ΕΛΛΗΝΙΚΟ ΜΕΣΟΓΕΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Πρόγραμμα Σπουδών Ηλεκτρολόγων Μηχανικών Τ.Ε.

Πτυχιακή Εργασία

Μελέτη και διερεύνηση των εφαρμογών εποπτικού ελέγχου και συλλογής δεδομένων (SCADA) σε συνδυασμό με τα PLC

ΘΕΟΔΩΡΟΣ ΛΙΘΟΞΟΠΟΥΛΟΣ

Α.Μ.: TH5980

Επιβλέπων: **Κυριάκος Μουράτης**

Ηράκλειο Κρήτης, Οκτώβριος 2023

HELLENIC MEDITERRANEAN UNIVERSITY

School of Engineering

Department of Electrical and Computer Engineering

Undergraduate Program of Electrical Engineering T.E.

Bachelor Thesis

Study and investigation of supervisory control and data acquisition (SCADA) applications in combination with PLCs

THEODOROS LITHOXOPOULOS

A.M.: TH5980

Supervisor: **Kyriakos Mouratis**

Heraklion Crete, October 2023

Ευχαριστίες

Η πτυχιακή εργασία αυτή αποτελεί το τελευταίο κομμάτι των αρμοδιοτήτων μου ως φοιτητής στο τμήμα Ηλεκτρολόγων Μηχανικών του ΤΕΙ Κρήτης. Με το πέρας της μπαίνει ένα τέλος στα φοιτητικά μου αυτά χρόνια τα οποία θα θυμάμαι για πάντα.

Θα ήθελα να ευχαριστήσω πολύ τον επιβλέποντα καθηγητή μου Κυριάκο Μουράτη για την καθοδήγηση του, τις συμβουλές του και τον χρόνο που αφιέρωσε έτσι ώστε να φέρω εις πέρας αυτήν την εργασία παρόλο το φορτωμένο του πρόγραμμα ως καθηγητής.

Ευχαριστώ τους φίλους μου για αυτά υπέροχα χρόνια που πέρασα ως φοιτητής.

Τέλος ένα τεράστιο ευχαριστώ στους γονείς μου Λιθοξόπουλο Σάββα και Λουλούδη Ανδρονίκη για την οικονομική υποστήριξη και την θετική ενέργεια που μου παρείχαν όλα αυτά τα χρόνια έτσι ώστε να έχω την δυνατότητα να σπουδάσω.

Περίληψη

Η παρούσα πτυχιακή εργασία εμβαθύνει στον κεντρικό ρόλο των συστημάτων εποπτικού ελέγχου και απόκτησης δεδομένων (SCADA) σε συνδυασμό με τους προγραμματιζόμενους λογικούς ελεγκτές (PLC) στον βιομηχανικό αυτοματισμό.

Σκοπός αυτής της έρευνας είναι να αποκαλύψει την συνεργασία μεταξύ του SCADA και των PLC διενεργώντας μια ολοκληρωμένη ανάλυση των αντίστοιχων λειτουργιών και των προσαρμόσιμων χρήσεων τους.

Ο πρωταρχικός στόχος είναι να διερευνηθεί πώς το SCADA και τα PLC μπορούν να ενσωματωθούν και να συνεργαστούν απρόσκοπτα για αποτελεσματικό έλεγχο και αυτοματοποίηση διεργασιών σε βιομηχανικά περιβάλλοντα. Επιπλέον, η μελέτη θα εμβαθύνει στη σημασία των συστημάτων SCADA στη συλλογή και ανάλυση δεδομένων, φωτίζοντας τον κρίσιμο ρόλο τους στη βελτιστοποίηση των διαδικασιών και στη λήψη τεκμηριωμένων αποφάσεων.

Με την παρουσίαση αυτής της μελέτης, η διατριβή στοχεύει να βελτιώσει την κατανόηση των εφαρμογών SCADA και PLC, προωθώντας τη χρήση τους ως ισχυρά εργαλεία για την ενίσχυση των βιομηχανικών διεργασιών και τον εποπτικό έλεγχο.

Abstract

This thesis delves into the central role of supervisory control and data acquisition (SCADA) systems combined with programmable logic controllers (PLC) in industrial automation.

The purpose of this research is to reveal the collaboration between SCADA and PLCs by conducting a comprehensive analysis of their respective functions and customizable uses.

The primary objective is to explore how SCADA and PLCs can be integrated and work together seamlessly for effective process control and automation in industrial environments. In addition, the study will delve into the importance of SCADA systems in data collection and analysis, illuminating their critical role in optimizing processes and making informed decisions.

By presenting this study, the thesis aims to improve the understanding of SCADA and PLC applications, promoting their use as powerful tools for industrial process enhancement and supervisory control.

Περιεχόμενα

ΚΕΦΑΛΑΙΟ 1^{Ο}

1.1 Εισαγωγή στα συστήματα SCADA

Ένα σύστημα SCADA, ή σύστημα εποπτικού ελέγχου και απόκτησης δεδομένων, αποτελείται από πολλαπλές απομακρυσμένες τερματικές μονάδες ή RTU, οι οποίες συλλέγουν δεδομένα από το πεδίο και συνδέονται με έναν κεντρικό σταθμό μέσω ενός συστήματος επικοινωνίας. Ο κεντρικός σταθμός παρουσιάζει τα συλλεγμένα δεδομένα στον χειριστή και του δίνει τη δυνατότητα να εκτελέσει εργασίες τηλεχειρισμού, συμπεριλαμβανομένων των λειτουργιών τηλεμετρίας και τηλεχειρισμού. Τα ακριβή και έγκαιρα δεδομένα, συνήθως σε πραγματικό χρόνο, βοηθούν στη βελτιστοποίηση της λειτουργίας του εγκατεστημένου συστήματος και της διεργασίας. Επιπλέον, προσφέρουν αποδοτικότητα, αξιοπιστία και ασφάλεια στη λειτουργία. Αυτά τα οφέλη οδηγούν σε μειωμένο κόστος συντήρησης σε σύγκριση με τα μη αυτοματοποιημένα συστήματα του παρελθόντος. Στην ουσία, το SCADA αναφέρεται στον τηλεχειρισμό από απόσταση. Κρίσιμο είναι το πόσο μακριά είναι το “απομακρυσμένο”, συνήθως αναφέρεται σε αποστάσεις που δεν επιτρέπουν τον άμεσο καλωδιακό έλεγχο. Η επιτυχία της εγκατάστασης του SCADA εξαρτάται από τη χρήση αξιόπιστης τεχνολογίας και την κατάλληλη εκπαίδευση του προσωπικού στη λειτουργία του συστήματος.

1.2 Ιστορική αναδρομή

Η ανάγκη για την δημιουργία ενός συστήματος εποπτικού ελέγχου και συλλογής πληροφοριών (SCADA) προέκυψε από την προσπάθεια του βιομηχανικού τομέα να αντιμετωπίσει ζητήματα που αφορούν τη διαχείριση των βιομηχανικών εγκαταστάσεων. Κατά την αλλαγή του 20ου αιώνα, τα εργοστάσια και οι απομονωμένες εγκαταστάσεις εξαρτιόνταν από τον χειροκίνητο έλεγχο και τη συνεχή επαγρύπνηση των εργαζομένων για τη διαχείριση διαφορετικών διαδικασιών και εξοπλισμού. Καθώς ο αριθμός των βιομηχανικών και απομακρυσμένων εγκαταστάσεων αυξανόταν, κατέστη αναγκαία η εξεύρεση λύσεων για τον τηλεχειρισμό του εξοπλισμού. Τα ρελέ και οι χρονοδιακόπτες ήταν ένα είδος αυτοματισμού που βοήθησε και έλυσε αρκετά προβλήματα βάση των δεδομένων της μέχρι τότε εποχής , αλλά είχαν περιορισμένη λειτουργικότητα . Η συνεχής εξέλιξη και ανάπτυξη των βιομηχανιών απαιτούσαν καινούριες μεθόδους .

Στις αρχές της δεκαετίας του 1940, έγινε προσπάθεια να συνδεθεί όλος ο εξοπλισμός της βιομηχανικής μονάδας σε έναν απομακρυσμένο υποσταθμό μέσω ενός ζεύγους καλωδίων. Πιο συγκεκριμένα, ήταν η πρώτη προσπάθεια εκμετάλλευσης της πολυπλεξίας μέσα σε ένα ζεύγος τηλεφωνικών γραμμών και εμπνεύστηκε από τους μαγνητικούς βαθμωτούς διακόπτες που αναπτύχθηκαν από εταιρείες τηλεφωνίας τη δεκαετία του 1930. Στη συνέχεια, τη δεκαετία του 1950, οι ψηφιακοί υπολογιστές άρχισαν να χρησιμοποιούνται στον βιομηχανικό έλεγχο λόγω της ανάγκης για πιο αποτελεσματικά, αυτοματοποιημένα συστήματα ελέγχου και παρακολούθησης. Οι εποπτικοί έλεγχοι έγιναν δημοφιλείς και έλαβαν την προσοχή από μεγάλες εταιρείες.

Η τεχνολογία τηλεμετρίας άρχισε να εμφανίζεται στη δεκαετία του 1960 και χρησιμοποιείται για τον έλεγχο και την παρακολούθηση περιβαλλόντων , επίτρεπε την άμεση μετάδοση πληροφοριών μεταξύ εξοπλισμού σε μια εγκατάσταση και απομακρυσμένων τοποθεσιών. Οι εξελίξεις στην τηλεμετρία, τα τηλεφωνικά συστήματα αναμετάδοσης και τα συστήματα κωδικοποίησης επέτρεψαν στη Westinghouse και τη Northern Electric να αναπτύξουν ένα σύστημα επιτήρησης που ονομάζεται Visicode. Στις αρχές της δεκαετίας του 1950 και του 1965, τόσο η General Electric όσο και η Control Corporation ξεκίνησαν τη δημιουργία των επιμέρους προγραμμάτων τους για παρακολούθηση. Αυτά τα προγράμματα τέθηκαν σε άμεση χρήση σε διάφορους κλάδους, όπως αγωγούς μεγάλων αποστάσεων, εταιρείες φυσικού αερίου και φώτα αεροδρομίων.

Μετά την αρχική ανάπτυξη της τεχνολογίας αυτοματισμού, η ακόλουθη σημαντική πρόοδος ήταν η εισαγωγή των μικροεπεξεργαστών και των προγραμματιζόμενων λογικών ελεγκτών (PLC).

Η Bedford Associates παρήγαγε το πρώτο PLC στον κόσμο τη δεκαετία του 1970, γεγονός που οδήγησε σε αύξηση της εφαρμογής αυτοματισμού εντός των εταιρειών. Αυτή η πρόοδος οδήγησε τελικά στη δημιουργία του όρου SCADA.

Τα πρώτα συστήματα SCADA δεν είχαν δυνατότητες διασύνδεσης .Το 1980, η τεχνολογία του διαδικτύου ξεκίνησε να αναπτύσσεται και έδωσε τη δυνατότητα για την επικοινωνία και τον έλεγχο των συστημάτων SCADA από απομακρυσμένους υπολογιστές. Το 1990 οι εφαρμογές SCADA εξελίχθηκαν περαιτέρω με τη χρήση προηγμένων αλγορίθμων επεξεργασίας σήματος και ανάλυσης δεδομένων. Η ανάπτυξη τους , τους προσφέρει τεχνολογίες διεπαφή ανθρώπου- μηχανής και τοπικά δίκτυα . Με αυτές τις νέες δυνατότητες, τα συστήματα SCADA μπορούν να συνδεθούν με άλλα παρόμοια συστήματα και να υποστηρίξουν ορισμένες συνδέσεις. Η ενσωμάτωση σύγχρονων πρακτικών και τεχνολογιών πληροφορικής ξεκίνησε τη δεκαετία του 2000 μέσω εφαρμογών βασισμένων στο Διαδίκτυο και στη γλώσσα SQL. Οι αλλαγές που έγιναν στα συστήματα SCADA οδήγησαν σε σημαντικές βελτιώσεις στην αποτελεσματικότητα, την αξιοπιστία και την ασφάλεια. Τα σύγχρονα συστήματα είναι πολύ πιο εκλεπτυσμένα, επιτρέποντας στους μηχανικούς να δημιουργούν εφαρμογές με μεγαλύτερη ευκολία και ταχύτητα, χωρίς να απαιτείται εκτεταμένη τεχνογνωσία στην ανάπτυξη λογισμικού. Επιπλέον, οι χρήστες έχουν πλέον πρόσβαση σε δεδομένα σε πραγματικό χρόνο που είναι προσβάσιμα παγκοσμίως.

1.3 Αρχή λειτουργιάς

Τα συστήματα SCADA αποτελούνται από λογισμικό παρακολούθησης και ελέγχου, επιπλέον από μια σειρά αισθητήρων και μετατροπέων που συνδέονται με τις RTU που είναι διάσπαρτα σε όλο το υπό εξέταση δίκτυο. Αυτά τα RTU δημιουργούν στη συνέχεια επικοινωνία με έναν κεντρικό υπολογιστή ή μια κύρια τερματική μονάδα (MTU).

Το σύστημα SCADA είναι ένα ολοκληρωμένο σύστημα τηλεμετρίας και τηλεχειρισμού, όπως αναφέρθηκε προηγουμένως. Για το λόγο αυτό, είναι ιδιαίτερα χρήσιμο σε περιπτώσεις όπου το διαχειριζόμενο σύστημα βρίσκεται μακριά από την περιοχή διαχείρισης. Για τη δημιουργία συστήματος SCADA είναι απαραίτητο, μεταξύ άλλων, ένα σύστημα τηλεμετρίας. Αυτό το σύστημα τίθεται σε εφαρμογή με τη βοήθεια σταθμών RTU, γνωστών και ως Μονάδες Απομακρυσμένης Τηλεμετρίας. Αυτές οι μονάδες συνδέονται με τη διαδικασία παραγωγής και είναι υπεύθυνες για την ανάγνωση τιμών διαφόρων φυσικών μεγεθών που

ενδιαφέρουν, όπως θερμοκρασία, πίεση και συχνότητα. Αυτές οι μετρήσεις στη συνέχεια μετατρέπονται σε ηλεκτρικά σήματα και μεταδίδονται περιοδικά μέσω ενσύρματου ή ασύρματου διαύλου (ανάλογα με τις ανάγκες της εφαρμογής) σε υπολογιστή εξοπλισμένο με λογισμικό SCADA. Η συχνότητα αυτών των μεταδόσεων εξαρτάται από την ταχύτητα με την οποία εξελίσσεται η παρακολουθούμενη διαδικασία, καθώς και από την επιθυμητή ακρίβεια για το σύστημα. Για την υλοποίηση του SCADA, εκτός από τα RTU, είναι απαραίτητος ένας κεντρικός υπολογιστής με επαρκείς υπολογιστικές δυνατότητες. Αυτός ο κεντρικός υπολογιστής θα είναι υπεύθυνος για τη φιλοξενία του λογισμικού SCADA και τον τερματισμό όλων των μετρήσεων που λαμβάνονται από τους σταθμούς RTU, καθώς και τη διαχείριση των βασικών τηλεπικοινωνιακών συνδέσεων μεταξύ των σταθμών RTU και του κεντρικού υπολογιστή.

Δύο σημαντικοί ορισμοί της έννοιας των SCADA είναι:

- Ο όρος SCADA αναφέρεται σε μια τεχνολογία που επιτρέπει στους χρήστες να συλλέγουν δεδομένα από μία ή περισσότερες εγκαταστάσεις και να εκδίδουν απλές εντολές ελέγχου σε αυτές, επιτρέποντας την παρακολούθηση και τον έλεγχο από απόσταση των συστημάτων μέσω του διαδικτύου [31].
- Αποτελεί ένα σύστημα που λειτουργεί με κωδικοποιημένα σήματα μέσω επικοινωνιακών καναλιών, με στόχο την αποστολή εντολών ελέγχου σε εξοπλισμό ή συσκευές RTU [32].

1.4 Εξέλιξη των συστημάτων SCADA

Τα συστήματα SCADA συνεχίζουν να προοδεύουν καθώς η σύγχρονη τεχνολογία υπολογιστών αναπτύσσεται και ωριμάζει. Ακολουθούν τέσσερις γενιές συστημάτων SCADA:

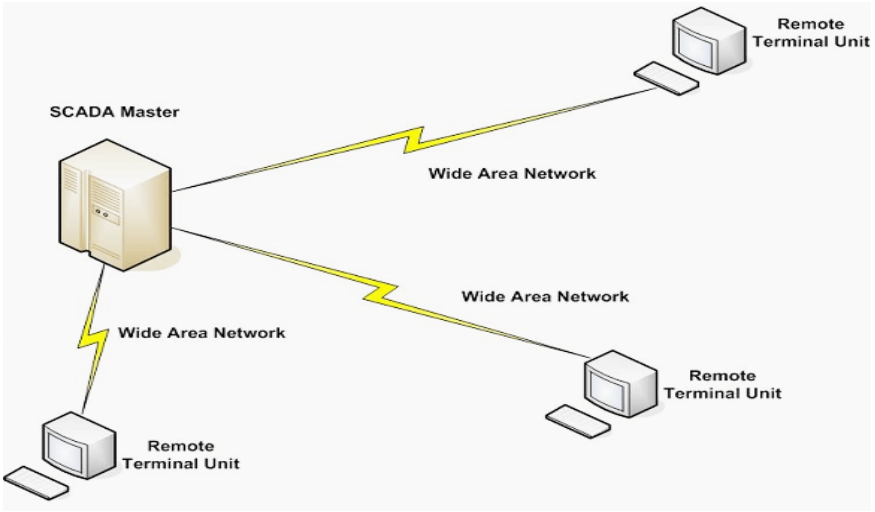
- Πρώτη Γενιά – Μονολιθικά Συστήματα (Monolithic)
- Δεύτερη Γενιά – Κατανεμημένα Συστήματα (Distributed)
- Τρίτη Γενιά – Δικτυωμένα Συστήματα (Networked)
- Τέταρτη Γενιά - IoT based SCADA

1.4.1 Μονολιθικά Συστήματα SCADA

Η βασική δομή αυτών των συστημάτων στηριζόταν σε ένα κεντρικό υπολογιστικό σύστημα μεγάλης υπολογιστικής ισχύος (mainframe computer- PDP 111 από την Digital Equipment Corporation) το οποίο συνδεόταν και αντάλλασσε δεδομένα με διάφορα RTUs (Remote Terminal Units). Αυτά τα RTU είχαν τον ρόλο να μεταφέρουν δεδομένα τηλεμετρίας στο mainframe σύστημα και να λαμβάνουν από αυτό μηνύματα και εντολές ελέγχου για της συσκευές της έλεγχο.

Χαρακτηριστικό αυτών των συστημάτων ήταν η απουσία ουσιαστικής δικτύωσης. Ακόμη και αν τα δίκτυα ευρείας περιοχής (WAN) είχαν αναπτυχθεί εκείνη την περίοδο, ο μόνος ρόλος αυτών στα μονολιθικά συστήματα SCADA ήταν η ανταλλαγή δεδομένων μεταξύ RTU και MTU

(mainframe computer). Έτσι πρακτικά τα πρώτα συστήματα ελέγχου δεν είχαν την ικανότητα της διασύνδεσής με άλλα, και ουσιαστικά ήταν αυτόνομα συστήματα (standalone systems). Όσον αφορά τα πρωτόκολλα επικοινωνίας που ήταν διαθέσιμα, αυτά είχαν αναπτυχθεί από διάφορους κατασκευαστές RTU και εφαρμόζονταν μόνο για την επικοινωνία των RTU με το master computer του ιδίου κατασκευαστή και έτσι, τα πρωτόκολλα ήταν σε θέση να επιτρέψουν μόνο τη σάρωση, τον έλεγχο και την ανταλλαγή δεδομένων μεταξύ των MTU και των RTU . Η διασύνδεση μεταξύ διαφορετικής προέλευσης RTU και MTU δεν ήταν δυνατή.



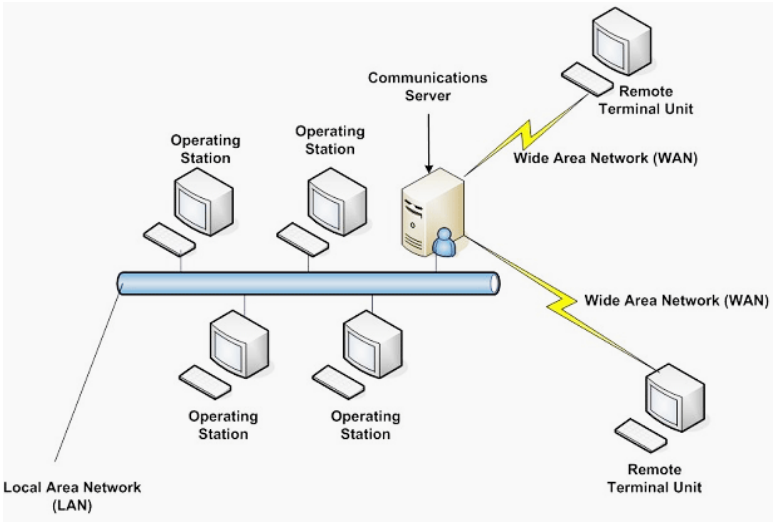
Εικόνα 1 Παράδειγμα, αρχιτεκτονικής μονολιθικού συστήματος SCADA

Η σύνδεση μεταξύ MTU και RTU γινόταν με την χρήση ενός δίαυλου (πχ με χρήση πρότυπων επικοινωνίας RS-232) ή χρησιμοποιώντας έναν αποκλειστικό προσαρμογέα συνδεδεμένο απευθείας στην κεντρική μονάδα επεξεργασίας (CPU). Η λειτουργικότητα αυτών των συστημάτων πρώτης γενιάς ολοκληρώθηκε με την χρήση ενός δεύτερου εφεδρικού κεντρικού υπολογιστή . Σκοπός του είναι να ελέγχει τον αρχικό υπολογιστή και να αναλάβει τον έλεγχο σε περίπτωση που εντοπιστεί βλάβη.

1.4.2 Κατανεμημένα συστήματα SCADA

Η δεύτερη γενιά των συστημάτων SCADA αναγνωρίζει την ανάγκη για μεγαλύτερη αξιοπιστία, ασφάλεια και δυνατότητα λειτουργίας σε σχέση με την πρώτη γενιά**.** Η ανάπτυξη και εξέλιξη των τοπικών δικτύων υπολογιστών (LANs – Local Area Networks) αποτέλεσαν τον παράγοντα κλειδί για την εμφάνιση των κατανεμημένων συστημάτων SCADA. Η βασική διαφορά σε σχέση με τα μονολιθικά συστήματα είναι ότι πλέον χρησιμοποιούνται πολλαπλοί σταθμοί, καθένας εκ των οποίων επιτελεί μια διαφορετική λειτουργία στο δίκτυο. Έτσι, για παράδειγμα υπάρχουν σταθμοί υπεύθυνοι για την επικοινωνία του συστήματος (communication processors), σταθμοί επεξεργασίας των δεδομένων (calculation processors), εξυπηρετητές βάσεων δεδομένων (database servers) κ.α. Αυτές οι κατανεμημένες υπολογιστικές μονάδες είχαν τη δυνατότητα να ανταλλάσσουν δεδομένα σε πραγματικό χρόνο μέσω του δικτύου LAN. Με αυτόν τον τρόπο επιτυγχάνεται καταμερισμός των

διεργασιών του συστήματος SCADA σε πολλαπλούς σταθμούς εργασίας οι οποίοι είναι μικρότεροι και πιο οικονομικοί από mainframe συστήματα της 1ης γενιάς. Το δίκτυο LAN που υποστήριζε αυτού του είδους τα συστήματα βασιζόταν σε πρωτόκολλα επικοινωνίας που είχαν αναπτυχθεί από εταιρίες εμπορίας και σχεδίασης τέτοιων εφαρμογών, προσδίδοντας στο δίκτυο αυξημένη ταχύτητα επικοινωνίας, αξιοπιστία και βελτιστοποίηση δρομολόγησης σε πραγματικό χρόνο. Ωστόσο, οι συσκευές που ήταν συνδεδεμένες στο SCADA LAN δεν μπορούσαν να επικοινωνήσουν με τις εξωτερικές συσκευές που χρησιμοποιούσαν διαφορετικά πρωτόκολλα. Επομένως τα συστήματα ήταν κατανεμημένα και μπορούσαν να επικοινωνούν το ένα με το άλλο αλλά μόνο μέσω πρωτοκόλλων που είχαν αναπτυχθεί από συγκεκριμένους κατασκευαστές που είχαν προμηθεύσει τον εξοπλισμό, περιορίζοντας τη σύνδεση του συστήματος με συσκευές άλλων κατασκευαστών στο τοπικό δίκτυο SCADA LAN
.



