωση μιας ransomware επίθεσης. Σε αυτήν την περίπτωση οι εισβολείς κατάφεραν τελικά να υποκλέψουν σημαντικές πληροφορίες με την κατοχή των οποίων απειλούσαν τους κατασκευαστές.

4. Η Κυβερνοασφάλεια στα Πρωτόκολλα Επικοινωνίας

4.1. Εισαγωγή στην Κυβερνοασφάλεια – Βασικές Αρχές

Η αυξανόμενη εξάρτηση των κύριων και δευτερευόντων συστημάτων ελέγχου στην παραγωγή ηλεκτρικής ενέργειας από τα συστήματα επικοινωνίας και την αυτοματοποίηση λειτουργιών καθιστά τα ζητήματα κυβερνοασφάλειας ιδιαιτέρως κρίσιμα. Η διάρρηξη βασικών αρχών που διέπουν την ασφαλή επικοινωνία από κακόβουλους εξωτερικούς ή εσωτερικούς χρήστες, μπορεί να οδηγήσει σε δυσλειτουργία, απώλεια παραγωγικότητας και ακόμα και σοβαρά ατυχήματα.

Σχήμα 4.1 – Οι τρεις αρχές της ασφάλειας

Οι βασικές αρχές ασφαλείας της επικοινωνίας που πρέπει να διασφαλίζει ένας αμυντικός μηχανισμός είναι η **εμπιστευτικότητα**, η **ακεραιότητα** και η

διαθεσιμότητα των δεδομένων που μεταδίδονται αδιάλειπτα μεταξύ του βιομηχανικού εξοπλισμού και των εφαρμογών που εποπτεύουν την καθολική λειτουργία τους συστήματος. Τα δεδομένα αυτά, δηλαδή, θα πρέπει ανά πάσα στιγμή να είναι διαθέσιμα, έγκυρα και προσβάσιμα μόνο σε εξουσιοδοτημένους νόμιμους χρήστες, υποσυστήματα και εφαρμογές του συνολικού δικτυακού συστήματος. Όλα τα δικτυακά συστήματα οφείλουν να περιλαμβάνουν μηχανισμούς διασφάλισης των παραπάνω αρχών προστασίας.

Το προηγούμενο κεφάλαιο ανέδειξε ένα μεγάλο εύρος κινδύνων που μπορεί να αντιμετωπίσει ένα κυβερνοφυσικό σύστημα, το οποίο αποτελεί στόχο κυβερνοεπιθέσεων. Συνεπώς, η ανάπτυξη αποτελεσματικών μηχανισμών πρόληψης και προστασίας στα βιομηχανικά δίκτυα επικοινωνιών αποτελεί μια κομβική διαδικασία για την ενίσχυση της ασφάλειας των βιομηχανικών εγκαταστάσεων.

4.2. Συστήματα πρόληψης και προστασίας της επικοινωνίας

Κάθε διάταξη κυβερνοασφάλειας έχεις ως βασικό σκοπό την εξουδετέρωση των κινδύνων που μπορεί να παρουσιαστούν στο, κυβερνοχώρο του φυσικού ηλεκτρικού συστήματος. Η ενδεδειγμένη μεθοδολογία αντιμετώπισης των πιθανών κυβερνοαπειλών προϋποθέτει την ανάπτυξη αποτελεσματικών συστημάτων ασφαλείας που θα ικανοποιούν δύο βασικές έννοιες ασφαλείας: τον **εντοπισμό** κυβερνοεπιθέσεων και την **πρόληψη**.

Η έννοια της πρόληψης εμφανίζεται πριν την ανάγκη αντιμετώπισης κάποιου συγκεκριμένου κινδύνου που είναι ορατός και στοχεύει στην δημιουργία μιας στιβαρής επικοινωνίας απέναντι σε κακή χρήση της επικοινωνίας ή συχνές παραβιάσεις των κανόνων που την διέπουν, ανά εφαρμογή. Οι προληπτικοί μηχανισμοί μπορούν να αναπτυχθούν είτε σε επίπεδο δικτύου είτε σε επίπεδο πρωτοκόλλου επικοινωνίας. Σε επίπεδο πρωτοκόλλων επικοινωνίας, έχουν αναπτυχθεί αρκετά σημαντικές μέθοδοι που ενισχύουν τα επίπεδα ασφάλειας του πρωτοκόλλου, καμουφλάροντας κάποιες από τις αδυναμίες που εντοπίστηκαν στα προηγούμενα κεφάλαια. Για παράδειγμα, η **ενσωμάτωση μηχανισμών αυθεντικοποίησης στα πακέτα** που ανταλλάσσονται στο δίκτυο είναι μια τεχνική πρόληψης, η οποία προσθέτει στα μηνύματα αιτημάτων και απάντησης ένα πεδίο που ταυτοποιεί τον αποστολέα και τον παραλήπτη της συνομιλίας. Μια διαφορετική τεχνική είναι η **κρυπτογράφηση μηνυμάτων**, των οποίων η αποκρυπτογράφηση θα γίνεται με χρήση κλειδιών ασφαλείας. Αυτός ο μηχανισμός πρόληψης, ναι μεν δεν μπορεί να προστατεύσει την επικοινωνία από επιτυχημένες κυβερνοεισβολές, ωστόσο προσδίδει υψηλό βαθμό εμπιστευτικότητας στην πληροφορία που μεταδίδεται. Από την άλλη, τα **συστήματα παρεμπόδισης εισβολών, γνωστά ως IPS**, έχουν την δυνατότητα να αναλύουν το δίκτυο και να απορρίπτουν κινήσεις που θεωρούνται κακόβουλες για το σύστημα. Αυτά τα συστήματα ασφαλώς προϋποθέτουν την ανίχνευση τέτοιων ύποπτων συμπεριφορών, διαδικασία που εντάσσεται στους μηχανισμούς εντοπισμού όπως θα δούμε στην συνέχεια.

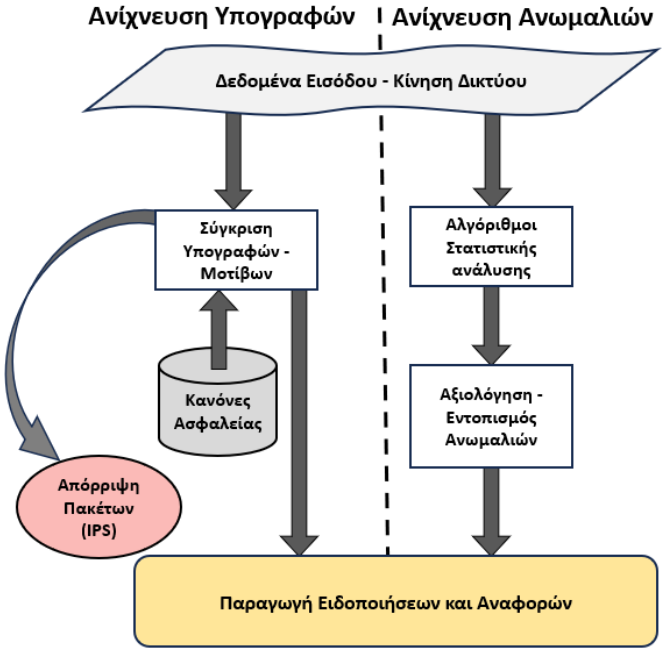
Η βασική έννοια η οποία τελικά θα καθορίσει τα επίπεδα προστασίας του κυβερνοσυστήματος είναι αυτή του εντοπισμού. Η γρήγορη και σωστή ανίχνευση κακόβουλων συμπεριφορών στην κίνηση του δικτύου είναι η ουσία μιας αποτελεσματικής διάταξης κυβερνοασφάλειας, καθώς αυτό θα καθορίσει τελικά τις αποφάσεις που θα παρθούν ενάντια στους εισβολείς. Τους μηχανισμούς εντοπισμού κυβερνοεπιθέσεων θα ονομάζουμε από εδώ και στο εξής συστήματα IDS (Intrusion Detection Systems). Συγκεκριμένα, ως **Συστήματα Ανίχνευσης διείσδυσης ή εισβολής,** ορίζουμε τα συστήματα ασφαλείας που επιτηρούν την κυκλοφορία δεδομένων, τις επικοινωνίες και τη συμπεριφορά συσκευών και δικτύου στο βιομηχανικό περιβάλλον, με σκοπό την ανίχνευση πιθανών εισβολών ή κακόβουλων

δραστηριοτήτων. Τα IDS συστήματα επιδιώκουν να αναγνωρίσουν απειλές που μπορεί να προκαλέσουν προβλήματα ασφάλειας, να διαταράξουν την παραγωγή ή πλήττουν τη λειτουργία του φυσικού συστήματος. Τα συστήματα αυτά χρησιμοποιούν αρκετές διαφορετικές τεχνικές για να ανιχνεύσουν τις κακόβουλες δραστηριότητες που συντελούνται στο δίκτυο ενός βιομηχανικού συστήματος ελέγχου. Έτσι μπορούν να κατηγοριοποιηθούν με βάση τις διάφορες λειτουργίες που χρησιμοποιούν για τον τελικό σκοπό τους, την ανίχνευση κυβερνοεπιθέσεων.

Πολλοί ερευνητές έχουν αναπτύξει συστήματα **IDS βασισμένα σε στατιστικά στοιχεία (ή σε ανωμαλίες).** Τα στατιστικά συστήματα ανίχνευσης αυτά χρησιμοποιούν στατιστικές μεθόδους για να κατηγοριοποιήσουν την κίνηση του δικτύου ως φυσιολογική ή ανώμαλη. Η λειτουργία αυτή γίνεται με στατιστική ανάλυση και αλγόριθμους μηχανικής μάθησης, καθιερώνοντας πρότυπα κανονικής συμπεριφοράς για να εντοπίσει ανώμαλες δραστηριότητες που μπορεί να υποδηλώνουν μια εισβολή. **Το πλεονέκτημα του στατιστικών IDS** είναι η ικανότητά τους να ανιχνεύουν "zero-day" επιθέσεις (δηλ. προηγουμένως άγνωστες), καθώς δεν βασίζονται σε γνωστά πρότυπα και μοτίβα. Παρ' όλα αυτά, η μέθοδος αυτή μπορεί να παράγει ψευδώς θετικά αποτελέσματα σε περίπτωση που εμφανιστεί μια νόμιμη, αλλά ασυνήθιστη δραστηριότητα, καθιστώντας δύσκολο τον διαχωρισμό μεταξύ αθώας ή κακόβουλης συμπεριφοράς. Η απόρριψη έγκυρων πακέτων επικοινωνίας μπορεί τελικά να επιφέρει καταστροφικά αποτελέσματα σε ένα βιομηχανικό σύστημα ελέγχου.

Η δεύτερη και ίσως η πιο ενδιαφέρουσα μέθοδος που θα αναφερθούμε είναι η **ανίχνευση βασισμένη σε υπογραφές (signature-based IDS)**, η οποία σχεδιάστηκε για να εντοπίζει πρότυπα στην κίνηση του δικτύου που υποδηλώνουν κακόβουλη δραστηριότητα ή μη εξουσιοδοτημένη πρόσβαση. Ως κακόβουλη δραστηριότητα ονομάζουμε οποιοδήποτε κακόβουλο (malware) πρόγραμμα ή κώδικας που είναι επιβλαβής για τα υπολογιστικά συστήματα (π.χ., rojans, viruses, worms). Η ανίχνευση βασισμένη σε υπογραφές είναι μία από τις πιο καθιερωμένες και άμεσες μεθόδους για την εντοπισμό κακόβουλης δραστηριότητας. Η κύριες λειτουργίες είναι να **εξετάζει την κίνηση του δικτύου**, **τη συγκρίνει με υπογραφές**, δηλαδή πρότυπα γνωστών επιθέσεων, **και παράγει μια ειδοποίηση όταν γίνεται αντιστοίχιση της υπογραφής με την εισερχόμενη κυκλοφορία**. Ένα διαδεδομένο παράδειγμα IDS βασισμένο σε υπογραφές είναι το Snort, ως ένα εργαλείο ανίχνευσης και πρόληψης εισβολών στο δίκτυο, που βασίζεται σε κανόνες και είναι ανοιχτού κώδικα. Σε ένα σύστημα ασφαλείας IDS, το Snort συλλέγει και καταγράφει και αναλύει την κίνηση του δικτύου, ψάχνοντας για παραβιάσεις προαποφασισμένων κανόνων και ειδοποιεί τον διαχειριστή για ύποπτες δραστηριότητες. Συνήθως, το Snort χρησιμοποιείται για να παρακολουθεί την κίνηση των Ethernet και TCP/IP επικοινωνιών, ωστόσο υπό προϋποθέσεις μπορεί να εφαρμοστεί και σε σειριακά πρωτόκολλα.

Το κύριο πλεονέκτημα ενός συστήματος IDS βασισμένο σε υπογραφές, είναι η υψηλή ακρίβειά του στην ανίχνευση κοινών επιθέσεων, καθιστώντας το αποτελεσματικό και αξιόπιστο για την προστασία από γνωστούς κινδύνους. Ωστόσο, το σύστημα ανίχνευσης βασισμένο σε υπογραφές μπορεί να παραλείψει νέες ή προηγουμένως αγνώστους κινδύνους, καθώς εξαρτάται από τη διαθεσιμότητα και την σωστή ενημέρωση της βάσης των υπογραφών. Δηλαδή, η αποτελεσματικότητά του εξαρτάται σε μεγάλο βαθμό από τον ανθρώπινο παράγοντα και την σχολαστικότητα του υπευθύνου μηχανικού επικοινωνιών στο να συμπεριλάβει την μεγαλύτερη δυνατή γκάμα γνωστών επιθέσεων. Τέλος, το εξελιγμένο εργαλείο Snort περιλαμβάνει και δυνατότητες πρόληψης ενάντια σε επιθέσεις, κατά τις οποίες εκτός από την παραγωγή ειδοποιήσεων μπορεί να απορρίπτει τα κακόβουλα πακέτα που εντοπίζει. Σε αυτές τις περιπτώσεις μιλάμε για Συστήματα Παρεμπόδισης Εισβολών (Intrusion Prevention System) ή αλλιώς IPS, τα οποία εντάσσονται κυρίως στους μηχανισμούς πρόληψης.



Σχήμα 4.2 – Διάγραμμα μεθόδων ανίχνευσης εισβολών

Στην συνέχεια θα μελετήσουμε πειράματα που αναπτύχθηκαν γενικώς για την προστασία κάθε πρωτοκόλλου και ειδικά για τις κυβερνοεπιθέσεις που αναφέρθηκαν στο προηγούμενο κεφάλαιο. Κάθε ενότητα περιλαμβάνει αναλύσεις συστημάτων ανίχνευσης βασισμένα σε στατιστικές, σε υπογραφές αλλά και παραδείγματα συστημάτων πρόληψης.

4.3. Συστήματα πρόληψης και ανίχνευσης εισβολών σε επικοινωνία Modbus

4.3.1. Ανάπτυξη κανόνων ασφαλείας

Η μελέτη που διεξήχθη σχετικά με την ανάπτυξη αμυντικών μηχανισμών και συστημάτων ανίχνευσης εισβολών, αρχικά, επικεντρώνεται στην παρουσίαση βασικών, **βασισμένων σε «υπογραφές», κανόνων ανίχνευσης (signature-based rules) για τα πρωτόκολλα Modbus/TCP και Modbus-Serial**. Στην διαθέσιμη βιβλιογραφία εντοπίστηκαν συνολικά 50 σημαντικοί τέτοιοι κανόνες που περιλαμβάνουν λεπτομέρειες σχετικά με τις απαιτήσεις του πρωτοκόλλου και την

κατασκευή των «υπογραφών» του συστήματος ανίχνευσης διείσδυσης (IDS). Αν και οι κανόνες που θα δούμε στην συνέχεια προορίζονται για χρήση μέσω του SNORT, η περιγραφή τους γίνεται σε απλουστευμένη μορφή ώστε η παρουσίαση αυτή να είναι χρήσιμη για οποιοδήποτε σύστημα IDS, βασισμένο σε «υπογραφές». Από τους 50 κανόνες που καταγράφηκαν, επιλέχθηκαν προς μελέτη 17 αντιπροσωπευτικοί για τα σημεία ενός Modbus μηνύματος, όπου η παρουσία μηχανισμού ασφαλείας είναι επιτακτική. Κάθε κανόνας που θα αναφερθεί συνοδεύεται με ένα πίνακα που περιλαμβάνει: την σχετική αρίθμηση του αντίστοιχου κανόνα (βάση βιβλιογραφίας), ένα συνοπτικό όνομα για τον κανόνα, το κατάλληλο Modbus πρωτόκολλο (TCP και/ή Serial), εάν ο κανόνας είναι αυτόνομος (standalone) ή απαιτεί προεπεξεργαστή (preprocessor) και ένα πεδίο σύνταξης του κανόνα, σε μορφή απλού κειμένου. Σημειώνεται επίσης ότι, λόγω του κοινού φορτίου δεδομένων (PDU) των δύο πρωτοκόλλων, πολλοί κανόνες μπορούν να αναπτυχθούν σε συστήματα επικοινωνίας είτε βασισμένα στο TCP, είτε σε σειριακές γραμμές επικοινωνίας.

Κάθε περιγραφή κανόνα αναφέρεται στην παραγωγή ειδοποιήσεων, όπου κάθε ειδοποίηση παρέχει ένα σήμα που ενημερώνει τον διαχειριστή του συστήματος για το τι πυροδότησε τον κανόνα. Η εφαρμογή των κανόνων αυτών δηλαδή προσφέρουν αποκλειστικά την δυνατότητα ανίχνευσης κάποιας ανωμαλίας στην επικοινωνία, χωρίς να μπλοκάρουν την μετάδοση της ύποπτης δραστηριότητας. Ωστόσο, ορισμένοι κανόνες ειδοποίησης **μπορούν να μετατραπούν σε κανόνες απόρριψης**, ώστε τα ύποπτα πακέτα που ταιριάζουν με τις προδιαγραφές του κανόνα, τελικά να αποβάλλονται πριν φτάσουν στον προορισμό τους. Για παράδειγμα ο πρώτος κανόνας που ανιχνεύει αν είναι σωστό το αναγνωριστικό πρωτοκόλλου για τα Modbus πακέτα που μεταδίδονται, μπορεί με ασφάλεια να οριστεί και ως κανόνας απόρριψης πακέτων με λάθος αναγνωριστικό. Αυτή η δυνατότητα προσφέρεται από τους μηχανισμούς πρόληψης που περιλαμβάνει το εργαλείο Snort.

Για λόγους ευκολότερης κατανόησης, **η σύνταξη των παρακάτω κανόνων χρησιμοποιεί τη θεωρία συνόλων**, η οποία εξηγείται στην συνοδευόμενη παράγραφο του κάθε κανόνα:

- **Κανόνας 1 - Ειδοποιεί εάν το πεδίο αναγνωριστικού πρωτοκόλλου του MODBUS/TCP δεν είναι 0**.

1	Protocol Identifier	TCP	standalone	trans.protid != 0

Όπως είδαμε στο κεφάλαιο 2, όλα τα πακέτα Modbus/TCP περιλαμβάνουν το πεδίο αναγνωριστικού πρωτοκόλλου το οποίο ορίζεται ως 0 για όλα τα πακέτα Modbus/TCP, ενώ κάθε άλλη τιμή δεν είναι επιτρεπτή. Επομένως, απαιτείται ένας κανόνας ειδοποίησης για μια πιθανή κίνηση TCP πακέτου στη συνεδρία, του οποίου το πεδίο αναγνωριστικού πρωτοκόλλου δεν είναι ορισμένο σε μηδέν. Στην πραγματικότητα, αυτό σημαίνει ότι οποιοδήποτε πακέτο με το δεύτερο byte του φορτίου διάφορο του μηδενός είναι απαγορευμένο και θα πρέπει να οδηγήσει σε ειδοποίηση και απόρριψη.

- **Κανόνας 2 - Ειδοποιεί όταν το αναγνωριστικό συναλλαγής (transaction identifier) της απάντησης δεν ταιριάζει με το αναγνωριστικό συναλλαγής της ερώτησης.**

2	**Query Response Pairs**	TCP	preprocessor	query.transid **!=** response.transid

Κάθε Modbus/TCP πακέτο περιλαμβάνει το, ενός byte, πεδίο αναγνωριστικού συναλλαγής (transaction ID), το οποίο μπορεί να πάρει οποιαδήποτε τιμή και είναι μοναδικό για την τρέχουσα συνδιαλλαγή. Ο κανόνας αυτός βλέπει ζεύγη πακέτων ερώτησης-απάντησης και ελέγχει εάν τα αναγνωριστικά συναλλαγής του ζεύγους ταιριάζει («!=» διάφορο). Όταν το πεδίο αυτό στο μήνυμα ερωτήματος δεν ταιριάζει με το πεδίο της αντίστοιχης απάντησης, πρέπει να σταλεί ειδοποίηση. Οι χρήστες οφείλουν να δοκιμάσουν τη συμπεριφορά του κάθε μεμονωμένου πελάτη και εξυπηρετητή Modbus/TCP ώστε να προσδιορίσουν την αντίδραση του συστήματος σε μη ταιριαστά πεδία αναγνωριστικού συναλλαγής. Τότε, βασιζόμενοι στην αντίδραση αυτή, οι χρήστες μπορούν να αποφασίσουν εάν θα μετατρέψουν αυτόν τον κανόνα ειδοποίησης σε έναν κανόνα απόρριψης. Τέλος, ο κανόνας 2 απαιτεί τη χρήση ενός προεπεξεργαστή που θα αποθηκεύει τα περιεχόμενα της τελευταίας ερώτησης για σύγκριση με την τρέχουσα απάντηση.

- **Κανόνας 3 – Ειδοποιεί εάν το μήκος του πεδίου μεγέθους δεν ταιριάζει με το πραγματικό υπόλοιπο μέγεθος του πακέτου.**

3	**Length**	TCP	standalone	trans.length **!=** actual_length

Το πεδίο μεγέθους (length field) του Modbus/TCP είναι ενός byte και καθορίζει τον αριθμό των bytes που απομένουν στο πακέτο μετά το πεδίο μήκους. Τα μεγέθη των πεδίων αναγνωριστικού μονάδας (unit ID) και κωδικού λειτουργίας (function code) είναι σταθερά και ανέρχονται σε 1 byte το καθένα. Η **εξίσωση επαλήθευσης** που χρησιμοποιεί ο κανόνας είναι: *Μέγεθος της συναλλαγής = Περιεχόμενο πεδίου μήκους (length field) + 1 byte (μέγεθος πεδίου αναγνωριστικού μονάδας) + 1 byte (μέγεθος πεδίου κωδικού λειτουργίας).*

- **Κανόνας 7 – Ειδοποιεί εάν η διεύθυνση MODBUS RTU δεν βρίσκεται στη λίστα των χρησιμοποιούμενων διευθύνσεων για το προστατευόμενο σύστημα.**

7	Serial Address	Serial	standalone	trans. addr $\notin$ usedADDR

Τα συστήματα Modbus/RTU και ASCII περιλαμβάνουν μια, μοναδιαίου byte, διεύθυνση που απευθύνεται σε έναν μοναδικό πελάτη για να απευθύνει πολλούς outstations. Κάθε διακομιστής MODBUS αντιστοιχίζεται με μια μοναδική διεύθυνση. Τα συστήματα Modbus συνήθως έχουν μια στατική διαμόρφωση, στην οποία ο αριθμός των σταθμών δεν αλλάζει και η ανάθεση διευθύνσεων των μεμονωμένων πελατών δεν αλλάζει. Η εξίσωση 5 ορίζει το νόμιμο εύρος διευθύνσεων για τα συστήματα MODBUS RTU και ASCII. Οι παρακάτω εξισώσεις ορίζουν τα σύνολα των χρησιμοποιούμενων διευθύνσεων για ένα συγκεκριμένο σύστημα Modbus, όπου το used(a) επιστρέφει τις διευθύνσεις που χρησιμοποιούνται για το προστατευόμενο σύστημα. Η διεύθυνση 0 είναι για πολλαπλή εκπομπή προς όλους τους σταθμούς και σημειώνεται ότι πολλά συστήματα απαγορεύουν τη χρήση της διεύθυνσης, για λόγους ασφάλειας. **Τα σύνολα που εξετάζονται** είναι:

α. $ADDR \in \{0, \ldots, 247\}$, ***β.*** $usedADDR \in \{used(a): a \in ADDR\}$

- **Κανόνας 9 – Ειδοποιεί όταν ο κώδικας λειτουργίας μιας ερώτησης δεν βρίσκεται στο σύνολο των επιτρεπόμενων κωδικών λειτουργίας.**

Σύμφωνα με τις προδιαγραφές του πρωτοκόλλου, ορίζονται 4 τύποι κωδικών λειτουργίας: οι δημόσιοι *(PC)*, εκείνοι που καθορίζονται από τον χρήστη *(UD)*, οι κρατούμενοι *(RD)* και κώδικες λειτουργίας σφάλματος.

9	**Query Function Codes**	TCP & Serial	standalone	query.fc ∉ allowedPC ∪ implementedUD ∪ usedRC

Κάθε τύπος ορίζεται από ένα σύνολο επιτρεπτών τιμών *(πχ. PC = {1,2,3,4,5,6,7,8,11,12,15,16,17,20,21,22,23,24,43})*. Οι δημόσιοι κώδικες μπορούν να περιοριστούν σε ένα υποσύνολο διαθέσιμων κωδικών *(allowedPC)* ανάλογα με την εφαρμογή και ορίζονται από τον χρήστη. Συνεπώς, οι κώδικες UD θα πρέπει να ανήκουν σε αυτό το εύρος τιμών. Οι χρήστες μπορούν να ορίσουν ένα ακόμη μικρότερο υποσύνολο *(implementedUD)* το οποίο ορίζει εκείνους τους κώδικες που τελικά εφαρμόζονται από τους χρήστες. Πριν την εφαρμογή του κανόνα, οι χρήστες θα πρέπει να ορίσουν ένα τελευταίο υποσύνολο, το οποίο περιλαμβάνει συνηθισμένους κώδικες που χρησιμοποιούσαν παλαιότερες συσκευές αλλά δεν περιλαμβάνονται πλέον στους δημόσιους. Οι κώδικες αυτοί αποτελούν το σύνολο των κρατούμενων κωδικών που χρησιμοποιεί το προστατευμένο σύστημα *(usedRC).* Με τον ίδιο τρόπο ορίζεται και ο κανόνας (ν.10) επιτρεπτών κωδικών λειτουργίας για τα αντίστοιχα μηνύματα απαντήσεων.

- **Κανόνας 11 – Εκπέμπει σφάλμα αν ο κωδικός λειτουργίας της απάντησης δεν ταιριάζει με τον αντίστοιχο της ερώτησης.**

11	**FC Query Response**	TCP & Serial	preprocessor	resp.fc ∉ {query. fc, query. fc + 0x80}

Οι κώδικες λειτουργίας της ερώτησης και της απάντησης πρέπει είτε να ταυτίζονται είτε ο κώδικας λειτουργίας της απάντησης να ισούται με τον αντίστοιχο της ερώτησης συν 0x80, το οποίο υποδηλώνει περίπτωση σφάλματος.

- **Κανόνες 15 έως 18 – Ειδοποιούν όταν ο κώδικας λειτουργίας είναι επιτρεπτός αλλά η διεύθυνση έναρξης των δεδομένων δεν ανήκει στη λίστα των χρησιμοποιημένων διευθύνσεων.**

15	**Coil Starting Address**	TCP & Serial	standalone	query. fc ∈ ca & query.starting_address ∉ usedA
16	**Discrete Input Starting Address**	TCP & Serial	standalone	query. fc ∈ da & query.starting_address ∉ usedA
17	**Holding Register Starting Address**	TCP & Serial	standalone	query. fc ∈ hra & query.starting_address∉ usedA
18	**Input Register Starting Address**	TCP & Serial	standalone	query. fc ∈ ira & query.starting_address∉ usedA

Το Modbus περιλαμβάνει ένα σύνολο κωδικών λειτουργίας για πρόσβαση σε δεδομένα και την ανάγνωση ή την εγγραφή διαφορετικών τύπων δεδομένων, όπως διακριτές εισόδους, «πηνία» και καταχωρητές. Αυτοί καθορίζονται από σύνολα κωδικών πρόσβασης στα πηνία *(ca)*, στις διακριτές εισόδους *(da)*, στους εσωτερικούς καταχωρητές *(hra)* και στους καταχωρητές εισόδου *(ira)*. Όπου *ca∈ {1, 5, 15}, da ∈ {2}, hra ∈ {3,6,16,23}, ira ∈ {4}, dafc ∈ ca ∪da ∪hra ∪ira.* Από το υπερσύνολο που ορίζει η τελευταία εξίσωση, οι διευθύνσεις δεν χρησιμοποιούνται καθολικά, από όλους τους Modbus servers. Το πρόγραμμα του διακομιστή θα δημιουργήσει μια κενή λίστα στην οποία θα γράψει εκείνες τις διευθύνσεις που χρησιμοποιεί *(usedA)*.

- **Κανόνες 28 και 29 – Ειδοποιούν εάν το πεδίο bytecount σε ένα μήνυμα απάντησης πακέτου πρόσβασης δεδομένων δεν ταιριάζει με τον αριθμό των αντικειμένων που ζητήθηκαν από το προηγούμενο αίτημα.**

Επιβεβαιώνοντας ότι οι κωδικοί λειτουργίας τόσο του αιτήματος όσο και της απάντησης ταιριάζουν, βεβαιώνει ότι οι κανόνες 28-29 δεν θα εκπέμψουν ειδοποίηση αν το πακέτο απάντησης περιέχει σφάλμα.