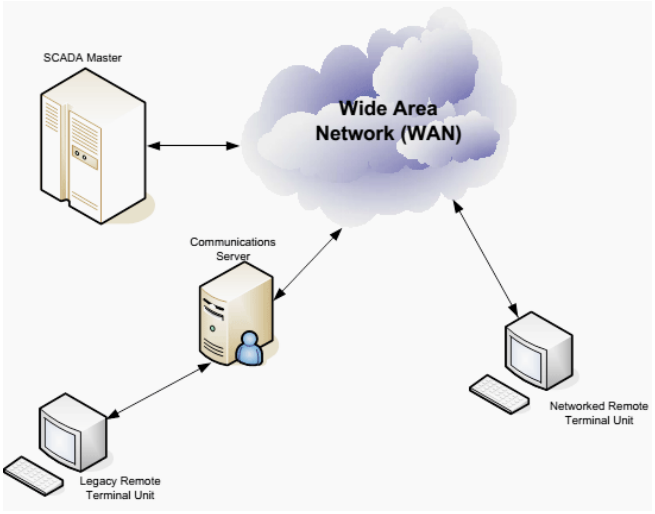
Εικόνα 2 Παράδειγμα, αρχιτεκτονική κατανεμημένου συστήματος SCADA

Στη δεύτερη γενιά, επιπλέον, περιορίστηκαν και οι ανάγκες σε υλικό, λογισμικό και περιφερειακές συσκευές που ήταν απαραίτητες.

1.4.3 Δικτυωμένα συστήματα SCADA

Η ολοένα και μεγαλύτερη ανάπτυξη των βιομηχανικών μονάδων, η αυξημένη ανάγκη για αυτοματοποίηση καθώς και το άνοιγμα της αγοράς των συστημάτων αυτοματισμού και ελέγχου με την εισαγωγή νέων εταιριών και προμηθευτών οδήγησε στο επόμενο βήμα την εξέλιξη των συστημάτων SCADA κα ουσιαστικά στην εμφάνιση των δικτυωμένων συστημάτων (Networked systems). Η Τρίτη γενιά συστημάτων έχει ομοιότητες με τα συστήματα της προηγούμενης γενιάς, παρατηρείται όμως μια σημαντική διαφορά. Αυτή η διαφορά είναι ότι τα νέα συστήματα SCADA είναι κατά βάση συστήματα ανοικτής αρχιτεκτονικής σε σχέση με τα συστήματα της 2ης γενιάς τα οποία περιορίζονται από αρχιτεκτονικές και πρωτόκολλα ελεγχόμενα από συγκεκριμένους προμηθευτές. Σε αυτό το

είδος των συστημάτων η επικοινωνία βασίζεται σε ανοιχτά πρωτόκολλα που επιτρέπουν της λειτουργίες του συστήματος SCADA να είναι κατανεμημένες σε δίκτυα ευρείας περιοχής (WANs – Wide Area Networks) και όχι σε ένα περιορισμένο τοπικό δίκτυο LAN. Έτσι ο κύριος παράγοντας που βοήθησε στην ανάπτυξη των συστημάτων 3ης γενιάς ήταν η χρήση πρωτοκόλλων επικοινωνίας που χρησιμοποιούνται σε WAN δίκτυα όπως το Πρωτόκολλο Διαδικτύου (IP – Internet Protocol) για επικοινωνίες μεταξύ master station και περιφερειακών . Ένα σημαντικό πλεονέκτημα των δικτυωμένων SCADA συστημάτων είναι ότι με τη διανομή της επεξεργασίας σε διαφορετικούς σταθμούς, είναι δυνατόν ένα σύστημα να αντέξει την απώλεια ενός επιμέρους στοιχείου του, ακόμη και του κεντρικού σταθμού, πράγμα πολύ σημαντικό για μεγάλες επιχειρήσεις και βιομηχανίες όπου το σύστημα SCADA υποστηρίζει εξαιρετικά κρίσιμες λειτουργίες.



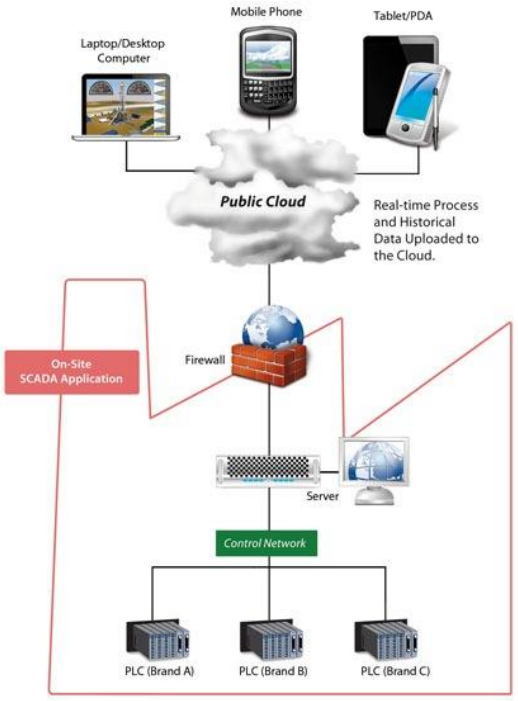
Εικόνα 3 Παράδειγμα, αρχιτεκτονική δικτυωμένου συστήματος SCADA

Αυτή η εξέλιξη ανάγκασε της εταιρίες που ανέπτυσσαν εφαρμογές για συστήματα SCADA να ενσωματώσουν σε αυτές νέες δυνατότητές, δημιουργώντας καινούργιες υπολογιστικές πλατφόρμες και λογισμικά. Στην κατεύθυνση αυτή το 1996 ιδρύεται η βιομηχανική κοινοπραξία OPC (Open Platform Communication) σκοπός της οποίας είναι ειδικά πρωτόκολλα PLC της το Modbus, το Profibus και άλλα να τυποποιηθούν σε ένα περιβάλλον εργασίας που επιτρέπει συστήματα SCADA να διασυνδέονται με συσκευές από διάφορους προμηθευτές, χρησιμοποιώντας ανοικτά πρότυπα και πρωτόκολλα. Το OPC αποτελεί το πρότυπο δια λειτουργικότητας για την ασφαλή και αξιόπιστη ανταλλαγή δεδομένων στον χώρο του βιομηχανικού αυτοματισμού αλλά και της βιομηχανίες. Αυτή η ανεξάρτητη πλατφόρμα εξασφαλίζει την ομαλή ροή πληροφοριών μεταξύ συσκευών από πολλούς προμηθευτές. Το ίδρυμα OPC είναι υπεύθυνο για την ανάπτυξη και τη συντήρηση αυτού του προτύπου[1-5] .

1.4.4 Διαδίκτυο των πραγμάτων & συστήματα SCADA (IoT – Internet of Things)

Το Διαδίκτυο των πραγμάτων, γνωστό και ως IoT, είναι μια έννοια που σχετίζεται με τη δυνατότητα σύνδεσης συσκευών απομακρυσμένης παρακολούθησης σε υπάρχουσα υποδομή μέσω του Διαδικτύου. Το λεγόμενο υπολογιστικό νέφος (Cloud Computing)

αποτελεί τον ακρογωνιαίο λίθο πάνω στον οποίο βασίζεται η 4η γενιά εξέλιξης των συστημάτων SCADA και αποτελεί μία συνεχώς αναπτυσσόμενη τάση στον σύγχρονο τεχνικό αλλά και επιχειρηματικό κόσμο. Μέσω του cloud computing δίνεται η δυνατότητα σε διακομιστές (servers) που μπορεί να απέχουν χιλιάδες χιλιόμετρα μακριά να λειτουργήσουν μέσα σε ένα δίκτυο. Η διασύνδεση αυτή δημιουργεί το λεγόμενο «σύννεφο» το οποίο αναπτύσσεται σε μία αφηρημένη γεωγραφική περιοχή πολλές φορές άγνωστη στον χρήστη που το χρησιμοποιεί. Η επικοινωνία και η πρόσβαση σε αυτό το υπολογιστικό νέφος γίνεται μέσω του Internet προσφέροντας με αυτό τον τρόπο δυνατότητες κεντρικής αποθήκευσης των δεδομένων, επεξεργασία αυτών αλλά και ταυτόχρονης πρόσβασης σε υπηρεσίες από οποιουδήποτε μέρος του κόσμου. Οι πρωτόγνωρες αυτές δυνατότητες που προσφέρει η τεχνολογία του IoT κάνει τα συστήματα SCADA να προσαρμόζονται και να την υιοθετούν όλο και περισσότερο, εξασφαλίζοντας σημαντική μείωση του κόστους υποδομών και συντήρησης και αυξάνοντας ταυτόχρονα την αμεσότητα στην πρόσβαση και στην εποπτεία των βιομηχανικών συστημάτων

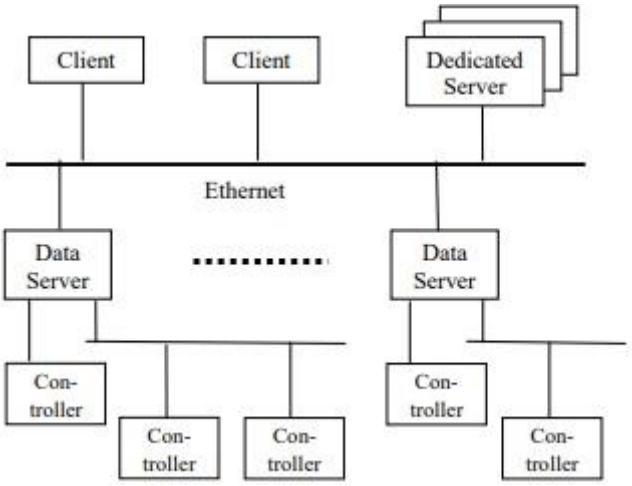


Εικόνα 4 Παράδειγμα , IoT και σύστημα SCADA

1.5 Αρχιτεκτονική SCADA

Αρχιτεκτονική υλικού

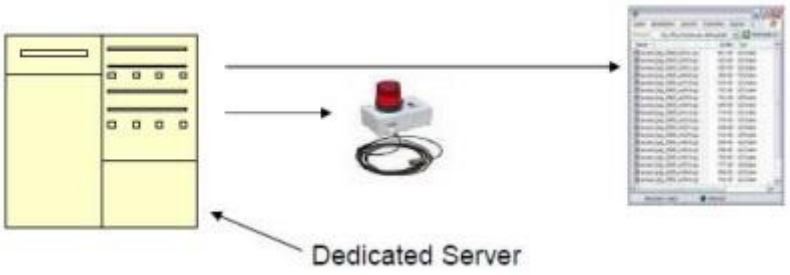
Το σύστημα SCADA διακρίνεται από δύο κύρια επίπεδα: το επίπεδο πελάτη, το οποίο είναι υπεύθυνο για την αλληλεπίδραση ανθρώπου-μηχανής, και το επίπεδο διακομιστή δεδομένων, το οποίο διαχειρίζεται τις περισσότερες από τις δραστηριότητες ελέγχου διεργασιών. Οι διακομιστές δεδομένων επικοινωνούν με συσκευές πεδίου μέσω ελεγκτών διεργασίας, όπως προγραμματιζόμενοι λογικοί ελεγκτές (PLC). Αυτοί οι ελεγκτές διεργασιών μπορούν να συνδεθούν απευθείας ή μέσω δικτύων ή διαύλων πεδίου, τα οποία μπορεί να είναι είτε ιδιόκτητα, όπως η Siemens H1, είτε μη ιδιόκτητα, όπως το Profibus. Για τη σύνδεση διακομιστών δεδομένων και σταθμών πελατών, χρησιμοποιείται ένα LAN Ethernet. Ενώ οι διακομιστές δεδομένων και οι διακομιστές-πελάτες λειτουργούν σε πλατφόρμες NT, ορισμένα προϊόντα ενδέχεται να απαιτούν μηχανές W95 για τους διακομιστές-πελάτες. [34].



Εικόνα 5 Χαρακτηριστικά αρχιτεκτονικής υλικού

Αρχιτεκτονική λογισμικού

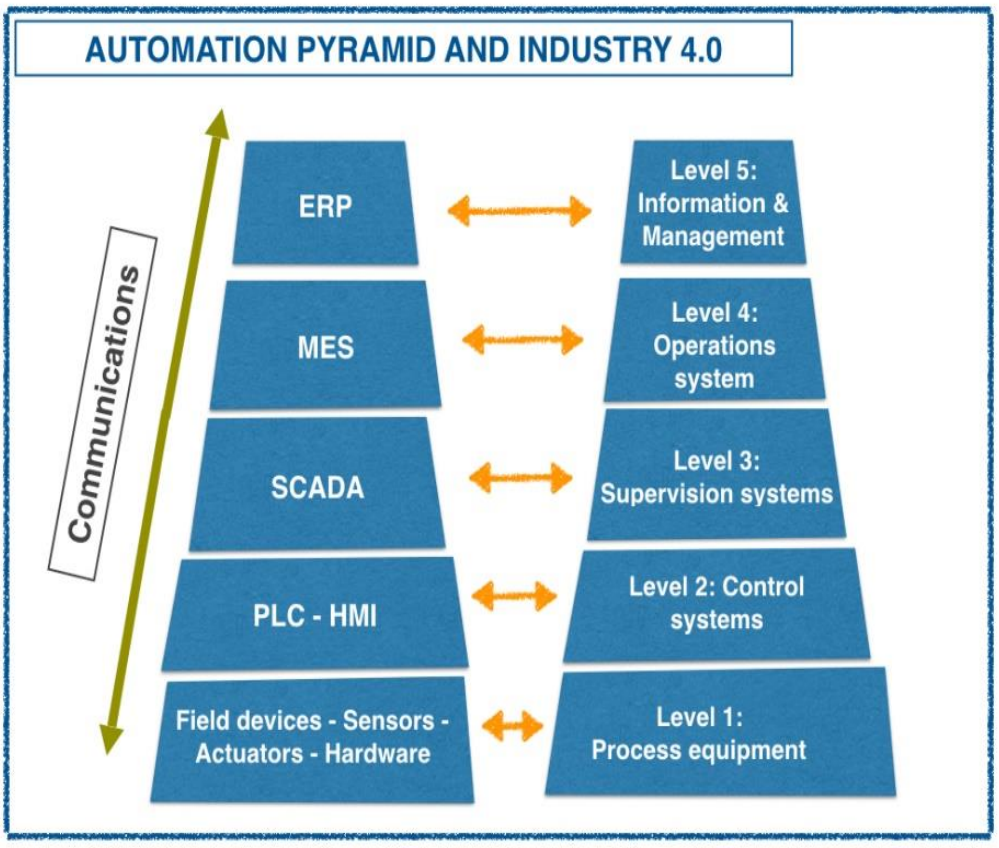
Τα προϊόντα είναι πολλαπλών εργασιών (multi-tasking) και βασίζονται σε μια βάση δεδομένων πραγματικού χρόνου (RTDB), η οποία βρίσκεται σε έναν ή περισσότερους κεντρικούς servers. Οι servers είναι αρμόδιοι για την απόκτηση και τη διαχείριση δεδομένων(data acquisition and management), περιλαμβανομένων εργασιών όπως ελεγκτές δημοσκόπησης, διαχείριση συναγερμών, υπολογισμοί, καταγραφή και αρχειοθέτηση, συνήθως σχετικά με τις παραμέτρους με τις οποίες συνδέονται. Ωστόσο, είναι δυνατό να υπάρχουν Dedicated Servers για συγκεκριμένες εργασίες, όπως ιστορικός, καταγραφέας δεδομένων, χειριστής συναγερμών. Το σχήμα 6 δείχνει την αρχιτεκτονική SCADA που είναι γενική για τα evaluated (αποτιμημένα) προϊόντα[34].



Εικόνα 6 Αποκλειστικός διακοσμητής

1.6 Επίπεδα έλεγχου

Ένα σύστημα SCADA το οποίο πραγματοποιεί εποπτικό έλεγχο μπορεί να χωριστεί σε πέντε λειτουργικά σταδία κατασκευής, όπως φαίνονται στο παρακάτω σχήμα και στη συνέχεια αναλύονται με περισσότερες λεπτομέρειες.



Εικόνα 7 Πυραμίδα αυτοματισμού, διαχείριση της διαδικασίας.

Επίπεδο 1: Δίκτυο διεργασιών (συσκευές πεδίου - αισθητήρες - ενεργοποιητές - υλικό)

Αυτές οι συσκευές αποτελούν μέρη μιας παραγωγικής ή βιομηχανικής ομάδας και επικοινωνούν με τον έλεγχο στο επίπεδο 2 (PLC) για να μεταφέρουν πληροφορίες σχετικά με την κατάσταση των συσκευών, όπως θερμοκρασία, θέση/απόσταση, κατάσταση "ανοικτό/κλειστό" και άλλες. Επιπλέον, ανταποκρίνονται σε εντολές που λαμβάνουν από το PLC. Οι ταχύτητες μετάδοσης δεδομένων είναι πολύ υψηλές, συχνά σε χιλιοστά του δευτερολέπτου, και η συχνότητα μετάδοσης δεδομένων μπορεί να προσαρμοστεί ανάλογα με τις απαιτήσεις του επιπέδου ελέγχου της διεργασίας (PLC-επίπεδο-2). Επιπλέον, ορισμένες από αυτές τις συσκευές μπορούν να αποθηκεύουν πληροφορίες, ακόμη και αν αυτό δεν είναι η κύρια λειτουργία τους. [33]

Επίπεδο 2: Δίκτυο ελέγχου (PLC-HMI)

Αυτές οι συσκευές αποτελούν μέρη μιας παραγωγικής ή βιομηχανικής ομάδας και εκτελούν κύρια λειτουργία ελέγχου και διακυβέρνησης της ομάδας αυτής. Λαμβάνουν πληροφορίες από το επίπεδο 1, ελέγχοντας την κατάσταση των συσκευών σχετικά με παραμέτρους όπως θερμοκρασία, θέση/απόσταση, κατάσταση "ανοικτό/κλειστό" και άλλα. Επίσης, στέλνουν εντολές ώστε οι συσκευές αυτές να εκτελέσουν τις αντίστοιχες λειτουργίες τους. Οι ταχύτητες μετάδοσης πληροφοριών μπορεί να είναι σε χιλιοστά του δευτερολέπτου. Στην ιεραρχία του πρωτοκόλλου επικοινωνίας, το Επίπεδο 2 χρησιμεύει ως ενδιάμεσος μεταξύ των επιπέδων 1 και 3. Η συχνότητα μετάδοσης δεδομένων στο Επίπεδο 1 ποικίλλει ανάλογα με την εκάστοτε εργασία, που κυμαίνεται από απλά χιλιοστά του δευτερολέπτου έως αρκετά δευτερόλεπτα ή και λεπτά. Η συχνότητα μετάδοσης μεταξύ Layer 2 και Layer 3 μπορεί επίσης να είναι υψηλή, ανάλογα με τις ιδιαίτερες απαιτήσεις του συστήματος. Η αποθήκευση πληροφοριών είναι ένα κρίσιμο στοιχείο του Industry 4.0, καθώς διευκολύνει τη διαθεσιμότητα δεδομένων για ανάλυση και λήψη αποφάσεων. Με τη χρήση ενός προγραμματιζόμενου λογικού ελεγκτή (PLC), οι πληροφορίες σε πραγματικό χρόνο μπορούν να συλλέγονται συχνά για την παρακολούθηση της κατάστασης των διαδικασιών παραγωγής και τη μετάδοση των δεδομένων σε υψηλότερα επίπεδα, όπου αποθηκεύονται για μελλοντική ανάλυση. [33].

Επίπεδο 3: Δίκτυο εποπτείας - SCADA

Ένα SCADA μπορεί να παρακολουθεί σε πραγματικό χρόνο το επίπεδο 2 ενός ή περισσότερων PLC ταυτόχρονα και να στέλνει εντολές σε αυτά, συντονίζοντας τη λειτουργία τους. Τα PLC, επίπεδου 2, ρυθμίζουν και ελέγχουν τα συστήματα που βρίσκονται υπό τον έλεγχό τους. Το περιβάλλον SCADA προσφέρει δυνατότητες αποθήκευσης δεδομένων μέσω βάσεων δεδομένων SQL ή NoSQL, και περιλαμβάνει επίσης διάφορα λογισμικά για εφαρμογές στον τομέα της βιομηχανίας. Επιπλέον, μπορεί να συνδέεται με ένα MES (Σύστημα Εκτέλεσης Κατασκευαστικών Εντολών), αν και στην πυραμίδα της βιομηχανίας αναπαρίσταται συνήθως στο επίπεδο 4[33].

Επίπεδο 4: Δίκτυο λειτουργίας - MES (Σύστημα εκτέλεσης παραγωγής)

Ο όρος MES (Σύστημα Εκτέλεσης Κατασκευαστικών Εντολών) σχετίζεται με τις λειτουργίες που εκτελούνται στις βιομηχανικές εγκαταστάσεις. Αυτό το σύστημα περιλαμβάνει πληροφορίες σχετικά με την παραγωγή, την εφοδιαστική αλυσίδα, τη συντήρηση, την ποιότητα και την ασφάλεια στο πλαίσιο της βιομηχανικής διαδικασίας. Επιπλέον, μπορεί να παρέχει πληροφορίες σχετικά με προϊόντα και διαδικασίες, βοηθώντας έτσι στη βελτίωση της απόδοσης και της διαχείρισης των εργασιών σε μια βιομηχανική εγκατάσταση[33].

Επίπεδο 5: Δίκτυο πληροφοριών - ERP

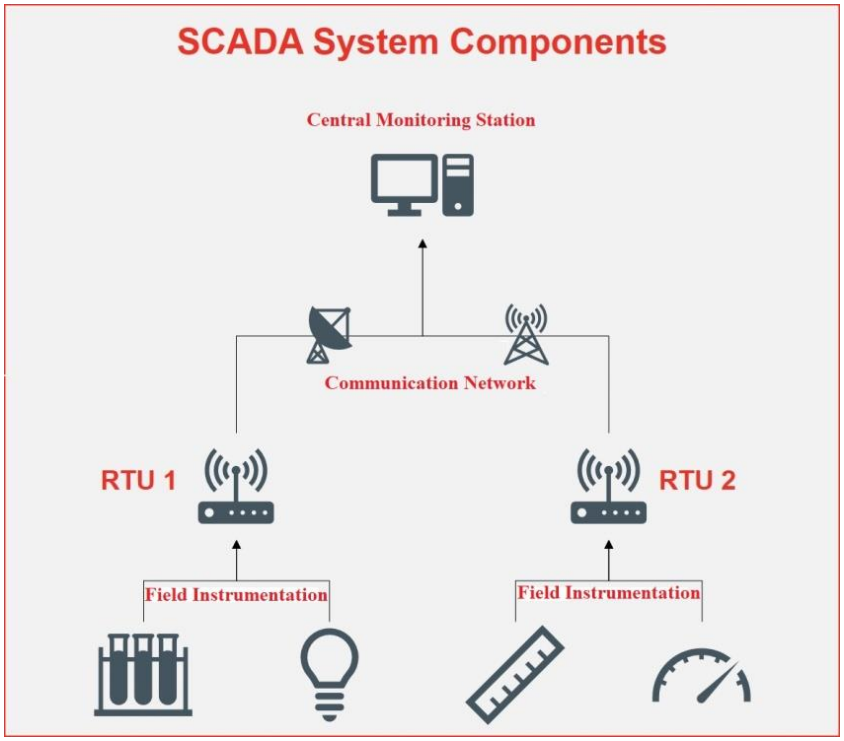
Οι πληροφορίες στο ERP είναι συνήθως στατικές και ενημερώνονται λιγότερο συχνά από ό,τι στα κατώτερα επίπεδα (επίπεδα 1, 2, 3 και 4). Σε αυτό το επίπεδο συγκεντρώνονται πληροφορίες σχετικές με πελάτες, προμηθευτές, συμβάσεις, οικονομικά δεδομένα, διαχείριση έργων και άλλες λειτουργίες διαχείρισης επιχειρήσεων.[33]

ΚΕΦΑΛΑΙΟ 2^{Ο}

2.1 Δομή των συστημάτων SCADA

Το σύστημα SCADA είναι ένας συνδυασμός εξαρτημάτων υλικού και προγραμμάτων λογισμικού. Μέσα από την πορεία εξέλιξης τους τα τελευταία 50 χρόνια τα συστήματα SCADA έχουν πλέον λάβει μια σταθερή δομή. Η δομή αποτελείται από διάφορα στοιχεία καθένα από αυτά έχει ένα συγκεκριμένο ρόλο και επιτελεί μία συγκεκριμένη λειτουργία. Τα σύγχρονα συστήματα αποτελούνται από τα ακόλουθα τέσσερα βασικά στοιχεία

- Όργανα Πεδίου - Field Instrumentation.
- Απομακρυσμένους Σταθμούς - Remote Stations.
- Δίκτυο Επικοινωνίας - Communication Network.
- Κεντρικό Σταθμό Παρακολούθησης - Central Monitoring Station.