28	**bytecount coil/discrete**	TCP & Serial	preprocessor	query.fc ∈ {ca∪da} & resp.fc == query.fc & resp.bytecount ≠ bytecount(coil)
29	**bytecount register**	TCP & Serial	preprocessor	query.fc ∈ {hra∪ira} & resp.fc == query.fc & resp.bytecount ≠ bytecount(register)

Όπως γνωρίζουμε, τα πακέτα απάντησης περιλαμβάνουν τον κώδικα λειτουργίας, το bytecount και τα αντικείμενα δεδομένων που επιστρέφονται. Ο κάθε κώδικας λειτουργίας πρόσβασης δεδομένων ενεργοποιεί μια απάντηση από τον διακομιστή, η οποία περιλαμβάνει τη ζητούμενη ποσότητα δεδομένων «πηνίων», διακριτών εισόδων ή καταχωρητών. Το μέγεθος των πακέτων απάντησης διαφέρει ανάλογα με τον τύπο των δεδομένων που ζητήθηκαν αλλά και την ποσότητα των ζητηθέντων αντικειμένων. Από την μία τα πηνία και οι διακριτές είσοδοι είναι μονοδυναμικά, αλλά η ποσότητά αυτών που επιστρέφονται στρογγυλεύεται προς τα πάνω, δηλαδή στο πλησιέστερο byte. Από την άλλη, οι καταχωρητές έχουν 2 ολόκληρα bytes έκαστος. Συνεπώς, ο υπολογισμός των bytecounts, που περιλαμβάνεται στους κανόνες εκτελείται ως εξής: **α.** bytecount(coil) = quantity%8 + (quantity/8), **β.** bytecount(register) = quantity*23.

- **Κανόνες 42 και 43 – Εκπέμπουν ειδοποίηση όταν το εύρος διευθύνσεων πρόσβασης δεδομένων είναι έγκυρο, αλλά η απάντηση υποδεικνύει ένα σφάλμα με τον κωδικό εξαίρεσης 02.**

42	**Single Access Address Error**	TCP & Serial	pre-processor	query.fc ∈ sa & (query.starting address) ∈ usedA & resp.fc == query.fc+0x80 & resp.exception code==2
43	**Multiple Access Address Error**	TCP & Serial	pre-processor	query.fc ∈ ma & (query.starting address + query.quantity) ∈ usedA & resp.fc == query.fc+0x80 & resp.exception code==2

Ο κώδικας εξαίρεσης 02 χρησιμοποιείται για πολλαπλούς κωδικούς λειτουργίας και η πιο συνηθισμένη χρήση του είναι για εντολές πρόσβασης δεδομένων όταν το αιτούμενο εύρος διεύθυνσης δεν είναι έγκυρο. Για εντολές πρόσβασης δεδομένων που διαβάζουν ή γράφουν σε μονοδυναμικές θέσεις μνήμης, ο κώδικας 02 χρησιμοποιείται για να αναφέρει κάποιο σφάλμα στην αρχική διεύθυνση. Οι κωδικοί λειτουργίας πρόσβασης 1bit δεδομένων καθορίζονται από το σύνολο $sa \in \{5,6\}$, ενώ για πολλαπλές διευθύνσεις το σύνολο τιμών είναι $ma \in \{1,2,3,4,15,16,23\}$. Οι κανόνες 42 και 43 αναφέρονται στη μεταβλητή usedA, η οποία καθορίζεται από τον τύπο που δόθηκε στους κανόνες 15-18.

- **Κανόνες 44 και 45 – Εκπέμπουν ειδοποίηση όταν το εύρος διευθύνσεων δεν είναι έγκυρο, αλλά η απάντηση δεν είναι σφάλμα.**

42	**Single Access Address Error (2)**	TCP & Serial	pre-processor	query.fc ∈ sa & (query.starting address) ∉ usedA & resp.fc != query.fc+0x80
43	**Multiple Access Address Error (2)**	TCP & Serial	pre-processor	query.fc ∈ ma & (query.starting address + query.quantity) ∉ usedA & resp.fc != query.fc+0x80

- **Κανόνας 50 – Ειδοποιεί σε απάντηση με κώδικα εξαίρεσης 04.**

Αυτός ο κανόνας μπορεί να υποδείξει μια κυβερνοεπίθεση ή ένα ελαττωματικό Modbus-διακομιστή. Και τα δύο σενάρια είναι σημαντικά για την εφαρμογή του συγκεκριμένου κανόνα από τους διαχειριστές του συστήματος.

50	**Exception 04**	TCP & Serial	standalone	resp. exception code == 04

Ο κώδικας 04 υποδεικνύει ότι όλοι οι έλεγχοι του αιτήματος πέρασαν, ωστόσο η λειτουργία δεν υλοποιήθηκε με επιτυχία. Αυτός ο κώδικας εξαίρεσης μπορεί να υποδείξει είτε κάποιο απροσδιόριστο πρόβλημα με τον διακομιστή, είτε ότι ένας **εισβολέας έχει εισάγει μια κακόβουλη απάντηση για ένα έγκυρο αίτημα**.

4.3.2 Ανίχνευση κυβερνοεπιθέσεων SMOD

Στην σχετική έρευνα όπου μελετήθηκαν οι κυβερνοεπιθέσεις τύπου SMOD (βλ. 3.2.2), προτείνεται η ανάπτυξη μιας αρχιτεκτονικής IDS για την ενίσχυση της ασφάλειας σε Modbus/TCP επικοινωνίες. Το προτεινόμενο σύστημα ανίχνευσης εισβολών αποτελείται από δύο κύρια στοιχεία: τους αισθητήρες και τον διακομιστή. Οι αισθητήρες διανέμονται σε όλο το δίκτυο και είναι υπεύθυνοι για την καταγραφή και την ανάλυση της κίνησης των πακέτων Modbus/TCP σε κάθε υποδίκτυο. Συγκεκριμένα, κάθε αισθητήρας αποτελείται από δύο μονάδες: την Μονάδα Παρακολούθησης Κίνησης Δικτύου και την Μονάδα Εξαγωγής Ροής-Modbus. Ο διακομιστής, από την άλλη, λαμβάνει από τους διάφορους αισθητήρες τις ροές Modbus και αναγνωρίζει ποιες από αυτές σχετίζονται με μια επίθεση DoS. Ο διακομιστής περιλαμβάνει και αυτός δύο μονάδες: την Μονάδα Ανίχνευσης DoS και την Μονάδα Απάντησης. Παρακάτω διεξάγεται μια συνοπτική ανάλυση των λειτουργιών κάθε μονάδας του IDS συστήματος.

- **Μονάδα Παρακολούθησης Κίνησης Δικτύου:** Οι δραστηριότητες αυτής της μονάδας αποτελούν το πρώτο και βασικό στάδιο για την ανάπτυξη ενός αμυντικού μηχανισμού καθώς είναι υπεύθυνη για την τακτική παρακολούθηση της κίνησης στο δίκτυο. Για το σκοπό αυτό, χρησιμοποιήθηκε μια βιβλιοθήκη Scapy. Τα διάφορα **αρχεία καταγραφής πακέτων (PCAP)** δημιουργούνται βάσει δύο κριτηρίων: α) όταν το μέγεθος τους είναι ίσο με ένα συγκεκριμένο όριο ή β) όταν μια ορισμένη χρονική περίοδος ισούται με ένα δεύτερο όριο. Αυτά τα όρια καθορίζονται κάθε φορά ανάλογα με την περίπτωση χρήσης του IDS.
- **Μονάδα Εξαγωγής Ροών Modbus:** Η μονάδα εξαγωγής αρχικά λαμβάνει τα PCAP αρχεία που δημιουργήθηκαν από τη μονάδα που παρακολουθεί το δίκτυο. Στην συνέχεια, είναι υπεύθυνη για την εξαγωγή των αντίστοιχων ροών Modbus/TCP χρησιμοποιώντας ένα εξειδικευμένο λογισμικό (CICFlowMeter), το οποίο παράγει 83 χαρακτηριστικά για κάθε ροή Modbus. Αυτές οι ροές αποθηκεύονται σε μια βάση δεδομένων του διακομιστή και θα χρησιμοποιηθούν για την ανίχνευση DoS επιθέσεων.

- **Μονάδα Ανίχνευσης DoS:** Η μονάδα ανίχνευσης του διακομιστή, με την σειρά της, λαμβάνει τις ροές Modbus/TCP από τη βάση δεδομένων και αναλαμβάνει να εντοπίσει πιθανές επιθέσεις DoS. Η διαδικασία της ανίχνευσης χρησιμοποιεί μοντέλα μηχανικής μάθησης και ταξινόμησης. Τα παραγόμενα συμβάντα ασφαλείας της παραπάνω διαδικασίας αποθηκεύονται σε ένα διαφορετικό ευρετήριο της βάσης δεδομένων του διακομιστή. Η αποτελεσματικότητα αυτού του μοντέλου επεξεργασίας στην μονάδα ανίχνευσης σχολιάζεται παρακάτω.
- **Μονάδα Απάντησης:** Μέσω αυτής της μονάδας, ο διακομιστής ενημερώνει τον χρήστη για τα συμβάντα ασφαλείας που καταχωρήθηκαν μέσω μιας web-απεικόνισης.

Η σχετική έρευνα, από την οποία αντλήσαμε πληροφορίες, για να εκπαιδεύσει και να ελέγξει τα μοντέλα επεξεργασίας συνδύασε τα δεδομένα που συγκέντρωσε από ελληνική εγκατάσταση παραγωγής ενέργειας με διάφορα άλλα διαθέσιμα δεδομένα επιθέσεων DoS. Τα αποτελέσματα των έξι διαφορετικών αλγόριθμων που «έτρεξαν» τα δεδομένα αξιολογούνται στον παρακάτω, ώστε τα μοντέλα ανίχνευσης να εκπαιδευτούν κατάλληλα. Για αυτήν την αξιολόγηση, χρησιμοποιήθηκαν οι τέσσερις κρίσιμοι **μετρητικοί δείκτες: Accuracy, F1 score, True Positive Rate (TPR) και Precision**.

- $$\boldsymbol{Accuracy} = \frac{(\boldsymbol{True\ Positives + True\ Negatives})}{\boldsymbol{Total\ Samples}}$$
- $$\boldsymbol{Precision} = \frac{\boldsymbol{True\ Positives}}{(\boldsymbol{True\ Positives + False\ Positives})}$$
- $$\boldsymbol{True\ Positive\ Rate\ (TPR)} = \frac{\boldsymbol{True\ Positives}}{(\boldsymbol{True\ Positives + False\ Negatives})}$$
- $$\boldsymbol{F1 - score} = \frac{\boldsymbol{2 * (Precision * TPR)}}{(\boldsymbol{Precision + TPR})}$$

Μοντέλο	**Δείκτες**			
Αλγόριθμοι	Accuracy	Precision	TPR	F1
SVM-Linear	0.645	0.879	0.336	0.487
Random Forest	**0.811**	**0.964**	**0.647**	**0.774**
Naive Bayes	0.650	0.989	0.304	0.465
KNN	0.667	0.996	0.336	0.503
MLP	0.8017	0.942	0.642	0.764
AdaBoost	**0.812**	**0.964**	**0.647**	**0.775**

Σχήμα 4.3 - Αξιολόγηση αποτελεσμάτων ανίχνευσης DoS επιθέσεων.

Οι δείκτες μέτρησης τους πίνακα (4.1) καθορίζονται και περιγράφονται λεπτομερώς στην μελέτη που δημοσιεύτηκε από τους Π. Γραμματική και Π. Σαρηγιαννίδη, σχετικά με την αξιολόγηση IDS συστημάτων [45].

4.3.3 Ανίχνευση επιθέσεων υπερχείλισης

Η δεύτερη παρουσίαση εφαρμογών IDS σε επικοινωνίες Modbus/TCP, αφορά την **ανάπτυξη αμυντικού μηχανισμού προστασίας κατά των επιθέσεων υπερχείλισης (flood attacks)** που επίσης αναλύθηκαν στο κεφάλαιο 3. Στην προκειμένη περίπτωση θα εξετάσουμε τόσο μεθόδους ανίχνευσης βασισμένες στα ανωμαλίες (anomaly-based), όσο και βάσει υπογραφών.

A. IDS βάσει στατιστικής ή ανωμαλίας

Γενικότερα, η εφαρμογή της στατιστικής μεθόδου ανίχνευσης **σε επιθέσεις DoS**, είναι αρκετά χρήσιμη, διότι τέτοιες επιθέσεις **συνήθως συνοδεύονται από μεγάλες αλλαγές στις στατιστικές ιδιότητες** των παραμέτρων της επικοινωνίας. Ωστόσο, μια στατιστική μέθοδος κρίνεται τόσο από την ικανότητα ανίχνευσης των αλλαγών αυτών όσο και από το ποσοστό εσφαλμένων θετικών ενδείξεων. Μια αποδοτική στατιστική τεχνική, λόγω ανθεκτικότητας σε μεγάλες διακυμάνσεις των μοτίβων της φυσιολογικής επικοινωνίας, είναι ο Εκθετικά Σταθμισμένος Κινούμενος Μέσος Όρος (EWMA). Την τεχνική αυτή χρησιμοποιεί ο παρακάτω προτεινόμενος αλγόριθμος.

Ο αλγόριθμος ανίχνευσης αλλαγών EWMA χρησιμοποιεί ένα δυναμικό και προσαρμοστικό όριο για της παρατηρούμενες παραμέτρους του δικτύου δεδομένων, για τις οποίες ελέγχει εάν το έχουν υπερβεί. Αυτό το προσαρμοστικό κατώφλι βασίζεται στον εκτιμώμενο μέσο όρο, ο οποίος αναδιαμορφώνεται από τις πιο πρόσφατες παρατηρήσεις. Έτσι το σταθμισμένο όριο - για κάθε διάστημα λήψης δειγμάτων - χρησιμοποιείται για την λήψη αποφάσεων σχετικά με τις ανιχνευθείς αλλαγές στα εισερχόμενα πακέτα Modbus/TCP.

1. $x_t \geq (1 + \eta)\mu_t - 1$: Αυτή η συνθήκη χρησιμοποιείται για να εντοπίσει θετικές αλλαγές στις παρατηρούμενες παραμέτρους όπου το x_t αντιπροσωπεύει τον αριθμό των πακέτων Modbus που παρατηρούνται στο χρονικό διάστημα **t**. Η τιμή του x_t μπορεί να είναι είτε μια ατομική παρατήρηση, είτε μια μέση τιμή που υπολογίζεται χρησιμοποιώντας μια συγκεκριμένη περίοδο δειγματοληψίας. Η θετική παράμετρος **η** δηλώνει την κλιμακούμενη αλλαγή από τον μέσο **(μ)**. Μια σημαντική αλλαγή στο x_t που θα ικανοποιήσει παραπάνω σχέση υποδηλώνει και μια ανώμαλη συμπεριφορά.
2. $\mu_t = \lambda x_t + (1 - \lambda)\mu_t - 1$: Η μέση τιμή της παραμέτρου μ_t υπολογίζεται της EWMA των προηγούμενων παρατηρήσεων μέχρι το κάποιο συγκεκριμένο χρονικό διάστημα δειγματοληψίας. Το **λ** αποτελεί τον EWMA παράγοντα ($0 \geq \lambda \geq 1$ ισούται με το αντίστοιχο βάρος που δίνεται στις πιο πρόσφατες τιμές της μ_t πριν από το τρέχον χρονικό διάστημα.

Β. IDS βάσει υπογραφής

Εδώ η μέθοδος ανίχνευσης βάσει υπογραφής χρησιμοποιεί πάλι το γνωστό σύστημα ανοιχτού κώδικα Snort, χρησιμοποιώντας έναν Modbus προεπεξεργαστή. Το μετασχηματισμένο buffer περνά στη συνέχεια στη μηχανή εντοπισμού του Snort, η οποία ανιχνεύει κίνηση που αντιστοιχεί σε μια υπογραφή ή κανόνα και δημιουργεί συναγερμούς. Παρόμοια με την προηγούμενη μέθοδο, τα αντίστοιχα κατώφλια του Snort εμπεριέχονται στους κανόνες του ή τμήματα κανόνων. Έτσι με βάσει τα όρια αυτά οι κατάλληλοι κανόνες εντοπίζουν τις διάφορες ανωμαλίες στην κίνηση του δικτύου που προκύπτουν από επιθέσεις DoS.

Η τυπική μορφή του κατωφλίου σε κανόνα Snort είναι η εξής: ***threshold****: type threshold, track <by src|by dst>, count <c>, seconds <s>.* Ο ρυθμός κατωφλίου μπορεί να παρακολουθείται ανάλογα με τη διεύθυνση προέλευσης *(by src)* ή τη διεύθυνση προορισμού *(by dst)* των πακέτων, για έναν αριθμό *(c)* που καθορίζει τον αριθμό των ειδοποιήσεων εντός του καθορισμένου χρόνου *(s)*. Παρόλο που μιλάμε για IDS βασισμένο στις υπογραφές, για να αποφευχθεί το παράδοξο των false-positive ειδοποιήσεων, οι οριακές τιμές που χρησιμοποιούνται στον κανόνα του Snort πρέπει να βασίζονται σε κάποιο στατιστικό μέσο της φυσιολογικής κίνησης. Διαφορετικά, οι τιμές αυτές πρέπει να προσδιορίζονται εμπειρικά ή βάσει κάποιων πειραματικών ενδείξεων. Δεδομένου ότι οι επιθέσεις που αναφέρθηκαν στο προηγούμενο κεφάλαιο, πλημμυρίζουν τη θύρα

TCP 502 για να εγγράψουν μια τιμή (πχ. σε ένα Modbus coil), οι κανόνες του Snort οφείλουν να εξεταστούν συνεχώς τα περιεχόμενα του Modbus φορτίου. Η λέξη κλειδί που χρησιμοποιείται για τον εντοπισμό συγκεκριμένων μοτίβων έχει την μορφή (content:[!]''<content string>'';). Οι κανόνες που αφορούν το περιεχόμενο, συνήθως εφαρμόζονται μαζί με τους κανόνες κατωφλίου ώστε να επιτευχθεί υψηλότερη ακρίβεια στην ανίχνευση των επιθέσεων.

Η σύγκριση των παραπάνω μεθόδων διεξάγεται στα συμπεράσματα της παρούσας εργασίας (κεφάλαιο 5.)

4.4. Συστήματα πρόληψης και ανίχνευσης εισβολών σε επικοινωνία DNP3

4.4.1. Στατιστική ανίχνευση επίθεσης ενδιάμεσου εισβολέα

Σε κάθε σύστημα IDS, έτσι και για τις DNP3 επικοινωνίες, υπάρχουν δύο σημεία στα οποία είναι εφικτός ο εντοπισμός μιας εισβολής. Στην προηγούμενη ανάλυση ασχοληθήκαμε με συστήματα ανίχνευσης που επικεντρώνονται στην παρακολούθηση της κίνησης σε όλο δίκτυο, ενώ τώρα θα αναλυθεί περισσότερο η **δυνατότητα εντοπισμού κακόβουλης δραστηριότητας στο επίπεδο του υπολογιστή-οικοδεσπότη (host)**. Αντιστοίχως και σε αυτήν την περίπτωση, μπορούν να χρησιμοποιηθούν αρχεία καταγραφής και τεχνικές μηχανικής μάθησης (πχ. στατιστική ανάλυση), προκειμένου να βελτιστοποιηθούν οι διαδικασίες για την αντιμετώπιση των εισβολών. Επιπλέον, η αποτροπή κακόβουλων ενεργειών μπορεί να επιτευχθεί και μέσω αναγνώρισης προτύπων και μοτίβων πάνω στην δικτυακή κίνηση μεταξύ των νόμιμων συσκευών και των επιτιθέμενων.

Στην παρούσα ενότητα, αναπτύσσονται στρατηγικές και τεχνικές αντιμετώπισης θεωρώντας ως κύριο κίνδυνο επιθέσεις ενδιάμεσου εισβολέας σε περιβάλλον DNP3 επικοινωνίας. Η βασική ιδέα και στρατηγική είναι η συνεχής μέτρηση της μέσης καθυστέρησης χρόνου επιστροφής T_{rtrip} , μεταξύ των νόμιμων συσκευών που επικοινωνούν, για κάθε αίτημα και απάντηση, εκτελώντας δυναμικές προσαρμογές στο μέγιστο επιτρεπτό χρονικό διάστημα. Το μετρούμενο διάστημα πρέπει πάντα να είναι ισοδύναμο με το διάστημα $T_{rtrip} + \Delta_{SM}$, όπου το Δ_{SM} είναι ένα ασφαλές επιπλέον χρονικό όριο για την εκτέλεση του κύκλου και ορίζεται από τον διαχειριστή. Η υπέρβαση αυτού του χρονικού διαστήματος αποτελεί και το βασικό κριτήριο που θα αποτρέψει τους επιτιθέμενους από το να εκτελέσουν οποιαδήποτε επίθεση εισαγωγής ψευδών στοιχείων, καθώς τα πλαστά πακέτα θα απορρίπτονται αυτόματα από τον παραλήπτη. Οι τρεις τεχνικές που παρουσιάζονται στην βιβλιογραφική έρευνα είναι οι παρακάτω:

Α. Ρύθμιση της μέσης διάρκειας επιστροφής

Η μέση διάρκεια επιστροφής ισούται με την μέση τιμή του χρόνου που απαιτείται για έναν κύκλο ερωτο-απάντησης σε έναν κεντρικό ελεγκτή ή μια απομακρυσμένη μονάδα. Για την μέτρηση χρησιμοποιείται εσωτερικά το εργαλείο RTTA (Round Trip Timing Agent), ενώ τα βήματα που πρέπει να εκτελεστούν για την σωστή μέτρηση είναι ως εξής.

- ✓ Εγκαθίδρυση μιας συνεδρίας DNP3, ανάμεσα στον κεντρικό ελεγκτή και την απομακρυσμένη μονάδα.
- ✓ Υπολογισμός του μέσου χρονικού διαστήματος κύκλου επιστροφής (T_{rtrip}),για τα πακέτα DNP3, εκτελώντας το RTTA στον κεντρικό ελεγκτή και την απομακρυσμένη μονάδα.
- ✓ Δημιουργία ενός αρχείου απλού κειμένου για την καταγραφή των καθυστερήσεων για κάθε ανταλλαγή DNP3πακέτου.

✓ Υπολογισμός του μέσου χρόνου καθυστέρησης επιστροφής T_{rtrip} .

Β. Αλγόριθμος Διέλευσης/Απόρριψης

Κατά την ανταλλαγή πακέτων μεταξύ του κεντρικού ελεγκτή και της απομακρυσμένης μονάδας, υπολογίζεται η καθυστέρηση στην επιστροφή για κάθε ανταλλαγή πακέτων DNP3. Κατόπιν, δημιουργείται ο μέσος όρος των καθυστερήσεων, ως T_{rtrip} . Στην συνέχει εκτελείται η ακόλουθη εξίσωση:

$$\boldsymbol{\Delta} = (T_{arrival} - T_{transmitted} - \tfrac{1}{2}T_{rtrip})$$

Οι τιμές $T_{arrival}, T_{transmitted}$ αντιστοιχούν στις πραγματικές χρονοσημάνσεις για το επιστρεφόμενο πακέτο και για τη συμμετρική ανταλλαγή πακέτων μεταξύ των master/slave, το $\boldsymbol{\frac{1}{2}T_{rtrip}}$ αντιπροσωπεύει το μισό του μέσου χρόνου επιστροφής για είτε τα αιτήματα είτε τις απαντήσεις πακέτων και το **Δ** αντιπροσωπεύει την απόκλιση από τη μέση τιμή. Αν η απόκλιση είναι μεταξύ του μηδενός και μιας ασφαλούς απόστασης Δ_{SM} (safety margin), τότε ο κεντρικός ελεγκτής θα αποδεχτεί το πακέτο, διαφορετικά το πακέτο θα απορριφθεί. Η τιμή Δ_{SM} πρέπει να επιλεγεί προσεκτικά ώστε ο επιτιθέμενος να μην έχει αρκετό χρόνο για την εκτέλεση οποιασδήποτε επίθεσης. Ο ακόλουθος αλγόριθμος εξηγεί την ακολουθία των απαιτούμενων ενεργειών:

✓ Κάθε κόμβος θα μετρά τον μέσο χρόνο γύρου επιστροφής T_{rtrip} για κάθε ανταλλαγή πακέτων DNP3.
✓ Ο κεντρικός ελεγκτής στέλνει ένα πακέτο DNP3/TCP στην απομακρυσμένη μονάδα, με τους αριθμούς ακολουθίας (SN) και τον αριθμό αναγνώρισης (AN) στην κεφαλίδα του.
✓ Η απομακρυσμένη μονάδα επιστρέφει την αντίστοιχη απάντηση στο αίτημα του κεντρικού ελεγκτή.
✓ Ο κεντρικός ελεγκτής ταυτόχρονα παρακολουθεί τον χρόνο κύκλου, για το πακέτο απάντησης που λαμβάνει, και τον συγκρίνει με το υπολογισμένο T_{rtrip} . Αν η απόκλιση υπερβαίνει την ασφαλή απόσταση, τότε το πακέτο απορρίπτεται και πραγματοποιείται επανάληψη αποστολής.

Γ. Τεχνική περιορισμού κινδύνου

Την παραπάνω στρατηγική επαναλήψεων, μετρήσεων και υπολογισμών ακολουθούν οι τεχνικές αντιμετώπισης των κινδύνων. Στο προκείμενο παράδειγμα, καταγράφονται δύο βασικοί κίνδυνοι. Ο πρώτος είναι, κατεστραμμένα πλαίσια-TCP στα πακέτα που μεταδίδονται και ο δεύτερος είναι η αποτυχία παραλαβής των πλαισίων αυτών από τον παραλήπτη. Εάν το πλαίσιο αυτό δεν φτάσει με επιτυχία, ο εσωτερικός χρονοδιακόπτης που συσχετίζεται με κάθε πλαίσιο θα λήξει πριν από την επιβεβαίωση λήψης του πλαισίου. Δηλαδή, ο χρονοδιακόπτης TCP που ενθυλακώνει τα πακέτα DNP3, δεν πρέπει να είναι ούτε πολύ μικρός ώστε να προκαλεί πολλές περιττές επαναλήψεις, ούτε πολύ μεγάλος ώστε να προκαλεί καθυστέρηση απόκρισης για τα χαμένα πλαίσια. Σε κάθε περίπτωση θα πρέπει να ρυθμιστεί έτσι ώστε να είναι μεγαλύτερος από την καθυστέρηση του χρόνου επιστροφής.

Η σωστή ρύθμιση θα επιτευχθεί μετά από απαραίτητες δοκιμές στην επικοινωνία και είναι αυτή που τελικά θα καθορίσει εάν θα αποτραπούν οι MitM επιθέσεις. Τόσο ο κεντρικός ελεγκτής όσο και η απομακρυσμένη μονάδα θα χρησιμοποιήσουν τη μέση καθυστέρηση του χρόνου επιστροφής που υπολογίστηκε στο μέρος Α, για να ρυθμίσουν τον χρονοδιακόπτη τους. Οποιεσδήποτε καθυστερήσεις προκαλούνται από τον επιτιθέμενο υπερβαίνοντας την ασφαλή

απόσταση, θα ενεργοποιήσουν μια επανάληψη αποστολής προς το αρχικό πακέτο και έτσι θα ανιχνευτεί η ανωμαλία που προκύπτει στην επικοινωνία.

4.4.2. Προτάσεις αντιμετώπισης υπερχείλισης μνήμης γεγονότων

Ο βασικός λόγος που η επίθεση υπερχείλισης μνήμης πετυχαίνει είναι ότι ο χώρος του buffer είναι κοινόχρηστος σε πολλούς πηγές και η χρήση του ακολουθεί τον κανόνα "πρώτα έρχεται, πρώτα εξυπηρετείται". Όταν η προσωρινή μνήμη είναι γεμάτη, η ροή δεδομένων που λαμβάνονται είναι πάντα ανάλογη του ρυθμού εισαγωγής των δεδομένων στην μνήμη, σύμφωνα με την παραπάνω πολιτική. Έτσι, μια ροή με υψηλό φορτίο (όπως αυτή της δοκιμής στο 3.3.3) μπορεί να καταλάβει το μεγαλύτερο μέρος του διαθέσιμου εύρους ζώνης και να επηρεάσει τις ροές χαμηλού φορτίου.

Μια διαφορετική πολιτική προγραμματισμού που σχεδιάστηκε με στόχο να παρέχει μια δίκαιη εξυπηρέτηση είναι η RR (round robin), η WRR (weighted round robin) και η σταθμισμένη ουρά (weighted fair queueing). Σε αυτό το πλαίσιο, οι πολιτικές προγραμματισμού δίκαιης εξυπηρέτησης προσπαθούν να διασφαλίσουν ότι κάθε ροή εισόδου έχει εξασφαλισμένο χώρο στην μνήμη παρέχοντας και έναν πρόσθετο χώρο, ο οποίος θα κατανέμεται ισότιμα ανάμεσα σε ροές που τον χρειάζονται περισσότερο. Επομένως, μια λογική αμυντική πρακτική κατά επιθέσεων υπερχείλισης μνήμης είναι η διάθεση χώρου σε ένα κοινό buffer γεγονότων, σύμφωνα με την παραπάνω πολιτική. Για παράδειγμα, ο RR-προγραμματισμός θα μπορούσε να είναι μια καλή επιλογή λόγω της χαμηλής πολυπλοκότητας χρόνου O(1) και του χαμηλού κόστους υλοποίησης.