Εικόνα 8 Τυπικά στοιχεία ενός συστήματος SCADA

Σε ένα σύστημα SCADA, οι πληροφορίες πρέπει να συλλέγονται από όλους τους απομακρυσμένους σταθμούς σε ένα κεντρικό σημείο. Από αυτό το σημείο , όλες οι λειτουργίες της εγκατάστασης μπορούν να παρακολουθούνται ενώ οι διαχειριστές συστημάτων μπορούν να εκδίδουν εντολές σε μεμονωμένες μονάδες.

Τα **Όργανα Πεδίου (Field Instrumentation)** είναι είτε αισθητήρες είτε ενεργοποιητές που συνδέονται απευθείας με διαφορετικά τμήματα της μονάδας παραγωγής ή του εξοπλισμού. Αυτά τα όργανα παράγουν σήματα είτε σε αναλογική είτε σε ψηφιακή μορφή που στη συνέχεια καταγράφονται από τον Απομακρυσμένο Σταθμό. Ως μέρος της διαδικασίας, αυτά

τα σήματα υφίστανται επεξεργασία, που αναφέρεται επίσης ως ρύθμιση σήματος (signal conditioning), προκειμένου να καταστούν συμβατά με τις εισόδους και τις εξόδους της μονάδας τηλεχειρισμού, όπως RTU ή PLC, του απομακρυσμένου σταθμού.

Ο **Απομακρυσμένος Σταθμός (Remote Station)** βρίσκεται εντός των ορίων του εξοπλισμού η της απομακρυσμένης μονάδας παραγωγής και οι λειτουργίες του επιβλέπονται από την κεντρική μονάδα. Ο απομακρυσμένος σταθμός μπορεί να λάβει μία από τις δύο πιθανές διαμορφώσεις: Remote Terminal Unit (RTU) ή Programmable Logic Controller (PLC).

Το **Δίκτυο Επικοινωνίας (Communications Network)** είναι το μέσο που χρησιμοποιείται για τη μετάδοση δεδομένων ή πληροφοριών από μια τοποθεσία σε μια άλλη. Αυτό μπορεί να επιτευχθεί με διάφορα μέσα, όπως τηλεφωνικές γραμμές, ράδιο εκπομπής ,καλωδιακά ή και ο συνδυασμός αυτών.

Ο **Κεντρικός Σταθμός Παρακολούθησης (Central Monitoring Station - CMS)** υποδηλώνει τη θέση όπου είναι εγκατεστημένος ο κεντρικός υπολογιστής (MTU) του συστήματος SCADA. Σε περίπτωση ανάγκης, είναι δυνατή η εγκατάσταση περισσότερων του ενός υπολογιστών στον Κεντρικό Σταθμό Παρακολούθησης. Για τη διευκόλυνση της λειτουργίας, ο CMS χρησιμοποιεί ένα πρόγραμμα Human Machine Interface για να καταγράφει διάφορους τύπους δεδομένων που απαιτούνται για τη λειτουργία.

2.2 Όργανα Πεδίου

"Δεν μπορείς να ελέγξεις αυτό που δεν μετράς" είναι ένα παλιό ρητό, που σημαίνει ότι τα όργανα αποτελούν βασικό στοιχείο ενός ασφαλούς και βελτιστοποιημένου συστήματος ελέγχου. Τα όργανα πεδίου αποτελούν τα αισθητήρια και τα εκτελεστικά μέρη ενός συστήματος SCADA. Μετρητές όπως οι μετρητές στάθμης δεξαμενής, οι μετρητές ροής νερού, οι πομποί θέσης βαλβίδας και οι αισθητήρες θερμοκρασίας, καθώς και μετρητές κατανάλωσης ενέργειας και πίεσης, παρέχουν πολύτιμες πληροφορίες που επιτρέπουν σε έναν έμπειρο χειριστή να αξιολογήσει την απόδοση ενός συστήματος διανομής νερού. Επιπλέον, εξοπλισμός όπως ηλεκτρικοί ενεργοποιητές βαλβίδων, πίνακες ελέγχου κινητήρων και συσκευές δοσομέτρησης χημικών ουσιών χρησιμοποιούνται για να εκτελέσουν τις εντολές του SCADA συστήματος και να συμβάλουν στην αυτοματοποίηση της διαδικασίας διανομής νερού.

Επομένως, τα όργανα πεδίου είναι συσκευές που μας επιτρέπουν να ανιχνεύουμε τυχαίες αλλαγές και αλλαγές σε ορισμένες θεμελιώδεις τιμές σε βιομηχανικά συστήματα που θέλουμε να παρακολουθήσουμε, δηλαδή πρόκειται για συσκευές όπως αισθητήρες και ενεργοποιητές. Οι αισθητήρες εκτελούν μετρήσεις και οι ενεργοποιητές εκτελούν τον έλεγχο. Οι αισθητήρες λαμβάνουν τα δεδομένα (εποπτεία και απόκτηση δεδομένων) και οι ενεργοποιητές εκτελούν ενέργειες που εξαρτώνται από αυτά τα δεδομένα (έλεγχος).

Πριν από την εφαρμογή οποιουδήποτε αυτοματισμού ή απομακρυσμένης παρακολούθησης, είναι απαραίτητο να γίνει η μετατροπή των πληροφοριών που ανταλλάσσονται από και προς τα όργανα πεδίου σε μια μορφή συμβατή με τη γλώσσα του συστήματος SCADA. Αυτό επιτυγχάνεται μέσω μιας μορφής ηλεκτρονικής διεπαφής δεδομένων πεδίου. Οι RTU (Remote Terminal Units), που είναι επίσης γνωστές ως

απομακρυσμένες μονάδες τηλεμετρίας, παρέχουν αυτήν τη διεπαφή. Ο κύριος στόχος τους είναι να μεταφράσουν ηλεκτρονικά σήματα που λαμβάνονται από συσκευές πεδίου σε μια γλώσσα επικοινωνίας που συνήθως αναφέρεται ως πρωτόκολλο επικοινωνίας. Αυτό το πρωτόκολλο χρησιμοποιείται για τη μετάδοση δεδομένων μέσω ενός καναλιού επικοινωνίας.

2.2.1 Αισθητήρες

Για τη μέτρηση φυσικών μεγεθών, χρησιμοποιούνται αισθητήρες. Αυτές οι συσκευές διαθέτουν μοναδικές ιδιότητες που μπορούν να μεταβληθούν με βάση τις αλλαγές στη φυσική ποσότητα που έχει αναλάβει να μετρήσει ο αισθητήρας. Χρησιμοποιούνται κυρίως σε δύο τομείς: για συλλογή πληροφοριών (μετρήσεις αισθητήρων) και για έλεγχο συστήματος (βιομηχανικές εφαρμογές). Ως ανιχνευτές συλλογής πληροφοριών, οι αισθητήρες παρέχουν δεδομένα για τη διαρκή παρακολούθηση και κατανόηση της κατάστασης παραμέτρων ενός συστήματος. Αντίθετα, οι αισθητήρες του συστήματος ελέγχου είναι παρόμοιοι σε εμφάνιση, αλλά συνήθως μεταδίδονται σε έναν ελεγκτή που παράγει μια έξοδο που τροποποιεί την τιμή της μετρούμενης παραμέτρου.
Οι «προδιαγραφές» των αισθητήρων αποτελούνται ουσιαστικά από κοινά χαρακτηριστικά που μοιράζονται. Αυτά τα χαρακτηριστικά περιλαμβάνουν τη γραμμικότητα, την ευαισθησία, την ακρίβεια, το εύρος εισόδου και εξόδου και θεωρούνται θεμελιώδη. Οι αισθητήρες μπορούν να κατηγοριοποιηθούν με βάση τις συγκεκριμένες ιδιότητες που διαθέτουν.
Στην πρώτη ταξινόμηση χωρίζονται σε ενεργούς και παθητικούς. Οι αισθητήρες μπορούν να ταξινομηθούν με βάση διάφορα κριτήρια. Ένα από τα κριτήρια αυτά είναι αν είναι ενεργοί ή παθητικοί. Οι ενεργοί αισθητήρες απαιτούν εξωτερικό σήμα διέγερσης ή ισχύος, ενώ οι παθητικοί παράγουν άμεσα απόκριση εξόδου χωρίς εξωτερική διέγερση. Ένα άλλο κριτήριο είναι το μέσο ανίχνευσης που χρησιμοποιείται, όπως ηλεκτρικά, βιολογικά, χημικά, ραδιενεργά κ.λπ. Τέλος, αισθητές μπορούν να ταξινομηθούν σε αναλογικούς και ψηφιακούς. Οι αναλογικοί παράγουν συνεχή έξοδο σε σχέση με τη μετρούμενη ποσότητα, ενώ οι ψηφιακοί λειτουργούν με διακριτά δεδομένα, όπως τα ψηφιακά bits, για τη μετάδοση και επεξεργασία των πληροφοριών.

Με βάση τα παραπάνω , οι αισθητήρες διακρίνονται για παράδειγμα σε :

Εικόνα 9 Διάφοροι τύποι αισθητήρων

- Αισθητήρες Θερμοκρασίας : Θερμοηλεκτρικά ζεύγη ή θερμοζεύγη, Θερμίστορ Θερμόμετρα Αντίστασης (RTDs)
- Οπτικοί Αισθητήρες : Φωτοδιόδοι και φωτοτρανζίστορ, Φωτοαντιστάσεις (LDRs)
- Αισθητήρες Πίεσης και Βάρους : Χωρητικοί αισθητήρες, Επαγωγικοί αισθητήρες, Πιεζοηλεκτρικοί αισθητήρες και αισθητήρες πιεζοαντίστασης,
- Αισθητήρες Στάθμης και Όγκου
- Αισθητήρες Μετατόπισης και Κίνησης
- Αισθητήρες Χημικοί και Αερίου
- Αισθητήρες Ηλεκτρικοί και Μαγνητικοί

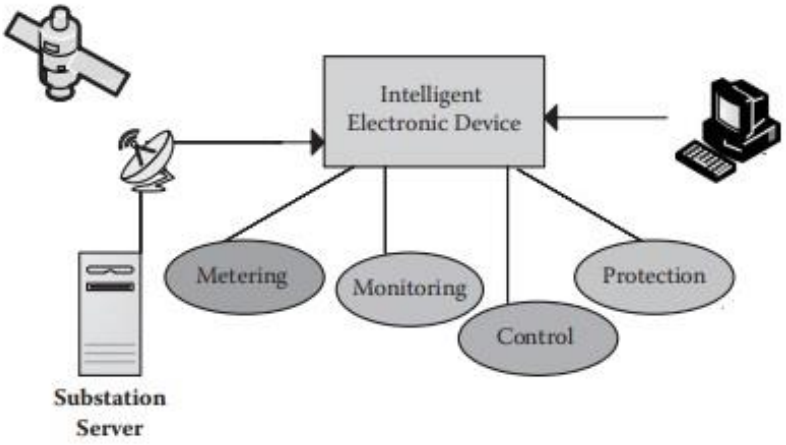
2.2.3 Ενεργοποιητές

Οι ενεργοποιητές είναι συσκευές που μετατρέπουν την ενέργεια της πηγής σε φυσική ποσότητα, όπως κίνηση ή δύναμη, ως απόκριση σε ένα σήμα ελέγχου. Αυτές οι συσκευές μπορούν να χρησιμοποιούν πνευματική, υδραυλική ή ηλεκτρική πηγή ενέργειας και η προκύπτουσα κίνηση μπορεί να είναι είτε γραμμική είτε περιστροφική. Ως συσκευές εξόδου, οι ενεργοποιητές διαδραματίζουν κρίσιμο ρόλο στην παροχή φυσικών αποκρίσεων στα σήματα ελέγχου. Για να δώσουμε ένα παράδειγμα, υπάρχουν διάφορες ποικιλίες ενεργοποιητών:

- Ηλεκτρικοί κινητήρες
- Θερμαντήρες
- Ηλεκτροπνευματικός ενεργοποιητής
- Ηλεκτροϋδραυλικός ενεργοποιητής
- Μαγνητικός ενεργοποιητής κλπ

2.2.4 IED's

Οι ευφυείς ηλεκτρονικές συσκευές (IED) σύμφωνα με τον τυποποιημένο ορισμό είναι "Κάθε συσκευή που ενσωματώνει έναν ή περισσότερους επεξεργαστές με δυνατότητα λήψης ή αποστολής δεδομένων/ελέγχου από ή προς μια εξωτερική πηγή" ή μπορούν να οριστούν απλά ως ευφυείς αισθητήρες ή ενεργοποιητές. Αυτές οι συσκευές έχουν την ικανότητα να εκτελούν εργασίες συλλογής δεδομένων, επικοινωνίας, ελέγχου και διεργασιών.



Εικόνα 10

Τα IED (Intelligent Electronic Devices) αντιπροσωπεύουν μια εξέλιξη στον τομέα του αυτοματισμού ισχύος. Αυτές οι συσκευές έχουν ενσωματωμένη ευφυΐα και μικροεπεξεργαστές, παρέχοντας υψηλή ολοκλήρωση και δυνατότητες διαλειτουργικότητας. Η εμφάνισή τους στις αρχές της δεκαετίας του 1980 σηματοδοτεί έναν σημαντικό άλμα στην τεχνολογία του ελέγχου και του αυτοματισμού στον τομέα της ηλεκτρικής ενέργειας. Η ανάπτυξη των IEDs έφερε επανάσταση στην προστασία, στον αυτοματισμό υποσταθμών διανομής, καθώς και στις λειτουργίες συλλογής και ανάλυσης δεδομένων των επιχειρήσεων. Η ανάπτυξη της υποδομής επικοινωνίας, η τυποποίηση των πρωτοκόλλων και η διαλειτουργικότητα ήταν σημαντικοί παράγοντες που οδήγησαν στην έκρηξη των IED. Οι IED, ή οι Ευφυείς Ηλεκτρονικές Συσκευές, χρησιμεύουν ως αισθητήρια και εκτελεστικά στοιχεία ενός πολύπλοκου δικτύου συστημάτων αυτοματισμού. Αυτές οι συσκευές διαθέτουν ολοκληρωμένες ικανότητες παρακολούθησης και ελέγχου και μπορούν να επιβλέπουν με επιτυχία τους υποσταθμούς μέσω της ανάλυσης αναφορών δεδομένων σχετικά με σφάλματα. Αξιοποιώντας πλήρως τις δυνατότητες των IED, ο κίνδυνος εσφαλμένης ενεργοποίησης κυκλωμάτων μπορεί να αποφευχθεί πλήρως.

2.3 Προγραμματιζόμενοι Λογικοί Ελεγκτές

Το 1968, η General Motors Company ήταν η πρώτη που χρησιμοποίησε τον όρο σε σχέση με το σχεδιασμό ψηφιακών συστημάτων που θα μπορούσαν να προγραμματίσουν και να αντικαταστήσουν τα πάνελ αυτοματισμού. Τα πάνελ αρχικά χρησιμοποιούσαν ρελέ και ηλεκτρονικές πλακέτες που αποτελούνταν από AND, OR και άλλες λογικές πύλες. Η Ένωση Κατασκευαστών Ηλεκτρονικού Εξοπλισμού των Ηνωμένων Πολιτειών (National Electrical Manufacturers Association) εξέδωσε αργότερα μια πιο συγκεκριμένη ερμηνεία που ορίζει τόσο την τεχνική κατασκευής προγραμματιζόμενων λογικών ελεγκτών όσο και τους τομείς εφαρμογής τους. Σύμφωνα με αυτή την ερμηνεία, ένας προγραμματιζόμενος λογικός ελεγκτής είναι μια ψηφιακή ηλεκτρονική συσκευή που έχει προγραμματιζόμενη μνήμη και είναι ικανή να εκτελεί λειτουργίες λογικής, ακολουθίας, χρόνου, μέτρησης και αριθμητικής αποθήκευσης εντολών. Αυτές οι λειτουργίες επιτρέπουν τον αυτόματο έλεγχο μηχανών και διαδικασιών[6].

Εικόνα 11 PLC και συστημα I/O

2.3.1 Αρχές Λειτουργίας των Προγραμματιζόμενων Λογικών Ελεγκτών

Οι προγραμματιζόμενοι λογικοί ελεγκτές αποτελούνται από τρία βασικά στοιχεία: το υλικό, το λειτουργικό σύστημα (ή υλικολογισμικό) και το λογισμικό. Η αρχιτεκτονική του υλικού είναι η θεμελιώδης περιγραφή των βασικών στοιχείων που το αποτελούν και του τρόπου διασύνδεσής τους για τη διευκόλυνση της ροής των δεδομένων. Από την άλλη πλευρά, το λειτουργικό σύστημα είναι υπεύθυνο για τη διαχείριση των στοιχείων υλικού και την εκτέλεση του λογισμικού εφαρμογής.

Οι προγραμματιζόμενοι ελεγκτές χρησιμοποιούνται ευρέως σε διάφορες βιομηχανίες, όπως χαλυβουργεία, εργοστάσια χαρτοπολτού και χαρτιού, εργοστάσια επεξεργασίας τροφίμων, χημικά και πετροχημικά εργοστάσια, αυτοκινητοβιομηχανία και εργοστάσια παραγωγής ενέργειας. Αυτοί οι ελεγκτές χρησιμοποιούνται για βασικούς αυτοματισμούς σε αυτά τα πεδία. Οι προγραμματιζόμενοι ελεγκτές λειτουργούν με διάφορους τρόπους,

συμπεριλαμβανομένου του διαδοχικού και μεταγωγής (ON/OFF) ελέγχου μηχανών και διεργασιών, ελέγχου κλειστού βρόχου μιας ή περισσότερων μεταβλητών και αλληλοκλειδώματος (interlocks) μεταβλητών σε ασφαλείς τιμές. Για να καλύψει τόσο τις παραδοσιακές όσο και τις σύγχρονες ανάγκες, ένας προγραμματιζόμενος ελεγκτής πρέπει να ολοκληρώσει όλες τις λειτουργίες μέσα σε ένα καθορισμένο χρονικό πλαίσιο. Επιπλέον, το υλικό ενός συστήματος δεν είναι ο μόνος σημαντικός παράγοντας που πρέπει να ληφθεί υπόψη. Εξίσου σημαντική είναι η ικανότητα του συστήματος να συνδέεται με αισθητήρες και ενεργοποιητές στα τελικά στάδια παραγωγής χωρίς να απαιτείται η κατασκευή ή η χρήση πρόσθετων κυκλωμάτων. Οι σύγχρονοι ελεγκτές ικανοποιούν αυτήν την απαίτηση χρησιμοποιώντας μια αρχιτεκτονική υλικού που αποτελείται από δύο κύρια στοιχεία: την Κεντρική Μονάδα Επεξεργασίας (CPU) και τα κυκλώματα εισόδου και εξόδου (I/O). Η CPU περιλαμβάνει τρεις ξεχωριστές μονάδες: τον επεξεργαστή, τη μνήμη και το τροφοδοτικό.

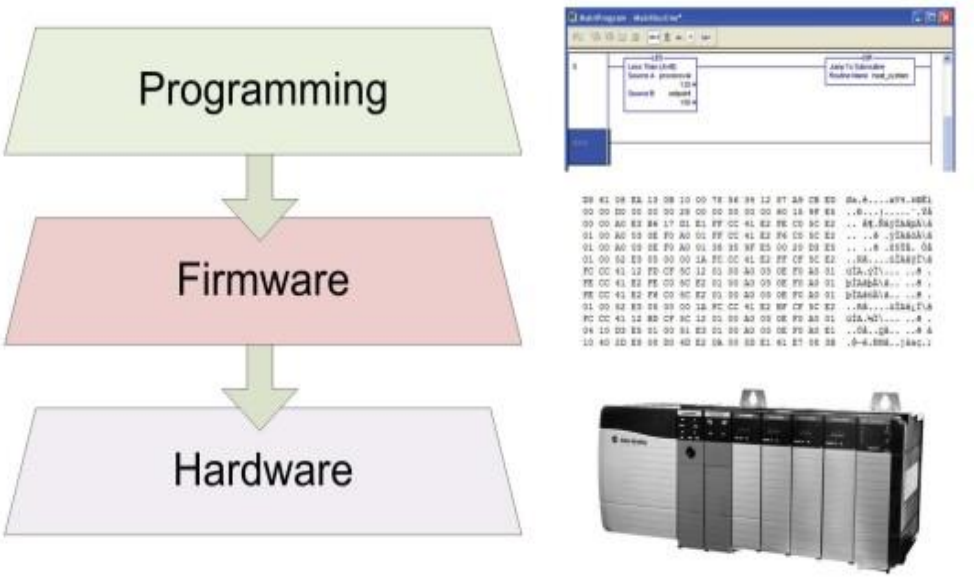
Ο ρόλος κάθε μονάδας του προγραμματιζόμενου ελεγκτή περιγράφεται συνοπτικά παρακάτω. Η ΚΜΕ είναι υπεύθυνη για τη λήψη δεδομένων απο τους αισθητήρες, την εκτέλεση του λογισμικού εφαρμογής που είναι αποθηκευμένο στη μνήμη και τη μετάδοση των απαραίτητων εντολών για τον έλεγχο των μεταβλητών. Η διαδικασία της ανάγνωσης των αισθητήρων, της εκτέλεση του προγράμματος εφαρμογής και της έκδοσης εντολών, εκτελείται με συνεχή και κυκλικό τρόπο, που πραγματοποιείται επανειλημμένα από το λειτουργικό σύστημα.

Η παροχή ηλεκτρικής ενέργειας που είναι απαραίτητη για τη λειτουργία του επεξεργαστή, της μνήμης και των κυκλωμάτων εισόδου/εξόδου είναι ευθύνη του τροφοδοτικού. Η μεταφορά πληροφοριών από τους αισθητήρες στην CPU, ή αντίστροφα, διευκολύνεται από τα κυκλώματα εισόδου/εξόδου. Αυτά τα κυκλώματα μετατρέπουν τα σήματα που λαμβάνονται από τους αισθητήρες σε μορφή που μπορεί να διαβαστεί από την κεντρική μονάδα επεξεργασίας. Ομοίως, μετατρέπουν τις εντολές που δίνει η CPU σε σήματα που έχουν τη δύναμη να επηρεάσουν τα τελικά στοιχεία του συστήματος. Αυτή η διαδικασία μετατροπής είναι ζωτικής σημασίας για τη διασφάλιση ομαλής επικοινωνίας μεταξύ των διαφορετικών στοιχείων του συστήματος. Τα κυκλώματα I/O εκτελούν μια ποικιλία λειτουργιών, συμπεριλαμβανομένης της αλλαγής των ηλεκτρικών χαρακτηριστικών των διακριτών σημάτων, της περιοδικής δειγματοληψίας αναλογικών σημάτων και της μετατροπής των τιμών του δείγματος σε ψηφιακά σήματα. Επιπλέον, απομονώνουν ηλεκτρικά τα ευαίσθητα ψηφιακά κυκλώματα της Κ.Μ.Ε, προστατεύοντάς την από υπερτάσεις που προκαλούνται από τοπικά ηλεκτρομαγνητικά πεδία.

Ο προγραμματιστής είναι ένα ουσιαστικό εργαλείο για την αποτελεσματική χρήση ενός προγραμματιζόμενου λογικού ελεγκτή, παρόλο που δεν αποτελεί φυσικό μέρος του ίδιου του ελεγκτή. Συνήθως, αυτό το εργαλείο έχει τη μορφή προσωπικού υπολογιστή γενικής χρήσης που έχει φορτωθεί με λογισμικό σχεδιασμένο για τον προγραμματισμό του ελεγκτή. Ωστόσο, σε ένα ολοκληρωμένο σύστημα βιομηχανικού ελέγχου, οποιοσδήποτε υπολογιστής εντός του συστήματος που επικοινωνεί απευθείας με την CPU του προγραμματιζόμενου ελεγκτή, είτε απευθείας είτε μέσω τοπικού δικτύου, μπορεί να χρησιμεύσει ως προγραμματιστής. Ουσιαστικά, η συσκευή προγραμματισμού επιτρέπει στο χρήστη να γράψει τον πηγαίο κώδικα για το πρόγραμμα εφαρμογής του σε μία ή πολλές γλώσσες, να τον μεταγλωττίσει σε γλώσσα μηχανής, να φορτώσει τον αντικείμενο κώδικα στη μνήμη του

ελεγκτή και τη βηματική ή τμηματική παρακολούθηση της εκτέλεσης του προγράμματος για σκοπούς εντοπισμού σφαλμάτων [7-9].