Σύμφωνα με την ανάλυση που προηγήθηκε στο κεφάλαιο 2 για το πρωτόκολλο DNP3, η κεφαλίδα εφαρμογής στην απάντηση κάθε εξωτερικού DNP3-σταθμού περιέχει τις **εσωτερικές ενδείξεις - IIN**. Τα bits σε αυτές τις δύο οκτάδες υποδηλώνουν συγκεκριμένες καταστάσεις του σταθμού, **όπου το 3ο bit της δεύτερης οκτάδας υποδεικνύει ότι υπάρχει υπερχείλιση της μνήμης-γεγονότων.** Δηλαδή, τουλάχιστον ένα μη επιβεβαιωμένο γεγονός χάθηκε επειδή τα ο συγκεκριμένος buffer δεν παρείχε αρκετό χώρο για την προσωρινή αποθήκευση της πληροφορίας. Αυτή η ένδειξη, ουσιαστικά παρέχει στην κύρια DNP3-συσκευή ένα μέσο ανίχνευσης για το πότε συμβαίνει μια υπερχείλιση. Καθώς αυτή η λειτουργία παρέχεται εξ' αρχής στο πρωτόκολλο, η ομάδα χρηστών του DNP3 παρέχει και τις αντίστοιχες οδηγίες αντιμετώπισης του ζητήματος. Έτσι πολλοί κατασκευαστές ήδη ακολουθούν τις οδηγίες αυτές εκδίδοντας έναν **έλεγχο ακεραιότητας,** κατά τον οποίο **αποκαθίσταται εκ νέου η τρέχουσα κατάσταση όλων των δεδομένων** στον εξωτερικό σταθμό. Δυστυχώς, αυτή η ενέργεια δεν είναι αρκετή για να προστατεύσει τη συσκευή από επιθέσεις υπερχείλισης, διότι ο έλεγχος ακεραιότητας εκδίδεται παθητικά με την παραλαβή μιας απάντησης από το σταθμό και άρα μπορεί μόνο να καθυστερήσει την επόμενη και σχεδόν βέβαιη υπερχείλιση της μνήμης. Πιο συγκεκριμένα, ο έλεγχος ακεραιότητας αντί απλώς να ζητήσει τα αλλαγμένα γεγονότα, ζητά όλα τα στατικά δεδομένα δημιουργώντας έτσι πολλούς ελέγχους ακεραιότητας. Αυτό ενδέχεται να οδηγήσει σε υπερχείλιση δικτυακής σύνδεσης μεταξύ του συλλέκτη δεδομένων και του κέντρου ελέγχου, με αποτέλεσμα να σπαταλήσει κατά λάθος πόρους επεξεργασίας και το διαθέσιμο εύρος ζώνης. Μια πιθανή επίλυση θα ήταν η **εφαρμογή πολιτικών βασισμένων σε κανόνες** για τον περιορισμό και το φιλτράρισμα της κυκλοφορίας σε κατάσταση επίθεσης. Για παράδειγμα, όταν ένας ρελέ προκαλεί τρεις συνεχόμενες θετικές ενδείξεις υπερχείλισης μνήμης γεγονότων, τότε ο συλλέκτης δεδομένων θα φιλτράρει κάθε κυκλοφορία DNP3-δεδομένων όπου η διεύθυνση αποστολής αντιστοιχεί στο αντίστοιχο ρελέ. Ο κανόνας θα συνεχίζει να ισχύει εφόσον οι

επακόλουθες κινήσεις του ρελέ υπερβούν ένα καθορισμένο όριο. Εάν επίσης, οι κανόνες εφαρμοστούν σε συνδυασμό με αλγορίθμους δίκαιης εξυπηρέτησης, τότε ο δείκτης υπερχείλισης μπορεί να συσχετιστεί με ένα ελάχιστο βάρος και, ως εκ τούτου, να ελαχιστοποιηθεί το μέγεθος της κυκλοφορίας δεδομένων επίθεσης που εισέρχεται στην μνήμη γεγονότων.

Τέλος, θα πρέπει οπωσδήποτε να αναφερθούμε στην **έλλειψη αυθεντικοποίησης του DNP3**, η οποία επιτρέπει στους επιτιθέμενους να πλαστογραφούν τους νόμιμους εξωτερικούς σταθμούς του DNP3 συστήματος. Οι ερευνητές εργάζονται ενεργά πάνω σε διάφορες **μορφές λύσεων βασισμένων στην κρυπτογράφηση** για να ενισχύσουν τα επίπεδα αυθεντικοποίησης στα περιβάλλοντα των SCADA. Οι μελέτες αυτές επικεντρώνονται στην εφαρμοσιμότητα διάφορων μορφών διαχείρισης κλειδιών, τεχνικών βασισμένων σε γρίφους για την αποτροπή των επιθέσεων DoS σε ένα δίκτυο μεγάλης κλίμακας ή την αξιολόγηση βελτιωμένων πρωτοκόλλων DNP3, όπως το DNP3 Secure Authentication ή το DNPSec. Καθώς το τελευταίο επικεντρώνεται στην ενίσχυση του ίδιου του πρωτοκόλλου, θα αναπτυχθεί περισσότερο στην επόμενη ενότητα.

4.4.3. Πλαίσια πρόληψης της DNP3 επικοινωνίας

Για την αντιμετώπιση υποκλοπών και τροποποίησης πακέτων DNP3, αλλά και για την πληθώρα πιθανών κυβερνοεπιθέσεων που εκμεταλλεύονται την έλλειψη αυθεντικοποίησης, προτείνονται διάφορες λύσεις ενίσχυσης της ασφάλειας του πρωτοκόλλου. Η έκδοση των παρακάτω βελτιωμένων πρωτοκόλλων προτύπου DNP3, επιτελούν ακριβώς αυτήν την ανάγκη.

- ✓ **DNPSec:** Το DNPSec είναι ένα προτεινόμενο πλαίσιο ασφαλείας για το DNP3, το οποίο **παρέχει αποτελεσματικά εχεμύθεια, αυθεντικότητα και ακεραιότητα** στην επικοινωνία. Για να κρυπτογραφήσει και να αυθεντικοποιήσει τα DNP3 πλαίσια, το DNPSec τροποποιεί την κλασική δομή του επιπέδου σύνδεσης-δεδομένων. Στο πλαίσιο αυτό, η κρυπτογράφηση και η αυθεντικοποίηση εκτελούνται χωριστά. Το DNPSec ενθυλακώνει το αρχικό πλαίσιο ενός DNP3 πακέτου με μια νέα κεφαλίδα, έναν νέο αριθμό ακολουθίας πλαισίου και δεδομένα αυθεντικοποίησης. Επιπλέον, χρησιμοποιεί ένα κλειδί συνεδρίας για να κρυπτογραφήσει και να αυθεντικοποιήσει το πλαίσιο, το οποίο ενημερώνεται κάθε φορά που λήγει ο χρόνος της συνεδρίας ή όταν ο νέος αριθμός ακολουθίας φτάσει το όριό του. Σε αυτό το πρωτόκολλο μπορούν να χρησιμοποιηθούν αρκετοί αλγόριθμοι κρυπτογράφησης και αυθεντικοποίησης, όπως το πρότυπο τριπλής κρυπτογράφησης δεδομένων (3-DES) και ο αλγόριθμος ασφαλούς κατακερματισμού (HMAC-SHA-1).
- ✓ **DNP3 Secure Authentication**: Το DNP3 SA είναι μια επέκταση ασφαλείας για το επίπεδο εφαρμογής DNP3 και εισάγει στο πρωτόκολλο λειτουργίες αυθεντικοποίησης. Η αυθεντικοποίηση αυτή βασίζεται σε τεχνολογίες ανοικτού κώδικα και χρησιμοποιεί έναν μηχανισμό πρόκλησης-απόκρισης μέσω του HMAC αλγορίθμου. Υποστηρίζει επίσης την ασύμμετρη και συμμετρική κρυπτογραφία για τη διαχείριση κλειδιών. Το DNP3 SA είναι αρκετά αποτελεσματικό και καταφέρνει να προστατεύσει το σύστημα SCADA από επιθέσεις πλαστογράφησης, τροποποίησης και επανάληψης πακέτων.
- ✓ **Authenticated Encryption:** Η αυθεντικοποιημένη κρυπτογράφηση είναι ένας διαφορετικός τρόπος λειτουργίας της κρυπτογράφησης που προτείνεται στην υπάρχουσα βιβλιογραφία, η οποία παρέχει ταυτόχρονα εμπιστευτικότητα, ακεραιότητα και αυθεντικότητα στο σύστημα επικοινωνίας. Η διαδικασία αυτή πετυχαίνει να συνδυάζει αποδοτικά την κρυπτογράφηση και την αυθεντικοποίηση, σε μια μόνο λειτουργία. Ο σκοπός της λειτουργίας να

προστατεύει τα δεδομένα από μη εξουσιοδοτημένη πρόσβαση και εξωτερικές παρεμβολές, παρέχοντας εγγύηση για την αληθινή ταυτότητα του αποστολέα. Συνήθως χρησιμοποιείται σε πολλά πρωτόκολλα ασφαλείας για την ασφάλεια των επικοινωνιών και την πρόληψη επιθέσεων. Στο DNP3 ανακατασκευάζει το πλαίσιο εφαρμογής και προσθέτει ένα νέο με τις απαραίτητες λειτουργίες κρυπτογράφησης. Χρησιμοποιεί τον GCM (Galois / Counter Mode) τρόπο κρυπτογράφησης ο οποίος είναι πολύ αποδοτικός από άποψη κόστους , καθώς απαιτεί λιγότερο χώρος μνήμης.

4.5. Συστήματα πρόληψης και ανίχνευσης εισβολών στο IEC 60870-5

4.5.1. Το πρότυπο ασφαλείας IEC 62351 - για επικοινωνίες IEC 60870-5

Η Διεθνής Ηλεκτροτεχνική Επιτροπή (IEC) **για την ενίσχυση και επίλυση ζητημάτων ασφαλείας σε συστήματα και πρωτόκολλα** που χρησιμοποιούνται κυρίως σε αυτοματοποιημένα συστήματα ηλεκτρικής ενέργειας, **εκδίδει το πρότυπο IEC 62351**. Δεν πρόκειται για κάποια καθοριστική εξέλιξη στον τομέα της κυβερνοασφάλειας των πρωτοκόλλων της IEC, αλλά μια λογική αναβάθμιση των πρωτοκόλλων που περιλαμβάνει μέτρα πρόληψης και αντιμετώπισης κάποιον ζητημάτων. Πριν ασχοληθούμε λοιπόν με εξειδικευμένα συστήματα IDS για τα IEC 60870-5 και IEC 61850, θα αξιολογηθεί αρχικά το πώς το πρότυπο IEC 62351 αντιμετωπίζει τα θέματα ασφαλείας σε υπάρχοντα συστήματα και σε ποιο βαθμό μπορεί να επιλύσει αυτά τα θέματα. Το IEC 62351 αποτελείται από κάποια βασικά μέρη, ωστόσο βρίσκεται ακόμη υπό συνεχή εξέλιξη και πιθανότατα θα περιλαμβάνει επιπλέον μέρη στο μέλλον. Το πρότυπο ασχολείται με την IT-ασφάλεια για διεργασίες ελέγχου σε συστήματα ενέργειας και ο **απώτερος στόχος του είναι να διατηρηθούν οι ιδιότητες της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας** σε ένα σύστημα, κυρίως μέσω της εισαγωγής μηχανισμών αυθεντικοποίησης.

Παρακάτω γίνεται μια παρουσίαση του περιεχομένου και των δυνατοτήτων του προτύπου ως προς την ασφάλεια που προσφέρει, δίνοντας βάρος στα τμήματα που αναφέρονται σε επικοινωνίες IEC 60870-5. Συγκεκριμένα, το πρότυπο διαιρείται σε δέκα διαφορετικά μέρη που περιλαμβάνουν προδιαγραφές ασφαλείας σε διάφορους τομείς. Παρακάτω περιγράφονται τα πρώτα πέντε, ενώ τα υπόλοιπα θα παρουσιαστούν στην ενότητα 4.5 του παρόντος κεφαλαίου.

Μέρος προτύπου	Τίτλος	Περιεχόμενο
IEC 62351-1	Εισαγωγή στα Ζητήματα Ασφάλειας Επικοινωνιακών Δικτύων και Συστημάτων	Γενική επισκόπηση του προτύπου IEC 62351. Γενικές πληροφορίες σχετικά με την ασφάλεια. Παραδείγματα κυβερνοαπειλών Επισκόπηση δυνατών μέτρων αντιμετώπισης. Περιγραφή εννοιών, όπως αξιολόγηση κινδύνων, διαχείριση κλειδιών και διαδικασίες ασφαλείας.
IEC 62351-2	Γλωσσάρι Όρων	Εξηγούνται όροι, όπως Έλεγχος Πρόσβασης, Ασφάλεια Δεδομένων, κ.λπ.
IEC 62351-3	Προφίλ που περιλαμβάνουν TCP/IP	Προστασία χρήσης του Επιπέδου Μεταφοράς Ασφάλειας (TLS) για πρωτόκολλα βασισμένα σε TCP/IP. Διασφάλιση αυθεντικότητας και ακεραιότητας των δεδομένων στο επίπεδο μεταφοράς, χρησιμοποιώντας μηχανισμούς κρυπτογράφησης του TLS. Απαίτηση διπλής πιστοποίησης πελάτη-εξυπηρετητή, κ.ά.
IEC 62351-4	Προφίλ που περιλαμβάνουν MMS	Ασφάλεια του προφίλ επικοινωνίας MMS και συστάσεις για τα A-Προφίλ και T-Προφίλ βάσει TCP/IP. A-Προφίλ: Περιγράφεται μια πιστοποίηση εφαρμογών. T-Προφίλ/TCP: Χρήση του TLS ως ένα επίπεδο μεταξύ TCP και ISO Transport Service, χρησιμοποιώντας διαφορετική θύρα-TCP για ασφαλείς συνδέσεις. Σουίτες κρυπτογράφησης TLS.

IEC 62351-5	**Ασφάλεια για το IEC 60870-5 και τα παράγωγά του**	Προδιαγραφή ασφάλειας για πρωτόκολλα ανταλλαγής μηνυμάτων που σχετίζονται με το IEC 60870-5, όπου η πιστοποίηση πρέπει να γίνεται για κάθε μήνυμα ξεχωριστά. Οι μηχανισμοί ασφαλείας λαμβάνουν υπόψη την περιορισμένη διαθέσιμη επεξεργαστική ισχύ στις επηρεαζόμενες συσκευές. Περιγραφή μηχανισμών απομακρυσμένης και τακτικής ενημέρωσης κλειδιών ασφαλείας.

Σχήμα 4.4 – Προδιαγραφές προτύπου ασφαλείας IEC 62351 – Μέρος Α.

Το βασικό περιεχόμενο του μέρους -5 στο πρότυπο IEC 62351 είναι η προδιαγραφή ενός πρόσθετου **μηχανισμού πρόληψης και αυθεντικοποίησης που χρησιμοποιεί το HMAC,** με τον αντίστοιχο τρόπο που παρουσιάστηκε στην προηγούμενη ενότητα. Τα μηνύματα ASDU που θεωρούνται κρίσιμα περιλαμβάνουν πεδία αυθεντικοποίησης του μηνύματος αιτήματος ή απάντησης, όπου ο αποστολέας με τον παραλήπτη οφείλουν να ανταλλάσσουν μεταξύ τους σε μια αλληλουχία. Η ενημέρωση των κλειδιών αυθεντικοποίησης είναι ένα σημαντικό κομμάτι της προδιαγραφής, όπου περιγράφονται διατάξεις για την απομακρυσμένη και τακτική ενημέρωσή τους, χρησιμοποιώντας τόσο συμμετρικά όσο και ασύμμετρα κλειδιά.

Αξιολογώντας τους αλγορίθμους που περιλαμβάνει το IEC 62351-5 φαίνεται ότι το πρότυπο είναι αρκετά αποτελεσματικό ως προς τους στόχους που είχε η ανάπτυξή του. Δηλαδή πετυχαίνει σε ικανοποιητικό βαθμό να αντιμετωπίσει τα θέματα αυθεντικοποίησης και ακεραιότητας κρίσιμων μηνυμάτων. Ωστόσο, το θέμα της εμπιστευτικότητα των μηνυμάτων, εκτός από εκείνα της ενημέρωσης κλειδιών, παραμένει ένα «κενό» σημείο στην συγκεκριμένη προδιαγραφή. Στην συνέχεια μελετάμε **τα βασικά προβλήματα ασφαλείας του προτύπου**, σύμφωνα με την διαθέσιμη βιβλιογραφία:

- **Ακύρωση κλειδιών συνεδρίας:** Η διαχείριση μηνυμάτων, κατά το πρότυπο, περιγράφει ότι τα κλειδιά συνεδρίας ακυρώνονται αφού ένας σταθμός έχει λάβει έναν συγκεκριμένο αριθμό μηνυμάτων που περιέχουν μη έγκυρα δεδομένα αυθεντικοποίησης. Ωστόσο, καθώς δεν υπάρχει βασική αυθεντικοποίηση των υπόλοιπων μηνυμάτων εκτός προδιαγραφής IEC 62351-5, είναι πιθανό ληφθούν παραποιημένα μηνύματα με πλαστά δεδομένα αυθεντικοποίησης. Για παράδειγμα, ένας σταθμός «Γ» στέλνει ένα μήνυμα με μη-έγκυρα δεδομένα αυθεντικοποίησης σε έναν σταθμό «Β», παραποιώντας το μήνυμα ώστε να φαίνεται ότι είχε αποσταλεί από τον σταθμό «Α». Μετά από αρκετά τέτοια μηνύματα, ο σταθμός-Β θα ακυρώσει το κλειδί συνεδρίας που έχει ανταλλάξει με τον σταθμό-Α, παρόλο που Α δεν έχει στείλει κανένα παραποιημένο μήνυμα. Έτσι, την επόμενη φορά που ο σταθμός-Α θα προσπαθήσει να επικοινωνήσει με τον Β, τότε ο πρώτος θα ενημερωθεί ότι το κλειδί συνεδρίας είναι άκυρο και χρειάζεται ανανέωση. Εάν αυτές οι επιθέσεις συνεχίζονται αέναα, η αποστολή κρίσιμων μηνυμάτων μεταξύ των σταθμών Α και Β καταρρέει ολοκληρωτικά. Συνεπώς, η συγκεκριμένη διαχείριση των κλειδιών αντί να εντοπίζει το πραγματικό σημείο της επίθεσης, οδηγεί την επικοινωνία άλλων σημείων σε αδιέξοδο. Αντίστοιχα ζητήματα κακοδιαχείρισης των κλειδιών ισχύουν και σε άλλες περιπτώσεις και σε καμιά περίπτωση δεν μπορεί η συγκεκριμένη λειτουργιά να θεωρηθεί αποτελεσματική προστασία της επικοινωνίας από κυβερνοεισβολείς.
- **Εκμετάλλευση μηχανής καταστάσεων – DoS:** Το πρότυπο IEC 62351-5 περιέχει μια λεπτομερή περιγραφή των μηχανών καταστάσεων που διέπουν τη συμπεριφορά των σταθμών κατά τη χρήση των χαρακτηριστικών ασφαλείας που περιγράφονται. Συγκεκριμένα, το πρότυπο δηλώνει ότι όταν ένας σταθμός περιμένει μια απάντηση μηνύματος αυθεντικοποίησης, οφείλει να απορρίπτει οποιαδήποτε άλλα μη σχετικά μηνύματα που λαμβάνει σε αυτό το χρονικό διάστημα. Αυτό, εύκολα μπορεί να χρησιμοποιηθεί από έναν τρίτο και κακόβουλα ελεγχόμενο σταθμό για να εμποδίσει την επικοινωνία μεταξύ δύο άλλων

σταθμών. Για το ίδιο παράδειγμα που αναφέρθηκε προηγούμενος, ο τρίτος σταθμός αποστέλλοντας μήνυμα με απαίτηση αυθεντικοποίησης στον Α ή Β σταθμό, εμποδίζει την επικοινωνία τους έως ότου λήξει ο εσωτερικός χρονοδιακόπτης. Η επανάληψη της επίθεσης αυτής με σωστά χρονικά διαστήματα (σχετικά με τον περιορισμό του χρονοδιακόπτη) μπορεί επίσης να αδρανοποιήσει την επικοινωνία μεταξύ δύο νόμιμων σταθμών.

- **Απόρριψη νόμιμων μηνυμάτων:** Παρόμοια με το παραπάνω πρόβλημα, εάν τώρα ο σταθμός-Β λαμβάνει ένα έγκυρο μήνυμα από τον σταθμό-Α που χρειάζεται αυθεντικοποίηση, θα στείλει μια πρόκληση πίσω στον Α. Κατά την διάρκεια αναμονής της απόκρισης, ο κακόβουλος σταθμός-Γ, μπορεί να παραποιήσει ένα μήνυμα απάντησης με μη έγκυρα δεδομένα αυθεντικοποίησης. Αυτό θα οδηγήσει τον Β σε απόρριψη της απόκρισης του Α.

Τα παραπάνω αποτελούν απλώς παραδείγματα των ζητημάτων που προκύπτουν από την προτεινόμενη προδιαγραφή ασφαλείας. Στην διαθέσιμη βιβλιογραφία παρουσιάζονται ακόμη περισσότερα δυνητικά προβλήματα που μπορούν να εμφανιστούν στις επικοινωνίες IEC 62351-5. Μια **εναλλακτική προσέγγιση** που θα μπορούσε να επιλύσει κάποια από αυτά, είναι η αλλαγή της κατάστασης αυθεντικοποίησης μεταξύ δύο σταθμών βάση του χρόνου όπου τα κλειδιά της συνεδρίας θα έχουν ημερομηνία λήξης. Έτσι ίσως τα μη έγκυρα δεδομένα αυθεντικοποίησης απλώς θα καταγράφονται και στη συνέχεια θα απορρίπτονται.

Εμφανώς, η παραπάνω προσέγγιση δεν μπορεί να αποτελεί λύση για όλα τα ζητήματα πρόληψης, πόσο μάλλον για τον εντοπισμό κυβερνοαπειλών. Πιο ριζοσπαστικές λύσεις είναι η ανάπτυξη ολοκληρωμένων συστημάτων IDS και IPS για τις επικοινωνίες IEC 60870-5, τα οποία θα προσφέρουν δυνατότητες παρακολούθησης της κίνησης τον μηνυμάτων και υψηλότερα επίπεδα προστασίας.

4.5.2. Συστήματα IDS βασισμένα σε ανωμαλίες για επικοινωνίας IEC/104

Το πρωτόκολλο IEC/104, όπως συμπεράναμε στο κεφάλαιο 3, λόγω της εξάρτησης από την στοίβα TCP/IP εμφανίζει μια σειρά ζητημάτων στα θέματα της κυβερνοασφάλειας. Ένα σοβαρό πρόβλημα ασφαλείας και του IEC/104 είναι η **μετάδοση δεδομένων χωρίς κανένα μηχανισμό κρυπτογράφησης**, επιτρέποντας σε πιθανούς εισβολής να υποκλέψουν και να αναλύσουν δεδομένα από την δικτυακή κίνηση και να εκτελέσουν με επιτυχία MiTM επιθέσεις. Επίσης, πολλές εντολές επαναφοράς, ανάκρισης ή ανάγνωσης, δεν ενσωματώνουν διεργασίες αυθεντικοποίησης, επιτρέποντας έτσι την μη εξουσιοδοτημένη πρόσβαση στην επικοινωνία. Αυτή η ευπάθεια καθιστά έναν επιτιθέμενο ικανό στο να ελέγξει συσκευές πεδίου και, πιθανόν, τη συνολική λειτουργία της βιομηχανικής υποδομής. Παρόλο που η έκδοση του προτύπου IEC 62351 παρέχει σημαντικές κατευθυντήριες γραμμές που μπορούν να ενισχύσουν την ασφάλεια του IEC/104, η βιομηχανική φύση των SCADA δυσκολεύει την άμεση και αποτελεσματική αναβάθμισή τους. Συνεπώς, η **ενσωμάτωση νέων αμυντικών μηχανισμών στην επικοινωνία IEC/104** είναι ιδιαίτερα κρίσιμη ώστε να θωρακιστεί η όποια ακεραιότητα και εμπιστευτικότητα υπάρχει στην επικοινωνία του φυσικού συστήματος και να ενισχυθεί ακόμη περισσότερο.

Ένα προτεινόμενο IDS σύστημα ανίχνευσης ανωμαλιών [61] ακολουθεί αντίστοιχη αρχιτεκτονική με το σύστημα ενάντια σε DoS επιθέσεις που παρουσιάστηκε στην ενότητα του Modbus και αποτελείται από δύο κύρια στοιχεία, μια ομάδα αισθητήρων και ο διακομιστής. Σε αυτήν την περίπτωση, η ομάδα αισθητήρων απαρτίζεται από τρεις κατηγορίες: α) την παρακολούθησης κίνησης

δικτύου, β) τον έλεγχο πρόσβασης πακέτων και γ) την εξαγωγή ροών IEC-104 που είναι υπεύθυνες αντίστοιχα για την παρακολούθηση και ανάλυση της συνολικής κίνησης του δικτύου που παράγεται στη βιομηχανική υποδομή. Από την άλλη, ο διακομιστής αποτελεί το κεντρικό σημείο του IDS όπου λαμβάνουν χώρα οι διαδικασίες ανίχνευσης ανωμαλιών και αποθηκεύονται τα γεγονότα ασφαλείας. Για την επιτέλεση του ρόλου αυτού απαρτίζεται από, δ) την συσκευή ανίχνευσης, ε) την συσκευή απόκρισης και στ) μια αντίστοιχη βάση δεδομένων.

- **Μονάδα Παρακολούθησης Κίνησης Δικτύου:** Ο τρόπος παρακολούθησης της κίνησης στο δίκτυο είναι αντίστοιχος του προηγούμενου παραδείγματος. Η μονάδα παρακολούθησης είναι υπεύθυνη για την παρακολούθηση και την καταγραφή της συνολικής κίνησης του δικτύου βάσει μιας προκαθορισμένης συχνότητας που καθορίζεται από τον χρήστη.
- **Μονάδα Ελέγχου Πρόσβασης Πακέτων:** Αυτή η μονάδα λαμβάνει την καταγεγραμμένη κίνηση του δικτύου, για να εφαρμόσει ορισμένους αρχικούς ελέγχους ασφαλείας. Συγκεκριμένα, χρησιμοποιεί μια κενή λίστα στην οποία αποθηκεύονται όλες οι νόμιμες MAC και IP διευθύνσεις. Εάν κάποιο πακέτο περιέχει μια διεύθυνση που δεν περιλαμβάνεται στη λίστα, τότε δημιουργείται ένα γεγονός ασφαλείας και αποθηκεύεται στη βάση δεδομένων του διακομιστή. Οι νόμιμες διευθύνσεις MAC και IP πρέπει να καθοριστούν από τον χειριστή του συστήματος ή τον διαχειριστή ασφαλείας. Επιπλέον, αυτή η λίστα καθορίζει τις επιτρεπόμενες θύρες TCP και UDP. Αντίστοιχα, λοιπόν, εάν ένα πακέτο περιλαμβάνει μια μη-νόμιμη θύρα, δημιουργείται το αντίστοιχο γεγονός ασφαλείας.
- **Μονάδα Εξαγωγής Ροών IEC-104:** Αυτή η μονάδα λαμβάνει επίσης τα καταγεγραμμένα IEC-104 πακέτα και εξάγει τις αντίστοιχες ροές διπλής κατεύθυνσης, χρησιμοποιώντας το λογισμικό CICFlowMeter. Αξίζει να σημειωθεί ότι μπορούν να χρησιμοποιηθούν διάφορα όρια χρονικού περιορισμού για την εξαγωγή των αντίστοιχων ροών IEC-104.
- **Μονάδα Ανίχνευσης Ανωμαλιών:** Η μονάδα ανίχνευσης ανωμαλιών στην κίνηση είναι και ο πυλώνας του προτεινόμενου IDS. Αρχικά, λαμβάνει τις καταγεγραμμένες ροές IEC-104 από τη βάση δεδομένων και εφαρμόζει μοντέλα εντοπισμού ανωμαλιών για να ανιχνεύσει και να αποφασίσει ποιες από αυτές είναι όντως ανωμαλίες. Δεύτερον, αποθηκεύει τα αντίστοιχα γεγονότα ασφαλείας, δηλαδή ανώμαλες ροές IEC-104, σε ένα διαφορετικό σημείο της βάσης δεδομένων.
- **Μονάδα Ενημέρωσης:** Η μονάδα ενημέρωσης (ή απαντήσεων) αναλαμβάνει τον ρόλο της ενημέρωσης του χρήστη για τα διάφορα γεγονότα που καταγράφηκαν, παρέχοντας στατιστικές αναλύσεις και γραφικές παραστάσεις.

Σαφώς, τα γεγονότα ασφαλείας που εντοπίζει το συγκεκριμένο IDS σχετίζονται με μορφή των ελέγχων της μονάδας πρόσβασης πακέτων και της μονάδας ανίχνευσης ανωμαλιών. Στην παρούσα εργασία μας ενδιαφέρει να αξιολογήσουμε κυρίως το βασικό στοιχείο του IDS, την μονάδα ανίχνευσης ανωμαλιών στο δίκτυο επικοινωνίας. Στην πειραματική δοκιμή που παρουσιάζεται στην βιβλιογραφία, **εφαρμόζονται και στην συνέχεια αξιολογούνται τρία διαφορετικά μοντέλα ασφαλείας** που χρησιμοποιεί η μονάδα και βασίζονται σε αλγορίθμους μηχανικής εκμάθησης.

Οι μέθοδοι ανίχνευσης ανωμαλιών με την χρήση μηχανικής μάθησης μπορούν να κατηγοριοποιηθούν ως εξής: οι μοντελο-προσανατολισμένες (model-based), οι βασισμένες σε ομαδοποίηση (clustering-based), οι βασισμένες στα χαρακτηριστικά (attribute-based), οι βασισμένες σε ανακατασκευή (reconstruction-based) ή οι προσαρμοσμένες στην εγγύτητα (proximity-based). Για παράδειγμα, οι

μοντελο-προσανατολισμένες προσεγγίσεις περιλαμβάνουν «Γκαουσ-ιανά» μοντέλα (GMM) που εφαρμόζουν ένα μίγμα κανονικής κατανομής στα δεδομένα. Οι παράμετροι του GMM συνήθως εκτιμώνται με λύσεις «προσδοκίας-μεγιστοποίησης» ή με deep-estimation δίκτυα. Αντίθετα, στην περίπτωση του αλγορίθμου Isolation Forest, το μοντέλο είναι υπερβολικά προσαρμοσμένο στην κάθε περίπτωση και εντοπίζει ανωμαλίες απομνημονεύοντας τα ακριβή χαρακτηριστικά των δεδομένων. Από την άλλη, σε **μεθόδους που βασίζονται σε ομαδοποίηση**, όπως η LOF, γίνεται η υπόθεση ότι τα κανονικά δεδομένα βρίσκονται κοντά στην πιο κοντινή τους ομάδα. Η ανακατασκευή είναι μια επίσης προσεγγιστική μέθοδος όπου χαρτογραφεί διάφορους χώρους (ανώτερα και χαμηλότερα) στο δίκτυο για να εντοπίσει γενικά σημεία υψηλής συγκέντρωσης σφαλμάτων ανακατασκευής. Τέτοια παραδείγματα είναι οι αλγόριθμοι, PCA, MF και SOS. Τέλος, η One-Class Support Vector Machine (OC-SVM) στοχεύει να βρει ένα υπερεπίπεδο, όπου θα μπορεί να χωρίσει την συντριπτική πλειονότητα των δεδομένων από την αρχή χωρίς να κάνει καμία υπόθεση για την κατανομή τους. Η γενική ιδέα του OC-SVM για την ανίχνευση ανωμαλιών, είναι να βρει μια συνάρτηση που είναι θετική για περιοχές με υψηλή πυκνότητα σημείων και αρνητική για μικρές πυκνότητες.

Οι **OC-SVM, Isolation Forest** και **LOF, είναι οι αλγόριθμοι που επιλέχθηκαν** για τα πειράματα ανίχνευσης ανωμαλιών [61] έπειτα από κυβερνοεπίθεση, σε τέσσερις διαφορετικούς χρονικούς περιορισμούς: 15, 30, 60 και 120 δευτερόλεπτα. Για την εκπαίδευση των μοντέλων αυτών, συμπεριλήφθηκαν και πραγματικά δεδομένα από έναν υποσταθμό. Τα χαρακτηριστικά της κίνησης που επιλέχθηκαν να εξεταστούν σχετικά με ανωμαλίες στο δίκτυο είναι: α) το συνολικό αριθμό πακέτων προς την αρχική κατεύθυνση, β) το συνολικό μέγεθος των πακέτων προς την αντίστροφη κατεύθυνση, γ) το πρότυπο απόκλισης του μεγέθους των πακέτων της αρχικής κατεύθυνσης, δ) ο αριθμός των bytes ανά δευτερόλεπτο, ε) ο μέγιστος χρόνος μεταξύ δύο πακέτων που στάλθηκαν, στ) το ελάχιστο μήκος ενός πακέτου, ζ) ο μέσος αριθμός bytes προς την αντίστροφη κατεύθυνση και η) ο μέγιστος χρόνος κατά τον οποίο μια ροή ήταν ενεργή πριν γίνει ανενεργή.

Μοντέλο		**Δείκτες**			
Αλγόριθμοι	Flow-timeout	Accuracy	Precision	TPR	F1
OS-SVM	15 sec.	0.519	0.509	0.993	0.673
	30 sec.	0.805	0.943	0.65	0.769
	60 sec.	0.811	0.964	0.647	0.774
	120 sec.	**0.812**	**0.962**	**0.647**	**0.774**
LOF	15 sec.	0.65	0.98	0.3	0.46
	30 sec.	0.783	0.886	0.65	0.75
	60 sec.	0.79	0.941	0.62	0.747
	120 sec.	**0.812**	**0.964**	**0.647**	**0.775**
Isolation Forest	15 sec.	0.536	0.519	0.992	0.6817
	30 sec.	0.811	0.964	0.647	0.774
	60 sec.	0.812	0.964	0.647	0.775
	120 sec.	**0.982**	**0.99**	**0.777**	**0.875**

Σχήμα 4.5 – Αποτελέσματα αλγορίθμων ανίχνευσης ανωμαλιών.

4.5.3. Μοντελοποιημένα συστήματα IDS για επικοινωνίες IEC/104

Για τα συστήματα ανίχνευσης διείσδυσης βασισμένα σε κανόνες, η διαθέσιμη βιβλιογραφία επικεντρώνεται κυρίως στα συστήματα Modbus, τα οποία είναι και τα πιο δημοφιλή όταν αναφερόμαστε σε παραδοσιακά βιομηχανικά συστήματα αυτοματισμού. Το εργαλείο Snort, για παράδειγμα, έχει σχεδιαστεί κυρίως για τα κλασικά IP δίκτυα και η υποστήριξη του IEC/104 πρωτοκόλλου μπορεί ίσως να

επιτευχθεί ύστερα από νέες προγραμματιστικές προσαρμογές. Η μοναδική ερευνητική εργασία που εντοπίστηκε σχετικά με την ανάπτυξη μοντέλων υπογραφών σε επικοινωνίες IEC/104, προτείνει εξειδικευμένες τεχνολογίες που αναλύουν σε βάθος την δομή και την λειτουργία του πρωτοκόλλου [24].

Η ανίχνευση βάσει υπογραφής, όπως είδαμε προηγουμένως, είναι μια πολύ αποτελεσματική μέθοδος αντιμετώπισης γνωστών επιθέσεων στα επικοινωνιακά δίκτυα μιας βιομηχανικής εφαρμογής. Οι κανόνες-υπογραφές θα μπορούσαμε να πούμε ότι διαμορφώνουν μια «μαύρη λίστα» απαγορευμένων συμπεριφορών στην κίνηση δικτύου, όπου βάσει αυτής σηματοδοτούνται πιθανές παραβιάσεις (κανόνων). Συνήθως, οι κανόνες αυτοί θα πρέπει να είναι σχεδιασμένοι να αναγνωρίζουν γνωστές επιθέσεις που συναντήσαμε στο 3ο κεφάλαιο, για το IEC/104 όπως για παράδειγμα επιθέσεις πλημμύρας, μη-εξουσιοδοτημένες ερωτο-απαντήσεις και πλαστές εντολές τηλεχειρισμού και ρυθμίσεων συσκευών. Ωστόσο, αυτήν την φορά, γίνεται προσπάθεια ανάπτυξης μοντελοποιημένων υπογραφών που θα μπορούν να αναγνωρίζουν ανωμαλίες, των οποίων η επίδραση στην κίνηση δικτύου δεν έχει προηγουμένως σχηματοποιηθεί.

Για να επιτευχθεί η ανίχνευση τέτοιων άγνωστων επιθέσεων, λοιπόν, προτείνεται μια **προσέγγιση βασισμένη σε μοντέλα**, ως μια συμπληρωματική λειτουργία ανίχνευσης στην προσέγγιση βασισμένη σε υπογραφές. Η βασική αρχή αυτής μεθοδολογίας είναι η δημιουργία μοντέλων που χαρακτηρίζουν μια αναμενόμενη συμπεριφορά του πρωτοκόλλου και της δικτυακής κίνησης, η οποία προκύπτει από μια λεπτομερής - και σε βάθος - ανάλυσή των χαρακτηριστικών τους. Η λογική μιας τέτοιας προσέγγισης είναι αρκετά διαφορετική από τις παραδοσιακές τεχνικές, όπως τακτικές ροές κίνησης και πρότυπα πρόβλεψης συμπεριφοράς.

Το πρότυπο IEC/104, καθορίζει με σαφήνεια τα αναμενόμενα χαρακτηριστικά μιας επικοινωνίας μεταξύ πελάτη-διακομιστή. Συνεπώς, εάν σε μια κίνηση δικτύου που παρακολουθείται από το IDS σύστημα, παραβιάζονται βασικά χαρακτηριστικά στην δομή του πρωτοκόλλου, τότε **το μοντέλο βάσει δομής** οφείλει να παράγει σχετικές ειδοποιήσεις. Ο βασικός τύπος τέτοιων μοντέλων **χρησιμοποιεί ένα μεμονωμένο και ανεξάρτητο πεδίο στο ASDU**, όπως το TI ή το CoT.

Σύμφωνα με την ανάλυσή μας στο 2ο κεφάλαιο, το αναγνωριστικό TI ενός ASDU που αντιπροσωπεύει τον τύπο του ASDU, έχει μέγεθος 1-byte και άρα υπάρχουν 256 δυνατές τιμές για το πεδίο αυτό. Σημειώνεται ότι, η τιμή «0» δεν είναι έγκυρη και το εύρος των αριθμών 128 έως 255 δεν ορίζεται. Συνεπώς οι επιτρεπτές τιμές του πεδίου TI ανήκουν στο διάστημα των «1» έως «127». Σημειώνεται επίσης ότι ορισμένες από τις επιτρεπτές τιμές δεσμεύονται για διάφορους συμβατούς ορισμούς. Τα **μοντέλα αναγνωριστικού - TI** αναπτύσσονται σύμφωνα παραπάνω ορισμό. Για παράδειγμα, όταν σε ένα αίτημα ASDU *μορφής-I* αποστέλλεται από τον πελάτη στο διακομιστή, το αντίστοιχο μοντέλο συνόλων ακολουθεί την εξής μορφή:

$$\forall C \in 104Request \cdot TIField(C) \in \begin{Bmatrix} 45-51,58-64,100- \\ 103,105,107,110-113 \end{Bmatrix}$$

Το *C* αντιπροσωπεύει το IEC/104-πακέτο αιτήματος στην κατεύθυνση ελέγχου, ενώ το *TIField* αναπαριστά την τιμή του πεδίου «αναγνωριστικό ΤΙ». Τότε, το αντίστοιχο πεδίο ΤΙ στην αντίστοιχη απάντηση ASDU που αποστέλλεται από τον διακομιστή, θα πρέπει να ανήκει στο παρακάτω σύνολο επιτρεπτών τιμών:

$$\forall M \in 104Response \cdot TIField(M) \in \begin{Bmatrix} 1,3,5,7,9,11,13,15,20,21,30-40,70,45- \\ 51,58-64,100,101,103,105,107,110-113 \end{Bmatrix}$$

Το *M* αντιπροσωπεύει το αντίστοιχο πακέτο απάντησης στην κατεύθυνση παρακολούθησης. Με βάση αυτό το παράδειγμα μοντέλου, μπορούν να αναπτυχθούν διάφορα μοντέλα-ΤΙ με πιο εξειδικευμένα σύνολα τα οποία καλύπτουν συγκεκριμένα σενάρια ανταλλαγής πακέτων ASDU.

Ένα άλλο παράδειγμα κανόνων βάσει δομής πρωτοκόλλου περιλαμβάνει το πεδίο CoT σε ένα ASDU (1 ή 2 bytes). Ο ρόλος του πεδίου αυτού είναι πολύ σημαντικός για την επικοινωνία διότι καθοδηγεί το ASDU-πακέτο σε μια συγκεκριμένη εργασία της εφαρμογή (περιοδική, αυθόρμητη, απάντηση κατόπιν αιτήματος, ατομικά ή ομαδική αιτήματα ενημέρωσης του σταθμό, κλπ.). Συνήθως, υπάρχουν 64 δυνατές τιμές για το πεδίο CoT, όπου το «0» δεν υποστηρίζεται και το εύρος των αριθμών «14-19» και «42-63» είναι δεσμευμένο. Έτσι ένα γενικό **μοντέλο αιτίας μετάδοσης - CoT** μπορεί να αναπαρασταθεί ως εξής:

$$\forall P \in 104(I)\ format \cdot CoTField \in \{1-13, 20-41\}$$

Όπου το *P* είναι το καταγεγραμμένο πακέτο IEC/104 και το πεδίο *CoTField* αναπαριστά την τιμή του πεδίου αιτίας μετάδοσης στο ASDU.

Πάνω σε αυτήν την λογική μπορούν να αναπτυχθούν πιο σύνθετα μοντέλα κανόνων που να περιλαμβάνουν διάφορες επιτρεπτές συσχετίσεις μεταξύ διαφορετικών πεδίων ενός ASDU. Τα **μοντέλα πολλαπλών πεδίων** ορίζουν επιτρεπτές τιμές για κάποιο πεδίο, οι οποίες έχουν άμεση σχέση με την τιμή ενός διαφορετικού πεδίου στο ίδιο πακέτο IEC/104. Χαρακτηριστικό παράδειγμα τέτοιων κανόνων είναι τα μοντέλα πεδίου μεγέθους και μοντέλα συσχετίσεων αναγνώρισης τύπου με την αιτία μετάδοση. Αυτές οι δύο περιπτώσεις αναλύονται στην συνέχεια.

Το πεδίο μεγέθους (1 byte) καθορίζει το μήκος του σώματος ενός APDU, το οποίο περιλαμβάνει ολόκληρο το ASDU και 4 bytes των πεδίων ελέγχου APCI. Λόγω του ελάχιστου και του μέγιστου επιτρεπτού μεγέθους του APDU, που είναι αντίστοιχα 4 bytes και 253 bytes, η τιμή του πεδίου αυτού ανήκει στο εύρος «4-253». Ωστόσο, το **μοντέλο μεγέθους πεδίου** αναγκαστικά αποτελεί μια περίπτωση συσχέτισης με το πραγματικό μέγεθος του υπόλοιπου μηνύματος. Δηλαδή, σε *S-* και *U- μορφές* APDU το πεδίο μεγέθους θα πρέπει να ισούται με «4», καθώς σε αυτά τα μηνύματα το APCI δεν ακολουθείται από APDU πακέτο. Στην παρακάτω σχέση, η μεταβλητή *lenField* αντιπροσωπεύει το πεδίο μεγέθους το APDU.

$$\forall P \in 104(S \mid U)\ format \Rightarrow lenField(P) = 4$$

Από την άλλη, σε πακέτα *μορφής-I* η τιμή του πεδίου μεγέθους θα πρέπει να είναι μεγαλύτερη του «4» και μικρότερη από «253». Παρόλο που η τιμή αυτή είναι μεταβλητή, πάντα θα πρέπει να συσχετίζεται με το αναγνωριστικό ΙΤ. Για

παράδειγμα, όταν η τιμή του IT είναι «45» (μονή εντολή) ή «46» (διπλή εντολή), το τυπικό μέγεθος πεδίου είναι «14»:

Οι **συσχετίσεις του πεδίου αναγνώρισης TI** πακέτου μορφής-I είναι

$$\forall P \in 104(I)\, format \cdot TIField(P) \in \{45,46\} \Rightarrow lenField(P) = 14$$

$$\forall P \in 104 Request \cdot TIField(P) = \{45-48,100,101\} \Rightarrow CoTField(P) = 6$$

$$\forall P \in 104 Response \cdot TIField(P) = \{45-48,100,101\} \Rightarrow CoTField(P) = \{7,10\}$$

περισσότερο σύνθετες. Εκτός από το πεδίο μεγέθους, συνδέεται άρρηκτα **με το πεδίο αιτίας μετάδοσης CoT**. Παρακάτω αναφέρονται δύο ενδεικτικοί κανόνες συσχέτισης των δύο πεδίων:

Οποιαδήποτε ανίχνευση τιμών εκτός των παραπάνω συνόλων συσχέτισης θα πρέπει να θεωρείται μη έγκυρη και να υποδεικνύει ανωμαλία στην κίνηση των πακέτων. Με παρόμοιο τρόπο, μπορούν να οριστούν πολλά άλλα μοντέλα συσχέτισης.

Στην συνέχεια, δίνονται συνοπτικά **παραδείγματα ανάπτυξης μοντελοποιημένων κανόνων** στα πλαίσια του Snort. Σύμφωνα με τα μοντέλα TI αιτημάτων ASDU και *μορφής-I* προς την κατεύθυνση ελέγχου, εάν το μήνυμα παραβιάζει το καθορισμένο μοντέλο, θα ενεργοποιηθεί ο αντίστοιχος κανόνας Snort και θα παραχθεί ένα μήνυμα ειδοποίησης. Το κείμενο κώδικα για αυτόν τον κανόνα είναι η παρακάτω.

```
alert tcp $104_CLIENT any -> $104_SERVER $104_PORT (flow:
established;     content:"|68|";     offset:0;     depth:1;
byte_test:1,    !&,    1,    2;    pcre:"/[\S\s]{5}(?![\x2D-
\x33]|[\x3A-\x40]|[\x64-\x67]|\x69|\x6B|[\x6E-\x71])/iAR";
msg:"SCADA_IDS: IEC 60870-5-104 - Suspicious Value of Type
Identification Field in the Control Direction with I
Format";    classtype:bad-unknown;    sid:6666611;    rev:1;
priority:2;)
```

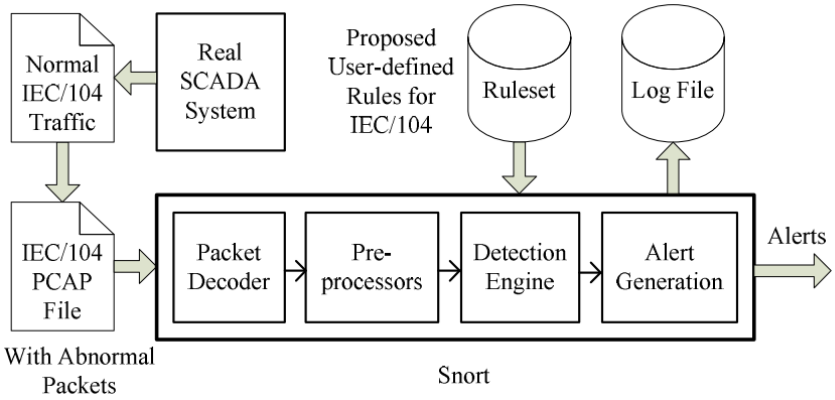
Στο **μοντέλο συσχέτισης πεδίων TI και CoT**, ένα πακέτο στην κατεύθυνση ελέγχου δεν πρέπει να παραβιάζει τον εξής Snort rule:

```
alert tcp $104_CLIENT any -> $104_SERVER $104_PORT (flow:
established;     content:"|68|";     offset:0;     depth:1;
pcre:"/[\S\s]{5}(\x2D|\x2E|\x2F|\x30|\x64|\x65)/iAR";
content:!"|06|"; offset: 8; depth: 1; msg:"SCADA_IDS: IEC
60870-5-104 - Suspicious Value of Transmission Cause
Field";    classtype:bad-unknown;    sid:6666617;    rev:1;
priority:2;)
```

Για άλλα μοντέλα δικτύου, όπως **μοντέλα μορφής κίνησης TCP/IP,** ο αριθμός θύρας της αρχικής σύνδεσης TCP προς έναν εξυπηρετητή IEC/104 πρέπει να είναι «2404». Ο κανόνας Snort που χρησιμοποιείται για την αναγνώριση πλαστών πακέτων που παραβιάζουν αυτήν την προδιαγραφή, είναι ο εξής:

```
alert tcp any any -> $104_SERVER !$104_PORT (msg:
"SCADA_IDS: IEC 60870-5-104 - Unauthorized Connection
Attempt to a non-IEC/104 Port of a Server"; flags:S;
classtype:bad-unknown; sid:6666623; rev:1; priority:2;)
```

Τα παραπάνω θεωρητικά μοντέλα ανίχνευσης ανωμαλιών προσαρμόστηκαν κατάλληλα και εφαρμόστηκαν **σε μια πειραματική διάταξη που χρησιμοποιεί το Snort**. Συνοπτικά, στο πείραμα καταγράφηκε η κανονική κίνηση IEC/104 ανάμεσα σε πελάτες και εξυπηρετητές στο πειραματικό σύστημα SCADA. Έπειτα, δημιουργήθηκαν πλαστά δεδομένα που προήλθαν από ενδεδειγμένη τροποποίηση των καταγεγραμμένων δεδομένων ή από εισαγωγή καινούργιων κακόβουλων πακέτων στο Packet Capture (PCAP). Το Snort στην συνέχεια αποκωδικοποιεί πακέτα για την ανίχνευση ανωμαλιών συνδυάζοντας τους προτεινόμενους κανόνες βάσει υπογραφής, αλλά και των μοντελοποιημένων. Τα τελικά μηνύματα-ειδοποιήσεις του Snort καταγράφονται κατάλληλα σε μια λίστα καταγραφής ανωμαλιών.



Σχήμα 4.6 – Διάγραμμα διεργασιών του Snort εργαλείου.

Οι δοκιμές είχαν στόχο την αναγνώριση ανωμαλιών σύμφωνα με τους κανόνες Snort προαναφέρθηκαν, σε ένα δείγμα 364 πακέτων από τα οποία τα 41 ήταν κακόβουλα.

4.6. Συστήματα πρόληψης εισβολών στο IEC 61850

Οι ερευνητικές προσπάθειες για την ενίσχυση της ασφάλειας των επικοινωνιών IEC 61850 είναι αρκετά φτωχές, καθώς η διαθέσιμη βιβλιογραφία δεν περιλαμβάνει επαρκείς δοκιμές για την ανάπτυξη συστημάτων ανίχνευσης κυβερνοεπιθέσεων. Αντίθετα, υπάρχει επάρκεια δημοσιεύσεων κυρίως στην ανάπτυξη αποτελεσματικών μηχανισμών αυθεντικοποίησης των μηνυμάτων που ανταλλάσσονται στους υποσταθμούς. Οι έρευνες αυτές είναι αρκετά σημαντικές για την κυβερνοασφάλεια του πρωτοκόλλου, αλλά εντάσσονται αποκλειστικά στην έννοια της πρόληψης και δεν έχουν την ικανότητα να εντοπίζουν καταστάσεις κυβερνοεπίθεσης στο σύστημα. Στην συνέχεια, μελετώνται κάποιες ενδιαφέρουσες μέθοδοι πρόληψης, καθώς και μια πρόσφατη προσπάθεια ανάπτυξης IDS βασισμένο στην μηχανική μάθηση [72].

4.6.1. Το πρότυπο ασφαλείας IEC 62351 - για επικοινωνίες IEC 61850

Αρχικά θα αξιολογηθεί το βασικό πρότυπο ασφαλείας που εκδίδει η IEC και επικεντρώνεται σε στοιχεία επικοινωνίας του IEC 61850. Παρακάτω παρουσιάζονται τα υπόλοιπα μέρη της προδιαγραφής IEC 62351 και υπογραμμίζονται τα τμήματα που θα εξεταστούν στην συνέχεια.

Μέρος προτύπου	Τίτλος	Περιεχόμενο
IEC 62351-4	**Προφίλ που περιλαμβάνουν MMS**	Ασφάλεια του προφίλ επικοινωνίας MMS και συστάσεις για τα A-Προφίλ και T-Προφίλ βάσει TCP/IP. A-Προφίλ: Περιγράφεται μια πιστοποίηση εφαρμογών. T-Προφίλ/TCP: Χρήση του TLS ως ένα επίπεδο μεταξύ TCP και ISO Transport Service, χρησιμοποιώντας διαφορετική θύρα-TCP για ασφαλείς συνδέσεις. Σουίτες κρυπτογράφησης TLS.
IEC 62351-6	**Ασφάλεια για το IEC 61850**	**Ασφάλεια πρωτοκόλλων IEC 61850 (εκτός TCP/IP και MMS).** **Προσθήκη επιπλέον πεδίου, στο PDU των GOOSE και SMV, που περιέχει πληροφορίες ασφαλείας και επαληθεύει ένα PDU. Επεκτάσεις στη γλώσσα διαμόρφωσης των υποσταθμών (SCL) που εισάγουν πιστοποιήσεις στην λειτουργία διαμόρφωσης.**
IEC 62351-7	Μοντέλα Αντικειμένων Διαχείρισης Δικτύων και Συστημάτων (NSM)	Πολλές ηλεκτρικές υποδομές χρησιμοποιούν διασυνδεδεμένα συστήματα πληροφοριών για τη διαχείριση των λειτουργιών. Η ασφαλής διαχείριση γίνεται με τη χρήση του Simple Network Management Protocol (SNMP). Το Μέρος 7 περιγράφει τα αντίστοιχα μοντέλα αντικειμένων δεδομένων που πρέπει να χρησιμοποιηθούν.
IEC 62351-8	Έλεγχος Πρόσβασης βάσει Ρόλων	Καθορίζονται οι ρόλοι πρόσβασης στο σύστημα επικοινωνίας. Τρόποι πρόσβασης: άμεση και απομακρυσμένη πρόσβαση, πρόσβαση από ανθρώπινους χρήστες και αυτοματοποιημένη πρόσβαση από υπολογιστικούς χρήστες. Καθορίζονται επίσης, ορισμένα υποχρεωτικά δικαιώματα και ρόλοι.
IEC 62351-9	Διαχείριση Κλειδιών Κυβερνοασφάλειας για Εξοπλισμό Ηλεκτρικών Συστημάτων Ισχύος	Αποτελεσματική διαχείριση πιστοποιητικών και κλειδιών ασφαλείας.
IEC 62351-10	Οδηγίες για μια Αρχιτεκτονική Ασφαλείας	Γενικές κατευθυντήριες γραμμές για την αρχιτεκτονική ασφαλείας των συστημάτων ηλεκτρικής ενέργειας. Αυτό περιλαμβάνει μια επισκόπηση ελέγχων ασφαλείας που μπορούν να εφαρμοστούν, καθώς και συμβουλές αρχιτεκτονικής συστήματος για το πώς να δομηθεί μια υποδομή επικοινωνίας σε ένα ηλεκτρικό σύστημα.

Σχήμα 4.7 – Προδιαγραφές προτύπου ασφαλείας IEC 62351 – Μέρος Β.

Το Μέρος 4 του προτύπου IEC 62351 περιγράφει συγκεκριμένα **μέτρα πρόληψης για τα μηνύματα MMS**. Ειδικότερα, περιγράφει τόσο την ασφάλεια για το Α-Προφίλ των μηνυμάτων, δηλαδή στο επίπεδο εφαρμογής, όσο και την ασφάλεια για το Τ-Προφίλ βασισμένο σε TCP/IP. Γενικότερα, η προδιαγραφή αυτή δεν περιλαμβάνει κρυπτογράφηση μηνυμάτων καθώς ο βασικός στόχος είναι απλώς η πρόληψη για περιπτώσεις μη εξουσιοδοτημένης πρόσβασης σε κρίσιμες πληροφορίες. Για λειτουργιές κρυπτογράφησης θα πρέπει να συνδυαστεί με την IEC 62351-3 και μόνο τότε οι μηχανισμοί που περιγράφονται σε αυτό το μέρος επιτυγχάνουν διαφορετικούς στόχους ασφαλείας.

- ✓ **Ασφάλεια Α-Προφίλ:** Η ασφάλεια για το προφίλ επιπέδου εφαρμογής επιτυγχάνεται μέσω της πιστοποιημένης αυθεντικοποίησης κατά τη δημιουργία μιας συσχέτισης οντοτήτων. Συγκεκριμένα, μια συσκευή περιλαμβάνει ένα πιστοποιητικό X.509 με μια χρονική επισήμανση και μια χρονική υπογραφή, χρησιμοποιώντας το πιστοποιητικό αυτό στο αίτημα συσχέτισης. Η συσκευή-παραλήπτης θα επαληθεύσει την χρονική επισήμανση και θα αποδεχτεί το αίτημα εάν η επισήμανση δεν διαφέρει περισσότερο από 10 λεπτά από την τοπική ώρα. Επιπλέον, ο παραλήπτης δεν θα αποδεχθεί ένα μήνυμα που έχει ήδη παραλάβει εντός των τελευταίων 10 λεπτών.
- ✓ **Ασφάλεια Τ-Προφίλ:** Για τα προφίλ μεταφοράς TCP, το πρότυπο συνιστά τη χρήση TLS, μεταξύ του TCP και της υπηρεσίας μεταφοράς RFC 1006, σε ξεχωριστή θύρα (3782). Επίσης, συνιστά μια λίστα κρυπτογραφιών για το TLS, με έναν υποχρεωτικό κρυπτο-σύνδεσμο (TLS_DH_DSS_WITH_AES_256_SHA).