2.3.2 Η δομή του προγραμματιζόμενου λογικού ελεγκτή



Εικόνα 12 Διαδικασία λειτουργιας PLC

2.3.2.1 Στρώμα υλικού (hardware layer).

Το PLC (Προγραμματιζόμενος Λογικός Ελεγκτής) αποτελεί μια εξειδικευμένη αρχιτεκτονική υπολογιστικών συστημάτων. Συνήθως, αποτελείται από έναν μικροεπεξεργαστή, πτητική και μη πτητική μνήμη (RAM και ROM), εκτεταμένο αποθηκευτικό χώρο για τη λογική προγραμματισμού (μνήμη flash), τροφοδοσία ρεύματος, και πρόσθετους μικροελεγκτές που διαχειρίζονται συσκευές εισόδου και εξόδου. Ο ελεγκτής μπορεί να λειτουργεί αυτόνομα ή να ενσωματώνεται σε ένα σύστημα "ραφιού" μαζί με άλλες συσκευές.

Κεντρική Μονάδα Επεξεργασίας-CPU

Η CPU, ή η Κεντρική Μονάδα Επεξεργασίας, είναι υπεύθυνη για την υλοποίηση, την αποθήκευση και την εκτέλεση της λογικής του προγράμματος. Επιπλέον, επιβλέπει την κίνηση των πληροφοριών εντός του PLC. Για περισσότερες λεπτομέρειες, η CPU συλλέγει πληροφορίες από τους αισθητήρες και τα όργανα μέτρησης που συνδέονται με τις εισόδους του PLC. Με αυτά τα δεδομένα, προχωρά στην εκτέλεση του αποθηκευμένου προγράμματος για την αξιολόγηση των παρεχόμενων πληροφοριών και το συμπέρασμα σχετικά με την κατάλληλη πορεία δράσης. Τελικά, κατευθύνει τις εντολές του προγράμματος στις συσκευές ελέγχου που είναι συνδεδεμένες με τις εξόδους του PLC.

Η Κεντρική Μονάδα Επεξεργασίας αποτελείται από έναν ή περισσότερους μικροεπεξεργαστές και μπορεί να περιέχει συμπληρωματική μνήμη καθώς και κυκλώματα επικοινωνίας με τα υπόλοιπα μέρη του προγραμματιζόμενο λογικό ελεγκτή . Ο

μικροεπεξεργαστής είναι ένα είδος ημιαγωγού που έχει σχεδιαστεί για να έχει όλες τις απαραίτητες λειτουργίες ενός υπολογιστή ενσωματωμένες σε αυτόν. Αυτές οι λειτουργίες πραγματοποιούνται, εκτελώντας ένα πρόγραμμα που ονομάζεται λειτουργικό σύστημα. Οι βασικές λειτουργίες του μικροεπεξεργαστή είναι:

- Λειτουργίες εισόδων/εξόδων (I/O) : Επικοινωνία του μικροεπεξεργαστή με τα υπόλοιπα μέρη της κεντρικής μονάδας επεξεργασίας.
- Εκτέλεση τόσο αριθμητικών όσο και λογικών πράξεων.
- Διαχείριση των περιεχομένου στη μνήμη, που περιλαμβάνει δεδομένα και εντολές.

Όπως αναφέρθηκε προηγουμένως, είναι δυνατό για την ΚΜΕ να ενσωματώνει πολλαπλούς μικροεπεξεργαστές. Εάν υπάρχουν συγκεκριμένες απαιτήσεις για τη χρήση του PLC, μπορεί να χρησιμοποιηθεί μια συσκευή που συνδυάζει δύο ή τρεις μικροεπεξεργαστές που είναι σε θέση να επικοινωνούν μεταξύ τους.
Όταν ένα σύστημα περιέχει πολλούς μικροεπεξεργαστές, υποδηλώνει ότι κάθε επεξεργαστής έχει μοναδικές ευθύνες να εκπληρώσει μέσα στο σύστημα. Ο προγραμματιζόμενος λογικός ελεγκτής (PLC) βασίζεται στον μικροεπεξεργαστή ελέγχου για το σύστημα ελέγχου του. Ο μικροεπεξεργαστής ελέγχου είναι επιφορτισμένος με το χειρισμό πολύπλοκων διεργασιών που περιλαμβάνουν τον χειρισμό δεδομένων. Οι λειτουργίες του μικροεπεξεργαστή ποικίλλουν αρκετά, που κυμαίνονται από τον χρονισμό και την καταμέτρηση έως τον χειρισμό της λογικής και την εκτέλεση προγραμμάτων χρήστη. Η λογική του είναι υπεύθυνη για όλες αυτές τις λειτουργίες. Οι μικροεπεξεργαστές που είναι εξειδικευμένοι είναι σχεδιασμένοι να λειτουργούν με συγκεκριμένο τρόπο, ο οποίος μπορεί να περιλαμβάνει την εκτέλεση μαθηματικών υπολογισμών, μετρήσεων, διαγνωστικών, συναρτήσεων επικοινωνίας και άλλων σχετικών εργασιών.

Κεντρική Μνήμη

Ο πρωταρχικός σκοπός της κύριας μνήμης είναι να αποθηκεύει και να διατηρεί όλες τις πληροφορίες που σχετίζονται με το PLC. Αυτό περιλαμβάνει το λειτουργικό σύστημα, το πρόγραμμα, τις καταστάσεις εισόδου και εξόδου, καθώς και τυχόν ενδιάμεσα αποτελέσματα ή πληροφορίες που σχετίζονται με το πρόγραμμα.
Ο μικροεπεξεργαστής χρησιμοποιεί bytes ως τη μικρότερη μονάδα πληροφοριών στις εντολές του για την οργάνωση της μνήμης. Κάθε byte αποτελείται από 8 bit, τα οποία χρησιμεύουν ως τα πιο βασικά στοιχεία των πληροφοριών. Αυτά τα bit μπορούν να αποδοθούν είτε με τιμή μηδέν (0) είτε τιμή ενός (1).
Οι μνήμες μπορούν να ταξινομηθούν σε δύο κύριες κατηγορίες. Η πρώτη κατηγορία αποτελείται από μνήμες που είναι ασταθείς ή απαιτούν πηγή ενέργειας για τη διατήρηση των αποθηκευμένων πληροφοριών τους. Η δεύτερη κατηγορία αποτελείται από μνήμες που είναι μη ασταθείς και ικανές να διατηρούν το περιεχόμενό τους για αόριστο χρονικό διάστημα. Επιπλέον, υπάρχουν διάφορες υποκατηγορίες μνήμης που ισχύουν για προγραμματιζόμενους λογικούς ελεγκτές (PLC)Q

- Μνήμη τυχαίας προσπέλασης (Random Access Memory-RAM): στην πτητική μνήμη αυτή αποθηκεύονται πληροφορίες του προγράμματος, ενίοτε και το ίδιο το πρόγραμμα.

- Μνήμη μόνο ανάγνωσης (Read Only Memory-ROM): τα περιεχόμενα αυτής της μη πτητικής μνήμης δεν μπορούν να τροποποιηθούν. Η μόνη λειτουργία μιας ROM είναι να επιτρέπει την ανάγνωση, καθώς όλες οι προσπάθειες αλλαγής του περιεχομένου της θα ήταν μάταιες. Αν και μπορεί να περιέχει το λειτουργικό σύστημα, δεν περιέχει το προγράμματα, καθώς αυτά υπόκεινται σε αλλαγές ανά πάσα στιγμή.
- Προγραμματιζόμενη μνήμη μόνο ανάγνωσης: είναι μια μορφή μη πτητικής μνήμης που λειτουργεί παρόμοια με τη ROM. Ωστόσο, σε αντίθεση με τη ROM, τα περιεχόμενα του PROM μπορούν να τροποποιηθούν σβήνοντάς τα πρώτα. Αυτό επιτυγχάνεται με τη λάμψη υπεριώδους φωτός σε ένα συγκεκριμένο σημείο της μνήμης, στην περίπτωση του EPROM, ή με την εφαρμογή μιας προκαθορισμένης τάσης σε μια καθορισμένη ακίδα στην περίπτωση του EEPROM. Η τελευταία κατηγορία προγραμματιζόμενης μνήμης είναι πιο ευέλικτη και απαιτεί πολύ λιγότερο χρόνο για τη διαγραφή.

Μονάδα Τροφοδοσίας

Προκειμένου να τροφοδοτηθούν τα διάφορα ηλεκτρονικά εξαρτήματα εντός του ελεγκτή, όπως πυκνωτές, τρανζίστορ και ολοκληρωμένα κυκλώματα, είναι απαραίτητο να υπάρχει μια μονάδα τροφοδοσίας για τη δημιουργία των απαραίτητων εσωτερικών τάσεων. Επιπλέον, η μονάδα τροφοδοσίας διαδραματίζει κρίσιμο ρόλο στην πρόληψη της απώλειας πληροφοριών που είναι αποθηκευμένες στη μνήμη RAM σε περίπτωση ξαφνικής διακοπής ρεύματος, χρησιμοποιώντας ένα εφεδρικό σύστημα μπαταρίας. Αυτή η μονάδα διαθέτει τρία βασικά χαρακτηριστικά, και συγκεκριμένα :

- Είσοδο: ονομαστική τάση, αποδεκτές ανοχές τάσης, συχνότητες και μέτρα προστασίας.
- Έξοδο: ονομαστική τάση, ονομαστική ρεύμα, προστασία βραχυκυκλωμάτων.
- Διάφορα : μπαταρία έτσι ώστε να μην χαθούν οι πληροφορίες της μνήμης RAM)

Για να αποφθεχθεί η απώλεια των δεδομένων που είναι αποθηκευμένα στη μνήμη RAM σε περίπτωση απροσδόκητης διακοπής ρεύματος, είναι απαραίτητο να χρησιμοποιηθεί μπαταρία.

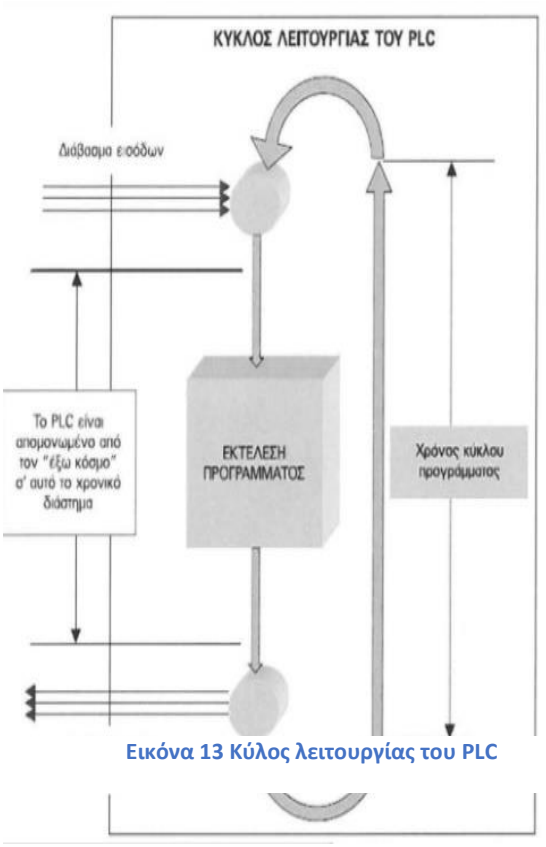
Τμήμα εισόδων/εξόδων

Το τμήμα εισόδων/εξόδων, που συνήθως συντομεύεται ως I/O, αποτελείται από δύο κύριες μονάδες: τη μονάδα διασύνδεσης εισόδου και τη μονάδα διασύνδεσης εξόδου. Η Μονάδα Διασύνδεσης Εισόδου είναι υπεύθυνη για τη μετατροπή των λαμβανόμενων πραγματικών σημάτων από τους αισθητήρες που συνδέονται με τις εισόδους των PLC σε σήματα χαμηλής ισχύος, που είναι κατάλληλα με τη ΚΜΕ. Επιπλέον, χρησιμεύει ως προστατευτικό φράγμα μεταξύ του εξωτερικού περιβάλλοντος και της ΚΜΕ χρησιμοποιώντας γαλβανική απομόνωση για την πρόληψη ζημιών που προκαλούνται από τις εισερχόμενες τάσεις και ρεύματα στις εισόδους.
Η επικοινωνία μεταξύ του τμήματος εισόδου/εξόδου και της ΚΜΕ δεν είναι σταθερή, αλλά συμβαίνει σε σταθερά διαστήματα γνωστά ως κύκλοι σάρωσης. Στην περίπτωση των

ψηφιακών εισόδων και εξόδων PLC, μπορούν να βρίσκονται μόνο σε μία από τις δύο καταστάσεις, είτε ενεργές (ON) είτε ανενεργές (OFF) και μπορούν να αναπαρασταθούν από ένα μόνο bit γνωστό ως bit κατάστασης.
Το διαθέσιμο εύρος τάσεων που μπορεί να χρησιμοποιηθεί με τις αναλογικές εισόδους και εξόδους ενός PLC ποικίλλει από (0-5) VDC, (0-10) VDC έως (-10, +10) VDC. Το πλήθος των διαφορετικών αναλογικών τάσεων που μπορεί να διαχειριστεί η κάθε μονάδα ταυτόχρονα (πλήθος καναλιών), διαφέρει από PLC σε PLC. Αξίζει να σημειωθεί ότι ο αριθμός των καναλιών εισόδου συνήθως υπερβαίνει τον αριθμό των καναλιών εξόδου.

2.3.2.2 Επίπεδο υλικολογισμικού (firmware)

Το επίπεδο υλικολογισμικού του PLC αναφέρεται στο λογισμικό που διοικεί το PLC και ελέγχει τις συσκευές εισόδου και εξόδου. Αυτό περιλαμβάνει το λειτουργικό σύστημα και το λογισμικό οδηγούς που χειρίζονται συσκευές όπως αντλίες, σωληνοειδή, ρομπότ και αισθητήρες τηλεμετρίας. Υπάρχει ένας βαθμός μεταβλητότητας στα λειτουργικά συστήματα των PLC. Ορισμένα μοντέλα παρουσιάζουν μια διεπαφή παρόμοια με τα Windows, ενώ άλλα χρησιμοποιούν ένα μονολιθικό λειτουργικό σύστημα που δεν επιτρέπει την άμεση πρόσβαση στο περιβάλλον PLC. Τα PLC λειτουργούν μέσω τεσσάρων διακριτών σταδίων σάρωσης. Αρχικά, το πρώτο στάδιο επιβλέπει διοικητικές εργασίες, όπως η επαλήθευση της ακεραιότητας I/O και η διάγνωση προβλημάτων υλικού. Αυτό το στάδιο χρησιμεύει επίσης ως χαρακτηριστικό ασφαλείας, επιτρέποντας στον χρονοδιακόπτη παρακολούθησης να σταματήσει τις λειτουργίες εάν εντοπιστούν προβλήματα. Το δεύτερο στάδιο είναι αφιερωμένο στην επεξεργασία δεδομένων εισόδου από συσκευές και στην καταγραφή μετρήσεων αισθητήρων. Το τρίτο στάδιο είναι υπεύθυνο για την εκτέλεση του πρωτεύοντος προγράμματος, ενώ το τέταρτο στάδιο εγγράφει τα αποτελέσματα των λογικών υπολογισμών στη μνήμη εξόδου, η οποία είναι υπεύθυνη για την επικοινωνία με τις συσκευές εξόδου. Αυτά τα τέσσερα στάδια επαναλαμβάνονται και αποτελούν τις βασικές λειτουργίες ενός PLC. Επιπλέον, το υλικολογισμικό του PLC είναι αναβαθμίσιμο και μπορεί να ενημερωθεί εύκολα μέσω σειριακού καλωδίου RS-232 ή σύνδεσης Ethernet. Κάποια PLC ενδέχεται να απαιτούν ειδική καλωδιακή σύνδεση, όπως το Allen Bradley Micrologix 1000, όπου απαιτείται να τοποθετηθεί το PLC σε προγραμματιζόμενη κατάσταση και να χρησιμοποιηθεί το λογισμικό και το πακέτο ενημέρωσης υλικολογισμικού του κατασκευαστή για την ενημέρωση.



Εικόνα 13 Κύλος λειτουργίας του PLC

2.3.2.3 Προγραμματιζόμενο επίπεδο

Το προγραμματιζόμενο επίπεδο του PLC μπορεί να αντιπροσωπεύεται από μια από τις πέντε γλώσσες προγραμματισμού (Ladder diagram, Structured text, Fuction Block Diagram,Instruction list, Sequential function charts), η οποία κατευθύνει το PLC να εκτελεί συγκεκριμένες λογικές εργασίες. Κατά την διάρκεια του τρίτου κύκλου σάρωσης, τα δεδομένα γράφτηκαν στον πίνακα μνήμης εισόδου. Τα δεδομένα αυτά μεταφράζονται σε εισόδους που προγραμματίζονται στην επιλεγόμενη γλώσσα . Η πρ. γλώσσα καθορίζει το είδος της εισόδου (π.χ. βαλβίδα ή μοτέρ), όπως επίσης καθορίζει το τι αντιπροσωπεύει η τιμή από την είσοδο (π.χ. on, off, true, false, time, count) και πως θα τοποθετηθεί η τιμή που προκύπτει σε μια άλλη συγκεκριμένη συσκευή (π.χ. φως αναμμένο). Αυτό το προγραμματιζόμενο στρώμα γεφυρώνει το τμήμα του λειτουργικού συστήματος του υλικολογισμικού με το ειδικό για τη συσκευή λογισμικό οδήγησης . Η δημιουργία ή ο σχεδιασμός του προγράμματος γίνεται με το ειδικό λογισμικό του κατασκευαστή, και η μεταφορά του στο PLC πραγματοποιείται με αντίστοιχο τρόπο όπως και η αναβάθμιση του υλικολογισμικού. Οι λεπτομέρειες αυτής της διαδικασίας ποικίλουν ανάλογα με τον κατασκευαστή του PLC.

2.4 RTU

Οι συσκευές ελέγχου που βασίζονται σε μικροεπεξεργαστή, οι γνωστές ως Remote Terminal Units (RTUs) συνδέονται με αισθητήρες και ενεργοποιητές σε μια διαδικασία. Ως αποτέλεσμα, οι RTU λαμβάνουν φυσικά σήματα από αισθητήρες, συμπεριλαμβανομένων, ενδεικτικά, των καταστάσεων μεταγωγής, των επαφών, του ρεύματος, της τάσης, του παλμού, της ροής και της πίεσης. Αυτά τα σήματα μετατρέπονται από τα RTU σε ψηφιακά δεδομένα, τα οποία στη συνέχεια μεταδίδονται είτε μέσω ενσύρματων ή ασύρματων πρωτοκόλλων επικοινωνίας. Τέλος, το κέντρο ελέγχου επεξεργάζεται περαιτέρω τα δεδομένα.

Το RTU επίσης μετατρέπει εισερχόμενα σήματα από άλλο RTU ή από κεντρικό υπολογιστή σε σήματα εξόδου, τα οποία με τη σειρά τους δρουν για το άνοιγμα ή το κλείσιμο των ρελέ, των βαλβίδων, καθώς και την εκκίνηση και τη διακοπή κινητήρων και άλλες σχετικές λειτουργίες.

Οι συνθήκες υπό τις οποίες αναμένεται να εκτελούν τις λειτουργίες τους οι απομακρυσμένες τερματικές μονάδες (RTU) είναι συχνά σκληρές και απαιτητικές. Ως εκ τούτου, ο σχεδιασμός των RTU πραγματοποιείται με αυστηρές προδιαγραφές για τη διασφάλιση της ανθεκτικότητας και της αξιοπιστίας τους. Ένα κρίσιμο ζήτημα για την τροφοδοσία των RTU που βρίσκονται σε απομακρυσμένες τοποθεσίες είναι η εξοικονόμηση ενέργειας. Για να μεγιστοποιηθεί η απόδοση, χρησιμοποιούνται συνήθως τεχνικές εξοικονόμησης ενέργειας, όπως η αναστολή του επεξεργαστή και η ενεργοποίησή του μόνο όταν ανιχνεύεται αλλαγή κατάστασης. Επιπλέον, οι RTU μπορούν να εξοπλιστούν με εφεδρικά συστήματα ισχύος, όπως φωτοβολταϊκά πάνελ για την αποφυγή απροσδόκητων διακοπών λόγω αστοχιών της κύριας γραμμής.

Το Ladder, το FBD (Function Block Diagram) και το ST (Structure Text) είναι μερικές από τις γλώσσες προγραμματισμού που χρησιμοποιούνται στα RTU.

2.4.1 Σύγκριση RTUs και PLCs

Οι κοινές συναρτήσεις μεταξύ των RTU και των PLC είναι πολυάριθμες, καθώς πολλά RTU έχουν ενσωματώσει τις ίδιες λειτουργίες που βρίσκονται στα PLC και το αντίστροφο. Ωστόσο, είναι σημαντικό να σημειωθεί ότι οι RTU έχουν τις δικές τους μοναδικές λειτουργίες.

- Τείνουν να παρέχουν περισσότερες δυνατότητες σε σύγκριση με τους προγραμματιζόμενους λογικούς ελεγκτές (PLC), ιδιαίτερα όσον αφορά τη μετάδοση μετρήσεων και εντολών προς και από απομακρυσμένες τοποθεσίες.
- Διαθέτουν ενσωματωμένα modems σε αντίθεση με τα περισσότερα PLCs.
- Έχουν σχεδιαστεί για να ξεκινούν αμέσως μόλις τεθούν υπό τάση, κάτι που δεν συμβαίνει στα PLCs.
- Το κόστος ανά σημείο εισόδου/εξόδου για μια απομακρυσμένη τερματική μονάδα είναι χαμηλότερο από αυτό ενός προγραμματιζόμενου λογικού ελεγκτή.

Τα PLC, ωστόσο, παρουσιάζουν μια διαφορετική προοπτική :

- Όταν πρόκειται για τον τοπικό έλεγχο βιομηχανικών διαδικασιών τα PLC είναι πιο αποτελεσματικά από τα RTUs.
- Ένα από τα κύρια χαρακτηριστικά αυτών είναι ότι προγραμματίζονται ώστε να εκτελούν περίπλοκες διαδικασίες ελέγχου χωρίς ανθρώπινη παρέμβαση. Αυτή η συγκεκριμένη ικανότητα δεν είναι τόσο διαδεδομένη στα RTU.

Τα PLC προσφέρουν ξεχωριστά πλεονεκτήματα έναντι των RTU. Αυτά περιλαμβάνουν αυξημένη ευελιξία, ανώτερες επιλογές διαμόρφωσης και μειωμένο κόστος.

2.4.2 Συνεργασία RTUs και PLCs

Η αρμονική συνεργασία μεταξύ των Remote Terminal Units (RTUs) και των Programmable Logic Controllers (PLC) είναι ζωτικής σημασίας στις σύγχρονες βιομηχανικές λειτουργίες. Η αποτελεσματική λειτουργία αυτών των συστημάτων εξαρτάται από την ικανότητά τους να εργάζονται από κοινού προς έναν κοινό στόχο. Σε περιπτώσεις όπου υπάρχει ανάγκη για αυτοματοποιημένο έλεγχο σε ένα δεδομένο σημείο, μια επιλογή είναι να ενσωματωθεί ένας προγραμματιζόμενος λογικός ελεγκτής (PLC) σε μια απομακρυσμένη τερματική μονάδα (RTU). Η λειτουργία του PLC είναι να αναλάβει τη λήψη τόσο ψηφιακών όσο και αναλογικών σημείων ρύθμισης (setpoints) από το RTU. Το RTU χρησιμοποιείται κυρίως για τη μετάδοση πληροφοριών, την έκδοση απομακρυσμένων εντολών και τα σημεία ρύθμισης. Σε αυτό το σενάριο, το συνοδευτικό PLC αναλαμβάνει το έργο της διαχείρισης του τοπικού ελέγχου.