Ωστόσο, το IEC 62351-4 θεωρεί το T-Προφίλ που βασίζεται στο OSI ως εκτός του πεδίου δράσης του και άρα δεν μπορεί να εφαρμοστεί σε τέτοια περίπτωση.

Το κύριο ζήτημα με το A-Προφίλ, κατά IEC 62351-4, είναι ότι δεν εξασφαλίζονται πλήρως η ακεραιότητα και η εμπιστευτικότητα των μηνυμάτων, καθώς οι μηχανισμοί αυτοί δεν επεκτείνονται στα υπόλοιπα μηνύματα εντός της συνεδρίας. Επιπλέον, ο μηχανισμός αυθεντικοποίησης καθορίζεται μόνο από ένα χρονικό προσδιορισμό στο εσωτερικό των μηνυμάτων, το οποίο πρέπει να είναι ακριβές σε διάστημα 10 λεπτών από το τοπικό ρολόι μιας συσκευής. Μια τόσο απλή λειτουργία ασφαλείας αφήνει το A-Προφίλ ευάλωτο σε τουλάχιστον τρεις διαφορετικές επιθέσεις:

1. Ένα αρχικό PDU μπορεί να τροποποιηθεί χωρίς να ακυρωθεί η υπογραφή του, αρκεί η χρονική επισήμανση να παραμείνει αμετάβλητη.
2. Η χρονική επισήμανση και η τιμή αυθεντικοποίησης μπορούν να αντιγραφούν από ένα PDU και άρα να επαναχρησιμοποιηθούν σε ένα πλαστό PDU προς μια διαφορετική συσκευή εντός 10 λεπτών από την αρχική αποστολή.
3. Επειδή τα ενδιάμεσα μηνύματα δεν είναι προστατευμένα, μετά την αρχική αυθεντικοποίηση, ένας εισβολέας μπορεί να πλαστογραφήσει ή να τροποποιήσει τα PDU που ανταλλάσσονται μεταξύ δύο συσκευών.

Γίνεται κατανοητό λοιπόν ότι, ο μηχανισμός ασφαλείας του A-Προφίλ προσφέρει ελάχιστη ασφάλεια, αφού δεν μπορεί ούτε να εγγυηθεί την ακεραιότητα των μηνυμάτων, ούτε την αυθεντικότητα οποιουδήποτε ενδιάμεσου μηνύματος. Συνεπώς, κρίνεται απαραίτητη η χρήση του προτύπου για την ασφάλεια και του επιπέδου μεταφοράς, δηλαδή TLS για το T-Προφίλ που περιλαμβάνουν κάποιες απλές κρυπτογραφικές λειτουργίες για τις διευθύνσεις μεταφοράς. Ακόμη και αυτό όμως δεν είναι αρκετό να εμποδίσει έναν έμπειρο επιτιθέμενο που θα καταφέρει να υποκλέψει την κίνηση του δικτύου.

Το Μέρος 6 του προτύπου IEC 62351 καθορίζει την ασφάλεια για πρωτόκολλα στο IEC 61850, όπως τα GOOSE και το SMV, εκτός των MMS που περιεγράφηκαν στο προηγούμενο μέρος. Όπως είδαμε στην ανάλυση του πρωτοκόλλου, ορισμένες εφαρμογές μέσα στο IEC 61850 απαιτούν διάφορους ορισμένους χρόνους. Για την επίτευξη των χρόνων αυτών, το IEC 62351-6 δεν συνιστά κρυπτογράφηση για αυτές τις εφαρμογές, αφού το κρυπτογραφικό κόστος μπορεί να προκαλέσει καθυστερήσεις (πχ. μεγαλύτερες των 4ms). Αντιθέτως, το πρότυπο επικεντρώνεται κυρίως σε συστάσεις εμπιστευτικότητας για περιπτώσεις πιο χαλαρών απαιτήσεων πραγματικού χρόνου (δηλαδή άνω των 3ms). Το IEC 62351-6 περιγράφει επίσης πώς θα επεκταθεί η γλώσσα διαμόρφωσης του υποσταθμού (SCL), ώστε να οριστούν ξεχωριστά πιστοποιητικά για τα μηνύματα GOOSE και τα SMV.

4.6.2. Ενίσχυση εμπιστευτικότητας και ακεραιότητας στα μηνύματα GOOSE

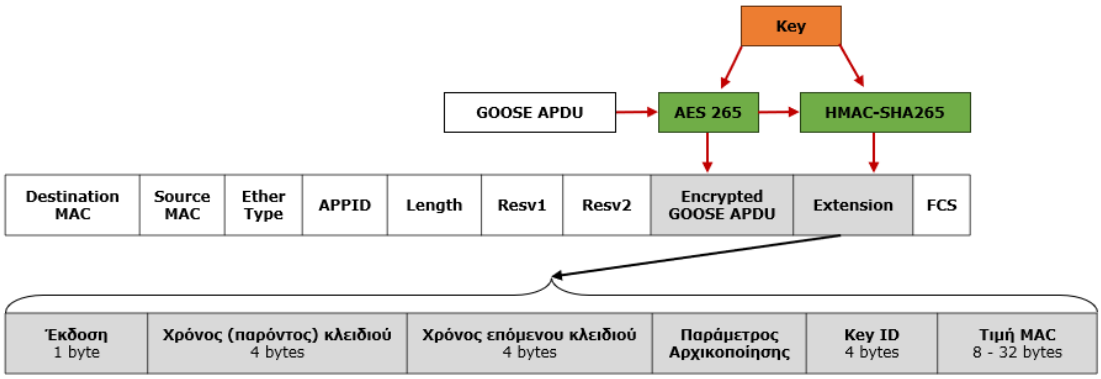
Το ζήτημα της εμπιστευτικότητας για τα μηνύματα GOOSE, ειδικά όταν χρησιμοποιούνται για την μετάδοση εντολών σε διάφορες DER συσκευές για τη διαχείριση ή για σκοπούς αγοράς ενέργειας, γίνεται πολύ σημαντικό. Επομένως, τα μηνύματα GOOSE σε αυτά τα νέα σενάρια πρέπει να κρυπτογραφηθούν. Λαμβάνοντας όμως υπόψη ότι, τα μηνύματα αυτά έχουν την πιο μεγάλη απαίτηση πραγματικού χρόνου παράδοσης, οι αλγόριθμοι κρυπτογράφησης που καθορίζει το IEC 62351 δεν πρέπει να εφαρμοστούν. Ο λόγος είναι ότι οι χρόνοι επεξεργασίας για την κρυπτογράφηση των μηνυμάτων GOOSE είναι υψηλοί για την περιορισμένη υπολογιστική ικανότητα των έξυπνων ηλεκτρονικών συσκευών (IEDs). Παρ' όλα αυτά, μέχρι στιγμής οι μηχανισμοί ασφαλείας που αναφέρονται στη βιβλιογραφία

για τα μηνύματα GOOSE δεν λαμβάνουν υπόψη την εμπιστευτικότητα. Η μοναδική ρεαλιστική πρόταση αναφέρει μια νέα μέθοδο διασφάλισης της εμπιστευτικότητας και αυθεντικοποίησης με τη χρήση αλγορίθμων Πιστοποιημένης Κρυπτογράφησης με Συνδεδεμένα Δεδομένα (AEAD). Στην προτεινόμενη μέθοδο, χρησιμοποιούνται **τρεις παραλλαγές των αλγορίθμων AEAD** για την επίτευξη εμπιστευτικότητας, ακεραιότητας και αυθεντικότητας των μηνυμάτων GOOSE: Encrypt-then-MAC (EtM), Encrypt-and-MAC (E&M) και MAC-then-Encrypt (MtE).

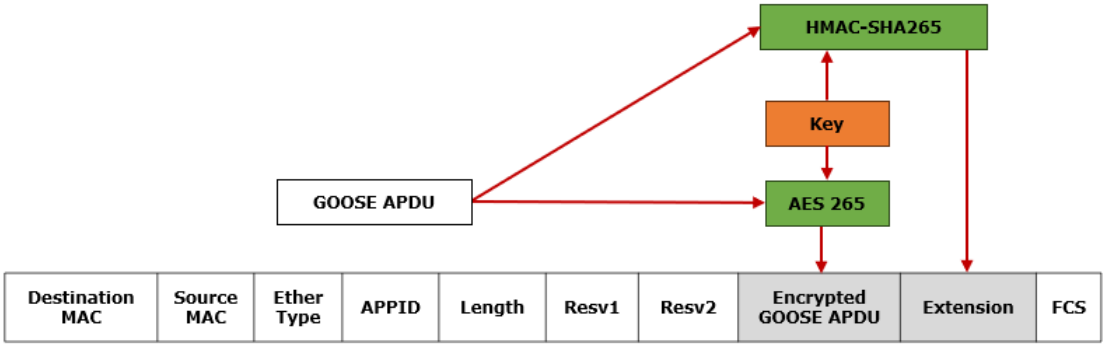
Στον αλγόριθμο EtM, η μονάδα δεδομένων APDU του πρωτοκόλλου GOOSE αρχικά κρυπτογραφείται χρησιμοποιώντας αλγόριθμους AES. Στη συνέχεια, δημιουργείται μια τιμή MAC με έναν από τους αλγορίθμους MAC και προσαρτάται στη μονάδα δεδομένων πρωτοκόλλου GOOSE (PDU) στο πεδίο “Επέκτασης” (Extension), όπως φαίνεται στο **σχήμα 4.8**. Καθώς αυτό αυξάνει το μήκος του πλαισίου GOOSE, η διαφορά αντανακλάται στο 2ο byte του πεδίου "Reserved1", το οποίο αντιπροσωπεύει το μέγεθος του πεδίου επέκτασης. Για παράδειγμα, όταν η τιμή του είναι 0, τότε δεν υπάρχει κάποια επέκταση και άρα υποδηλώνει ότι δεν έχει εφαρμοστεί κάποια μορφή ασφάλειας στα μηνύματα GOOSE. Ο αποδέκτης, όταν λάβει το κρυπτογραφημένο GOOSE πρώτα υπολογίζει την τιμή MAC της ληφθείσας κρυπτογραφημένης μονάδας δεδομένων και την συγκρίνει με την προσαρτημένη τιμή MAC. Εάν οι τιμές MAC ταιριάζουν, τότε το πακέτο GOOSE θεωρείται αυθεντικό και αποκρυπτογραφείται, σε διαφορετική περίπτωση το πακέτο απορρίπτεται.

Με τον αλγόριθμο E&M (σχήμα 4.9), η κρυπτογράφηση και η δημιουργία της τιμής MAC πραγματοποιούνται ταυτόχρονα στην αρχική μονάδα δεδομένων APDU και στην συνέχεια προστίθενται αντίστοιχα, στα πεδία "Μονάδας δεδομένων" και "Επέκτασης" του GOOSE PDU. Ο αποδέκτης οφείλει αρχικά να αποκρυπτογραφήσει το πακέτο και στην συνέχεια να εκτελέσει την αντίστοιχη διαδικασία υπολογισμού και σύγκρισης των MAC διευθύνσεων.

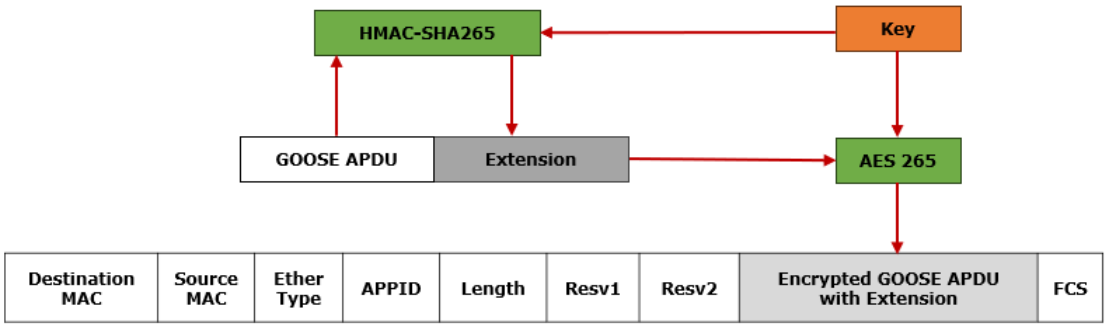
Η παραλλαγή MtE (σχήμα 4.10) εκτελεί μια αντίστροφη λειτουργία συγκριτικά με την EtM, καθώς η πρώτη ενέργεια είναι ο υπολογισμός της τιμής MAC για τη μονάδα δεδομένων GOOSE. Έτσι, η κανονική μονάδα δεδομένων και η υπολογισμένη τιμή MAC προστίθενται στα πεδία "Μονάδα δεδομένων" και "Επέκταση" πριν την όποια διαδικασία κρυπτογράφησης. Στη συνέχεια, η μονάδα δεδομένων GOOSE θα κρυπτογραφηθεί και θα αποσταλεί στον αποδέκτη. Ο αποδέκτης του GOOSE αφού αποκρυπτογραφήσει τη μονάδα δεδομένων GOOSE λαμβάνει την απεσταλμένη τιμή MAC. Τέλος, οι τιμές MAC που παραλήφθηκαν και οι υπολογισμένες τιμές MAC συγκρίνονται για να ανιχνεύσουν τυχόν παρεμβολές στο μήνυμα GOOSE.



Σχήμα 4.8 – Κρυπτογράφηση GOOSE – Αλγόριθμος Encrypt-then-MAC.



Σχήμα 4.9 – Κρυπτογράφηση GOOSE – Αλγόριθμος Encrypt-and-MAC.



Σχήμα 4.10 – Κρυπτογράφηση GOOSE – Αλγόριθμος MAC-then-Encrypt.

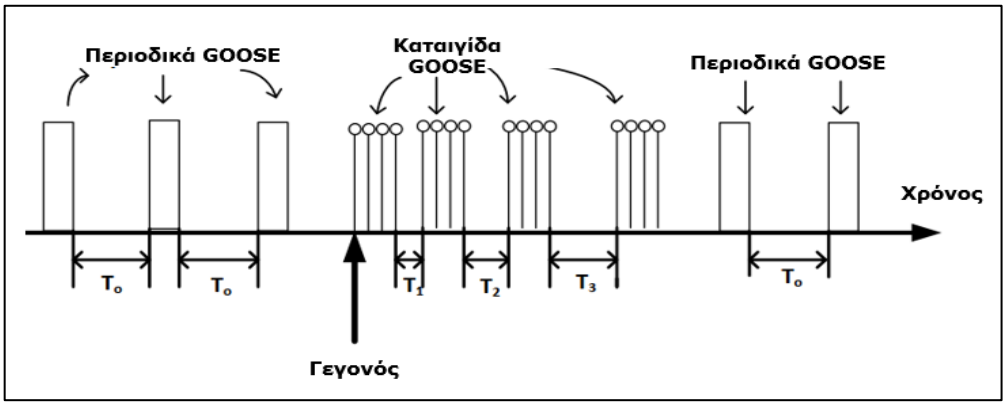
Για την επιβεβαίωση ότι οι αλγόριθμοι AEAD επιτρέπουν μια ασφαλή - ως προς την απαίτηση χρόνου - κρυπτογράφηση **διεξήχθησαν τα απαραίτητα εργαστηριακά πειράματα** εφαρμογής των παραπάνω μεθόδων σε μηνύματα GOOSE. Τα πειράματα αυτά έδειξαν ότι οι τρεις αλγόριθμοι AEAD είναι εφαρμόσιμοι στα μηνύματα GOOSE, καθώς κατά μέσο όρο απαιτούν 0.2 – 0.25 ms ως επιβάρυνση για τις λειτουργίες ασφάλειας. Πιο ειδικά, ανάμεσα στις τρεις παραλλαγές AEAD που δοκιμάστηκαν, ο αλγόριθμος EtM διαθέτει τα περισσότερα πλεονεκτήματα, αφού η τιμή MAC υπολογίζεται για τα κρυπτογραφημένα δεδομένα. Άρα, εφόσον εντοπιστεί οποιαδήποτε παρεμβολή τότε το πακέτο απορρίπτεται πριν εφαρμοστούν οι αλγόριθμοι αποκρυπτογράφησης. Αυτό εξοικονομεί πολύτιμο χρόνο σε σύγκριση με τους E&M και MtE, καθώς σε αυτούς τους αλγορίθμους πρέπει να γίνει πρώτα αποκρυπτογράφηση για τον έλεγχο της ακεραιότητας του μηνύματος.

4.6.3. Ανίχνευση διείσδυσης με Μηχανική Μάθηση για μηνύματα GOOSE

Τα μηνύματα GOOSE έχουν δύο βασικές παραμέτρους για την παρακολούθηση ακολουθιών μηνυμάτων, τα οποία αφορούν το ίδιο γεγονός και τις αλλαγές κατάστασης που συμβαίνουν σε μεμονωμένα γεγονότα. Αυτές οι παράμετροι μπορούν να γίνουν αντικείμενο αναφοράς σε ένα IDS που μελετά ανωμαλίες στην κίνηση των πακέτων. Γενικώς, βασικές λειτουργίες των γεγονότων GOOSE προορίζονται για την αποστολή σημάτων «τριπ» από έξυπνα ρελέ σε διακόπτες του ηλεκτρικού κυκλώματος. Αυτό σημαίνει ότι τα νέα γεγονότα εκδίδονται κυρίως όταν προκύπτει κάποιο σφάλμα στο φυσικό σύστημα. Συνεπώς, σε ένα υγιές ΣΑΥ αναμένεται ότι, τα μηνύματα GOOSE θα έχουν πολύ υψηλές τιμές ακολουθίας “sqNum” και σπάνιες αλλαγές στον αριθμό κατάστασης “stateNum”.

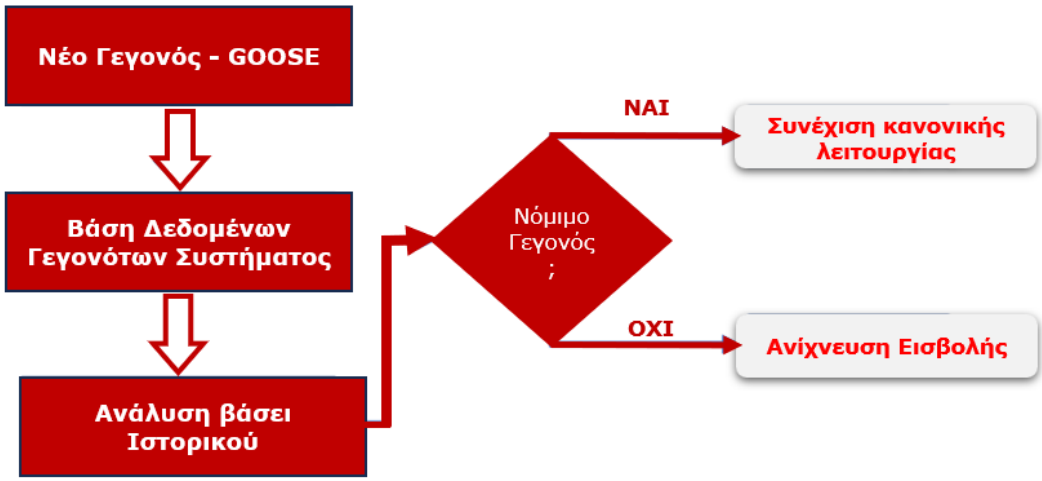
Δηλαδή τα γεγονότα (σφάλματος) δεν θα είναι πολύ συχνά, ενώ στο δίκτυο θα μεταδίδονται κυρίως κυκλικά μηνύματα με έναν αύξοντα αριθμό ακολουθίας.

Με την αντίστροφη λογική, εάν ένας δυνητικός εισβολέας επιθυμεί να προκαλέσει όσο το δυνατόν περισσότερη ζημιά σε σύντομο χρονικό διάστημα, τότε θα μπορούσε να στέλνει αδιαλείπτως πολλά μηνύματα "trip" που αφορούν κάποιον εξοπλισμό ισχύος. Τότε ο εξοπλισμός αυτός θα οδηγούταν είτε σε αποκλεισμό από το σύστημα ενέργειας, είτε θα άλλαζε η λειτουργία του με τρόπο που θα προκαλούσε διακοπή παροχής ρεύματος. Το φαινόμενο αυτό ονομάζεται καταιγίδα γεγονότων GOOSE και συνιστά κατάσταση κυβερνοεπίθεσης. Αυτή θα ήταν δυνατό να παρατηρηθεί, ανιχνεύοντας συχνές επαναφορές των τιμών stNum για κάθε νέα ακολουθία μηνυμάτων GOOSE με sqNum = 1. Στο παρακάτω σχήμα φαίνεται χαρακτηριστικά η διαφορά μεταξύ μιας ομαλής περιοδικής αποστολής μηνυμάτων GOOSE συγκριτικά με το φαινόμενο καταιγίδας.



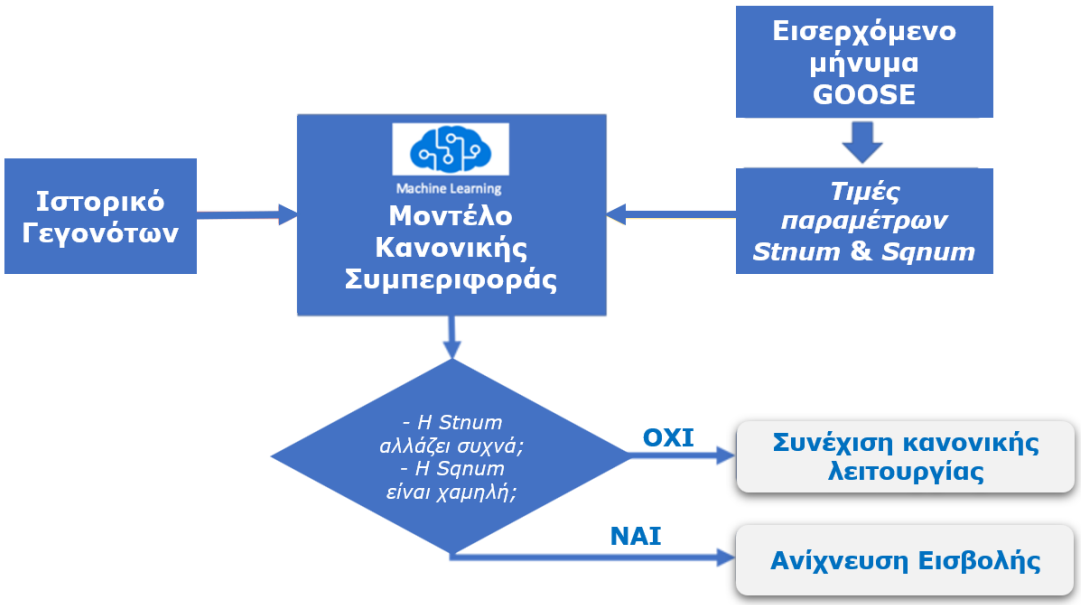
Σχήμα 4.11 – Φαινόμενο καταιγίδας γεγονότων GOOSE

Με βάση αυτό το σενάριο κυβερνοεπίθεσης, προτείνεται ένα σύστημα ανίχνευσης διείσδυσης, το οποίο βασίζεται στο ιστορικό γεγονότων του συστήματος. Δηλαδή κάθε νέο γεγονός εξετάζεται μεμονωμένα και συγκριτικά με παλαιότερες συμπεριφορές του συστήματος επικοινωνίας, ενώ στην συνέχεια το IDS αποφασίζει εάν αυτό είναι νόμιμο ή συνιστά έκδοση ειδοποίηση εισβολής.



Σχήμα 4.12 – IDS βάσει ιστορικού γεγονότων GOOSE

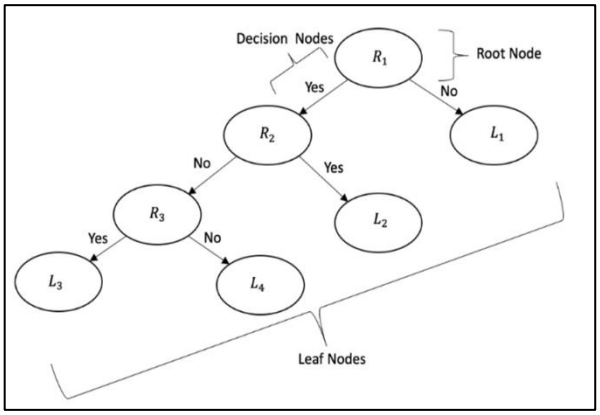
Είναι αυτονόητο ότι σε κάθε σύστημα ηλεκτρικής ενέργειας, όπως ένα μικροδίκτυο ή ένας υποσταθμός, η συμπεριφορά και η ακολουθία γεγονότων διαφέρει. Συνεπώς, η διαδικασία σύγκρισης των γεγονότων με το ιστορικό του συστήματος καθώς και η λήψη της απόφασης για το αν πρόκειται για παράνομη δραστηριότητα οφείλει να είναι εξατομικευμένη για κάθε εφαρμογή. Το μοντέλο συμπεριφοράς που προτείνεται χρησιμοποιεί την μηχανική μάθηση και έχει στόχο την ανάπτυξη ενός γενικού προτύπου για οποιοδήποτε δεδομένο σύστημα ενέργειας. Σε κάθε εισερχόμενο GOOSE εξάγονται οι τιμές *stNum* και *sqNum* και με βάση το ιστορικό γεγονότων συμπεραίνεται εάν υπάρχει οποιαδήποτε ασυμφωνία.



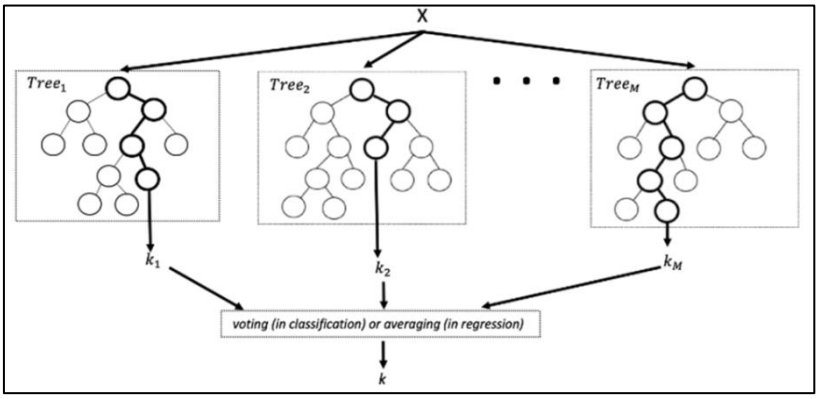
Σχήμα 4.13 – IDS με Μηχανική Μάθηση για γεγονότα GOOSE

Ορισμένοι από τους αλγόριθμους μηχανικής μάθησης που χρησιμοποιούνται για εντοπισμό ανωμαλιών σε GOOSE γεγονότα έχουν αναφερθεί σε συστήματα ανίχνευσης άλλων πρωτοκόλλων. Παρακάτω παρουσιάζονται ενδεικτικά πέντε αλγόριθμοι, οι οποίοι θεωρούνται αποδοτικοί για αυτήν την εφαρμογή και στην συνέχεια γίνεται μια προσπάθεια αξιολόγησής τους.

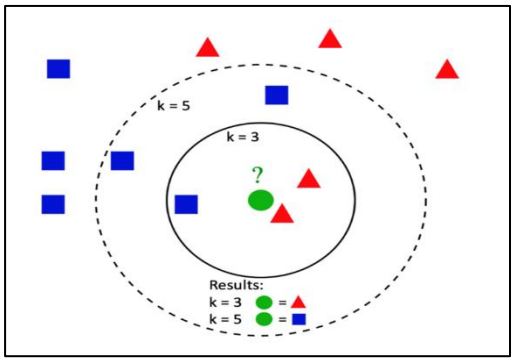
1. **Δέντρο Απόφασης – Decision Tree**: Ο αλγόριθμος DT χρησιμοποιεί δέντρα αποφάσεων και εξάγει συμπεράσματα σύμφωνα με παρατηρήσεις που σχετίζονται με ένα συγκεκριμένο στοιχείο. Οι παρατηρήσεις αναπαρίστανται ως κλαδιά, ενώ τα συμπεράσματα ως φύλλα του δέντρου. Ο σκοπός του αλγορίθμου είναι να αξιολογηθεί την τιμή ενός κόμβου-στόχου και παράγει ικανοποιητικά αποτελέσματα όταν οι τιμές των *stNum* και *sqNum* αξιολογούνται σε ένα ευρύ πλαίσιο.



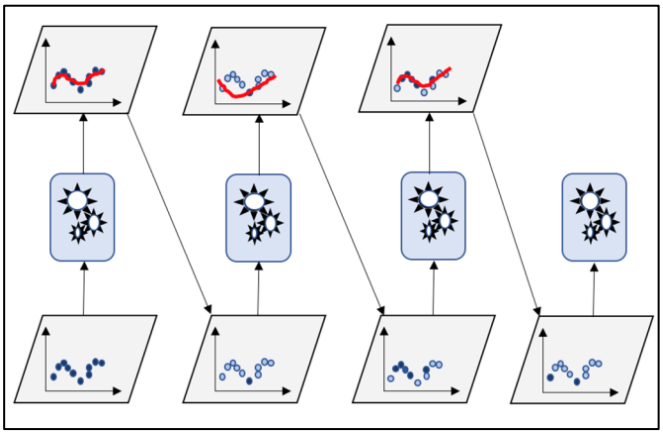
2. **Τυχαίο Δάσος – Random Forest**: Μια συλλογή από δέντρα αποφάσεων δημιουργεί έναν αλγόριθμο RF. Με άλλα λόγια, οι αποφάσεις που λαμβάνονται χρησιμοποιούν πολλά DT όπου τα μεμονωμένα αποτελέσματα από κάθε DT επεξεργάζονται για να φτάσουν σε μια τελική συμπερασματική απόφαση του RF. Οι αποφάσεις λαμβάνονται ακολουθώντας τον πιο αποτελεσματικό δρόμο σε κάθε DT.