2.5 Δίκτυο

Η ύπαρξη συστήματος SCADA είναι δυνατή μόνο με την παρουσία ενός καλά σχεδιασμένου συστήματος δικτύου επικοινωνίας. Κάθε πτυχή του εποπτικού ελέγχου και της απόκτησης δεδομένων εντός του συστήματος SCADA εξαρτάται εξ ολοκλήρου από τη λειτουργικότητα του συστήματος επικοινωνίας. Σε ένα σύστημα SCADA, τα δεδομένα συλλέγονται από

απομακρυσμένους αισθητήρες και συσκευές και διαβιβάζονται σε ένα κεντρικό σταθμό , όπου παρακολουθούνται και αναλύονται. Τα δεδομένα αυτά μπορεί να περιλαμβάνουν πληροφορίες σχετικά με τη θερμοκρασία, την πίεση, τους ρυθμούς ροής και άλλες παραμέτρους. Το δίκτυο επικοινωνίας είναι υπεύθυνο για τη μετάδοση αυτών των δεδομένων σε πραγματικό ή σχεδόν πραγματικό χρόνο από τις απομακρυσμένες συσκευές στο κέντρο ελέγχου. Οι εξελίξεις στον τομέα της επικοινωνίας έχουν βοηθήσει σημαντικά την επικοινωνία SCADA, καθώς με την πάροδο των ετών έχουν αναπτυχθεί νέες τεχνολογίες. Η ανάπτυξη του διαδικτύου και του υλικού έχουν συνεισφέρει σημαντικά στην επικοινωνία, επιτρέποντας την επίτευξη υψηλότερων επιπέδων ταχύτητας και ακρίβειας με μειωμένο κόστος. Ο σχεδιαστής του συστήματος μπορεί να επιλέξει μια ποικιλία μέσων επικοινωνίας ανάλογα με την ταχύτητα και τις απαιτήσεις μεταφοράς δεδομένων. Κατά την επιλογή μιας μορφής επικοινωνίας, πρέπει να λαμβάνονται υπόψη αρκετοί κρίσιμοι παράγοντες. Αυτοί οι παράγοντες περιλαμβάνουν την απόσταση μεταξύ των συσκευών, το απαιτούμενο επίπεδο αξιοπιστίας του μέσου επικοινωνίας, τη διαθεσιμότητα επιλογών επικοινωνίας, το κόστος κάθε επιλογής για μια συγκεκριμένη εφαρμογή και τη διαθεσιμότητα πηγών ενέργειας. Η εφαρμογή αυτών των μεθόδων επικοινωνίας μπορεί να επιτευχθεί με τη χρήση καλωδίων, τηλεφωνικών γραμμών ή ραδιοσυχνοτήτων (RF).

Το δίκτυο επικοινωνίας σε ένα σύστημα SCADA είναι κρίσιμο για τη λειτουργία του, καθώς τυχόν διαταραχές ή αστοχίες μπορεί να οδηγήσουν σε καθυστερήσεις στη μετάδοση δεδομένων ή σε απώλεια κρίσιμων πληροφοριών, οι οποίες με τη σειρά τους μπορεί να επηρεάσουν την ασφάλεια και την αποτελεσματικότητα του συστήματος.

Για την ανάπτυξη του Δικτυού Επικοινωνίας χρησιμοποιείται ένας από τους παρακάτω τρόπους:

2.5.1 Καθοδηγούμενα (ενσύρματα) μέσα

Συνεστραμμένου Ζεύγους - (Twisted Pair)

Εικόνα 14 Συνεστραμμενιου ζεύγους - 4 ζευγών

Το καλώδιο τηλεπικοινωνιών συνεστραμμένου ζεύγους χρησιμοποιείται εδώ και πολλά χρόνια , από τις επιχειρήσεις κοινής ωφέλειας και υπάρχει στη σημερινή του μορφή για πολλά χρόνια. Τα καλώδια που αναφέρεστε είναι παρόμοια με αυτά που χρησιμοποιούνται από τις τηλεφωνικές εταιρείες και ανήκουν στην κατηγορία των συνεστραμμένων ζευγών. Κάθε ζεύγος αγωγών περιέχει έναν μεταλλικό (συνήθως χάλκινο) αγωγό με πλαστική μόνωση, όπου το ένα από αυτά χρησιμοποιείται για την αποστολή του σήματος στον δέκτη, ενώ το άλλο αποτελεί σημείο αναφοράς γείωσης.

Η δομή του συνεστραμμένου ζεύγους είναι σχεδιασμένη έτσι ώστε να αντιμετωπίζει την παρεμβολή θορύβου εξίσου στα δύο καλώδια. Ένα σημαντικό πλεονέκτημα είναι ότι στην

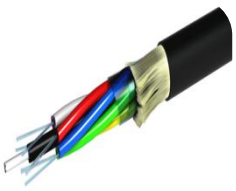
πλευρά του δέκτη, τα ανεπιθύμητα σήματα μπορούν να ακυρωθούν σχεδόν πλήρως, καθώς ο δέκτης υπολογίζει τη διαφορά μεταξύ των δύο αγωγών.
Ωστόσο, πρέπει να σημειωθεί ότι το συνεστραμμένο ζεύγος καλωδίων κατάλληλο για μικρές αποστάσεις και μπορεί να υποστηρίξει χωρητικότητα καναλιού μέχρι 1,54 MHz. Παρ' όλα αυτά, πρέπει να ληφθούν υπόψη πιθανά μειονεκτήματα, όπως τα θέματα θραύσης και εισροής νερού. Επιπλέον, η εντοπισμός βλαβών σε αυτό τον τύπο καλωδίων μπορεί να είναι δύσκολος, και υπάρχει δυνατότητα δυναμικής γείωσης λόγω σφαλμάτων ρεύματος και κεραυνών.

Ομοαξονικό μεταλλικό καλώδιο - (Coaxial Cable)

Εικόνα 15 Ομοαξονικό μεταλλικό καλώδιο

Το ομοαξονικό καλώδιο είναι ένα είδος καλωδίου που χρησιμοποιείται για τη μεταφορά σήματων υψηλών συχνοτήτων. Αποτελείται από έναν κεντρικό αγωγό (πυρήνα) κατασκευασμένο από συμπαγές ή πολύκλωνο σύρμα, στον οποίο περιβάλλεται από μια πλαστική μόνωση. Ο πυρήνας αυτός περικλείεται από έναν εξωτερικό μεταλλικό αγωγό που λειτουργεί ως θωράκιση και δεύτερος αγωγός. Το καλώδιο προστατεύεται από ένα πλαστικό κάλυμμα.
Το ομοαξονικό καλώδιο έχει μια ποικιλία εφαρμογών, συμπεριλαμβανομένων τόσο των αναλογικών όσο και των ψηφιακών τηλεφωνικών δικτύων. Ωστόσο, η χρήση ομοαξονικού καλωδίου στις τηλεφωνικές υπηρεσίες έχει μειωθεί με την πάροδο του χρόνου, καθώς έχει αντικατασταθεί από καλώδια οπτικών ινών.
Ο τρόπος εγκατάστασης του ομοαξονικού καλωδίου μπορεί να είναι υπόγειος, εναέριος, άμεση ταφή ή στα πλαίσια υπάρχοντα δίκτυα μεταφοράς ηλεκτρικής ενέργειας.
Παρέχει περιορισμένη απαίτηση εύρους ζώνης, είναι οικονομικό για μικρές αποστάσεις, και έχει μεγάλη ανοσία στις παρεμβολές θορύβου RF, καθιστώντας το κατάλληλο για σύνδεση σε σημείο-προς-σημείο επικοινωνία. Τα μέσα αυτά υποστηρίζουν συνήθως φωνή, δεδομένα, αναμετάδοση πλαισίων, μεταγωγικές υπηρεσίες T1, μεταγωγικές υπηρεσίες πολυμεσικών δεδομένων (SMDS), κλασσικές T1, και διακλαδώσεις μεταξύ γραφείων. Τα μειονεκτήματα του ομοαξονικού καλωδίου μοιάζουν με αυτά των συνεστραμμένων ζευγών. [1]

Οπτική ίνα (Fiber Optic Cable)



Εικόνα 16 Οπτική ίνα

Ένα καλώδιο οπτικών ινών παρασκευάζεται από γυαλί ή πλαστικό και μεταφέρει σήματα με τη μορφή φωτός. Αυτό το μέσο προσφέρει ευρύ εύρος ζώνης και είναι ανθεκτικό στις ηλεκτρομαγνητικές παρεμβολές. Οι φυσικές ιδιότητες των οπτικών ινών εξαρτώνται από τον τρόπο διάδοσης του φωτός. Η τρέχουσα τεχνολογία υποστηρίζει single mode και multi-mode. Λόγω της περιορισμένης απόστασης και των

χαρακτηριστικών εύρους ζώνης του multimode, η ζήτηση για single-mode ίνα υπερβαίνει αυτή του multimode. Η ίνα μονής λειτουργίας υποστηρίζει υψηλότερες ταχύτητες μετάδοσης σήματος λόγω της μικρότερης διαμέτρου της. Η φυσική δομή ενός καλωδίου αποτελείται από έναν πυρήνα στο κέντρο και μια εξωτερική επένδυση που το προστατεύει και το υποστηρίζει από φυσική φθορά και παρεμβολές.

Από την αρχή της το 1970, η τεχνολογία οπτικών ινών έχει υποστεί σημαντικές προόδους. Σήμερα, οι ίνες που είναι διαθέσιμες στην αγορά έχουν απώλειες μικρότερες από 0,3 dB/km. Οι χαμηλές απώλειες, σε συνδυασμό με τη δημιουργία κατάλληλων λέιζερ και οπτικών ανιχνευτών, επέτρεψαν στους σχεδιαστές να διερευνήσουν τη δυνατότητα χρήσης τεχνολογίας οπτικών ινών για συστήματα μεγάλης εμβέλειας που εκτείνονται πάνω από 140 km χωρίς να χρειάζεται να χρησιμοποιούν επαναλήπτες.

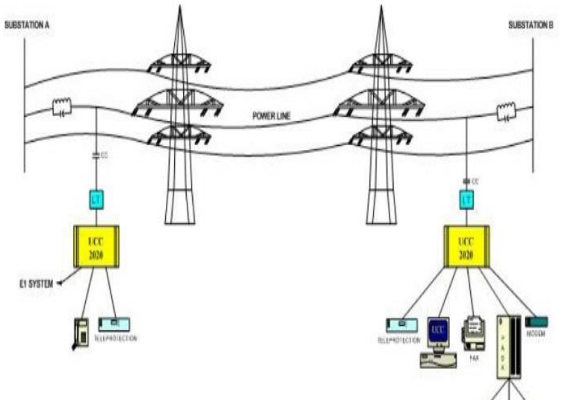
Υποστηρίζει υπηρεσίες επικοινωνίας όπως φωνή, ηλεκτρονόμηση προστασίας, τηλεμέτρηση, EMS/SCADA, τηλεδιάσκεψη, δεδομένα υψηλής ταχύτητας και τηλεφωνικές συνδέσεις.

Υπάρχουν τρεις διαφορετικοί τύποι καλωδίων οπτικών ινών για χρήση σε συστήματα SCADA. Το ένα είναι το οπτικό καλώδιο γείωσης ισχύος (OPGW- Optical Power Ground Wire) που έχει πυρήνα οπτικής ίνας μέσα στο καλώδιο γείωσης ή θωράκισης που αναρτάται πάνω από τις γραμμές μεταφοράς. Το πλήρως διηλεκτρικό αυτοφερόμενο καλώδιο (ADSS - All-Dielectric Self-Supporting) αποτελεί έναν τύπο καλωδίου που μπορεί να στερεώνεται σε πυλώνες γραμμών μεταφοράς υψηλής τάσης, χωρίς την ανάγκη για επιπρόσθετους αγωγούς. Ένας άλλος τύπος καλωδίου είναι το τυλιγμένο οπτικό καλώδιο (WOC - Wrapped Optical Cable), που συνήθως τυλίγεται γύρω από τον αγωγό φάσης ή την υπάρχουσα γείωση-καλώδιο της γραμμής μεταφοράς. Το εναέριο καλώδιο οπτικών ινών μπορεί να στερεωθεί στους πυλώνες διανομής κάτω από τις γραμμές ηλεκτρικής ενέργειας.

Οι οπτικές ίνες έχουν αρκετά αξιοσημείωτα πλεονεκτήματα που αξίζει να επισημανθούν. Πρώτον, μπορεί να λειτουργήσει με υψηλή χωρητικότητα καναλιού και χαμηλό κόστος χωρίς να χρειάζεται άδεια. Επιπλέον, τα οπτικά καλώδια είναι γνωστό ότι είναι αδιαπέραστα από ηλεκτρομαγνητικές παρεμβολές και προβλήματα γείωσης. Επιπλέον, σε σύγκριση με τα αντίστοιχα χάλκινα, είναι ελαφρύτερα και πιο ανθεκτικά στις φυσικές καταστροφές. Τα μειονεκτήματα είναι, ότι πρόκειται για νέα τεχνολογία και πρέπει να διδαχθούν νέες δεξιότητες, απαιτεί ακριβό εξοπλισμό δοκιμών. Επίσης το καλώδιο μπορεί να υποστεί θραύση και προβλήματα διαρροής νερού. [1]

Φορέας γραμμής ισχύος (PLC)

Το Power Line Carrier (PLC) αποτελούσε ένα από τα πρώτα αξιόπιστα μέσα επικοινωνίας που ήταν διαθέσιμα για τις ηλεκτρικές εταιρείες κοινής ωφέλειας. Χρησιμοποιούσε τις γραμμές μεταφοράς ηλεκτρικής ενέργειας για να μεταδίδει σήματα ραδιοσυχνοτήτων και ήταν κρίσιμο για τα κανάλια επικοινωνίας που δεν μπορούσαν να βασιστούν σε μισθωμένα τηλεφωνικά μέσα λόγω ανοχής και



Εικόνα 17 Παράδειγμα ενός φορεα γραμμής ισχύος

αναξιοπιστίας. Δεδομένου ότι οι αγωγοί μεταφοράς ρεύματος του συστήματος ηλεκτρικής ενέργειας προσφέρουν ένα ισχυρό, αξιόπιστο και οικονομικό σύνδεσμο για τις επικοινωνίες του συστήματος ηλεκτρικής ενέργειας, τα συστήματα PLC χρησιμοποιούνται για εφαρμογές αναμετάδοσης και ελέγχου του συστήματος ηλεκτρικής ενέργειας από τη δεκαετία του 1940. Τα συστήματα PLC (Programmable Logic Controller) είναι σχεδιασμένα να λειτουργούν με δυαδικό τρόπο, με λειτουργίες είτε "on" ή "off". Αυτά τα συστήματα χρησιμοποιούν επίσης σήματα ραδιοσυχνοτήτων στην περιοχή από 10 έως 500 kHz, τα οποία μεταδίδονται μέσω των γραμμών μεταφοράς ηλεκτρικής ενέργειας. Ο εξοπλισμός PLC βρίσκεται συνήθως εντός του υποσταθμού, εξασφαλίζοντας μέγιστη ασφάλεια. Τα στοιχεία στα οποία αναφερόμαστε περιλαμβάνουν τους ακροδέκτες πομπού και δέκτη, συσκευές αντιστοίχισης σύνθετης αντίστασης, ομοαξονικό καλώδιο και πυκνωτή ζεύξης, τα οποία είναι απαραίτητα για την έγχυση σήματος υψηλής συχνότητας στη γραμμή διανομής. Επιπλέον, εγκαθίστανται παγίδες γραμμής στον αγωγό τροφοδοσίας για να αποτρέψουν την είσοδο σημάτων στον υποσταθμό μέσω ακούσιων διαδρομών. Αυτό το σύστημα μετάδοσης έχει την ικανότητα να υποστηρίζει διάφορες υπηρεσίες όπως φωνή, τηλεμετρία, SCADA και αναμετάδοση.
Το διασυνδεδεμένο δίκτυο μεταφοράς ισχύος λειτουργεί στα 220/230 kV, 110/115 kV ή 66 kV και μπορεί να επιτύχει μέγιστο ρυθμό μετάδοσης δεδομένων έως και 9600 baud.
Ένα σημαντικό μειονέκτημα του PLC είναι η εξάρτησή του από ηλεκτροφόρα καλώδια, γεγονός που μπορεί να δημιουργήσει πρόβλημα σε περιοχές όπου η τροφοδοσία είναι αναξιόπιστη. Επιπλέον, η περιορισμένη διαθεσιμότητα καναλιών μπορεί να αποδειχθεί πρόκληση. Επιπλέον, η χρήση καναλιών PLC μπορεί να είναι μια δαπανηρή προσπάθεια ανά κανάλι. [1]

Τηλεφωνικές γραμμές (Telephone lines Dial-up and leased)

Η σύνδεση Dial-up που παρέχεται από την τηλεφωνική εταιρεία επιτρέπει προσωρινή πρόσβαση και είναι παρόμοια με αυτή που χρησιμοποιείται στο σπίτι, ενώ ένα μισθωμένο κύκλωμα είναι πάντα διαθέσιμο για χρήση από την εταιρεία κοινής ωφέλειας. Το μισθωμένο κύκλωμα μπορεί να είναι αποκλειστικό, με δική του δρομολόγηση για τις υπηρεσίες κοινής ωφέλειας, πράγμα που είναι εξαιρετικά επιθυμητό, καθώς επιτρέπει την εύκολη παρακολούθηση της απόδοσής του. Αντίθετα, η γραμμή Dial-up μπορεί να δρομολογείται μαζί με τις γραμμές άλλων πελατών και μπορεί να αλλάξει χωρίς προειδοποίηση προς την εταιρεία κοινής ωφέλειας.
Δύο κύρια οφέλη μπορούν να αποδοθούν στα μισθωμένα κυκλώματα. Το πρώτο είναι η ευκολία προσαρμογής τους, καθώς δεν απαιτούν ιδιαίτερη τεχνική εξειδίκευση και μπορούν να τροποποιηθούν όπως απαιτείται για να ικανοποιήσουν τις μεταβαλλόμενες απαιτήσεις κυκλοφορίας. Ωστόσο, η ασφάλειά τους είναι πολύ επιρρεπής σε συμβιβασμούς, καθώς μπορούν να παραβιαστούν κρυφά με μικρή δυσκολία. Επιπλέον, οι κακόβουλοι εισβολείς μπορούν εύκολα να το αναδρομολογήσουν. Συγκριτικά, τα κυκλώματα dial-up μπορούν να παρακαμφθούν με μια απλή τηλεφωνική κλήση από οποιοδήποτε δημόσιο τηλεφωνικό δίκτυο. Και τα δύο αυτά κυκλώματα είναι επίσης επιρρεπή σε ηλεκτρομαγνητικές παρεμβολές, γεγονός που καθιστά απαραίτητη την προστασία της τηλεφωνικής γραμμής από τέτοιους πιθανούς κινδύνους μέσω κατάλληλων μέτρων απομόνωσης και προστασίας. [1]

2.5.2 Μη καθοδηγούμενα (ασύρματα) μέσα

Δορυφορική επικοινωνία (Satellite)

Τα δορυφορικά συστήματα παρέχουν υπηρεσίες υψηλής ταχύτητας με τη χρήση δορυφόρων που κινούνται σε γεωστατικές τροχιές πάνω από τον ισημερινό της Γης, προσφέροντας συνεχή κάλυψη σε συγκεκριμένες περιοχές. Τα δορυφορικά συστήματα αποτελούνται από ραδιοφωνικούς αναμεταδότες που μεταφέρουν συχνότητες σε επίγειους σταθμούς που βρίσκονται εντός του εύρους κάλυψής τους. Τα δίκτυα παρακολούθησης εδάφους είναι υπεύθυνα για τη διαχείριση των δορυφόρων και οι επίγειοι σταθμοί συλλέγουν τα σήματα μέσω κεραιών. Η τεχνολογία πίσω από το Very Small Aperture Terminal (VSAT) εξελίσσεται συνεχώς, επιτρέποντας τη χρήση μικρότερων κεραιών περίπου ενός μέτρου για σκοπούς επικοινωνίας. Το κλειδί για επιτυχημένη επικοινωνία είναι η σωστή τροχιά για τους δορυφόρους, όπως η γεωσύγχρονη γήινη τροχιά (GEO), η μεσαία γήινη τροχιά (MEO) και η χαμηλή γήινη τροχιά (LEO). Το σύστημα GEO απαιτεί μεγάλες παραβολικές κεραίες για να διατηρείται ο δορυφόρος επίπεδα ισχύος του αναμεταδότη σε ένα διαχειρίσιμο επίπεδο, επειδή ο δορυφόρος είναι απομακρυσμένος. Η Hughes κατασκεύασε τον πρώτο δορυφόρο επικοινωνίας σε γεωσύγχρονη τροχιά (GEO) στις αρχές της δεκαετίας του 1960. Ένας δορυφόρος επικοινωνίας GEO λειτουργεί σε γήινη τροχιά σε ύψος 35.900 χιλιομέτρων (22.300 μίλια) πάνω από το έδαφος.

Εικόνα 18 Απεικόνιση των δορυφόρων στις γεωστατικές τροχιές

Οι τροχιές που λειτουργούν οι δορυφόροι MEO είναι συνήθως από 10.000 έως 20.000 km πάνω από την επιφάνεια της Γης. Μια τρίτη τεχνολογία είναι οι LEO που λειτουργούν σε χαμηλότερο υψόμετρο από 500 έως 2000 χλμ από την επιφάνεια της Γης. Λόγω των μικρότερων αποστάσεων, απαιτούνται χαμηλότερα επίπεδα ισχύος.

Τα δορυφορικά συστήματα προσφέρουν πολλά πλεονεκτήματα, το πιο σημαντικό από τα οποία είναι η ικανότητά τους να παρέχουν κάλυψη σε μεγάλες αποστάσεις, ακόμη και σε δύσκολες ή απρόσιτες τοποθεσίες. Επιπλέον, αυτά τα συστήματα είναι γνωστό ότι έχουν ένα μικρό περιθώριο σφάλματος και προσαρμόζονται συνεχώς σε παραλλαγές στα δίκτυα επικοινωνίας. Υπάρχουν πολλά μειονεκτήματα που συνοδεύουν τη χρήση δορυφορικών καναλιών επικοινωνίας. Αυτά περιλαμβάνουν πιο αργό χρόνο μετάδοσης σε απομακρυσμένες εγκαταστάσεις, μειωμένο έλεγχο της μετάδοσης και μείωση της μετάδοσης κατά τη διάρκεια της ηλιακής ισημερίας. Επιπλέον, από τη στιγμή που ένα κανάλι δορυφορικής επικοινωνίας μισθωθεί, μετατρέπεται σε πάγια δαπάνη που δεν μπορεί να αλλάξει.

Ραδιόφωνο Συχνοτήτων (VHF,UHF)

Είναι γεγονός πως τα ραδιοκύματα είναι γενικά πανκατευθυντικά και αποτελούν καλό μέσο για εκπομπή σε μεγάλες αποστάσεις. Τα κύματα που μεταδίδονται από μια κεραία διαδίδονται προς όλες τις κατευθύνσεις, αποφεύγοντας έτσι οποιαδήποτε ευθυγράμμιση για τις κεραίες αποστολής και λήψης. Τέλος, τα κύματα της κεραίας αποστολής μπορούν να ληφθούν από οποιαδήποτε κεραία λήψης. Υπάρχουν διάφοροι τύποι βασικών κεραιών που διαφέρουν ανάλογα με το μήκος κύματος, την ισχύ και τον σκοπό της μετάδοσης. Επιπλέον, είναι εφικτό ένας πομπός να έχει πολλούς δέκτες λόγω της διαδικασίας πολλαπλής εκπομπής.
Η ραδιοφωνική ζώνη πολύ υψηλών συχνοτήτων (VHF) βρίσκεται στο εύρος 30 έως 300 MHz. Αυτή η ραδιοσυχνότητα χρησιμοποιείται ευρέως από κινητές υπηρεσίες. Αυτό το σύστημα επικοινωνίας μπορεί να χρησιμοποιηθεί για τη συντήρηση των συστημάτων ηλεκτρικής ενέργειας, καθώς και για SCADA/DMS, για το οποίο πρέπει να εκχωρηθεί αποκλειστική συχνότητα. Το κύριο πλεονέκτημα του ραδιοφώνου VHF είναι η εκχώρηση μιας συγκεκριμένης συχνότητας για μια συγκεκριμένη υπηρεσία, με χαμηλότερο κόστος σε σχέση με τα μικροκύματα και ανεξαρτήτως του κοινού φορέα και των γραμμών ισχύος. Ωστόσο, έχει χαμηλό ρυθμό δεδομένων για την ψηφιακή επικοινωνία, περιορισμένη τεχνική μετάδοσης και χαμηλή χωρητικότητα καναλιού μετάδοσης.
Η ραδιοεπικοινωνία υπερυψηλών συχνοτήτων (UHF) συνήθως καλύπτει ζώνη συχνοτήτων από 300 έως 3000 MHz. Γενικά, η συχνότητα 400 έως 900 MHz για τη ραδιοεπικοινωνία UHF. Τα συστήματα UHF διατίθενται σε διάφορες μορφές, συμπεριλαμβανομένων των συστημάτων από σημείο σε σημείο (PTP), από σημείο σε πολλαπλό σημείο (PTM) ή MARS και συστήματα εξάπλωσης φάσματος (Trunked Mobile Radio).
Ένα **σύστημα UHF σημείο-προς-σημείο** χρησιμοποιείται κυρίως για την επικοινωνία μεταξύ κεντρικών σταθμών και μεμονωμένων υποσταθμών. Οι ραδιοσυχνότητες που χρησιμοποιούνται λειτουργούν εντός της κατώτερης ζώνης UHF, η οποία επιτρέπει μεγαλύτερες αποστάσεις και είναι η πλέον κατάλληλη για διαδρομές όπου δεν είναι δυνατή η οπτική επαφή.
Ένα **ραδιοσύστημα πολλαπλών διευθύνσεων (MARS)** αποτελείται γενικά από ένα κύριο σταθμό (συνήθως Hot Standby, full duplex) που εκπέμπει μέσω παντοειδούς κατεύθυνσης κεραία σε σταθερούς απομακρυσμένους σταθμούς (συνήθως Non Standby, half duplex) που λαμβάνουν τα σήματα μέσω μιας κατευθυντικής κεραίας . Το 400/900 MHz MARS Radio είναι ένα σύστημα ενός καναλιού που επικοινωνεί διαδοχικά με κάθε ένα από τα απομακρυσμένα σημεία. Οι υπηρεσίες που υποστηρίζονται κυρίως από το MARS είναι SCADA, τηλεμετρία/δεδομένα. και φωνή . Σε σύγκριση με το PTP, το κόστος αυτού είναι σημαντικά χαμηλότερο. Σε ένα σύστημα MARS, ωστόσο, ο ρυθμός μετάδοσης δεδομένων είναι χαμηλότερος λόγω της λειτουργίας πολλαπλών σημείων.

Τα **ραδιοσύστημα διάχυτου φάσματος** επιτρέπονται να λειτουργούν στη ζώνη 902-928 MHz, 2,4 και 5,3 GHz χωρίς άδειες. Η ανάπτυξη ραδιοδικτύων τύπου πακέτου για συστήματα δεδομένων ήταν αποτέλεσμα του Digital Multiples System (DMS). Επιπλέον, υπάρχουν συστήματα που λειτουργούν στη ζώνη 450-470 MHz από διάφορους κατασκευαστές. Κάθε

ζώνη μπορεί να προσφέρει διάφορους ρυθμούς και χαρακτηριστικά σηματοδοσίας για επικοινωνίες DMS, με τα συστήματα στα 900 MHz να φαίνεται ότι έχουν πιο προηγμένα χαρακτηριστικά σε αυτήν τη στιγμή. Η πρόοδος στα ραδιοδίκτυα επέτρεψε την αποτελεσματική μεταφορά δεδομένων και επικοινωνίας σε πολλαπλές ζώνες συχνοτήτων. Αυτή η πρόοδος έχει προσφέρει επιλογές για διαφορετικές τεχνικές και χαρακτηριστικά, που καλύπτουν τις ατομικές ανάγκες κάθε συστήματος επικοινωνίας. [1]

Microwave Radio

Εικόνα 19 Πύργος ραδιοκυμάτων μικροκυμάτων με κεραίες κινητής τηλεφωνίας

Τα μικροκύματα ορίζονται ως ηλεκτρομαγνητικά κύματα με εύρος συχνοτήτων από 1 έως 300 GHz. Αυτά, έχουν την δυνατότητα να υποστηρίξουν τόσο την αναλογική όσο και την ψηφιακή τεχνολογία μετάδοσης.
Το μέσο που χρησιμοποιείται για τη μετάδοση σήματος λειτουργεί μόνο σε μια μοναδική κατεύθυνση, με τις κεραίες να εκπέμπουν σήματα σε μια συγκεκριμένη διαδρομή. Ως αποτέλεσμα, είναι επιτακτική ανάγκη οι κεραίες του πομπού και του δέκτη να είναι σχολαστικά τοποθετημένες και προσανατολισμένες ώστε να διασφαλίζεται η βέλτιστη συγκέντρωση των μικροκυμάτων που εκπέμπονται .Το κυριότερο πλεονέκτημα των μικροκυμάτων είναι η μονοκατευθυντική τους ιδιότητα, καθώς μπορεί ένα ζεύγος κεραιών να ευθυγραμμιστεί χωρίς να επιδρά σε άλλα. Το ευρύ φάσμα συχνοτήτων των μικροκυμάτων επιτρέπει υψηλές ταχύτητες μετάδοσης δεδομένων. Παρά το πλεονεκτήματά του, η χρήση ορισμένων συχνοτήτων για επικοινωνία απαιτεί ειδική άδεια και υπάρχουν επίσης περιπτώσεις όπου απαιτείται άμεση οπτική επαφή μεταξύ των κεραιών. Επιπλέον, η επικοινωνία μεγάλων αποστάσεων μπορεί να απαιτεί τη χρήση επαναλήπτων σε ορισμένες περιπτώσεις, κάτι που μπορεί να θεωρηθεί μειονέκτημα. Τα κυριότερα πεδία χρήσης των μικροκυμάτων περιλαμβάνουν τις υπηρεσίες κινητής τηλεφωνίας, τα δορυφορικά δίκτυα και τα ασύρματα τοπικά δίκτυα. Βασικά χρησιμοποιούνται όπου απαιτείται επικοινωνία μίας εκπομπής (ένα προς ένα). Η χρήση ψηφιακών μικροκυμάτων είναι αρκετά ακριβή για μεμονωμένες εγκαταστάσεις υποσταθμών, αλλά θεωρείται μέσο υψηλής απόδοσης για τη δημιουργία μιας υποδομής επικοινωνίας κορμού. [1]

2.6 Τηλεμετρία

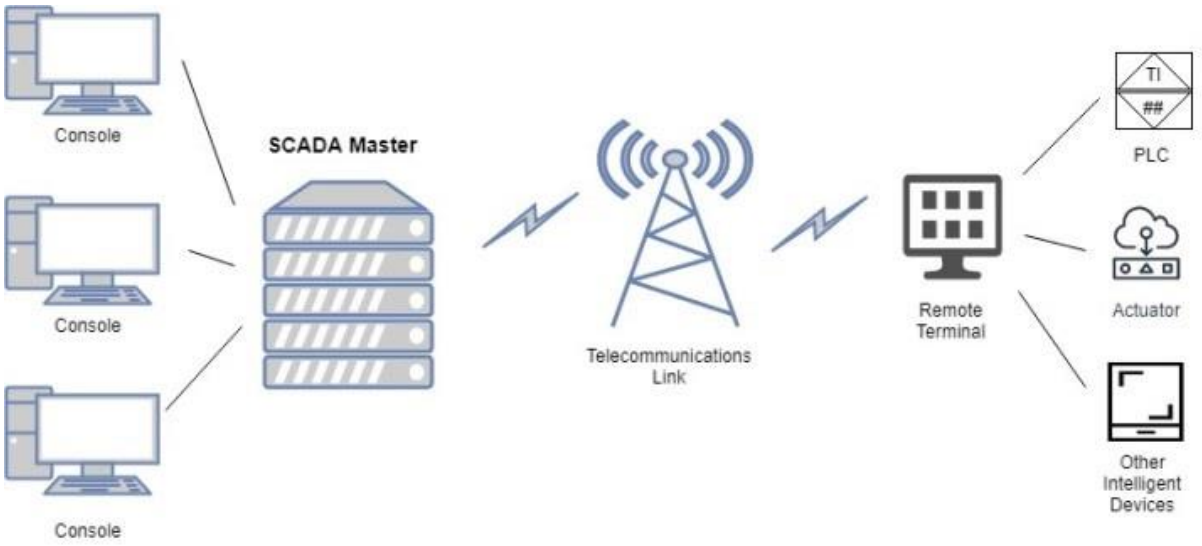
Ο όρος "τηλεμετρία" συνδέεται με τα συστήματα SCADA και προέρχεται από την ελληνική λέξη "τηλε", που σημαίνει μεγάλη απόσταση και "μετρώ". Η τηλεμετρία είναι μια μέθοδος μετάδοσης και λήψης πληροφοριών ή δεδομένων μέσω ενός συγκεκριμένου μέσου, όπως

ασύρματων μηχανισμών (π.χ. συστήματα ραδιοσυχνοτήτων, υπερήχων, δίκτυα υπέρυθρων) ή ενσύρματα δίκτυα (π.χ. Ethernet, σειριακά, οπτικές ίνες). Αυτά τα δεδομένα μπορεί να περιλαμβάνουν μετρήσεις όπως τάση, συχνότητα ή ροή και μπορεί να προέρχονται από πολλές πηγές. Το σύστημα SCADA περιλαμβάνει πρωτόκολλα για την αντιμετώπιση αυτών των διαφόρων τοποθεσιών και των δεδομένων τους

ΚΕΦΑΛΑΙΟ 3^{Ο}

3.1 Επικοινωνία

Η επικοινωνία εύκολα παρομοιάζεται με το νευρικό σύστημα του ανθρώπινου σώματος το οποίο εκτείνεται από τον εγκέφαλο σε κάθε μέρος του σώματος μεταφέροντας δεδομένα και σήματα εμπρός και πίσω συνεχώς. Συνεπώς, η επικοινωνία του εποπτικού ελέγχου και της απόκτησης δεδομένων (SCADA) αναφέρεται στα κανάλια επικοινωνίας που χρησιμοποιούνται μεταξύ του εξοπλισμού πεδίου (πχ. PLC , αισθητήρες) και του κεντρικού σταθμού. Το κανάλι παρέχει ένα μέσο για την πρόσβαση σε δεδομένα πεδίου σε πραγματικό χρόνο και τον έλεγχο του συστήματος από απόσταση. Επιπλέον, διευκολύνει τη μετάδοση εντολών ελέγχου από το κέντρο ελέγχου στον σχετικό εξοπλισμό στο πεδίο για άμεση εκτέλεση, διασφαλίζοντας τη σταθερότητα και την ασφάλεια του συστήματος.



Εικόνα 20 Δίαυλος τηλεπικοινωνίας

3.2 Απαιτήσεις και προκλήσεις των SCADA

Τα τρέχοντα συστήματα SCADA σήμερα αντιμετωπίζουν ένα πλήθος προκλήσεων και προϋποθέσεων όσον αφορά τη διαχείριση, την παραγωγή και τη διάδοση δεδομένων. Μερικοί από αυτούς τους παράγοντες περιλαμβάνουν: την πολυπλοκότητα, την αξιοπιστία, την ασφάλεια, την επεκτασιμότητα, την καθυστέρηση, τη διαλειτουργικότητα, τον πλεονασμό και την ελαστικότητα. Κάθε μία από αυτές τις προκλήσεις έχει τον δικό της μοναδικό ορισμό, καθώς και τους λόγους και τις συνέπειες πίσω από αυτές.

Πολυπλοκότητα (Complexity) : Πρόκειται για την ιδιότητα της σύνθετης σύνθεσης. Η πολυπλοκότητα χρησιμοποιείται για να περιγράψει κάτι με πολλά στοιχεία σε περίπλοκη διάταξη. Στα συστήματα SCADA, η πολυπλοκότητα αυξήθηκε με την εισαγωγή νέων συστατικών, όπως υπολογιστές, ελεγκτικοί σταθμοί, δίκτυα και άλλοι πόροι. Επιπλέον, η πολυπλοκότητα στα συστήματα SCADA οφείλεται στον αυξανόμενο όγκο δεδομένων και πληροφοριών διεργασιών, καθώς και στις αλληλεπιδράσεις μεταξύ των στοιχείων του συστήματος. Αυτή η πολυπλοκότητα επηρεάζει τα συστήματα SCADA, καθιστώντας τα άκαμπτα και δυσκολότερα να προσαρμοστούν σε νέες απαιτήσεις ή αλλαγές στον έλεγχο και τον εξοπλισμό παρακολούθησης.

Αξιοπιστία (Reliability): Τα συστήματα SCADA πρέπει να διαθέτουν υψηλό επίπεδο αξιοπιστίας, ώστε να διασφαλίζεται ότι τα δεδομένα μεταδίδονται και λαμβάνονται σωστά και έγκαιρα. Οι διαταραχές ή οι καθυστερήσεις της επικοινωνίας μπορούν να προκαλέσουν σημαντικά προβλήματα στις βιομηχανικές διαδικασίες, επομένως η υποδομή επικοινωνίας πρέπει να είναι σχεδιασμένη έτσι ώστε να ελαχιστοποιεί τον κίνδυνο αποτυχίας.

Ασφάλεια (Security): Τα συστήματα SCADA πρέπει να είναι ασφαλή ώστε να αποτρέπεται η μη εξουσιοδοτημένη πρόσβαση ή η αλλοίωση του συστήματος. Αυτό είναι ιδιαίτερα σημαντικό για κρίσιμες υποδομές όπως σταθμοί παραγωγής ενέργειας, εγκαταστάσεις επεξεργασίας νερού και συστήματα μεταφορών, όπου μια παραβίαση της ασφάλειας θα μπορούσε να έχει σοβαρές συνέπειες within the enterprise network.)

Επεκτασιμότητα (Scalability): Τα συστήματα SCADA πρέπει να είναι κλιμακούμενα για να μπορούν να εξυπηρετήσουν μελλοντική ανάπτυξη και επέκταση. Καθώς οι βιομηχανικές διεργασίες γίνονται πιο πολύπλοκες και απαιτούν περισσότερα δεδομένα, η υποδομή επικοινωνίας πρέπει να είναι σε θέση να διαχειριστεί τον αυξημένο όγκο δεδομένων και την αυξημένη κυκλοφορία.

Καθυστέρηση (Latency): Τα συστήματα SCADA πρέπει να έχουν χαμηλή καθυστέρηση, ώστε να διασφαλίζεται ότι τα δεδομένα μεταδίδονται και λαμβάνονται σε πραγματικό χρόνο. Αυτό είναι ζωτικής σημασίας για τον έλεγχο και την παρακολούθηση βιομηχανικών διεργασιών σε πραγματικό χρόνο, όπου οι καθυστερήσεις ή η καθυστέρηση μπορεί να προκαλέσουν σημαντικά προβλήματα.

Διαλειτουργικότητα (Interoperability): Τα συστήματα SCADA πρέπει να είναι διαλειτουργικά με μια ποικιλία συσκευών και συστημάτων. Αυτό περιλαμβάνει τη δυνατότητα επικοινωνίας με διαφορετικούς τύπους συσκευών πεδίου, όπως αισθητήρες και ενεργοποιητές, καθώς και με άλλα συστήματα ελέγχου και εφαρμογές λογισμικού.

Πλεονασμός (Redundancy): Τα συστήματα SCADA πρέπει να διαθέτουν πλεονασμό, ώστε να διασφαλίζεται η συνέχιση της επικοινωνίας σε περίπτωση βλάβης επικοινωνίας ή διακοπής λειτουργίας του συστήματος. Αυτό μπορεί να περιλαμβάνει εφεδρικά κανάλια επικοινωνίας, εφεδρικά τροφοδοτικά και εφεδρική αποθήκευση δεδομένων.

Ευελιξία (Flexibility) : Το σύστημα SCADA δεν περιορίζεται σε σταθερές διαδρομές επικοινωνίας, αλλά επιτρέπει την ανταλλαγή πληροφοριών ανάμεσα σε οποιαδήποτε σημεία χωρίς περιορισμούς. Αυτή η ευελιξία επιτυγχάνεται μέσω της ευέλικτης υποδομής της τεχνολογίας πληροφοριών και της προσαρμόσιμης φύσης των συστημάτων εφαρμογών, προσφέροντας τη δυνατότητα προσαρμογής της επικοινωνίας ανάλογα με τις συγκεκριμένες ανάγκες.

Ανθεκτικότητα (Robustness) : Η ανοχή στα σφάλματα είναι η δυνατότητα ενός συστήματος να διαχειρίζεται προβλήματα κατά τη λειτουργία του ή η ικανότητα ενός αλγορίθμου να παραμένει αποτελεσματικός, παρά τυχόν ανωμαλίες στην είσοδο, στις υπολογιστικές διαδικασίες και άλλες αντίξοες συνθήκες. Δεδομένου ότι η αξιοπιστία των ηλεκτρονικών συσκευών δεν είναι πάντα απόλυτη, είναι ουσιώδες να διασφαλίζεται ότι τα συστήματα SCADA έχουν σχεδιαστεί με ένα επίπεδο ανοχής στα σφάλματα που εξασφαλίζει την

ακεραιότητα των δεδομένων και τη συνεχή λειτουργία, ακόμα και σε περιπτώσεις δυσλειτουργίας ή προβλημάτων.

3.3 Τοπολογίες επικοινωνιών SCADA

Υπάρχουν διάφορες τοπολογίες επικοινωνίας που μπορούν να χρησιμοποιηθούν στα συστήματα SCADA για τη μεταφορά δεδομένων μεταξύ του κεντρικού υπολογιστή SCADA και των συσκευών πεδίου. Ορισμένες από τις κοινές τοπολογίες επικοινωνίας SCADA είναι οι εξής:

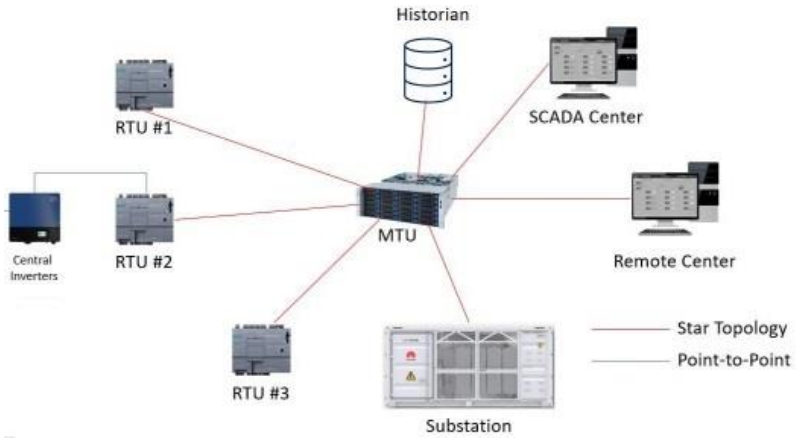
3.3.1 Point-to-point

Στην τοπολογία point-to-point κάθε συσκευή πεδίου συνδέεται με τον κεντρικό υπολογιστή SCADA μέσω μιας αποκλειστικής σύνδεσης επικοινωνίας. Αυτός ο τύπος τοπολογίας είναι κατάλληλος για συστήματα SCADA μικρής κλίμακας με λίγες συσκευές πεδίου.

Εικόνα 21 Τοπολογια Point-to-Point

3.3.2 Star

Στην τοπολογία του αστέρα (star), κάθε συσκευή πεδίου συνδέεται με έναν κεντρικό κόμβο, ο οποίος στη συνέχεια συνδέεται με τον κεντρικό υπολογιστή SCADA. Αυτή η τοπολογία επιτρέπει την εύκολη προσθήκη και η αφαίρεση κόμβων ωστόσο, αυτό δεν υποστηρίζει την άμεση επικοινωνία μεταξύ των κόμβων. Το μειονέκτημα το οποίο θεωρείται πιο σημαντικό, είναι το γεγονός ότι σε περίπτωση βλάβης του κεντρικού κόμβου, ολόκληρο το δίκτυο αποτυγχάνει.

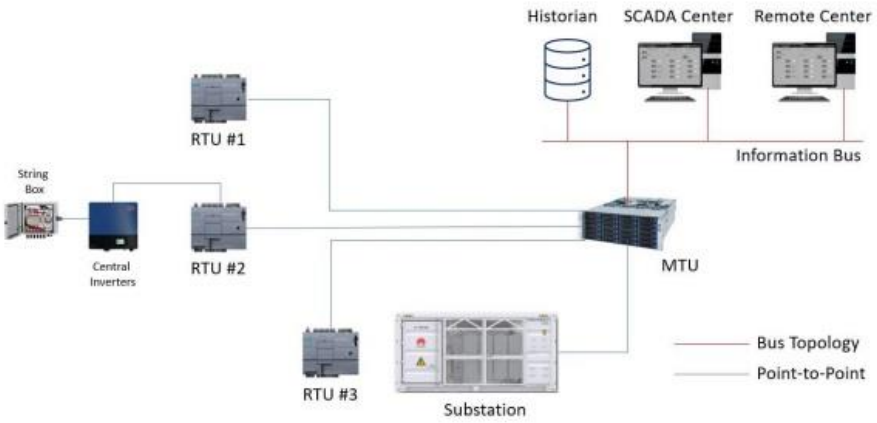


Εικόνα 22 Τοπολογία Star

3.3.3 Bus

Η τοπολογία επικοινωνίας που χρησιμοποιείται σε αυτό το σύστημα περιλαμβάνει τη σύνδεση όλων των συσκευών πεδίου σε έναν μεμονωμένο δίαυλο επικοινωνίας που στη συνέχεια συνδέεται με τον κεντρικό υπολογιστή SCADA. Η απλότητα και η οικονομική αποδοτικότητα αυτής της τοπολογίας την καθιστούν ιδανική για την προσαρμογή όλων των τύπων τεχνικών επικοινωνίας, master-slave, peer-to-peer, και ούτω καθεξής αλλά μπορεί να είναι επιρρεπής σε σφάλματα επικοινωνίας και συμφόρηση.

Κάθε κόμβος είναι συνδεδεμένος σε έναν μοναδικό διάδρομο, μέσω του οποίου μεταφέρονται τα μηνύματα. Οι κόμβοι λαμβάνουν μηνύματα που απευθύνονται σε αυτούς, και αν ένα μήνυμα δεν ληφθεί από κανέναν κόμβο, τερματίζεται ηλεκτρικά στο τέλος του διαδρόμου. Η τοπολογία bus είναι αξιόπιστη και μια βλάβη σε έναν κόμβο δεν επηρεάζει την επικοινωνία στον διάδρομο. Επιπλέον, ο αριθμός των κόμβων μπορεί να προσαρμοστεί εύκολα. Επικοινωνία μεταξύ κόμβων είναι εφικτή, και αυτή η τοπολογία δεν εξαρτάται από τον κεντρικό ελεγκτή. Ωστόσο, η τοπολογία bus έχει ανεπάρκειες. Οι βλάβες στο διάδρομο είναι δύσκολο να εντοπιστούν, τα μηνύματα που δεν φτάνουν στον κόμβο προορισμού χάνονται και σε περιόδους υψηλής κίνησης ο διάδρομος μπορεί να υπερφορτωθεί, εμποδίζοντας τους κόμβους να στείλουν μηνύματα έγκαιρα.

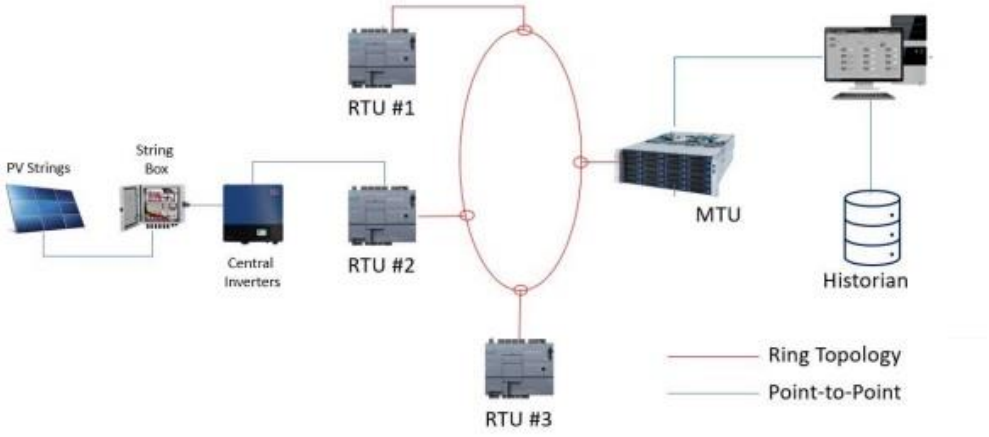


Εικόνα 23 Τοπολογία BUS

3.3.4 Ring

Στην τοπολογία δακτυλίου, οι συσκευές πεδίου συνδέονται κυκλικά και τα δεδομένα μεταδίδονται με μονόδρομο τρόπο(από κόμβο σε κόμβο προς μία κατεύθυνση). Το μήνυμα, εάν δεν γίνει αποδεκτό από κάποιον κόμβο, επιστρέφει στον αποστολέα, το οποίο είναι αρκετό για επιβεβαίωση. Η άμεση επικοινωνία από κόμβο σε κόμβο είναι δυνατή σε αυτή την τοπολογία και οποιοσδήποτε κόμβος μπορεί να είναι master.