3. **Support Vector Machine (SVM)**: Ο αλγόριθμος SVM είναι ένας μη-πιθανοτικός, δυαδικός και γραμμικός ταξινομητής που χρησιμοποιείται για την επεξεργασία των εισερχομένων δεδομένων και την ταξινόμησή τους σε νόμιμα ή προερχόμενα από εισβολή. Το μοντέλο SVM αναπαριστά τις εισόδους ως σημεία στο χώρο και τα χωρίζει σε αυτές τις δύο κατηγορίες.
4. **Κοντινότερου Γείτονα - K Nearest Neighbor**: Ο αλγόριθμος k-NN είναι μια τεχνική μάθησης όπου ένα εισερχόμενο GOOSE ταξινομείται βάσει μερικών πρόσφατων εισόδων. Για αυτόν τον λόγο, ονομάζεται επίσης αλγόριθμος ταξινόμησης με βάση τη μνήμη. Για ένα νέο, μη ταξινομημένο γεγονός η απόφαση που λαμβάνεται καθορίζεται από τον αριθμό k, δηλαδή των πιο πρόσφατων k γεγονότων. Συγκεκριμένα, για κάθε k αριθμό πιο πρόσφατων γεγονότων, το νέο GOOSE θα χαρακτηριστεί ανάλογα με την πλειοψηφική ταξινόμηση αυτού του δείγματος. Για το διπλανό σχήμα ας υποθέσουμε ότι τα κόκκινα τρίγωνα αντιπροσωπεύουν κακόβουλα γεγονότα, ενώ τα μπλε τετράγωνα αυθεντικά γεγονότα. Τότε ένα εισερχόμενο γεγονός θα κατηγοριοποιηθεί ως κακόβουλο για k = 3, ενώ για k = 5 θεωρείται νόμιμο.



5. **Προσαρμοσμένη Ενίσχυση - Adaptive Boost**: Ο Adaboost είναι ένας αλγόριθμος ταξινόμησης που χρησιμοποιείται για να ενώσει αρκετούς αδύναμους ταξινομητές, προκειμένου να δημιουργήσει έναν πολύ ισχυρότερο ταξινομητή. Ουσιαστικά, ο Adaboost χρησιμοποιεί άλλους ταξινομητές, αναγνωρίζει τα αδυναμίες του και προσπαθεί να βελτιώσει την απόδοσή του. Αρχικά, τα δεδομένα



εισόδου επεξεργάζονται με τον πρώτο επιλεγμένο ταξινομητή. Έπειτα, τα δεδομένα σφάλματος της πρώτης ταξινόμησης θα εισαχθούν στην δεύτερη ταξινόμηση με μεγαλύτερο βάρος. Το ίδιο ισχύει για την έξοδο του δεύτερου ταξινομητή πριν δοθεί ως είσοδος στον τρίτο, κοκ. Το μοναδικό χαρακτηριστικό του Adaboost είναι ότι το βάρος ενημερώνεται σε κάθε επανάληψη. Σε αυτήν τη μελέτη, το Adaboost χρησιμοποιείται με decision stumps. Και στοχεύει στην ενίσχυση της απόδοσης των δέντρων αποφάσεων.

Οι παραπάνω πέντε αλγόριθμοι χρησιμοποιήθηκαν για να ανιχνεύσουν τυχαίες και μεθοδικές επιθέσεις σύμφωνα με το σενάριο του φαινομένου καταιγίδας που περιγράφτηκε προηγουμένως. Η πειραματική διάταξη ακολουθεί την δομή ενός ΣΑΥ όπου τα μηνύματα GOOSE δημιουργούνται από έναν προσομοιωτή στο επίπεδο του Υποσταθμού. Η απόδοση των αλγορίθμων ταξινόμησης φαίνεται στον παρακάτω πίνακα.

Μοντέλα ταξινόμησης	Accuracy	Detection Rate	False Alarm Rate	Εκπαίδευση (seconds)	Εκτέλεση (seconds)
DT	**0.9448**	**0.9231**	**0.0408**	**1.36**	**0.0009**
RF	0.9519	0.8657	0.0000	59.7	0.0080
k-NN	0.9448	0.9231	0.0408	13.41	0.0019
SVM	0.9512	0.8718	0.0338	3427.69	0.0029
AdaBoost	0.9487	0.8507	0.0194	71.84	0.0169

Σχήμα 4.14 – Αξιολόγηση αλγορίθμων ταξινόμησης γεγονότων GOOSE

4.7. Ασφάλεια και πρωτόκολλο ICCP

Η ασφάλεια των επικοινωνιών ICCP αποτελεί ένα κρίσιμο ζήτημα την σημερινή εποχή, καθώς αναφερόμαστε σε σύγχρονα επικοινωνιακά δίκτυα που μεταδίδουν κρίσιμες πληροφορίες σε μακρινές αποστάσεις. Παρά την σημασία αυτή, οι διαθέσιμες ερευνητικές δημοσιεύσεις που ασχολούνται με την ανάπτυξη και δοκιμή συγκεκριμένων μηχανισμών ασφαλείας του ICCP είναι σε μεγάλο βαθμό ανεπαρκείς. Λόγω αυτής της συνθήκης δεν είναι εφικτή η παρουσίαση πειραματικών ή θεωρητικών μεθοδολογιών ανάπτυξης IDS συστημάτων. Παρόλα αυτά η μελέτη μας στην παρούσα ενότητα θα κινηθεί στους εξής άξονες. Αρχικά, θα γίνει μια περιγραφή της εξέλιξης του ίδιου του πρωτοκόλλου ως προς τα ζητήματα κυβερνοασφάλειας. Δεύτερον, με βάση την εμπειρία που αποκτήσαμε κατά την διάρκεια εκπόνησης της διπλωματικής εργασίας, θα αναφέρουμε κάποιες σημαντικές προτάσεις για μελλοντικές πειραματικές δοκιμές ασφαλείας των επικοινωνιών ICCP.

4.7.1. Βελτιώσεις ασφαλείας του πρωτοκόλλου ICCP

Το αρχικό ICCP γενικότερα είναι ένα μη προστατευμένο πρωτόκολλο και είναι ευάλωτο σε ενέργειες σχετικά με παραβιάσεις της εμπιστευτικότητας και της ακεραιότητας όπως, παρεμπόδιση, αλλοίωση, πλαστογράφηση και παράνομη καταγραφή της επικοινωνίας. Λόγω αυτών των ευπαθειών στη μη προστατευμένη επικοινωνία ICCP, προστέθηκαν διάφορες **βελτιώσεις ασφαλείας, γνωστές ως Secure ICCP** (δηλαδή Ασφαλές ICCP). Αυτό έχει ως αποτέλεσμα τη δημιουργία ενός νέου προϊόντος ICCP, του οποίου η επικοινωνία μπορεί να κρυπτογραφηθεί και να ελεγχθεί η αυθεντικότητά της, δίνοντας μια πρώτη απάντηση στα διάφορα ζητήματα εμπιστευτικότητας που αναδεικνύει η σημερινή εποχή. Αυτές οι νέες δυνατότητες του πρωτοκόλλου είναι οι ακόλουθες:

- ✓ **Επισκόπηση Ασφάλειας της ICCP επικοινωνίας:** Η μη-προστατευμένη έκδοση επικοινωνίας ICCP μεταδίδεται με τέτοιο τρόπο ώστε ένας εισβολέας που χρησιμοποιεί έναν αναλυτή δικτύου, όπως το Wireshark, να μπορεί να δει τα δεδομένα σε καθαρή μορφή. Ο αναλυτής του δικτύου μπορεί εύκολα να καταγράψει τα πακέτα πρωτοκόλλου διαδικτύου (IP), όπου τα πακέτα αυτά έχουν μια ευρέως γνωστή μορφή περιεχομένου (Πχ. κεφαλίδα, διεύθυνση προορισμού, φορτίο). Επίσης, το φορτίο δεδομένων σε ένα πακέτο ICCP αποστέλλεται σε καθαρό κείμενο και μπορεί να αναγνωστεί από οποιαδήποτε συσκευή εντός του δικτύου.

  Από την άλλη, τα ασφαλή πακέτα ICCP, ενώ δημιουργούνται με την ίδια μορφή με τα μη προστατευμένα πακέτα ICCP, διαθέτουν κρυπτογραφημένο φορτίο χρησιμοποιώντας τα σχετικά πιστοποιητικά που είναι εγκατεστημένα στον ICCP- διακομιστή. Έτσι ο διακομιστής λαμβάνει τα δεδομένα με τέτοιον τρόπο ώστε να μπορεί να επαληθεύει το περιεχόμενο και την ακεραιότητά τους.
- ✓ **Επιλογή ή Δημιουργία Διακομιστή Πιστοποίησης:** Για να εγκαθιδρυθεί μια ασφαλή σύνδεση ICCP, απαιτείται οπωσδήποτε ένας διακομιστής πιστοποίησης, στον οποίο θα πρέπει να έχουν πρόσβαση όλοι οι φορείς που χρησιμοποιούν την ασφαλή ICCP επικοινωνία για την επικύρωση των πιστοποιητικών. Η δημιουργία αυτού του διακομιστή και η καθιέρωση των πιστοποιητικών στην επικοινωνία αποτελούν κομβικό στάδιο για την διαχείριση των πιστοποιητικών για την κρυπτογράφηση.
- ✓ **Δημιουργία Πιστοποιητικών:** Ο διαχειριστής του διακομιστή πιστοποίησης θα πρέπει να διαθέτει πληροφορίες για όλους τους ICCP-διακομιστές ώστε να δημιουργήσει τα πιστοποιητικά που αφορούν συγκεκριμένες μηχανές. Κάθε διακομιστής χρειάζεται αρχικά τέσσερα πιστοποιητικά για την έναρξη, δηλαδή δύο πιστοποιητικά για την ασφάλεια MACE και ακόμη δύο για την ασφαλή κρυπτογράφηση. Αφού τα πιστοποιητικά δημιουργηθούν, τα -δημόσια- κλειδιά ασφαλείας (public keys) πρέπει να εκχωρηθούν σε όσους διακομιστές συμμετέχουν στην διαμόρφωση ασφάλειας της επικοινωνίας.
- ✓ **Ρύθμιση της Στοίβας SISCO:** Η στοίβα ICCP της SISCO είναι η πιο κοινή δομή δικτύου που χρησιμοποιείται για την υλοποίηση του ICCP σε ένα EMS. Η στοίβα αναλαμβάνει τους ελέγχους ICCP και μοιράζει τη διαχείριση των δεδομένων στο λογισμικό του EMS. Αυτή η κοινή στοίβα αφενός εξασφαλίζει τη διαλειτουργικότητα μεταξύ των εφαρμογών διαφορετικών προμηθευτών και αφετέρου διευκολύνει την υλοποίηση, καθώς προσφέρει και στις δύο πλευρές ένα κοινό εργαλείο για την αναγνώριση προβλημάτων σύνδεσης.

  Η στοίβα SISCO λοιπόν, οφείλει να αναβαθμιστεί για να εξυπηρετήσει το Secure ICCP και ενσωματώσει τα απαραίτητα πιστοποιητικά ασφαλείας. Η νέα διαμόρφωση, που προκύπτει, επιτρέπει στην SISCO στοίβα να πραγματοποίει ασφαλές συνδέσεις. Σε περίπτωση που μια ασφαλής σύνδεση αποτύχει, τότε διακόπτεται και μπαίνει σε κατάσταση σφάλματος.
- ✓ **Ρύθμιση του OAG:** Κάθε προμηθευτής διαθέτει διαφορετικά στοιχεία διεπαφής για τις ανταλλαγές δεδομένων ICCP. Για παράδειγμα, μια διαμόρφωση συστήματος μπορεί να περιλαμβάνει εργασίες για τη ρύθμιση των συνδέσεων σε επίπεδο μηχανής, τη διαμόρφωση των στοιχείων δεδομένων που περνούν, κ.λπ. Αφού το μοντέλο διαμόρφωσης όλων των πλευρών έχει κατασκευαστεί και δοκιμαστεί, τότε εφαρμόζεται στο λειτουργικό σύστημα και ενεργοποιείται η τελική.

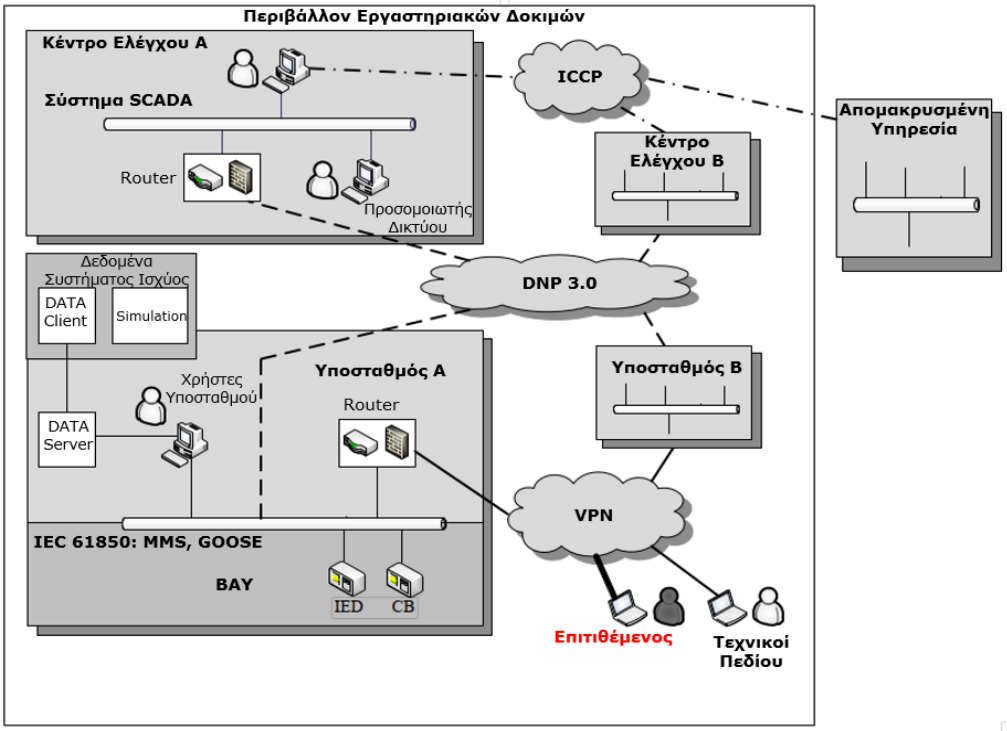
Ωστόσο, η υλοποίηση του κάθε κατασκευαστή μπορεί να διαφέρει. Η διαμόρφωση λοιπών του επιπέδου σύνδεσης, απαιτεί δύο βασικά πλαίσια για α) την επιλογή ασφαλούς σύνδεσης και β) το πλαίσιο επιστροφής σε μη ασφαλή σύνδεση που θα υποδείξει την ανάπτυξη ενός ενημερωμένου μοντέλου.

4.7.2. Ασφαλή διαμόρφωση δικτύου ICCP

Εκτός από ένα ασφαλές πρωτόκολλο επικοινωνίας είναι ιδιαίτερα σημαντικό να εφαρμόζονται **σωστές πρακτικές ασφαλείας σε επίπεδο διαμόρφωσης του ICCP δικτύου.** Τα δίκτυα ICCP, όπως γνωρίζουμε χρησιμοποιούνται ευρέως για την επικοινωνία μεταξύ κέντρων ελέγχου, αλλά και την διασύνδεση περιφερειακών και εθνικών λειτουργικών συστημάτων και εταίρων από διαφορετικά διασυνδεδεμένα ενεργειακά συστήματα. Οι διάφοροι συμμετέχοντες - στην ICCP επικοινωνία - μοιράζονται σημαντικές πληροφορίες με ένα σύστημα ανταλλαγής δεδομένων δημιουργώντας έτσι ένα αποτελεσματικό μέσο οργάνωσης και σχεδιασμού του εποπτικού ελέγχου του φυσικού συστήματος. Συνεπώς, το δίκτυο επικοινωνίας οφείλει να προσφέρει μια αξιόπιστη και συνεπή μετάδοση δεδομένων ανά πάσα στιγμή. Για την διασφάλιση των παραπάνω απαιτήσεων και υψηλών επιδόσεων δικτύου, πρέπει να ληφθούν υπόψη τα ζητήματα ασφάλειας για την προστασία των πληροφοριών μετάδοσης από μη εξουσιοδοτημένους ή κακόβουλους χρήστες.

Η πιο συνηθισμένη εφαρμογή του πρωτοκόλλου είναι η διαμόρφωση ενός δικτύου που επιτρέπει την ανταλλαγή (πραγματικού χρόνου) δεδομένων και ιστορικών (δηλ. δεδομένα μέτρησης, μηνύματα εντολών και δεδομένα προγραμματισμού) μεταξύ κέντρων ελέγχου. Ένα μελλοντικό πειραματικό περιβάλλον, λοιπόν, θα μπορούσε να περιλαμβάνει δύο κέντρα ελέγχου (Α και Β) στον ίδιο χώρο δοκιμών, καθώς και μια διαδικτυακή σύνδεση με το κέντρο ελέγχου (Γ) ενός τρίτου παράγοντα (πχ. μια στατιστική υπηρεσία). Ο εργαστηριακός πειραματικός χώρος θα υλοποιηθεί σε ένα τοπικό Ethernet LAN με σύνδεση στο διαδίκτυο. Σε μια τέτοια αρχιτεκτονική, το ICCP χρησιμοποιείται μέσω του Ethernet και η σύνδεση με απομακρυσμένη πρόσβαση στο διαδίκτυο βασίζεται σε εξωτερικούς δρομολογητές IP. Για τη σύνδεση του απομακρυσμένου κέντρου μπορεί να χρησιμοποιηθεί κάποιο Virtual Private Network (VPN), όπου κατά την προσπάθεια σύνδεσης, το λογισμικό του VPN-πελάτη θα συνδέεται με το VPN-διακομιστή χρησιμοποιώντας ένα πρωτόκολλο-σήραγγα (tunneling protocol). Η σύνδεση μεταξύ του πελάτη και του διακομιστή VPN θα πρέπει να είναι ασφαλής και όλα τα δεδομένα που ανταλλάσσονται μέσω αυτού του τούνελ θα πρέπει να κρυπτογραφηθούν προς κάθε κατεύθυνση. Επίσης, για την ασφαλή ανταλλαγή πληροφοριών μεταξύ των κέντρων ελέγχου μέσω του διαδικτύου και για την αποτροπή άλλων χρηστών να έχουν άμεση πρόσβαση σε κρίσιμα δεδομένα, η βάση δεδομένων πρέπει να είναι σε μορφή proxy. Για την περεταίρω ενίσχυση της ασφαλείας απαιτείται επίσης χρήση προστατευτικών τειχών (firewalls), στα όρια του LAN, για να λειτουργήσουν ως φίλτρα ασφαλείας του τοπικού δικτύου. Ουσιαστικά, το firewall θα αποτελεί μια συνοριακή γραμμή άμυνας εκτελώντας αναγνωρίσεις διεύθυνσης ή θύρας. **Το προτεινόμενο δοκιμαστικό περιβάλλον για μελλοντικά πειράματα κυβερνοασφάλειας** είναι το ακόλουθο πολυεπίπεδο δίκτυο επικοινωνίας και περιλαμβάνει DNP3, GOOSE, MMS και ICCP πρωτόκολλα:

Πέρα από τις σωστές πρακτικές δικτύωσης και διαμόρφωσης του ICCP, απαιτείται από τις ερευνητικές δοκιμές να αναπτύξουν και μέτρα ασφαλείας για την αναγνώριση ανωμαλίας στην κίνηση του ICCP. Θα πρέπει επίσης να δοκιμάσουν ένα ταιριαστό σύστημα IDS το οποίο θα καταφέρνει αποτελεσματικά να (α) αναγνωρίζει τα δεδομένα που μεταφέρονται στο δίκτυο, (β.) να παρακολουθεί όλες τις συνδιαλλαγές μεταξύ χρηστών και (γ.) να προλαμβάνει τις επιθέσεις πριν συμβούν. Η στατιστική μέθοδος ως μια αρχική δοκιμαστική προσπάθεια μελέτης και αναγνώρισης ανωμαλιών στην κίνηση ICCP, θα μπορούσε να είναι μια σωστή επιλογή, εάν κρίνουμε από την αποτελεσματικότητα που είχε στις πειραματικές δοκιμές που παρουσιάσαμε στα υπόλοιπα – βασισμένα στο Ethernet - πρωτόκολλα επικοινωνίας.



Σχήμα 4.15 – Αρχιτεκτονική δικτύωσης DNP3, GOOSE, MMS, ICCP

5. Συμπεράσματα και προκλήσεις στην κυβερνοασφάλεια

5.1. Τα επίπεδα ασφάλειας των βιομηχανικών πρωτοκόλλων επικοινωνίας

Η έννοια της ασφάλειας σε κάθε περίπτωση **επικαθορίζεται από τους δυνητικούς κινδύνους** που έχουν εμφανιστεί είτε σε πειραματικό στάδιο, είτε σε πραγματικές εφαρμογές. Όπως διαπιστώνουμε, οι κυβερνοεπιθέσεις που παρουσιάστηκαν διαφέρουν σε μεγάλο βαθμό από την λογική των επιθέσεων σε απλούς Υπολογιστές, λόγω των ειδικών ιδιαιτεροτήτων των βιομηχανικών επικοινωνιών. Δηλαδή, οι επιτιθέμενοι οφείλουν να κατανοούν τα πρότυπα επικοινωνίας που αναλύθηκαν και να διεξάγουν κακόβουλες ενέργειες προσαρμοσμένες στην δομή πακέτων του εκάστοτε πρωτοκόλλου. Ένα ακόμη συμπέρασμα που μπορούμε να εξάγουμε για όλα τα πρότυπα επικοινωνίας που αναφέρθηκαν στην διπλωματική εργασία είναι η **έλλειψη βασικών προδιαγραφών πρόληψης και αντιμετώπισης ζητημάτων ασφαλείας**. Ακόμη και τα βελτιωμένα πρότυπα πρωτοκόλλων που μπορεί να προσφέρουν κάποια επίπεδα ασφάλειας, εισάγοντας για παράδειγμα λειτουργίες αυθεντικοποίησης, δεν εξασφαλίζουν σε επαρκές βαθμό μια προστατευμένη επικοινωνία. Τα δύο αυτά

στοιχεία, φάνηκε ότι αξιοποιούνται από τους επιτιθέμενους στις πειραματικές δοκιμές που μελετήθηκαν. Δηλαδή, να κατέχουν βαθιά γνώση τόσο για τους κανόνες που διέπουν την επικοινωνία, όσο και για της ελλείψεις της ως προς την γενικότερη κυβερνοασφάλεια. Έτσι, οι επιθέσεις αυτές κατάφεραν να διαταράξουν την ομαλή ανταλλαγή πληροφοριών εισάγοντας μεγάλες καθυστερήσεις στην κίνηση του δικτύου, υποκλέπτοντας ή απορρίπτοντας αυθεντικά πακέτα και εισχωρώντας πλαστά δεδομένα. Εάν επίσης αναλογιστούμε ότι η ανάλυση που διεξήχθη βασίστηκε σε πειραματικές δοκιμές και εργαστηριακές προσομοιώσεις, τότε μπορούμε να αντιληφθούμε πόσο μεγαλύτερες μπορεί να είναι οι συνέπειες στο πραγματικό βιομηχανικό περιβάλλον. Σε ένα σύστημα Παραγωγής Ηλεκτρικής Ενέργειας, **οι επιπτώσεις** αντίστοιχων διαταραχών στην επικοινωνία θα είναι σίγουρα μεγαλύτερης κλίμακας και ιδιαίτερα καταστροφικές για την παραγωγή και την εξυπηρέτηση των φορτίων ισχύος. Συνεπώς, η εξέλιξη των δικτύων επικοινωνίας και της έννοιας του κυβερνοχώρου στα σύγχρονα δίκτυα διαμορφώνουν ένα νέο ερευνητικό πεδίο που αφορά αναπόφευκτα την ασφάλεια του συνολικού συστήματος ενέργειας.

Οι παραπάνω διαπιστώσεις αποτελούν κοινό σημείο αναφοράς για τα πρωτόκολλα επικοινωνίας που μελετήθηκαν στην παρούσα εργασία. Παρ' όλα αυτά η δυνατότητα διεξαγωγής κυβερνοεπίθεσης, αλλά και το εύρος των αντίστοιχων επιπτώσεων, διαφέρει για κάθε πρωτόκολλο που χρησιμοποιείται και για κάθε πεδίο εφαρμογής του. Για παράδειγμα, τα πρωτόκολλα Modbus, DNP3 και IEC/104 έχουν κυρίως χρήση σε εφαρμογές παρακολούθησης και αυτόματου ελέγχου χαμηλότερου επιπέδου και κοντά στο πεδίο. Τα αντίστοιχα συστήματα SCADA αφορούν ένα συγκεκριμένο τομέα λειτουργιών και αποτελούν μέρος ενός μεγαλύτερου συστήματος παρακολούθησης ή ελέγχου. Τα πρωτόκολλα μηνυμάτων GOOSE και MMS χρησιμοποιούνται κυρίως για τον απομακρυσμένο έλεγχο ολόκληρων υποσταθμών στην μεταφορά ή την διανομή, που σημαίνει ότι μια επιτυχημένη κυβερνοεπίθεση θα έχει αρνητικές επιπτώσεις σε πιο κρίσιμα σημεία του συστήματος, όπως οι Μ/Σ υψηλής τάσης. Από την άλλη, το ICCP φτάνει στα ανώτερα ιεραρχικά επίπεδα του ελέγχου καθώς έχει τον ρόλο του συντονισμού των υποσυστημάτων ολόκληρου του δικτύου. Για να επιτευχθεί αυτό, χρησιμοποίει ακόμα πιο ευάλωτες επικοινωνίες (ευρείας περιοχής) ενώ ταυτόχρονα μεταδίδει περισσότερα και πιο εμπιστευτικά δεδομένα, τα οποία αφορούν την συνολική κατάσταση λειτουργίας του συστήματος.

Συγκεκριμένα, τα συμπεράσματα που εξάγονται για τα **ζητήματα ασφαλείας σε κάθε πρότυπο επικοινωνίας** που μελετήθηκε, συνοψίζονται παρακάτω:

1. Modbus/TCP

Η έκδοση που βασίζεται στο TCP/IP, δημιουργεί δυνατότητες ανάπτυξης εφαρμογών Modbus που βασίζονται στο Ίντερνετ. Ωστόσο, σε αυτήν την διαδικασία δεν έχουν προβλεφθεί οι νέες απαιτήσεις που προκύπτουν για την κυβερνοασφάλεια. **Οι κυβερνοεπιθέσεις** που παρουσιάστηκαν ανέδειξαν ακριβώς αυτήν την ανάγκη καθώς **εκμεταλλεύονταν σε μεγάλο βαθμό την στοίβα TCP/IP** (βλ. ταξινόμηση επιθέσεων ενότητας 3.2). Επιπλέον, **η απλή δομή** των πακέτων και των υπηρεσιών που παρέχει το πρωτόκολλο σε επίπεδο εφαρμογής **βοηθούν τους επίδοξους κυβερνοεισβολείς να κατανοήσουν γρήγορα τα χαρακτηριστικά της επικοινωνίας**. Συνεπώς, οι επιθέσεις που τροποποιούν δεδομένα ή εισχωρούν πλαστογραφημένα πακέτα μπορούν να διεξαχθούν και από σχετικά άπειρους επιτιθέμενους.

Τα πειράματα επιθέσεων που αναφέραμε απέδειξαν ότι με την απλή καταγραφή των νόμιμων πακέτων που ανταλλάσσονται, οι επιτιθέμενοι ερευνητές μπόρεσαν εύκολα να κατασκευάσουν μεγάλο αριθμό νέων πλαστών πακέτων. Τα αποτελέσματα ήταν, μεγάλες καθυστερήσεις στην επικοινωνία και αποτελεσματική πλαστογράφηση των δεδομένων κατάστασης Modbus-συσκευών. Χαρακτηριστικό παράδειγμα ήταν οι επιθέσεις MITM (βλ. 3.2.3), όπου οι επιπτώσεις τους στο φυσικό σύστημα ενέργειας ήταν ιδιαίτερα σοβαρές. Ενώ το ηλεκτρικό σύστημα λειτουργούσε σε κανονικές συνθήκες (το ρεύμα και η τάση ήταν σταθερά), η εσφαλμένη μεταβολή της κατάστασης του διακόπτη ισχύος δημιούργησε προβλήματα. Μια απότομη πτώση τάσης **μειώνει σημαντικά το περιθώριο σταθερότητας του συστήματος και μπορεί να οδηγήσει ακόμη σε μεγάλα οικονομικά προβλήματα.** Αντίστοιχες κυβερνοεπιθέσεις σε πραγματικό περιβάλλον, πιθανόν να επηρεάσουν αλυσιδωτά τη λειτουργικότητα και άλλων προστατευτικών ρελέ στο σύστημα, προκαλώντας διαδοχικά σφάλματα πτώσης τάσης. Ακόμη, εάν ο επιτιθέμενος στόχευε ταυτόχρονα περισσότερες γραμμές μετάδοσης, η επίπτωση θα ήταν η γενική διακοπή της ηλεκτροδότησης των καταναλωτών.