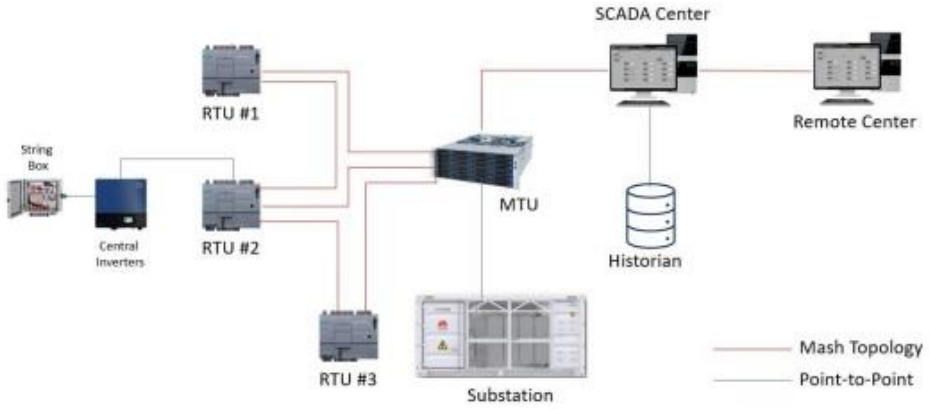
Η τοπολογία που χρησιμοποιείται σε αυτό το σύστημα είναι ευρέως αναγνωρισμένη για την αξιοπιστία της, ωστόσο, έχει ένα σημαντικό μειονέκτημα. Δηλαδή, εάν οποιοσδήποτε κόμβος εντός του δικτύου αποτύχει, θα προκαλέσει τη διακοπή της λειτουργίας ολόκληρου του συστήματος. Επιπλέον, οι διακυμάνσεις στον αριθμό των κόμβων εντός του δικτύου αποτελούν σημαντική πρόκληση, οδηγώντας σε διακοπές στην επικοινωνία. Τέλος, το έργο του εντοπισμού και της απομόνωσης σφαλμάτων εντός του δικτύου είναι επίσης αρκετά δύσκολο.



Εικόνα 24 Τοπολογία Ring

3.3.5 Mesh

Σε αυτή την τοπολογία, οι συσκευές πεδίου διασυνδέονται μεταξύ τους, αποτελώντας ένα δίκτυο πλέγματος. Ενώ αυτή η τοπολογία προσφέρει υψηλό πλεονασμό και ανοχή σε σφάλματα, μπορεί να είναι δύσκολο να καθιερωθεί και να διατηρηθεί..



Εικόνα 25 Τοπολογία Mesh

3.3.6 Ροή δεδομένων: Απλό και αμφίδρομο

Η μεταφορά δεδομένων μεταξύ δύο συσκευών μπορεί να λάβει χώρα με δύο διαφορετικούς τρόπους. Στην "απλή ροή," η επικοινωνία είναι μονόδρομη, με μία συσκευή που μπορεί να μεταδίδει δεδομένα στην άλλη, αλλά η δεύτερη συσκευή μπορεί μόνο να λαμβάνει. Η έννοια της αμφίδρομης ροής αναφέρεται στην ικανότητα δύο συσκευών να επικοινωνούν μεταξύ τους. Υπάρχουν δύο διακριτές μορφές επικοινωνίας μεταξύ συσκευών. Η πρώτη μορφή ονομάζεται "half duplex" και επιτρέπει και στις δύο συσκευές να στέλνουν και να λαμβάνουν πληροφορίες, αλλά όχι ταυτόχρονα. Η δεύτερη μορφή χαρακτηρίζεται ως "full duplex" και επιτρέπει και στις δύο συσκευές να μεταδίδουν και να λαμβάνουν δεδομένα ταυτόχρονα. Μπορείτε να επιτύχετε πλήρη αμφίδρομη συνδεσιμότητα μεταξύ συσκευών μέσω δύο ξεχωριστών καναλιών για μετάδοση και λήψη ή μέσω εξειδικευμένων τεχνικών που εκχωρούν χωρητικότητα καναλιού.

3.4 Τεχνικές επικοινωνίας δεδομένων SCADA

3.4.1 Master-slave

Η συγκεκριμένη τεχνική μπορεί να χρησιμοποιηθεί σε διαμόρφωση σημείο-προς-σημείο ή πολλαπλών σημείων και θεωρείται η απλούστερη τεχνική για χρήση.

Το σύστημα επικοινωνίας βρίσκεται υπό τον απόλυτο έλεγχο του master, ο οποίος μπορεί να είναι κεντρικός υπολογιστής SCADA. Ο κύριος υποβάλλει τακτικά αιτήματα για τη μεταφορά δεδομένων προς και από καθένα από τα slaves, τα οποία είναι συσκευές πεδίου. Οι σκλάβοι δεν είναι ικανοί να ξεκινούν συναλλαγές και βασίζονται αποκλειστικά στον κύριο. Πρόκειται ουσιαστικά για μια προσέγγιση half-duplex, όπου ο slave ανταποκρίνεται μόνο σε αίτημα από τον master. Εάν ένας slave δεν ανταποκριθεί σε συγκεκριμένο χρόνο, ο master επιχειρεί εκ νέου (συνήθως έως και τρεις φορές) και στη συνέχεια χαρακτηρίζει τον slave ως μη εξυπηρετούμενο πριν δοκιμάσει τον επόμενο slave-κόμβο στην ακολουθία. Είναι δυνατή η επανάληψη της προσπάθειας για τον μη εξυπηρετούμενο σκλάβο και πάλι στον επόμενο κύκλο του polling.

Μερικά από τα πλεονεκτήματα αυτής της προσέγγισης είναι τα εξής:

- Το λογισμικό είναι λιτό και αξιόπιστο λόγω της απλότητας της φιλοσοφίας που διαθέτει.
- Η αποτυχία σύνδεσης μεταξύ του master και ενός slave κόμβου ανιχνεύεται άμεσα.
- Δεν μπορούν να προκύψουν συγκρούσεις στο δίκτυο- το οποίο συνεπάγεται, με την απόδοση των δεδομένων να είναι προβλέψιμη και σταθερή.

Για πολύ φορτωμένα συστήματα με κάθε κόμβο να έχει σταθερές απαιτήσεις μεταφοράς δεδομένων αυτό δίνει ένα αναμενόμενο και αποδοτικό σύστημα.

Παρακάτω παρατίθενται μειονεκτήματα τα οποία είναι:

- Οι μεταβολές στις απαιτήσεις μεταφοράς δεδομένων του κάθε slave δεν μπορούν να αντιμετωπιστούν.
- Όταν ένας slave στέλνει ένα αίτημα για άμεση δράση, η διακοπή της συνεχιζόμενης επεξεργασίας του master δεν είναι βιώσιμη επιλογή, καθώς ο master μπορεί να ασχολείται με το χειρισμό του αιτήματος άλλου slave.
- Τα συστήματα που είναι ελαφρώς φορτισμένα με ελάχιστες αλλαγές δεδομένων από έναν slave είναι αρκετά αναποτελεσματικά και αργά χωρίς καμία ευδιάκριτη αιτία.
- Οι σκλάβοι που πρέπει να επικοινωνούν μεταξύ τους πρέπει να το κάνουν διαμέσου πρόσθετης πολυπλοκότητας στο σχεδιασμό του κύριου σταθμού

3.4.2 Peer-to-peer

Όταν λειτουργεί σε λειτουργία peer-to-peer, οποιαδήποτε συσκευή στο δίκτυο μπορεί να ξεκινήσει την επικοινωνία με οποιαδήποτε άλλη συσκευή χωρίς να χρειάζεται μια κεντρική συσκευή για τη ρύθμιση της επικοινωνίας. Όλες οι συσκευές είναι ισότιμες, αν και κατά καιρούς χρησιμοποιείται ένας διαχειριστής διαύλου για τον έλεγχο της κυκλοφορίας. Στα συστήματα SCADA, ο κεντρικός σταθμός εξακολουθεί να λαμβάνει τα περισσότερα δεδομένα και εκδίδει εντολές ελέγχου, αλλά και άλλες συσκευές μπορούν να ξεκινήσουν επικοινωνία. Σε περίπτωση αποτυχίας του πρωτεύοντος σταθμού, η επικοινωνία μπορεί να συνεχιστεί. Στην τοπολογία αστέρι, δεν υποστηρίζεται η peer-to-peer επικοινωνία, καθώς όλες οι συνδέσεις καταλήγουν στον κεντρικό κόμβο και δεν επιτρέπεται η άμεση επικοινωνία μεταξύ των κόμβων. Η τεχνική peer-to-peer αξιοποιεί τους διαθέσιμους πόρους επικοινωνίας με τον καλύτερο δυνατό τρόπο, αλλά με την αύξηση του αριθμού των κόμβων, η απόδοση μπορεί να μειωθεί.

3.4.3 Multi-peer (broadcast and multicast)

Multi-peer είναι ένα μοντέλο επικοινωνίας που χρησιμοποιείται σε ορισμένα συστήματα SCADA ,όπου πολλαπλές συσκευές επικοινωνούν μεταξύ τους με ομότιμο (peer-to-peer) τρόπο χωρίς κεντρικό ελεγκτή.

Η εκπομπή (broadcast) και η πολυεκπομπή (multicast) είναι δύο κοινές τεχνικές που χρησιμοποιούνται στην επικοινωνία πολλαπλών ομότιμων συσκευών. Στην επικοινωνία εκπομπής, ένα μήνυμα αποστέλλεται σε όλες τις συσκευές του δικτύου. Αυτή η τεχνική είναι χρήσιμη όταν ένα μήνυμα πρέπει να σταλεί σε όλες τις συσκευές του δικτύου, όπως μια ενημέρωση κατάστασης ή ένας συναγερμός σε όλο το σύστημα. Στην επικοινωνία πολλαπλής διανομής, ένα μήνυμα αποστέλλεται σε μια συγκεκριμένη ομάδα συσκευών που έχουν ενταχθεί σε μια ομάδα πολλαπλής διανομής. Οι συσκευές που δεν ανήκουν στην ομάδα πολλαπλής διανομής δεν λαμβάνουν το μήνυμα. Αυτή η τεχνική είναι χρήσιμη όταν ένα μήνυμα πρέπει να σταλεί σε ένα συγκεκριμένο σύνολο συσκευών, όπως ένα υποσύνολο συσκευών πεδίου που πρέπει να συντονίσουν τη λειτουργία τους. Η επικοινωνία πολλαπλής διανομής μπορεί να είναι πιο αποτελεσματική από την επικοινωνία μετάδοσης, ειδικά όταν ο αριθμός των συσκευών στο δίκτυο είναι μεγάλος. Αυτό συμβαίνει επειδή τα μηνύματα πολλαπλής διανομής χρειάζεται να σταλούν μόνο μία φορά και όλες οι συσκευές στην ομάδα πολλαπλής διανομής μπορούν να λάβουν το μήνυμα ταυτόχρονα. Ωστόσο, η εφαρμογή της επικοινωνίας πολλαπλής διανομής σε ένα σύστημα SCADA μπορεί να αποτελέσει πρόκληση, καθώς απαιτεί πρόσθετη υποδομή δικτύου για τη διαχείριση των ομάδων πολλαπλής διανομής και τη διασφάλιση ότι οι συσκευές μπορούν να ενταχθούν και να αποχωρήσουν από τις ομάδες δυναμικά.

3.5 Πρωτόκολλα SCADA

Τα πρωτόκολλα του συστήματος SCADA προέκυψαν από προϊόντα υλικού και λογισμικού που αρχικά αναπτύχθηκαν ειδικά για τις ανάγκες του SCADA. Αυτά τα πρωτόκολλα δημιουργήθηκαν ως απάντηση στην αυξανόμενη ζήτηση για εφαρμογές υπολογιστών σε πραγματικό χρόνο στον τομέα του ελέγχου. Στη συνέχεια, προσαρμόστηκαν για να ενσωματώσουν τεχνολογίες δικτύωσης και Internet, ακολουθώντας τις εξελίξεις σε αυτούς τους τομείς. Αυτή η προσέγγιση οδήγησε σε ορισμένα πρότυπα, αλλά ταυτόχρονα έθεσε τα συστήματα SCADA σε κίνδυνο από επιθέσεις που συνήθως αντιμετωπίζουν οι τεχνολογίες πληροφορικής. Τα πρωτόκολλα επικοινωνίας χρησιμεύουν ως μέσο για τα συστήματα SCADA για την επικοινωνία με συσκευές βιομηχανικής διεργασίας, όπως τα PLC. Ο κύριος σκοπός αυτής της επικοινωνίας είναι η απόκτηση δεδομένων και πληροφοριών σχετικά με τη λειτουργία της φυσικής διαδικασίας. Η μεταφόρτωση και η λήψη ζωτικών στρατηγικών ελέγχου, η έκδοση εντολών και η ανταλλαγή δεδομένων σχετικά με την ενεργοποίηση και απενεργοποίηση συσκευών πεδίου, όπως αισθητήρες, είναι όλες βασικές λειτουργίες που μπορούν να εκτελεστούν αποτελεσματικά μέσω της χρήσης αυτών των πρωτοκόλλων.

Παίζουν καθοριστικό ρόλο στην παρακολούθηση, τον έλεγχο και την αυτοματοποίηση βιομηχανικών διεργασιών σε πραγματικό χρόνο. Η μορφή των μηνυμάτων και οι κανόνες για την μορφή και την ανταλλαγή τους, ορίζεται από ένα πρωτόκολλο.

3.5.1 Μοντέλο OSI

Ένα επικοινωνιακό πλαίσιο που είχε τεράστιο αντίκτυπο στο σχεδιασμό των συστημάτων επικοινωνιών είναι το μοντέλο διασύνδεσης ανοικτών συστημάτων (OSI) που αναπτύχθηκε από τον Διεθνή Οργανισμό Τυποποίησης (ISO). Το μοντέλο αυτό στοχεύει στον συντονισμό της ανάπτυξης προτύπων, επιτρέποντας σε υπάρχουσες και αναπτυσσόμενες δραστηριότητες προτύπων να ενσωματωθούν σε ένα κοινό πλαίσιο. Η επικοινωνία μεταξύ συσκευών μέσω ψηφιακής διασύνδεσης αποτελεί το πρώτο βήμα προς τη δημιουργία δικτύου. Εκτός από τις απαιτήσεις υλικού, πρέπει να αντιμετωπιστούν και τα προβλήματα λογισμικού στην επικοινωνία. Σε περιπτώσεις όπου όλες οι συσκευές προέρχονται από τον ίδιο κατασκευαστή, τα προβλήματα υλικού και λογισμικού είναι συνήθως πιο εύκολο να λυθούν, καθώς το σύστημα συνήθως σχεδιάζεται σύμφωνα με τις ίδιες κατευθυντήριες γραμμές και προδιαγραφές. Αντίθετα, τα ανοικτά συστήματα συμμορφώνονται με προδιαγραφές που είναι "ανοικτές σε όλους", επιτρέποντας τη χρήση εξοπλισμού από διάφορους κατασκευαστές σε ένα δίκτυο. Αυτό έχει πλεονεκτήματα, όπως τη δυνατότητα επιλογής από πολλαπλούς προμηθευτές, χαμηλότερες τιμές και ευκολότερη ενσωμάτωση με άλλα στοιχεία.

Το 1978, ο ISO αντιμετώπισε το πρόβλημα των κλειστών συστημάτων και καθόρισε ένα "σύστημα αναφοράς" με το μοντέλο αναφοράς για την επικοινωνία μεταξύ ανοικτών συστημάτων (ISO 7498), γνωστό και ως μοντέλο OSI. Αυτό το μοντέλο διαχείρισης επικοινωνιών δεδομένων αναλύει τις επικοινωνίες σε επτά επίπεδα, επιτρέποντας την ανάπτυξη πρωτοκόλλων για κάθε επίπεδο ανεξάρτητα. Συμμορφούμενα με τα πρότυπα OSI, τα συστήματα μπορούν να επικοινωνήσουν με άλλα συμβατά συστήματα σε παγκόσμιο επίπεδο.

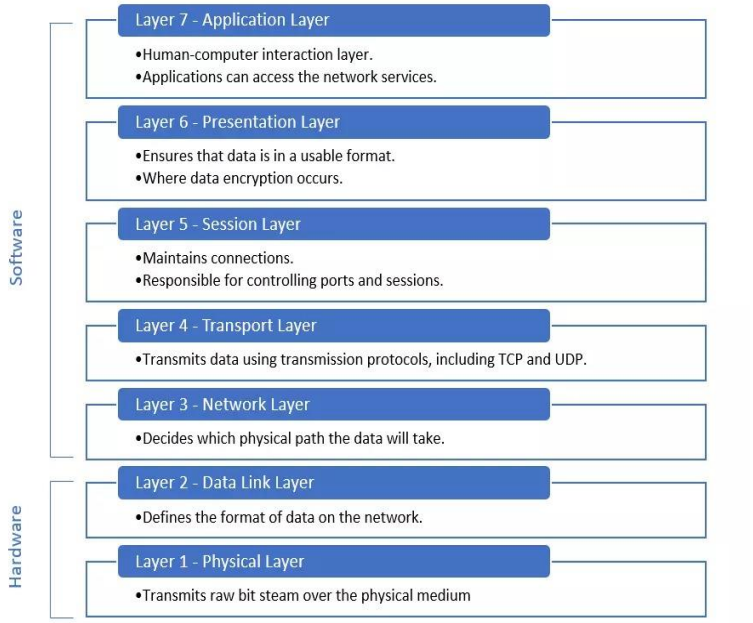
Τα επτά επίπεδα αυτά μπορούν να χωριστούν σε τρεις κατηγορίες: τα επίπεδα υποστήριξης δικτύου, τα επίπεδα χρήστη και το στρώμα μεταφοράς. Το μοντέλο OSI παρομοιάζεται με μια κλεψύδρα με διευρυμένη κορυφή και πυθμένα και μια στενή μέση, επιτρέποντας την χρήση πολλαπλών φυσικών στρωμάτων και επιπέδων εφαρμογής για τη μεταφορά δεδομένων.

Ωστόσο, όλες οι εφαρμογές πρέπει να συμφωνούν σε ένα κοινό σύνολο πρωτοκόλλων δικτύωσης που ορίζονται από τα μεσαία στρώματα του δικτύου, της μεταφοράς και της συνεδρίας, για τη χρήση του δικτύου, το οποίο μπορεί να τρέξει

Θα πρέπει να γίνει εξαρχής αντιληπτό ότι το μοντέλο αναφοράς OSI δεν είναι ένα πρωτόκολλο ή ένα σύνολο κανόνων για το πώς πρέπει να γραφτεί ένα πρωτόκολλο, αλλά μάλλον ένα γενικό πλαίσιο στο οποίο πρέπει να καθορίσει πρωτόκολλα. Το μοντέλο OSI

καθορίζει με σαφήνεια τις λειτουργίες και τις υπηρεσίες που πρέπει να παρέχονται σε κάθε από τα επτά επίπεδα.

Το παρακάτω διάγραμμα παρουσιάζει τα επτά επίπεδα του μοντέλου OSI.



Εικόνα 26 Μοντέλο OSI

Φυσικό (Physical): Το φυσικό επίπεδο αφορά μια μετάδοση (bit) μέσω ενός φυσικού μέσου. Το φυσικό επίπεδο αυτό, καθορίζει τα χαρακτηριστικά της ηλεκτρικής σύνδεσης μεταξύ των συσκευών, όπως τη συχνότητα και την ένταση των ηλεκτρικών παλμών που θα μεταδοθούν, καθώς και τον τύπο του μέσου μετάδοσης, όπως οπτικές ίνες ή μικροκύματα. Επιπλέον, απαιτεί τη μετατροπή των δεδομένων σε ηλεκτρικά ή οπτικά σήματα για τη μετάδοσή τους. Καθορίζει τον ρυθμό μετάδοσης δεδομένων, τον συγχρονισμό ανάμεσα σε αποστολέα και παραλήπτη, τον τρόπο σύνδεσης των συσκευών με το μέσο (σημείο-προς-σημείο ή πολλαπλά σημεία), τη φυσική τοπολογία (π.χ., πλέγμα, δακτύλιος, δίαυλος, αστέρας, ή υβριδική) και τον τρόπο μετάδοσης (simplex, half duplex, ή full duplex).

Σύνδεσμος δεδομένων (Data link): Το επίπεδο ζεύξης δεδομένων δημιουργεί τα πλαίσια (frames) που μεταφέρουν τα bits σε ένα ροή δεδομένων. Τα πλαίσια αναφέρονται ως διαχειρίσιμες ενότητες δεδομένων μέσα σε ένα ροή bits. Ο ρόλος αυτού του επιπέδου είναι να διασφαλίσει τη μεταφορά των πλαισίων από έναν κόμβο στον επόμενο. Το επίπεδο ζεύξης δεδομένων μπορεί να χρησιμοποιεί φυσικές διευθύνσεις, επισυνάπτοντας μια επικεφαλίδα στα πλαίσια που καθορίζει τη διεύθυνση του αποστολέα και/ή του παραλήπτη, ειδικά όταν τα πλαίσια πρέπει να μεταφερθούν σε διάφορα συστήματα εντός ενός δικτύου. Επιπλέον, προσφέρει δυνατότητες για έλεγχο ροής, έλεγχο σφαλμάτων, και μηχανισμούς ελέγχου πρόσβασης. Ο έλεγχος ροής αποτρέπει την υπερχείλιση του δέκτη με δεδομένα σε περίπτωση που ο ρυθμός δεδομένων διαφέρει ανάμεσα στον αποστολέα και τον παραλήπτη. Για τον έλεγχο σφαλμάτων προστίθεται ένα trailer στο τέλος του πλαισίου,

αναγνωρίζει το κατεστραμμένο ή χαμένο πλαίσιο και το αποστέλλει εκ νέου. Ο έλεγχος πρόσβασης αναφέρεται στον έλεγχο της πρόσβασης σε μια ζεύξη από οποιαδήποτε συγκεκριμένη συσκευή, ειδικά όταν πολλές συσκευές είναι συνδεδεμένες στην ίδια ζεύξη. Το επίπεδο ελέγχου πρόσβασης στα μέσα (MAC) ανήκει στο υποεπίπεδο του επιπέδου σύνδεσης δεδομένων στο μοντέλο OSI και καθορίζει πώς οι επικοινωνούσες συσκευές αποφασίζουν ποια από αυτές έχει πρόσβαση στο μέσο μετάδοσης. Συνδέει το επίπεδο σύνδεσης δεδομένων με το φυσικό μέσο.

Δίκτυο (Network): Το επίπεδο δικτύου χειρίζεται την μεταφορά των πακέτων μηνυμάτων από την αρχική συσκευή προέλευσης στην τελική συσκευή προορισμού, ειδικά όταν αυτές οι δύο συσκευές βρίσκονται σε διαφορετικά δίκτυα. Σε περιπτώσεις όπου οι συσκευές επικοινωνούν εντός του ίδιου δικτύου, δεν είναι απαραίτητο το επίπεδο δικτύου. Κυρίως, το επίπεδο δικτύου αναλαμβάνει τη λογική διευθυνσιοδότηση και τη δρομολόγηση των πακέτων. Όταν οι επικοινωνούσες συσκευές βρίσκονται σε διαφορετικά δίκτυα, το επίπεδο δικτύου προσθέτει μια επικεφαλίδα στα δεδομένα του πακέτου για την διευθυνσιοδότηση των συσκευών προέλευσης και προορισμού. Για τη σύνδεση αυτών των διαφορετικών δικτύων χρησιμοποιούνται συσκευές σύνδεσης, οι οποίες είναι οι δρομολογητές(routers). Οι δρομολογητές δημιουργούν δίκτυα και δρομολογούν τα πακέτα δεδομένων στον αντίστοιχο προορισμό τους.

Μεταφορά (Transport): Αυτό το επίπεδο αναλαμβάνει την παράδοση μηνυμάτων από μια διεργασία σε μια άλλη, διασφαλίζοντας τη σειριακή παράδοση τους. Περιλαμβάνει λειτουργίες όπως η διευθυνσιοδότηση σημείου εξυπηρέτησης, διαίρεση και επανασυναρμολόγηση των μηνυμάτων, καθώς και έλεγχο σύνδεσης, ροής και σφαλμάτων. Η διευθυνσιοδότηση σημείου εξυπηρέτησης εξασφαλίζει την παράδοση του μηνύματος στη σωστή διεργασία ανάμεσα σε πολλές εκτελούμενες σε έναν υπολογιστή. Για τον σκοπό αυτό, προστίθεται μια επικεφαλίδα στο μήνυμα που περιλαμβάνει τη διεύθυνση. Για να επανασυναρμολογηθούν τα μηνύματα στη συσκευή προορισμού, τα μηνύματα διακόπτονται σε τμήματα και κάθε τμήμα φέρει αριθμό ακολουθίας. Κατά τη λήψη των πακέτων δεδομένων, ανακτώνται και ανασυναρμολογούνται τα πακέτα με βάση τον αριθμό ακολουθίας, διορθώνοντας πιθανά χαμένα πακέτα κατά τη μετάδοση. Επιπλέον, παρέχονται μηχανισμοί ελέγχου ροής και διόρθωσης σφαλμάτων, ώστε το μήνυμα να φτάσει στον παραλήπτη χωρίς απώλειες ή βλάβες, και σε περίπτωση σφαλμάτων, γίνεται επαναμετάδοση για την διόρθωσή τους.