Συμπέρασμα: Το Modbus αρχικά σχεδιάστηκε για σειριακές επικοινωνίες που χρησιμοποιούνται σε τοπικά και σχετικά προστατευμένα δικτυακά περιβάλλοντα. Η απουσία μηχανισμών πρόληψης, αλλά και η ελλιπής έρευνα σχετικά με επεκτάσεις αυθεντικοποίησης πακέτων Modbus, καθιστούν γενικότερα το πρωτόκολλο μη ασφαλές για εφαρμογές σε κρίσιμες ενεργειακές υποδομές. Εάν όμως επιλεχθεί τότε είναι απαραίτητο να αναπτυχθούν παράλληλα IDS εφαρμογές που θα διασφαλίζουν την διαθεσιμότητα, την εμπιστευτικότητα και την ακεραιότητα της επικοινωνίας

2. DNP3

Ένα τρι-επίπεδο πρωτόκολλο εφαρμογής, από τη μία προσφέρει αυξημένη λειτουργικότητα στης εφαρμογές DNP3, ταυτόχρονα όμως διευρύνει το πεδίο στο οποίο μπορούν να πειραματιστούν επίδοξοι επιτιθέμενοι. Για παράδειγμα, οι ρίψεις συνεχόμενων πακέτων που εμπεριέχουν πλαστές σημαίες κατακερματισμού στο επίπεδο ψευδο-μεταφοράς μπορούν απλώς να καταστρέψουν την ομαλή επεξεργασία των δεδομένων εφαρμογής. Η ταξινόμηση που παρουσιάστηκε (βλ. 3.3.1) αφορά αυτήν την διαπίστωση και κατηγοριοποιεί κυβερνοεπιθέσεις ανάλογα με το επίπεδου (ή τα επίπεδα) που έχουν τεθεί ως στόχοι. τα οποία έχουν τεθεί ως στόχοι από τους επιτιθέμενους. Οι επιπτώσεις των επιθέσεων αφορούν τόσο και τον αποστολέα όσο και τον παραλήπτη και **θέτουν σε κίνδυνο την αξιοπιστία του συστήματος** ως προς:

- **Τον γενικότερο έλεγχο και την ακεραιότητα του συστήματος.**
- **Το επίπεδο ενημέρωσης των δεδομένων (διαθεσιμότητα).**
- **Την εμπιστευτικότητα του συστήματος και των δεδομένων του σε επίπεδο εφαρμογής.**

Στον παρακάτω πίνακα παρουσιάζεται μια αξιολόγηση των επιπτώσεων αυτών ανά επίπεδο-DNP3. Η αξιολόγηση γίνεται με βάση το μέγεθος της επίδρασης των επιθέσεων και σύμφωνα με τους εξής χαρακτηρισμούς: χαμηλή, κανονική, μεγάλη:

Επίπεδα Πρωτοκόλλων DNP3				
Επιπτώσεις Επιθέσεων	Σύνδεσης - Δεδομένων	Ψευδο-μεταφορά	Εφαρμογή	Κοινά
Εμπιστευτικότητα	-	-	Χαμηλή	Κανονική
Ενημέρωση	Υψηλή	Κανονική	Υψηλή	Υψηλή
Έλεγχος	Υψηλή	Κανονική	Υψηλή	Υψηλή

Σχόλιο: Η απώλεια εμπιστευτικότητας συμβαίνει όταν ένας εισβολέας αποκτά σημαντικές πληροφορίες σχετικά με τις διαμορφωμένες συσκευές ή την γενική τοπολογία του δικτύου. Αυτό, είναι συνήθως το πρώτο βήμα για μια πιο σοβαρή επίθεση που έπεται, διότι σε αυτό το σημείο γίνεται από τον εισβολέα η αναγνώριση των αδυναμιών και των σημείων εισόδου. Η απώλεια ενημέρωσης συμβαίνει όταν το κέντρο ελέγχου δεν έχει ακριβείς πληροφορίες για την κατάσταση του συστήματος. Ένα **χαρακτηριστικό παράδειγμα απώλειας της διαθεσιμότητας** είναι οι επιθέσεις που στοχεύουν στην υπερχείλιση της μνήμης DNP3-συσκευών (βλ. 3.3.2). Ο επιτιθέμενος γεμίζει τους buffer συλλεκτών δεδομένων με πλαστογραφημένα πακέτα, πράγμα που οδηγεί σε σημαντικών απώλειες πληροφοριών και γεγονότων από το πεδίο. Τέτοιες επιθέσεις μπορεί να οδηγήσουν σε σοβαρά περιστατικά, καθώς οι επιπτώσεις τους μπορεί να παραμείνουν απαρατήρητες μέχρι να είναι πολύ αργά. Ακόμη πιο επικίνδυνες είναι οι επιθέσεις που οδηγούν στην απώλεια του ελέγχου όπου ο εισβολέας που αποκτά τον έλεγχο ενός κεντρικού συστήματος SCADA μπορεί πραγματικά να προκαλέσει χάος στον έλεγχο και μεγάλη αναταραχή στο σύστημα.

Γενικότερα, το DNP3 επίσης σχεδιάστηκε για σειριακές επικοινωνίες τοπικών δικτύων. Το γεγονός αυτό οδήγησε στην ανάπτυξη πρόσθετων μηχανισμών ασφαλείας (βλ. DNP3Sec), οι οποίες όμως δεν είναι πάντα εφαρμόσιμες, όπως θα αξιολογήσουμε παρακάτω. Πλέον αρκετές εφαρμογές DNP3 δίνουν μεγαλύτερη σημασία στην κυβερνοασφάλεια του συστήματος χρησιμοποιώντας πρόσθετες άμυνες και εξωτερικούς μηχανισμούς ασφαλείας (πχ. τείχη προστασίας – firewalls). Παρόλα αυτά, είναι περισσότερο κρίσιμο να προστατευτεί το ίδιο το πρωτόκολλο επικοινωνίας και να αναπτυχθούν μέθοδοι ανίχνευσης επιθέσεων που στοχεύουν στις αδυναμίες του. Τα πειράματα (βλ. 3.3.3) ανέδειξαν ακριβώς αυτήν την ανάγκη, τονίζοντας τόσο τα ζητήματα αυθεντικοποίησης, όσο και την **αδυναμία των συστημάτων ελέγχου να αντιλαμβάνονται καταστάσεις κυβερνοεπιθέσεων**.

3. IEC/104

Η έλλειψη μηχανισμών πρόληψης στα επίπεδα εφαρμογής και συνδέσεων δεδομένων του πρωτοκόλλου έχει ως αποτέλεσμα τα συστήματα κρίσιμων ενεργειακών υποδομών να αντιμετωπίζουν μεγάλο κίνδυνο κυβερνοεπιθέσεων. Τα πειράματα που μελετήθηκαν από την διαθέσιμη βιβλιογραφία έδειξαν ξεκάθαρα ότι το IEC-60870-5-104 που χρησιμοποιείται περιβάλλοντα SCADA είναι ανασφαλές και ευάλωτο σε πολλές επιθέσεις που μπορούν να διαταράξουν την κανονική λειτουργία των κρίσιμων υποδομών. Συνεπώς, απαιτείται σημαντική προσπάθεια για να ενισχυθεί το επίπεδο ασφαλείας των συστημάτων που κάνουν χρήση του IEC/104.

Ως προς τα πακέτα του πρωτοκόλλου, το IEC/104 δεν γεννά τις αντίστοιχες ανησυχίες με το Modbus διότι η δομή του είναι περισσότερο πολύπλοκη. Αυτό

σημαίνει ότι οι επιτιθέμενοι που στοχεύουν το επίπεδο εφαρμογής πρέπει να έχουν βαθιά γνώση του πρωτοκόλλου. Ωστόσο, η πληθώρα των δεδομένων που μεταφέρονται και το προκαθορισμένο ανώτατο μέγεθος ενός APDU καθιστά **δύσκολη την ενσωμάτωση κλειδιών κρυπτογράφησης ή αυθεντικοποίησης.** Οι μηχανισμοί αυτοί απαιτούν αρκετά επιπλέον δεδομένα, συνεπώς η ανάπτυξή τους είναι δύσκολη σε απαιτητικές εφαρμογές.

Από τα πειράματα MITM καταλαβαίνουμε ότι, η επίθεση τροποποίησης δεδομένων που διεξήχθη στο περιβάλλον του πειραματικού εργαστηρίου **απαιτεί μεγάλο επίπεδο γνώσης του πεδίου εφαρμογής και του πρωτοκόλλου**. Αυτό εμφανώς υποδεικνύει και σαφή πρόθεση του επιτιθέμενου -όχι απλώς να πειραματιστεί- αλλά να βλάψει στοχευμένα το σύστημα αυτοματισμού και κατ' επέκταση το φυσικό ηλεκτρικό σύστημα. Πρέπει επίσης να σημειωθεί ότι, στο πείραμα η μηχανή Kali παρέχει το σημείο εκκίνησης για τις επιθέσεις των εργαστηριακών δοκιμών. Αντιθέτως σε μια πραγματική επίθεση σε ένα λειτουργικό σύστημα, αυτό το σημείο εκκίνησης πιθανόν θα γίνει μέσω της μόλυνσης με κακόβουλα λογισμικά ή μέσω μιας σχετικής εισβολής στο δίκτυο.

Σχόλιο: Η επιλογή τροποποίησης των πεδίων CoT και SPI ενός μηνύματος IEC/104 ήταν ενδεικτική. Ένας πραγματικός επιτιθέμενος που χρησιμοποιεί τα ίδια ή αντίστοιχα εργαλεία επιθέσεων μπορεί να αλλάξει οποιοδήποτε πεδίο είτε ολόκληρο το πακέτο μετάδοσης. Για παράδειγμα, θα μπορούσε να αποκρύπτει ή να παράγει ψευδείς καταστάσεις σφάλματος. Το γεγονός αυτό δημιουργεί μεγάλες ανησυχίες σε επίπεδο ανίχνευσης εισβολών, που αποτελούν και τον αποτελεσματικότερο τρόπο ενίσχυσης της ασφάλειας. Η δυνατότητα απόκρυψης σφαλμάτων από τις μονάδες ή συστήματα ελέγχου οδηγεί αναπόφευκτα σε σοβαρές επιπτώσεις στη λειτουργικότητα και την συνολική αξιοπιστία του ηλεκτρικού κυβερνοσυστήματος.

4. IEC 61850

Εδώ μιλάμε κυρίως για εφαρμογές Υποσταθμών, όπου οι βασικοί στόχοι των επιτιθέμενων είναι οι έξυπνες συσκευές, οι οποίες ελέγχουν τον φυσικό εξοπλισμό ισχύος. Όταν τα IED τεθούν υπό κατάσταση κυβερνοεπίθεσης, τότε οι εισβολείς αποκτούν τις ακόλουθες δυνατότητες:

- Πρόσβαση σε εμπιστευτικά δεδομένα
- Έλεγχος εξοπλισμού ισχύος
- Άρνηση εκτέλεσης υπηρεσιών πρωτοκόλλων
- Κατανάλωση μνήμης buffer & CPU

Το παράδειγμα που μελετήθηκε αφορούσε ενέργειες επιθέσεων σε σύστημα Φωτοβολταϊκών (βλ. 3.5.4). Ο επιτιθέμενος κατάφερε να εισάγει πλαστά δεδομένα και να περιορίσει την ικανότητα του Inverter να παρέχει την απαιτούμενη ισχύ. Την ίδια στιγμή ο IEC-61850/πελάτης (κέντρο ελέγχου) δεν διέκρινε κανένα σφάλμα κατά την διάρκεια της επίθεσης. Συγκεκριμένα, πριν την εκτέλεση οποιασδήποτε κυβερνοεπίθεσης, το σύστημα λειτουργούσε στο 100% της ονομαστικής ισχύος, δηλαδή 10.5 kW, με τον χειριστή στην συνέχεια να δίνει εντολή ανώτατου περιορισμού 60%, δηλαδή περίπου 7.1 kW. Όταν ο επιτιθέμενος καταφέρνει να εισβάλει στην επικοινωνία χειριστή – Inverter, όρισε ως μέγιστο όριο ισχύος το 10%. Το αποτέλεσμα ήταν ο αντιστροφέας να ρίξει κατακόρυφα την ισχύ εξόδου του, μέχρι την τελική απενεργοποίησή του. Η ένδειξη της συσκευής υποδεικνύει στους χρήστες κατάσταση λειτουργίας αναμονής (stand-by), από την οποία ο Inverter χρειάζεται αρκετά – και κρίσιμα για το σύστημα - λεπτά ώστε να επανέλθει. Βλέπουμε λοιπόν **σημαντικές επιπτώσεις στην ακεραιότητα του φυσικού**

συστήματος, οι οποίες σε μια πραγματική ενεργειακή υποδομή θα επηρέαζαν σε καταστροφικό βαθμό την ευστάθεια του ηλεκτρικού συστήματος.

Η μεγάλη διαφοροποίηση της IEC61850 επικοινωνίας με τις υπόλοιπες είναι ότι εισάγει **συγκεκριμένα προαπαιτούμενα που αφορούν τον χρόνο μετάδοσης** των δεδομένων. Οι απαιτήσεις αυτές είναι ιδιαίτερα αυστηρές για τα μηνύματα που σχετίζονται καταστάσεις σφάλματος της φυσικής υποδομής (δηλ. GOOSE).

Σχόλιο: Οι χρονικές απαιτήσεις μετάδοσης μηνυμάτων δημιουργού αρκετά εμπόδια σε επεκτάσεις αυθεντικοποίησης και κρυπτογράφησης. Πολλές από τις προτάσεις για τεχνικές πρόληψης των μηνυμάτων GOOSE επιβαρύνουν σημαντικά την επεξεργασία των μηνυμάτων και φτάνουν τα 3ms που απαιτούνται. Συνεπώς η εύρεση αποδοτικότερων και εφαρμόσιμων μεθόδων ασφάλειας για το πρότυπο είναι ακόμη ανοικτή.

5. ICCP

Η φύση του πρωτοκόλλου δημιουργεί εξ αρχής μεγάλους προβληματισμούς από την σκοπιά της κυβερνοασφάλειας. Οι επικοινωνίες ICCP διανύουν μεγάλες αποστάσεις και αξιοποιούνται σε εφαρμογές που απαιτούν την μετάδοση κρίσιμων πληροφοριών ενέργειας. Αφενός, η διαθέσιμη έρευνα δεν περιλαμβάνει αναφορές σχετικά με κυβερνοεπιθέσεις βασισμένες στα χαρακτηριστικά του πρωτοκόλλου και αφετέρου η ανάπτυξη μηχανισμών κυβερνοασφάλειας περιορίζονται σε κλασικές πρακτικές προστασίας του δικτύου (πχ. χρήση firewalls).

Παρ' όλα αυτά οι δικτυακές επιθέσεις στα αιολικά πάρκα (3.6.3) μας δείχνουν ότι υπάρχει τεράστιος κίνδυνος και για τις επικοινωνίες που χρησιμοποιούνται στα ανώτερα συστήματα ελέγχου και τα επιχειρησιακά περιβάλλοντα. Για αυτές τις επικοινωνίες και για τα πρωτοκόλλα που χρησιμοποιούν, η βιβλιογραφία έχει αρκετές ελλείψεις σχετικά με το ζήτημα της κυβερνοασφάλειας. Συνεπώς, η βαθύτερη μελέτη και διεξαγωγή εκτενών δοκιμαστικών κυβερνοεπιθέσεων σε «ανώτερα» πρωτόκολλα ελέγχου, όπως είναι το ICCP, είναι ζωτικής σημασίας.

5.2. Συμπεράσματα και ανοιχτά ζητήματα για τα IDS

Το μεγάλο μέρος των πειραματικών δοκιμών ανέδειξε την σημασία ανάπτυξης μηχανισμών κυβερνοασφάλειας που ανιχνεύουν και αντιμετωπίζουν αποτελεσματικά κυβερνοεπιθέσεις στα δίκτυα των ενεργειακών υποδομών. Ειδικά εάν αναλογιστούμε ότι ακόμη και σήμερα, πολλά δικτυακά συστήματα στον τομέα της ενέργειας δεν διαθέτουν ή δεν συντηρούν επαρκώς τους μηχανισμούς ασφάλειας της επικοινωνίας, όλες οι μέθοδοι ανίχνευσης εισβολών κρίνονται σημαντικές. Ένα ακόμη ζήτημα που ενισχύει την ανάγκη για εφαρμογές IDS στις βιομηχανικές επικοινωνίες είναι ότι, **οι περισσότεροι τρόποι αυθεντικοποίησης και κρυπτογράφησης εισάγουν μη αποδεκτή επιβάρυνση στο δίκτυο**. Η πλειοψηφία των δεδομένων που μεταδίδονται σε αυτά τα περιβάλλοντα είναι κρίσιμα ως προς τον χρόνο, καθώς αφορούν σε μεγάλο βαθμό την ασφάλεια του φυσικού εξοπλισμού. Επίσης, η παρακολούθηση τους συστήματος σε πραγματικό χρόνο παίζει καθοριστικό ρόλο για την λήψη σωστών αποφάσεων στα συστήματα διαχείρισης της παραγόμενης ενέργειας. Συνεπώς, οι εφαρμογές πρόληψης που μελετήσαμε σε πειραματικό περιβάλλον ενδέχεται να δυσκολέψουν τις παραπάνω δραστηριότητες ή να μην είναι γενικότερα εφαρμόσιμες στις πραγματικές συνθήκες.

Τα πιο ειδικά συμπεράσματα της έρευνας οφείλουν να επικεντρωθούν περισσότερο στην ανάδειξη αποδοτικών και αποτελεσματικών μοντέλων ανίχνευσης κυβερνοεισβολών. Η προσέγγιση που θα πρέπει να ακολουθείται από τις IDS

εφαρμογές (στατιστική ή υπογραφών) εξαρτάται από διάφορους παράγοντες, όπως: (α.) τον όγκο των διαθέσιμων δεδομένων κίνησης δικτύου, (β.) τα εκάστοτε χαρακτηριστικά και την πολυπλοκότητα της επικοινωνίας, (γ.) την πρόβλεψη των χαρακτηριστικών και δοκιμή των πιθανών κυβερνοεπιθέσεων και (δ.) τις διάφορες αρχιτεκτονικές του δικτύου επικοινωνίας που μπορούν να προσομοιωθούν στα πλαίσια ενός εργαστηρίου. Οι πειραματικές διατάξεις στην διαθέσιμη βιβλιογραφία αφενός δεν ικανοποιεί πάντα και τα τρία αυτά κριτήρια και αφετέρου δεν ασχολείται σε βάθος με όλα τα πρωτόκολλα που επιλέξαμε (πχ. IEC 61850, ICCP). Παρ' όλα αυτά, μπορούμε να βγάλουμε ως ένα ασφαλές συμπέρασμα ότι, όποια μέθοδος και αν επιλεχθεί, η μέγιστη απόδοση του συστήματος ανίχνευσης κρίνεται από την λεπτομερή και εξατομικευμένη δουλεία είτε στους αλγορίθμους είτε στους κανόνες που αναπτύσσονται σε κάθε εφαρμογή. Σε κάθε περίπτωση, έχει μεγάλη σημασία η συνεχής συντήρηση του συστήματος ασφαλείας και η ενημέρωσή του σύμφωνα με τις αλλαγές που προκύπτουν τόσο στα χαρακτηριστικά της επικοινωνίας, όσο και στους νέους κινδύνους που εμφανίζονται.

1. Modbus TCP

Αρχικά, η ανάπτυξη κανόνων ανίχνευσης βασισμένες σε υπογραφές για εφαρμογές Modbus είναι ιδιαίτερα σημαντική και αποτελεί ένα καθοριστικό βήμα θωράκισης της επικοινωνίας. Η εκτενής παρουσίαση βασικών κανόνων (4.3.1) αφορά βασικά χαρακτηριστικά των πακέτων Modbus, με βάση τα οποία μπορούν να εντοπιστούν ανωμαλίες στην κίνηση του δικτύου. **Το Modbus προσφέρεται για ανάπτυξη IDS βασισμένων σε υπογραφές**, καθώς η δομή του είναι απλή και κατανοητή, συνεπώς μπορούν να προβλεφθούν και αναπτυχθούν αντίστοιχα απλοί κανόνες. Πλέον στο διαδίκτυο υπάρχει εκτενές υλικό για ανάπτυξη κανόνων με το εργαλείο Snort, από τις οποίες μπορούν να αντληθούν ιδέες για τον σχεδιασμό εξατομικευμένων IDS για την εκάστοτε Modbus εφαρμογή και τις πιθανές ανωμαλίες που μπορεί να παρουσιαστούν στην επικοινωνία.

Επιπρόσθετα, οι **δοκιμές στατιστικών μεθόδων IDS** (4.3.2) παρήγαγαν ικανοποιητικά αποτελέσματα για τις επιθέσεις SMOD. Τα κριτήρια ήταν η γενική ακρίβεια ανίχνευσης (accuracy), την ακρίβεια αληθών-θετικών ανιχνεύσεων (precision), το F1-score και την αναλογία αληθών-θετικών (TPR).Για τους δείκτες που παρατηρήθηκαν μεγάλες αποκλίσεις (Accuracy, F1) τα αποτελέσματα της αξιολόγησης δείχνουν ότι οι μέθοδοι Adaboost και Random Forest παρουσιάζουν την μεγαλύτερη αποτελεσματικότητα όσον αφορά την ακρίβεια και το τελικό score ανίχνευσης DoS επιθέσεων. Παρ' όλα αυτά ορισμένοι δείκτες παραμένουν χαμηλοί ακόμα και στους αποδοτικότερους αλγορίθμους, όπως για παράδειγμα οι θετικές ενδείξεις σφάλματος σε σχέση το σύνολο των πραγματικών σφαλμάτων (TPR). Εδώ χρειάζεται οπωσδήποτε, μια πιο λεπτομερής δουλειά και ενσωμάτωση ακόμη περισσότερων ιστορικών δεδομένων ώστε να αυξηθεί η αποτελεσματικότητα του IDS.

Αλγόριθμοι	Accuracy	Precision	TPR	F1
Random Forest	0.811	0.964	0.647	0.774
AdaBoost	0.812	0.964	0.647	0.775

Για τις επιθέσεις υπερχείλισης (βλ. 3.2.4 & 4.3.3) εφαρμόστηκαν και οι δύο μέθοδοι ανίχνευσης εισβολών, οι οποίες ανίχνευσαν σωστά τις πλαστές κινήσεις πακέτων (μεταξύ των δευτερολέπτων 60-120). Το κοινό χαρακτηριστικό των μεθόδων είναι ότι χρησιμοποιούν ως «κανόνα» ένα όριο τιμών (κατώφλι), ως το

επιτρεπτό διάστημα τιμών για τις παρατηρούμενες παραμέτρους. Παρ' όλα αυτά, οι δύο παραπάνω τρόποι διαφέρουν και έχουν αντίστοιχα πλεονεκτήματα και μειονεκτήματά. Ενώ η ανίχνευση βάσει υπογραφής απαιτεί ένα σταθερό επιτρεπτό όριο που πρέπει να καθοριστεί εμπειρικά, ο αλγόριθμος ανίχνευσης αλλαγών EWMA χρησιμοποιεί ένα μεταβλητό κατώφλι που προσαρμόζεται αλγοριθμικά, ανάλογα με το χρόνο παρατήρησης. **Συγκριτικά**, καταλαβαίνουμε ότι ανάλογα με την περίπτωση στατιστικές τεχνικές ανίχνευσης μπορούν να είναι το ίδιο αποδοτικές με τα συστήματα βάσει υπογραφών. Ωστόσο για ένα πραγματικό περιβάλλον, το Snort θα είναι πολύ πιο εύκολο στην ανάπτυξή του συγκριτικά με την τεχνική κινούμενου μέσου όρου, καθώς το Snort παρέχει ήδη προεπεξεργαστή Modbus που μπορεί άμεσα να χρησιμοποιηθεί για σκοπούς ανίχνευσης επιθέσεων στο πρωτόκολλο αυτής της ενότητας. Σε κάθε περίπτωση, και οι δύο τεχνικές επιδέχονται συνεχής βελτίωση και επικαιροποίηση, ενώ η επιλογή τους κάθε φορά θα εξαρτηθεί από το σενάριο.

2. DNP3

Λόγω των πεδίων εφαρμογής του DNP3, θα πρέπει αρχικά να πούμε ότι, αρκετές συσκευές SCADA έχουν πολύ χαμηλή απόδοση, επομένως όποια μέθοδος προστασίας εφαρμοστεί πρέπει να έχει όσο το δυνατόν χαμηλό βαθμό επιβάρυνσης (overhead). Βάσει αυτού θα πρέπει να εξάγουμε κάποια συμπεράσματα σχετικά με τις επεκτάσεις κρυπτογράφησης του DNP3 που προτάθηκαν στην εργασία. Για παράδειγμα, για το DNPSec που απαιτεί κρυπτογράφηση στο επίπεδο σύνδεσης-δεδομένων δεν υπάρχει τρόπος να μειωθεί η επιβάρυνση του δικτύου. Αντίθετα, οι άλλες δύο επεκτάσεις φαίνεται να έχουν σχετικά μικρότερη επιβάρυνση στο δίκτυο καθώς οι προληπτικοί μηχανισμοί ασφαλείας προστίθενται στο επίπεδο εφαρμογής.

Οι μηχανισμοί αυτοί εφαρμόστηκαν απέναντι σε επιτιθέμενους που προσπάθησαν να καταγράψουν και να τροποποιήσουν αυθεντικά πακέτα. Η αξιολόγηση που προκύπτει (4.3.3) ανέδειξε τα παρακάτω αποτελέσματα.

	DNPSec	DNP3 – SA	DNP3 - AE
Εμπιστευτικότητα	ΝΑΙ	ΟΧΙ	ΝΑΙ
Ακεραιότητα	ΝΑΙ	ΝΑΙ	ΝΑΙ
Αυθεντικότητα	ΝΑΙ	ΝΑΙ	ΝΑΙ
Επίπεδο Κρυπτογράφησης	Σύνδεσης –Δεδομένων	Εφαρμογής	Εφαρμογής
Overhead	Υψηλό	Μεσαίο	Μεσαίο

Συμπεράσματα: Η παραπάνω αξιολόγηση υποδεικνύει ότι, το DNP3Sec δεν αποτελεί την βέλτιστη τεχνική ασφάλειας καθώς η ενσωμάτωσή του επιφέρει μεγάλη επιβάρυνση στο υπάρχον δίκτυο. Αυτό μπορεί να δημιουργήσει καθυστερήσεις ακόμη και σε απλές εφαρμογές. Από την άλλη, το λιγότερο απαιτητικό DNP3 – SA εξασφαλίζει σε μεγάλο βαθμό την ακεραιότητα και την αυθεντικότητα, ωστόσο δεν υπάρχει εγγύηση για την εμπιστευτικότητα των δεδομένων εφαρμογής. Για τον λόγο αυτό, η τεχνική DNP3 - AE μοιάζει πιο ενδεδειγμένη, καθώς συνδυάζει λειτουργίες κρυπτογράφησης - αυθεντικοποίησης για μικρότερη επιβάρυνση στο δίκτυο. Οι προσομοιώσεις επιθέσεων έδειξαν ότι η προσέγγισή αυτή μπορεί να βελτιώσει την ασφάλεια του DNP3 καλύτερα από τις άλλες πρακτικές ασφάλειας. Ωστόσο, υπάρχουν ακόμα πολλές βελτιώσεις που πρέπει να διερευνηθούν περαιτέρω.

- Χρειάζεται να μειωθεί σημαντικά το overhead της κρυπτογράφησης και αποκρυπτογράφησης (τώρα είναι 24-yte για κάθε μήνυμα).
- Οι δοκιμές χρειάζεται να υλοποιηθούν σε ένα πειραματικό περιβάλλον SCADA, μεγαλύτερου μεγέθους, ώστε να εξάγουμε πιο ακριβή συμπεράσματα.

Για τα ζητήματα που προκύπτουν στους συλλέκτες δεδομένων μετά από πολλαπλή ρίψη πλαστών πακέτων-DNP3, **προτάθηκαν διάφοροι μέθοδοι πρόληψης**. Αυτές περιλαμβάνουν τις παραπάνω επεκτάσεις, οι οποίες όμως ναι μεν προσφέρουν υπηρεσίες που ενισχύουν σημαντικά την εμπιστευτικότητα της επικοινωνίας ωστόσο, η επιβάρυνσή τους δεν υποστηρίζεται σε πιο απαιτητική παρόμοια εφαρμογή. Άλλες προτάσεις περιλαμβάνουν μια καλύτερη αναδιοργάνωση της μνήμης των συσκευών μια αποδοτικότερη πολιτική προγραμματισμού. Μια τέτοια τεχνική βοηθά στην αποφυγή καταστάσεων υπερχείλισης ωστόσο σε καμιά περίπτωση δεν συμβάλλει στην ανίχνευση των κυβερνοεπιθέσεων. Για τους παραπάνω λόγους **κρίνεται σημαντική η εφαρμογή συστημάτων IDS** είτε βάσει στατιστικών μεθόδων, είτε με την ανάπτυξη κανόνων στην επικοινωνία. Για παράδειγμα, σε μια φυσιολογική επικοινωνία δεν θα έπρεπε να προκύπτουν συχνές καταστάσεις υπερχείλισης. Ένας κανόνας που θα ειδοποιεί το σύστημα ελέγχου ότι ανίχνευση συνεχόμενες (πχ. 3 φορές) υπερχειλίσεις στους buffer των συλλεκτών δεδομένων θα ήταν μια πιο ασφαλής μέθοδος για την αντιμετώπιση του προβλήματος. Άλλες στατιστικές τεχνικές που ανιχνεύουν καθυστερήσεις στις ανταλλαγή πακέτων συσκευής-κέντρου ελέγχου επίσης θα έδειχναν μια πιο σαφή εικόνα για την κατάσταση του συστήματος επικοινωνίας.

3. IEC/104

Για τα πρωτόκολλα της IEC παρουσιάστηκαν βελτιωτικά πρότυπα που ενισχύουν την ασφάλεια όπως το IEC 62351-5. Ωστόσο, οι σημαντικές τους ελλείψεις και τα προβλήματα που ενδέχεται να εμφανιστούν στην ομαλή επικοινωνία (βλ. αξιολόγηση στην 4.5.1), είναι ο λόγος για τον οποίο το πρότυπο δεν μπορεί να θεωρηθεί προστατευμένο.

Οι μέθοδοι IDS που αναλύθηκαν, για επικοινωνίες IEC/104, είναι οι εξής:

- **IDS με αλγορίθμους μηχανικής μάθησης**

Στο σχήμα 4.6 παρουσιάστηκε η αποτελεσματικότητα των αλγορίθμων που εφαρμόστηκαν πειραματικά, υπό τις διάφορες τιμές χρονικού ορίου ροής. Τα κριτήρια ήταν η γενική ακρίβεια ανίχνευσης (accuracy), την ακρίβεια αληθών-θετικών ανιχνεύσεων (precision), το F1-score και την αναλογία αληθών-θετικών (TPR). Σύμφωνα με τα αποτελέσματα της δοκιμής, όταν η τιμή χρονικού ορίου ροής είναι ίση με 120 δευτερόλεπτα, ο αλγόριθμος **Isolation Forest**, **επιτυγχάνει τα υψηλότερα αποτελέσματα σε όλους τους δείκτες αξιολόγησης**.

Αλγόριθμος	Accuracy	Precision	TPR	F1
Isolation Forest	0.982	0.99	0.777	0.875

- **IDS βάσει υπογραφών ASDU**.

Η έκβαση του πειράματος (4.5.3) ανέδειξε ένα αποτελεσματικό μοντέλο ανίχνευσης με **μηδενικά ψευδώς-θετικά αποτελέσματα** για τους δοσμένους και προκαθορισμένους κανόνες. Παρά το μικρό δείγμα κανόνων που αναπτύχθηκαν, το μοντέλο που παρουσιάστηκε μπορεί να γίνει πολύ αποδοτικό με την ανάπτυξη και

ενσωμάτωση μιας μεγάλης λίστας ανωμαλιών που θα προκύπτουν από περιπτώσεις παραβιάσεων της προδιαγραφής IEC/104.

4. IEC 61850

Αρχικά αξιολογώντας τις προτεινόμενες επεκτάσεις IEC 62351-6 (4.6.1), μπορούμε να θεωρήσουμε ότι διασφαλίζουν κάποια σημαντικά ζητήματα πρόληψης, όπως την προστασία κατά την επανάληψη των μηνυμάτων αλλά και την ικανοποιητική ακεραιότητά τους. Ειδικότερα, για τα GOOSE και SMV, το επεκτεινόμενο PDU με την αντίστοιχη υπογραφή του εξασφαλίζει σε έναν μικρό βαθμό την αυθεντικότητα και την ακεραιότητα. Ωστόσο, οποιαδήποτε εισαγωγή κρυπτογραφικών μηχανισμών είναι δύσκολη καθώς δεν προβλέπονται χρονικές παραχωρήσεις για κινήσεις που απαιτούν μικρό χρόνο απόκρισης. Η χρήση υπογραφών RSA, που προτείνονται, για την παροχή αυθεντικότητας των επεκτεινόμενων PDU, είναι εξαιρετικά ακατάλληλη για εφαρμογές χρόνου απόκρισης 4ms, καθώς οι υπογραφές αυτές διαθέτουν μεγάλη απαίτηση υπολογιστικής ισχύος. Από την άλλη πλευρά, ένα HMAC, μπορεί να υλοποιηθεί καλύτερα, απαιτώντας μόνο περίπου 10μs για τη δημιουργία ενός τυπικού αυθεντικοποιημένου πακέτου IP. Σε κάθε περίπτωση το πρότυπο IEC 62351 δεν μπορεί να διασφαλίσει πλήρως την εμπιστευτικότητα, τη διαθεσιμότητας και την ακεραιότητα της επικοινωνίας.

Εκτός του παραπάνω προτύπου, προτείνονται κάποιοι ακόμα μηχανισμοί κρυπτογράφησης των GOOSE. Αυτοί χρησιμοποιούν αποδοτικούς αλγορίθμους EtM, E&M και MtE για να κρυπτογραφήσουν τα δεδομένα των μηνυμάτων ωστόσο οι επιβαρύνσεις τους στο δίκτυο είναι αρκετά οριακές ως προς την χρονική απαίτηση. Συνεπώς, η ανάπτυξη IDS (που θα δούμε παρακάτω) είναι αναγκαία στρατηγική για την προστασία μιας ηλεκτρικής υποδομής που μεταδίδει κρίσιμα δεδομένα με πρωτόκολλο IEC 61850.

Η πιο ενδιαφέρουσα μέθοδος IDS που εντοπίστηκε, αξιοποιεί την βάση δεδομένων για γεγονότα GOOSE και χρησιμοποιεί **μηχανική μάθηση για να αποφασίσει εάν κάθε νέο γεγονός είναι ύποπτο**, παράγοντας ειδοποιήσεις. Σε αυτό το πείραμα εισάγουμε δύο νέα κριτήρια αξιολόγησης που αφορούν δύο απαραίτητους χρονικούς δείκτες. Εκείνος που επιλέχθηκε ως βέλτιστη λύση, ήταν το Δέντρο Απόφασης.

Μοντέλο ταξινόμησης	Accuracy	Detection Rate	False Alarm Rate	Εκπαίδευση (seconds)	Εκτέλεση (seconds)
DT	0.9448	0.9231	0.0408	1.36	0.0009

Σχόλια: Στο Σχήμα 4.15 παρατηρείται ότι κατά κύριο λόγο και οι πέντε προτεινόμενοι αλγόριθμοι έχουν υψηλό δείκτη ακρίβειας. Θα περιμέναμε ωστόσο ότι ο Adaboost θα είχε καλύτερα αποτελέσματα καθώς σχεδιάστηκε για να βελτιώσει την απόδοση των σημείων απόφασης. Θεωρητικά, σε ένα σύστημα με πολύ περισσότερες εισόδους και αλληλεξαρτώμενες μεταβλητές, το Adaboost μπορεί να προσφέρει υψηλότερες αποδόσεις. Τα ποσοστά εντοπισμού είναι επίσης ικανοποιητικά, ιδιαίτερα για τους DT και k-NN οι οποίοι εντοπίζουν εισβολές με ρυθμό 92.31%. Παρ' όλα αυτά, οι ίδιοι δύο αλγόριθμοι έχουν πολύ υψηλά ποσοστά λανθασμένων ειδοποιήσεων, τα οποία μειώνουν τη συνολική ακρίβεια των αλγόριθμων. Ο μικρότερος ρυθμός εσφαλμένων εντοπισμών αναφέρεται στο Adaboost, το οποίο φαίνεται να έχει την καλύτερη ισορροπία ακρίβειας (ρυθμός

εσφαλμένων ειδοποιήσεων προς τα ποσοστά εντοπισμού). Το πιο σημαντικό κομμάτι των αποτελεσμάτων των δοκιμών είναι οι εξής χρονικές παράμετροι:

(i) Ο χρόνος που απαιτείται για την εκπαίδευση του συστήματος,
(ii) Ο χρόνος που απαιτείται για την εκτέλεση του αλγορίθμου και τον εντοπισμό μιας επίθεσης και
(iii) Ο συνολικός χρόνος που απαιτείται για εκπαίδευση και δοκιμή.

Οι χρόνοι εκπαίδευσης και δοκιμής είναι εντελώς διακριτοί και σχετίζονται με διαφορετικά στάδια της λειτουργίας των αλγορίθμων. Για την ορθή αξιολόγηση πρέπει να σημειωθεί ότι η εκπαίδευση μπορεί να πραγματοποιηθεί εκτός σύνδεσης ή πριν από την ανάπτυξη του συστήματος. Συνεπώς, δεν έχει άμεση επίδραση στη λειτουργία του συστήματος όταν λαμβάνονται μηνύματα GOOSE σε πραγματικό χρόνο. Από την άλλη πλευρά, ο χρόνος ανίχνευσης επιθέσεων αφορά την λειτουργία του προτεινόμενου συστήματος σε πραγματικό χρόνο και αντιπροσωπεύει το χρόνο που απαιτείται για το σύστημα, να επεξεργαστεί ένα εισερχόμενο μήνυμα GOOSE και να αποφασίσει εάν πρόκειται για κανονικό μήνυμα ή όχι. Τέλος, λαμβάνοντας υπόψη ότι το πρότυπο IEC 61850 καθορίζει ότι τα μηνύματα GOOSE πρέπει να παραδίδονται εντός 3ms, αυτός ο επιπρόσθετος χρόνος που εισάγεται από τον εκάστοτε αλγόριθμο είναι καθοριστικός για τα επίπεδα απόδοσής του.

Αναλύοντας τα χρονικά δεδομένα του πίνακα αποτελεσμάτων παρατηρείται ότι το DT μπορεί να χρησιμοποιηθεί με ασφάλεια για την ανίχνευση διείσδυσης σε ένα σύστημα που λειτουργεί με μηνύματα GOOSE. Ο χρόνος δοκιμής που απαιτείται για αυτόν τον αλγόριθμο είναι λιγότερος από 1msec και είναι εφικτός για την εκπλήρωση των απαιτήσεων του IEC 61850. Αντίθετα, οι αλγόριθμοι Adaboost, RF και SVM απαιτούν πολύ μεγαλύτερους χρόνους επεξεργασίας και αυτό τους καθιστά ανεφάρμοστους για συστήματα επικοινωνίας που βασίζονται σε GOOSE. Αυτοί οι αλγόριθμοι ναι μεν θεωρούνται πολύ ανθεκτικοί και ακριβείς για πολύπλοκα συστήματα, ωστόσο η επεξεργασία δεδομένων για το συγκεκριμένο σύστημα επικοινωνίας απαιτεί χρονική ακρίβεια. Επίσης, ο αλγόριθμος k-NN μπορεί να χρησιμοποιηθεί σε ένα πολύ γρήγορο σύστημα εάν τα μηνύματα GOOSE φτάνουν εντός 1ms, αφού η δοκιμή διαρκεί περίπου 2ms. Τελικά και σύμφωνα με τα παραπάνω συμπεράσματα, ο πιο αποδοτικός αλγόριθμος μηχανικής μάθησης είναι τα δέντρα αποφάσεων.

5.3. Σύνοψη και προτάσεις για περαιτέρω έρευνα

Τα γενικά συμπεράσματα που μπορούμε να εξάγουμε από την ερευνητική εργασία είναι τα ακόλουθα:

1. Τα βιομηχανικά πρωτόκολλα που μελετήθηκαν δεν παρέχουν ικανοποιητικά επίπεδα προστασίας για την επικοινωνία.
2. Οι επεκτάσεις πρόληψης και ασφάλειας που εκδοθεί για διάφορα πρωτόκολλα δεν εξασφαλίζουν την αποτελεσματική αντιμετώπιση σοβαρών κυβερνοεπιθέσεων.
3. Οι μηχανισμοί κρυπτογράφησης και αυθεντικοποίησης μπορούν να ενισχύσουν σε έναν βαθμό την ασφάλεια της επικοινωνίας. Ωστόσο δεν μπορούν να επιλεχθούν σε εφαρμογές με αυστηρές χρονικές απαιτήσεις στην ανταλλαγή δεδομένων.
4. Η ανάπτυξη Συστημάτων Ανίχνευσης Εισβολών είναι η πλέον ενδεδειγμένη πρακτική για την αποτελεσματική προστασία της επικοινωνίας.
5. Τα IDS που βασίζονται σε στατιστικά δεδομένα μπορούν θεωρηθούν αποδοτικά όταν είναι διαθέσιμα αρκετά ιστορικά δεδομένα της κίνησης των πακέτων. Επίσης

απαιτούν πειραματικές δοκιμές, σημαντικό χρόνο και εξειδικευμένο δυναμικό, ώστε να βρεθούν αλγόριθμοι με μικρό δείκτη φευδών-θετικών ειδοποιήσεων.

6. Τα IDS που βασίζονται στους κανόνες λειτουργίας των πακέτων και σε υπογραφές επιθέσεων είναι περισσότερο ενδεδειγμένα όταν υπάρχει βαθιά γνώση του πρωτοκόλλου και των πιθανών κινδύνων. Εάν αυτές οι προϋποθέσεις καλύπτονται, τότε αυτή η μέθοδος μπορεί να παράγει ελάχιστες ψευδείς ειδοποιήσεις. Επιπλέον, τα διαθέσιμα εργαλεία ανάπτυξης τέτοιων συστημάτων δίνουν επιπλέον δυνατότητες απόρριψης της κακόβουλης κίνησης.
7. Υπάρχει μεγάλο πειραματικό κενό για τα ζητήματα κυβερνοασφάλειας ορισμένων πρωτοκόλλων, με χαρακτηριστικό παράδειγμα το ICCP, το οποίο πρέπει να καλυφθεί από μελλοντικές έρευνες.

Σύμφωνα με τα παραπάνω οι μελλοντικές ερευνητικές προσπάθειες για το ζήτημα της κυβερνοασφάλειας στα δίκτυα ηλεκτρικής ενέργειας πρέπει να κινηθούν στους εξής άξονες:

1. Ανάδειξη της σημασίας της κυβερνοασφάλειας, ως έναν κρίσιμο ερευνητικό τομέα για τα ηλεκτρικά συστήματα του μέλλοντος.
2. Συντονισμένες μελέτες πάνω στα υπάρχοντα κυβερνοφυσικά συστήματα γύρω από τα ζητήματα της κυβερνοασφάλειας. Βασικός στόχος των μελετών αυτών θα πρέπει να είναι η αναβάθμιση της ασφαλείας σε κρίσιμες ενεργειακές υποδομές που δεν προστατεύονται επαρκώς από κυβερνοαπειλές.
3. Μεγαλύτερο βάθος στην έρευνα για την ανάπτυξη μεθόδων ανίχνευσης κυβερνοεισβολών για δίκτυα ευρείας περιοχής - WAN και πρωτόκολλα επικοινωνίας που διανύουν μεγάλες αποστάσεις, όπως το ICCP.
4. Ανάπτυξη αποτελεσματικών μεθόδων ανίχνευσης βάσει υπογραφών κίνησης του δικτύου για τα μηνύματα που περιλαμβάνει το πρότυπο IEC 61850 (πχ. GOOSE, SMV, κλπ.).
5. Διεξαγωγή πειραματικών δοκιμών κυβερνοεπιθέσεων σε μεγάλη κλίμακα για την ανάπτυξη και αξιολόγηση νέων τεχνικών ανίχνευσης και καταπολέμησης εισβολών. Μια προτεινόμενη στρατηγική που θα συνδυάζει τόσο τα IDS βασισμένα σε υπογραφές, όσο και στατιστικές τεχνικές, θα μπορούσε να δημιουργήσει νέα και αποτελεσματικότερα συστήματα ανίχνευσης.

Βιβλιογραφία

[1] Siddharth Sridhar, Adam Hahn and Manimaran Govindarasu, Cyber–Physical System Security for the Electric Power Grid.

[2] Liwei Cao, Xiaoning Jiang, Yumei Zhao, Shouguang Wang, Dan You and Xianli Xu, A Survey of Network Attacks on Cyber-Physical Systems, @March 2020.

[3] Pavlakis Nikolaos, Papoulidis Georgios and Exadaxtylos Pantelis, SCADA Systems.

[4] White Paper: Cybersecurity for Telecontrol, Version 06/2020, siemens.com/telecontrol.

[5] Cybersecurity for Industry Operational Guidelines, Version 2.2, © Siemens 2022.

[6] Xi Fang, Student Member, Satyajayant Misra, Guoliang Xue and Dejun Yang, Smart Grid – The New and Improved Power Grid: A Survey.

[7] Ruofei Ma, Hsiao-Hwa Chen, Yu-Ren Huang and Weixiao Meng, Smart Grid Communication: Its Challenges and Opportunities.

[8] Maria Lorena Tuballa and Michael Lochinvar Abundo, A review of the development of Smart Grid technologies, ©2016 Elsevier Ltd.

[9] Dileep G., A survey on smart grid technologies and applications, ©2019 Elsevier Ltd.

[10] Peeyush Jain and Paritosh Tripathi, SCADA security: a review and enhancement for DNP3 based systems, ©CSI Publications 2013.

[11] Samuel East, Jonathan Butts, Mauricio Papa and Sujeet Shenoi, A Taxonomy of Attacks on the DNP3 Protocol, ©IFIP International Federation for Information Processing 2009.

[12] Matthew Franz, ICCP Exposed: Assessing the Attack Surface of the "Utility Stack", Digital Bond Inc.

[13] M.J. Rice, G.K. Dayley, C.A. Bonebrake and L.J. Becker, Secure ICCP: Final Report, Pacific Northwest National Laboratory Richland, Washington.

[14] K. Jagan Mohan, Lagineni Mahendra, R.K. Senthil Kumar and B.S.Bindhumadhava, Self Healing ICCP.

[15] S. Mohagheghi, J. Stoupis and Z. Wang, Communication Protocols and Networks for Power Systems - Current Status and Future Trends, Conference Paper @August 2009.

[16] Petr Ilgner, Petr Cika and Martin Stusek, SCADA-Based Message Generator for Multi-Vendor Smart Grids: Distributed Integration and Verification of TASE.2, © 2021 by the authors.

[17] J.T. Robinson, T. Saxton, A. Vojdani, D. Ambrose, G. Schimmel, R.R. Blaesing, R. Larson, Development of the Intercontrol Center Communications Protocol (ICCP), ©1995 IEEE.

[18] Yichi Zhang, Yingmeng Xiang and Lingfeng Wang, Power System Reliability Assessment Incorporating Cyber Attacks Against Wind Farm Energy Management Systems, ©2016 IEEE.

[19] John T. Michalski, Andrew Lanzone, Jason Trent, and Sammy Smith, Secure ICCP Integration Considerations and Recommendations.

[20] Petr Matoušek, Description and analysis of IEC 104 Protocol: Technical Report ©2017, Brno University of Technology.

[21] Peter Maynard and Kieran McLaughlin, Towards Understanding Man-In-The-Middle Attacks on IEC 60870-5-104 SCADA Networks, ©Maynard et al. Published by BCS, Proceedings of the 2nd International Symposium for ICS & SCADA Cyber Security Research 2014.

[22] Qais Saif Qassim, Norziana Jamil, Maslina Daud, Norhamadi Ja'affar, Salman Yussof, Wan Azlan Wan Kamarulzaman and Roslan Ismail, Simulating command injection attacks on IEC 60870-5-104 protocol in SCADA system, © 2018 Qais Saif Qassim et al.

[23] Kelvin Mai, Xi Qin, Alvaro A. Cardenas and Neil Ortiz Silva, IEC 60870-5-104 Network Characterization of a Large-Scale Operational Power Grid, @May 2019.

[24] Y. Yang, K. McLaughlin, T. Littler, S. Sezer, B. Pranggono and H. F. Wang, Intrusion Detection System for IEC 60870-5-104 Based SCADA Networks, ©2013 IEEE.

[25] F. M. Cleveland, IEC 61850-7-420 Communications Standard for Distributed Energy Resources ©2008 IEEE.

[26] I. Xyngi and M. Popov, IEC61850 Overview - Where Protection Meets Communication, @ May 2010.

[27] S. M. Suhail Hussain, Taha Selim Ustun, and Akhtar Kalam, A Review of IEC 62351 Security Mechanisms for IEC 61850 Message Exchanges.

[28] R. E. Mackiewicz, Overview of IEC 61850 and Benefits, ©2006 IEEE.

[29] Mohd. Asim Aftab, S.M. Suhail Hussainb, Ikbal Alic and Taha Selim Ustunb, EC 61850 based substation automation system: A survey, ©2020 Elsevier Ltd.

[30] Christoph Brunner, IEC 61850 for Power System Communication Switzerland.

[31] Yingyi Liang and Roy H. Campbell, Understanding and Simulating the IEC 61850 Standard, ©NSF CNS 03-05537.

[32] Sajal Bhatia, Nishchal Kush, Chris Djamaludin, James Akande and Ernest Foo, Practical Modbus Flooding Attack and Detection ©2014 Australian Computer Society.

[33] Niv Goldenberg and Avishai Wool, Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems, ©2013 Elsevier B.V.

[34] MODBUS MESSAGING ON TCP/IP IMPLEMENTATION GUIDE, Modbus Organization.

[35] Santiago Figueroa-Lorenzo, Javier Añorga and Saioa Arrizabalaga, A Role-Based Access Control Model in Modbus SCADA Systems. A Centralized Model Approach, @October 2019.

[36] Dong Jin, David M. Nicol and Guanhua Yan, An event buffer flooding attack in DNP3 controlled SCADA systems, @2011 Winter Simulation Conference.

[37] Dongsoo Lee, HakJu Kim, Kwangjo Kim and Paul D. Yoo, Simulated Attack on DNP3 Protocol in SCADA System, ©2014 The Institute of Electronics, Information and Communication Engineers.

[38] Péter György and Tamás Holczer, Attacking IEC 60870-5-104 Protocol, ©2021 by its authors.

[39] G. Dondossola , F. Garrone and J. Szanto, Cyber Risk Assessment of Power Control Systems – A Metrics weighed by Attack Experiments, ©2011 IEEE.

[40] Panagiotis Radoglou-Grammatikis, Panagiotis Sarigiannidis and Ioannis Giannoulakis, Emmanouil Kafetzakis and Emmanouil Panaousis, Attacking IEC-60870-5-104 SCADA Systems.

[41] Suleman Ashraf, Mohammad H. Shawon, Haris M. Khalid and S. M. Muyeen, Denial-of-Service Attack on IEC 61850-Based Substation Automation System: A Crucial Cyber Threat towards Smart Substation Pathways, ©2021 by the authors.

[42] Ahmed Elgargouri and Mohammed Elmusrati, Analysis of Cyber-Attacks on IEC 61850 Networks, @September 2017 Conference Paper.

[43] BooJoong Kang, Peter Maynard, Kieran McLaughlin, Sakir Sezer, ilip Andrén, Christian Seitl, Friederich Kupzog and Thomas Strasser, Investigating Cyber-Physical Attacks against IEC 61850 Photovoltaic Inverter Installations, ©2015 IEEE.

[44] Bo Chen, Nishant Pattanaik, Ana Goulart, Karen L. Butler-Purry and Deepa Kundur, Implementing Attacks for Modbus/TCP Protocol in a Real-Time Cyber Physical System Test Bed, ©2015 IEEE.

[45] Panagiotis Radoglou-Grammatikis, Ilias Siniosoglou, Thanasis Liatifis, Anastasios Kourouniadis, Konstantinos Rompolos and Panagiotis Sarigiannidis, Implementation and Detection of Modbus Cyberattacks, @Department of Electrical and Computer Engineering, University of Western Macedonia, Kozani

[46] Christopher Parian, Terry Guldimann and Sajal Bhatia, Fooling the Master: Exploiting Weaknesses in the Modbus Protocol, ©2021 by the authors.

[47] Peter Huitsing, Rodrigo Chandia, Mauricio Papa and Sujeet Shenoi, Attack taxonomies for the Modbus protocols, ©2008 Elsevier B.V.

[48] Tafseer Akhtar and B.B. Gupta, Analysing smart power grid against different cyber attacks on SCADA system, ©2021 Inderscience Enterprises Ltd.

[49] Bonnie Zhu, Anthony Joseph and Shankar Sastry, A Taxonomy of Cyber Attacks on SCADA Systems, ©2011 IEEE.

[50] Sean Whalen, Matt Bishop and Sophie Engle, Protocol Vulnerability Analysis, @May 2005.

[51] Adam Hahn, Aditya Ashok, Siddharth Sridhar, and Manimaran Govindarasu, Cyber-Physical Security Testbeds: Architecture, Application, and Evaluation for Smart Grid, ©2013 IEEE.

[52] Nattawat Khamphakdee, Nunnapus Benjamas and Saiyan Saiyod, Improving Intrusion Detection System Based on Snort Rules for Network Probe Attack Detection, ©2014 IEEE.

[53] Roman Schlegel, Sebastian Obermeier and Johannes Schneider, Assessing the Security of IEC 62351, ©Schlegel et al. Published by BCS Learning & Development Ltd. Proceedings of the 3rd International Symposium for ICS & SCADA Cyber Security Research 2015.

[54] Haining Wang, Dandle Zhang and Kang G. Shin, Detecting SYN Flooding Attacks.

[55] Roman Schlegel, Sebastian Obermeier and Johannes Schneider, A security evaluation of IEC 62351, ©2016 Elsevier Ltd.

[56] Ihab Darwish, Obinna Igbe and Tarek Saadawi, Experimental and theoretical modeling of DNP3 attacks in smart grids, @September 2015.

[57] Irfan A. Siddavatam and Faruk Kazi, Security Assessment Framework for Cyber Physical Systems: A Case-study of DNP3 Protocol, ©2015 IEEE.

[58] Todd Mander, Farhad Nabhani, Richard Cheung and Lin Wang, Data Object Based Security for DNP3 Over TCP/IP for Increased Utility Commercial Aspects Security, ©2007 IEEE.

[59] Junho Hong, Shinn-Shyan Wu, Alexandru Stefanov, Ahmed Fshosha, Chen-Ching Liu, Pavel Gladyshev and Manimaran Govindarasu, An Intrusion and Defense Testbed in a Cyber-Power System Environment, ©2011 IEEE.

[60] MichaelEgger, GüntherEibl and Dominik Enge, Comparison of approaches for intrusion detection ins ubstations using the IEC 60870-5-104protocol, ©2020 by the authors.

[61] Panagiotis Radoglou Grammatikis, Panagiotis Sarigiannidis, Antonios Sarigiannidis, Apostolos Tsiakalos and Georgios Efstathopoulos, An Anomaly Detection Mechanism for IEC 60870-5-104, @European Unions Horizon 2020 research.

[62] Reshma Tawde and Ashwin Nivangune, Cyber Security in Smart Grid SCADA Automation, copyright by the authors.

[63] S. M. Suhail Hussain, Shaik Mullapathi Farooq, and Taha Selim Ustun, A Method for Achieving Confidentiality and Integrity in IEC 61850 GOOSE Messages, @with Fukushima Renewable Energy Institute, AIST (FREA), Koriyama.

[64] Thomas H. Morris, Bryan A. Jones, Rayford B. Vaughn and Yoginder S. Dandass, Deterministic Intrusion Detection Rules for MODBUS Protocols, ©2012 IEEE.

[65] Steven Cheung, Bruno Dutertre, Martin Fong, Ulf Lindqvist, Keith Skinner and Alfonso Valdes, Using Model-based Intrusion Detection for SCADA Networks, Institute for Information Infrastructure Protection (I3P) research program.

[66] Ivo Frazao, Pedro Henriques Abreu, Tiago Cruz, Helder Araujo and Paulo Simoes, Denial of Service Attacks: Detecting the Frailties of Machine Learning Algorithms in the Classification Process, ©Springer Nature Switzerland AG 2019.

[67] Panagiotis I. Radoglou - Grammatikis and Panagiotis G. Saragiannidis, Securing the Smart Grid: A Comprehensive Compilation of Intrusion Detection and Prevention Systems, ©2019 IEEE.

[68] S. Sridhar and G. Manimaran, Data integrity attacks and their impacts on SCADA control system, in Proc. Power Energy Soc. General Meeting, Jul. 2010

[69] Morris, T. H. and Gao, W. (2013) Industrial control system cyber attacks. In: First International Symposium for ICs & SCADA Cyber Security Research 2013. Leicester, U.K.

[70] U. Premaratne, J. Samarabandu, T.S. Sidhu, R. Beresh and J. Tan, An Intrusion Detection System for IEC61850 Automated Substations. IEEE Trans. Power Deliv. 2010.

[71] K. Choi, X. Chen, S. Li, M. Kim, K. Chae and J. Na, Intrusion Detection of NSM Based DoS Attacks Using Data Mining in Smart Grid. Energies 2012.

[72] T. S. Ustun, S. M. S. Hussain, A. Ulutas, A. Onen, M. Roomi and D. Mashima, Machine Learning-Based Intrusion Detection for Achieving Cybersecurity in Smart Grids Using IEC 61850 GOOSE Messages. Symmetry, 2021.