Σύνοδος (session): Στο επίπεδο συνόδου, υπάρχουν δύο διαθέσιμοι τρόποι επικοινωνίας: ημιαμφίδρομη και η πλήρης αμφίδρομη. Η υπηρεσία συγχρονισμού παρέχεται από το επίπεδο συνεδρίας για να διασφαλίσει την ακριβή παράδοση των μηνυμάτων στους καθορισμένους αποδέκτες τους. Αυτό επιτυγχάνεται με τη διαίρεση της ακολουθίας δεδομένων σε μηνύματα που έχουν ομοιόμορφο μήκος, το καθένα με ένα σημείο συγχρονισμού ή ένα σημείο ελέγχου ενσωματωμένο. Με αυτόν τον τρόπο, επιβεβαιώνεται

η παράδοση κάθε μηνύματος ανεξάρτητα. Σε περίπτωση απώλειας ή βλάβης σε ένα συγκεκριμένο μήνυμα σταθερού μήκους, επαναμεταδίδεται μόνο το συγκεκριμένο μήκους μήνυμα αντί να αποσταλεί το πλήρες μήνυμα.

Παρουσίαση (Presentation): Οι υπηρεσίες που παρέχονται από το επίπεδο παρουσίασης περιλαμβάνουν μετάφραση, κρυπτογράφηση και συμπίεση. Όταν τα μηνύματα μεταδίδονται, μετατρέπονται σε ροές bit. Ωστόσο, δεδομένου ότι δεν υπάρχει ομοιομορφία στην κωδικοποίηση που χρησιμοποιείται από διαφορετικά συστήματα για αυτές τις ροές bit, το επίπεδο παρουσίασης καθίσταται απαραίτητο. Αυτό το επίπεδο είναι υπεύθυνο για τη μετατροπή του κωδικοποιημένου μηνύματος που αποστέλλεται από τον αποστολέα σε μια κοινή μορφή, η οποία στη συνέχεια αποστέλλεται στον παραλήπτη.
Στην πλευρά του παραλήπτη, το επίπεδο παρουσίασης ανακτά την κατανοητή μορφή του μηνύματος. Για τα σημαντικά και ευαίσθητα μηνύματα, απαιτείται η προστασία της ιδιωτικότητας των δεδομένων, και η κρυπτογράφηση αναλαμβάνει να μετατρέψει το μήνυμα σε διαφορετική μορφή πριν από την μετάδοση μέσω του δικτύου. Στην πλευρά του παραλήπτη, τα αρχικά δεδομένα ανακτώνται μέσω της αποκρυπτογράφησης. Όσον αφορά τα πολυμέσα (κείμενο, ήχος, βίντεο), απαιτείται συμπίεση δεδομένων για να μειωθεί ο αριθμός των bits σε ένα συγκεκριμένο μήνυμα.

Εφαρμογή (Application) :Η παροχή υπηρεσιών δικτύου στα προγράμματα εφαρμογών του χρήστη Επίπεδο εφαρμογής: Είναι το ανώτερο επίπεδο, το οποίο παρέχει την δικτυακή πρόσβαση στο χρήστη, όπου υπηρεσίες όπως πρόσβαση και μεταφορά αρχείων, αλληλογραφία και υπηρεσίες καταλόγου. Το εικονικό τερματικό δικτύο επιτρέπει σε έναν χρήστη να συνδεθεί απομακρυσμένα σε έναν υπολογιστή. Όταν ο χρήστης προσπαθεί να επικοινωνήσει με τον κεντρικό υπολογιστή, το λογισμικό εικονικού τερματικού του χρήστη αναλαμβάνει τη σύνδεση με τον απομακρυσμένο υπολογιστή, επιτρέποντας την πρόσβαση στον χρήστη στον απομακρυσμένο υπολογιστή. Η εφαρμογή αυτή επιτρέπει
στον χρήστη να διαβάζει τα αρχεία του απομακρυσμένου κεντρικού υπολογιστή και να πραγματοποιεί αλλαγές, να διαχειρίζεται και να ελέγχει τα αρχεία του κεντρικού υπολογιστή, και επίσης μερικές φορές να αντλεί τα αρχεία του κεντρικού υπολογιστή για χρήση στον τοπικό υπολογιστή. Μέρος του επίσης αποτελούν οι υπηρεσίες αλληλογραφίας και καταλόγου που παρέχουν παγκόσμιες πληροφορίες σχετικά με διάφορες υπηρεσίες και αντικείμενα.

Fieldbus

Ο (Fieldbus) δίαυλος πεδίου είναι ένας τύπος συστήματος επικοινωνίας που χρησιμοποιείται σε συστήματα βιομηχανικού αυτοματισμού και ελέγχου, συμπεριλαμβανομένων των συστημάτων SCADA. Ο σκοπός ενός διαύλου πεδίου είναι να παρέχει μια υποδομή επικοινωνιών για τη μεταφορά δεδομένων μεταξύ συσκευών πεδίου (όπως αισθητήρες και ενεργοποιητές) και συστημάτων ελέγχου.
Στα συστήματα SCADA, to Field Bus παρέχει μια σύνδεση επικοινωνίας μεταξύ των συσκευών πεδίου και του συστήματος ελέγχου, επιτρέποντας στο σύστημα ελέγχου να συλλέγει δεδομένα από τις συσκευές πεδίου και να εκδίδει εντολές για τον έλεγχο των συσκευών. Η

χρήση ενός διαύλου πεδίου μπορεί να βελτιώσει τη συνολική αποδοτικότητα και αξιοπιστία του συστήματος SCADA, καθώς και να μειώσει το κόστος που συνδέεται με τα παραδοσιακά καλωδιωμένα συστήματα.
Υπάρχουν διάφοροι τύποι συστημάτων διαύλου πεδίου, συμπεριλαμβανομένων των PROFIBUS, DeviceNet, Foundation Fieldbus και AS-i. Κάθε ένα από αυτά τα συστήματα fieldbus έχει τα δικά του μοναδικά χαρακτηριστικά και δυνατότητες και η επιλογή του συστήματος fieldbus εξαρτάται από τις συγκεκριμένες απαιτήσεις του συστήματος SCADA και τις συσκευές που χρησιμοποιούνται.

3.6 Λειτουργιά των πρωτοκόλλων SCADA

Η λειτουργία των πρωτοκόλλων SCADA περιλαμβάνει συνήθως την ανταλλαγή δεδομένων μεταξύ δύο ή περισσότερων συσκευών σε ένα σύστημα SCADA. Τα βασικά βήματα που εμπλέκονται σε μια τυπική λειτουργία πρωτοκόλλου SCADA είναι τα εξής:

- Συλλογή δεδομένων: Το RTU ή το PLC συλλέγει δεδομένα από διάφορες συσκευές πεδίου, όπως αισθητήρες, διακόπτες και ενεργοποιητές, και τα μετατρέπει σε μορφή που μπορεί να μεταδοθεί μέσω του δικτύου επικοινωνίας.
- Μετάδοση δεδομένων: Τα μορφοποιημένα δεδομένα μεταδίδονται από την RTU ή το PLC στον εποπτικό υπολογιστή ή το κέντρο ελέγχου χρησιμοποιώντας το επιλεγμένο πρωτόκολλο SCADA.
- Επεξεργασία δεδομένων: Ο εποπτικός υπολογιστής ή το κέντρο ελέγχου επεξεργάζεται τα λαμβανόμενα δεδομένα και μπορεί να τα χρησιμοποιήσει για την ενημέρωση των οθονών, τον έλεγχο των ενεργοποιητών ή την ενεργοποίηση συναγερμών, ανάλογα με τις ανάγκες.
- Επιβεβαίωση δεδομένων: Ο εποπτικός υπολογιστής ή το κέντρο ελέγχου μπορεί να στείλει μια επιβεβαίωση πίσω στην RTU ή το PLC, υποδεικνύοντας ότι τα δεδομένα έχουν ληφθεί και επεξεργαστεί.
- Αποθήκευση δεδομένων: Τα ληφθέντα και επεξεργασμένα δεδομένα μπορούν να αποθηκευτούν σε μια βάση δεδομένων ή σε έναν ιστορικό για μελλοντική ανάλυση και αναφορά.

Αυτή η βασική διαδικασία μπορεί να διαφέρει ανάλογα με το συγκεκριμένο πρωτόκολλο SCADA και τις απαιτήσεις του συστήματος SCADA. Ορισμένα πρωτόκολλα, όπως το DNP3, μπορεί να περιλαμβάνουν πρόσθετα χαρακτηριστικά, όπως η αναφορά συμβάντων και η απόκριση εντολών, για την παροχή πιο προηγμένης λειτουργικότητας.
Είναι σημαντικό να σημειωθεί ότι τα πρωτόκολλα SCADA έχουν σχεδιαστεί για να είναι ιδιαίτερα αξιόπιστα και στιβαρά, με χαρακτηριστικά όπως η ανίχνευση και η διόρθωση σφαλμάτων και ο πλεονασμός, ώστε να διασφαλίζεται η συνεχής λειτουργία κρίσιμων βιομηχανικών διεργασιών, ακόμη και σε περίπτωση αποτυχιών επικοινωνίας ή άλλων διαταραχών. Τα πρωτόκολλα SCADA έχουν σχεδιαστεί με γνώμονα συγκεκριμένες απαιτήσεις, όπως η μετάδοση δεδομένων σε πραγματικό χρόνο, η χαμηλή καθυστέρηση και

η αξιόπιστη επικοινωνία, ακόμη και σε σκληρά βιομηχανικά περιβάλλοντα. Μπορούν επίσης να περιλαμβάνουν χαρακτηριστικά ασφαλείας, όπως κρυπτογράφηση και πιστοποίηση ταυτότητας, για την αποτροπή μη εξουσιοδοτημένης πρόσβασης σε κρίσιμες υποδομές.
Κάθε πρωτόκολλο έχει τα δικά του χαρακτηριστικά τα οποία είναι μοναδικά Οι δυνατότητες και η επιλογή του πρωτοκόλλου εξαρτάται από συγκεκριμένες απαιτήσεις του συστήματος SCADA. Για παράδειγμα, το Modbus χρησιμοποιείται ευρέως σε συστήματα SCADA λόγω της απλότητας και της ευκολίας υλοποίησής του, ενώ το DNP3 χρησιμοποιείται συνήθως στη βιομηχανία ηλεκτρικής ενέργειας για την ευρωστία του και την ικανότητά του να διαχειρίζεται μεγάλες ποσότητες δεδομένων. Επιπλέον, ορισμένα πρωτόκολλα SCADA μπορούν να χρησιμοποιηθούν σε συνδυασμό το ένα με το άλλο για τη δημιουργία ενός υβριδικού συστήματος, το οποίο μπορεί να προσφέρει τα πλεονεκτήματα πολλαπλών πρωτοκόλλων. Για παράδειγμα, ένα σύστημα μπορεί να χρησιμοποιεί το Modbus για την απόκτηση δεδομένων και το IEC 60870-5 για τον απομακρυσμένο έλεγχο, αξιοποιώντας τα πλεονεκτήματα κάθε πρωτοκόλλου. Είναι σημαντικό να σημειωθεί ότι τα πρωτόκολλα SCADA εξελίσσονται συνεχώς και αναπτύσσονται νέα πρωτόκολλα για να ανταποκρίνονται στις αυξανόμενες απαιτήσεις του βιομηχανικού αυτοματισμού και ελέγχου. Η επιλογή του σωστού πρωτοκόλλου είναι ζωτικής σημασίας για την επιτυχία και την αποτελεσματικότητα ενός συστήματος SCADA.

3.6.1 Modbus

Χρησιμοποιούμενο κυρίως σε εφαρμογές αυτοματισμού, το πρωτόκολλο Modbus έχει γίνει μια δημοφιλής μέθοδος μετάδοσης και λήψης δεδομένων. Θεωρείται πρότυπο ανοιχτού κώδικα, που καθιερώθηκε μέσω κοινής χρήσης και όχι με επίσημο διάταγμα. Αρχικά αναπτύχθηκε από τη Modicon στη δεκαετία του 1970, αρχικά προοριζόταν να είναι ένα σειριακό πρωτόκολλο επικοινωνίας μεταξύ προγραμματιζόμενων λογικών ελεγκτών (PLC) και απομακρυσμένων τερματικών μονάδων (RTU). Παρά τον αρχικό του σκοπό, το πρωτόκολλο απέκτησε γρήγορα φήμη και είναι πλέον το πιο συχνά χρησιμοποιούμενο πρότυπο βιομηχανικής παραγωγής. Αυτό οφείλεται στα πολυάριθμα οφέλη που προσφέρει:

- Απλό στη χρήση και μπορεί να επιτευχθεί με σχετική ευκολία.
- Το πρωτόκολλο θεωρείται ανοιχτού κώδικα, πράγμα που σημαίνει ότι έχει τη δυνατότητα να υποστηρίξει μια τεράστια ποικιλία συσκευών.
- Ειδικά σχεδιασμένο για βιομηχανικές εφαρμογές.

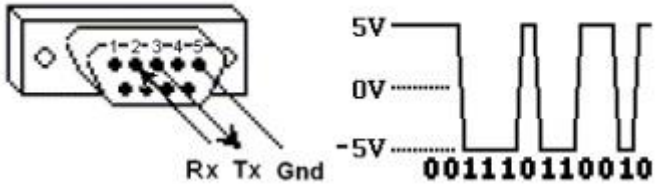
Το Modbus αποτελεί ένα πρωτόκολλο επιπέδου εφαρμογής ανταλλαγής μηνυμάτων. Χρησιμοποιεί τα επίπεδα 1, 2 και 7 του OSI και παρέχει επικοινωνία master-slave μεταξύ συσκευών που συνδέονται με διαφορετικούς τύπους μέσων σύνδεσης και δικτύων πρωτόκολλο. Το πρωτόκολλο επιτρέπει τη μετάδοση διακριτών αναλογικών σημάτων μεταξύ συσκευών και αξιοποιεί τα πρότυπα RS-232 και RS-422/485. Στις πιο πρόσφατες εκδόσεις, το πρωτόκολλο μπορεί να μεταδίδει δεδομένα μέσω Ethernet ή TCP/IP και να στέλνει πακέτα 1 ή 16 bit.
Το Modbus ορίζει δύο τύπους συσκευών οι οποίες επικοινωνούν: το Modbus Master και το Modbus Slave. Το Modbus Master είναι υπεύθυνο για τη μετάδοση μηνυμάτων στο Modbus Slave και το Modbus Slave είναι υπεύθυνο για την απάντηση στα ληφθέντα μηνύματα. Εάν

για κάποιο λόγο παρουσιαστεί σφάλμα κατά τη μετάδοση του μηνύματος στο Modbus Master, αποστέλλεται ένα μήνυμα σφάλματος από το Modbus Slave. Το μήνυμα ζητά από το Modbus Master να στείλει ξανά το μήνυμα. Συνήθως, το Modbus Master είναι η συσκευή που συλλέγει δεδομένα από πολυάριθμους περιφερειακούς σταθμούς μέτρησης και αυτοματισμού. Μέχρι 247 Modbus Slaves μπορούν να συνδεθούν στο ίδιο δίκτυο και το καθένα έχει τη δική του μοναδική διεύθυνση επικοινωνίας ή αριθμό αναγνώρισης σταθμού με τον οποίο επικοινωνεί.

Υπάρχουν πολλοί τύποι πρωτοκόλλων Modbus. Ένας δημοφιλής τύπος είναι το Modbus RTU, το οποίο χρησιμοποιεί σειριακές επικοινωνίες όπως τα RS485 και RS232. Υπάρχει επίσης το πρωτόκολλο Modbus ASCII. Το Modbus over Ethernet (γνωστό ως Modbus TCP) έχει αυξήσει σημαντικά τη δημοτικότητά του σήμερα. Το Modbus TCP ουσιαστικά ενσωματώνει το πρωτόκολλο Modbus RTU σε πακέτα TCP/IP. Επιπλέον, το Modbus αποτελεί ιδανική επιλογή για εφαρμογές RTU όπου απαιτείται ασύρματη επικοινωνία.

Η φύση του Modbus ενσωματώνει ορισμένα αναλλοίωτα χαρακτηριστικά, όπως η σύνθεση των πακέτων δεδομένων, η ακολουθία των πακέτων και η διαδικασία χειρισμού σφαλμάτων. Αντίθετα, άλλα χαρακτηριστικά του Modbus είναι τροποποιήσιμα, όπως ο τύπος του χρησιμοποιούμενου μέσου μετάδοσης, ο χρονισμός των μεταδόσεων ή η εναλλάξιμη χρήση των λειτουργιών ASCII ή RTU τόσο για λόγους κανονικής λειτουργίας όσο και για σκοπούς εντοπισμού σφαλμάτων. Το πιο αξιοσημείωτο πλεονέκτημα του Modbus είναι η ικανότητά του να εκτελεί έλεγχο σφαλμάτων μέσω διαφόρων τεχνικών, όπως ο έλεγχος ισοτιμίας, ο κυκλικός έλεγχος πλεονασμού (CRC) και η διαμόρφωση χαρακτήρων. Το Modbus είναι επίσης ικανό να λειτουργεί σε δίκτυα TCP/IP, τόσο τοπικά όσο και ευρέως, ενσωματώνοντας τα πακέτα του σε πακέτα TCP/IP.

Το πρωτόκολλο Modbus μεταδίδεται μεταξύ συσκευών μέσω σειριακής γραμμής. Μια απλή εγκατάσταση μπορεί να απαιτεί ένα σειριακό καλώδιο για τη σύνδεση των σειριακών θυρών δύο συσκευών, μιας ως master και μιας ως slave. Τα δεδομένα μεταδίδονται ως σειρές από "1" και "0", γνωστά και ως bits, όπου κάθε bit μεταδίδεται ως σήμα. Τα "0" μεταδίδονται ως θετικές τάσεις, ενώ τα "1" ως αρνητικές. Τα bits μεταδίδονται με υψηλή ταχύτητα, με μια τυπική ρύθμιση μετάδοσης στα 9600 baud (bit ανά δευτερόλεπτο).



Εικόνα 27 Σειριακή επικοινωνία με bits του Modbus

Υπάρχουν δύο κύριες φυσικές και ηλεκτρικές συνδέσεις για την σειριακή επικοινωνία. Γίνεται αναφορά για το RS-232 και το RS-485.

Το **RS-232** έχει αναπτυχθεί με σκοπό την οργάνωση της ανταλλαγής δεδομένων μεταξύ των συσκευών πομπού και δέκτη. Ακόμη και σήμερα χρησιμοποιείται ευρέως σε συσκευές SCADA για εργασίες μετάδοσης δεδομένων. Το πιο ευνοϊκό χαρακτηριστικό αυτού του

πρωτοκόλλου είναι ότι μόνο με τη χρήση δύο καλωδίων είναι δυνατή η μετάδοση δεδομένων full duplex (ταυτόχρονη αποστολή και λήψη δεδομένων). Ωστόσο, το σημαντικότερο μειονέκτημα είναι ότι η απόσταση μεταξύ των δυνητικών ανταλλασσόμενων σημείων δεδομένων περιορίζεται σε περίπου 15-20 μέτρα. Επιπλέον, η ανταλλαγή δεδομένων είναι δυνατή μόνο σε τοπολογία σημείου-προς-σημείο. Το πρωτόκολλο σειριακής επικοινωνίας RS-485 αναπτύχθηκε για να αντιμετωπίσει αυτά τα περιορισμένα χαρακτηριστικά του RS-232 και να ικανοποιήσει τις απαιτήσεις της βιομηχανίας. Η απόσταση μεταφοράς δεδομένων αυξάνεται σημαντικά σε περίπου 1200 μέτρα με αυτό το πρωτόκολλο. Το περιορισμό της ανταλλαγής δεδομένων μεταξύ ενός πομπού και ενός δέκτη στο RS-232 αποκαλύφθηκε επίσης με το πρωτόκολλο RS-485, το οποίο επιτρέπει τη μετάδοση δεδομένων ανάμεσα σε 32 πομπούς και 32 δέκτες. Λόγω αυτού του χαρακτηριστικού, το πρωτόκολλο αυτό υποστηρίζει τόσο τοπολογία πολλαπλών σημείων προς σημείο όσο και τοπολογία πολλαπλών σημείων προς πολλαπλά σημεία.

3.6.2 Profibus

Το πρωτόκολλο γνωστό ως Profibus, συντομογραφία του PROcess Field BUS, είναι ένα παγκοσμίως αναγνωρισμένο και ευρέως υιοθετημένο σύστημα, που χρησιμοποιείται συχνά σε εκτεταμένα βιομηχανικά συστήματα παρακολούθησης. Αποτελεί και αυτό ένα σειριακό πρωτόκολλο επικοινωνίας ανοικτού κώδικα που εμπίπτει στο επίπεδο 7 του μοντέλου OSI. Αναπτύχθηκε το 1989 από το Γερμανικό Υπουργείο Ερευνάς και Τεχνολογίας – BMFT και χρησιμοποιήθηκε από την εταιρία Siemens ως βασικό βιομηχανικό πρωτόκολλο επικοινωνιών.

Εξετάζοντας το Profibus από τεχνική άποψη, είναι δυνατό το πρωτόκολλο να υποστηρίζει έως και 127 κόμβους και μέγιστη απόσταση από άκρο σε άκρο 27 km. Αυτό επιτυγχάνεται κυρίως με τη χρήση οπτικών ινών και επαναλήπτων (repeater). Τα πακέτα μηνυμάτων έχουν μήκος 244 bytes/κόμβο με επιπλέον 12 byte overhead, συνολικά δηλαδή 256 bytes και στηρίζονται στην τεχνική polling-token passing. Το πρωτόκολλο Profibus λειτουργεί χρησιμοποιώντας αρχιτεκτονική master-slave, με τις κύριες συσκευές να έχουν τον έλεγχο του διαύλου όταν τους χορηγείται το δικαίωμα να το κάνουν. Σε αυτήν την κατάσταση μεταφέρουν τα μηνύματα χωρίς να έχει προηγηθεί απομακρυσμένο αίτημα. Οι συσκευές slave, από την άλλη πλευρά, είναι περιφερειακές συσκευές, όπως αισθητήρες, οι οποίοι μπορούν να επιβεβαιώσουν τη λήψη μηνυμάτων ή να στείλουν μηνύματα μόνο κατόπιν αιτήματος του κύριου. Αξίζει να σημειωθεί ότι το πρωτόκολλο Profibus μπορεί να χωριστεί σε τρεις κύριες κατηγορίες.

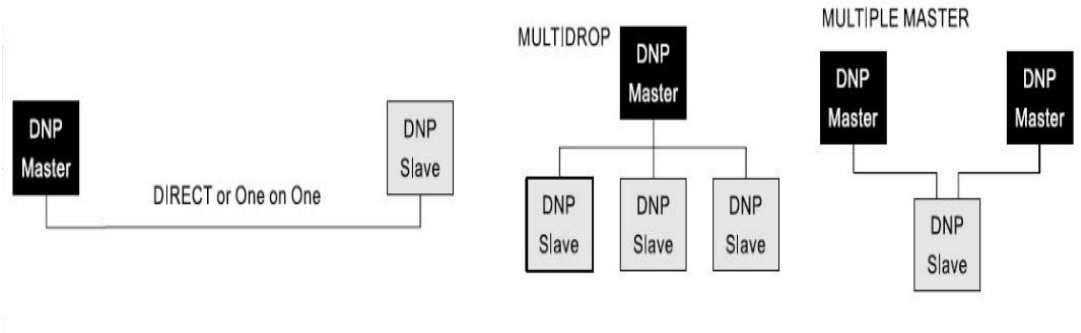
Πρωτόκολλο Profibus DP (Distributed Peripheral) , επιτρέπει τη χρήση πολυάριθμων κύριων συσκευών μαζί με τις αντίστοιχες υποτελείς συσκευές τους. Αυτό σημαίνει ότι ενώ όλες οι κύριες συσκευές έχουν τη δυνατότητα πρόσβασης σε όλες τις υποτελείς συσκευές, μόνο η κύρια συσκευή (που αντιστοιχεί στη συγκεκριμένη υποτελή συσκευή) έχει την εξουσία να τροποποιεί τα δεδομένα σε αυτήν. Ο ρυθμός επικοινωνίας είναι 93,75 Kbps ή χαμηλότερος, με εμβέλεια 1200 μέτρων. Ωστόσο, σε μικρότερη απόσταση 100 μέτρων, μπορεί να φτάσει έως και τα 12 Mbps. Είναι μια ιδανική λύση για εφαρμογές με περιορισμένο χρόνο καθώς χρειάζονται μόνο λιγότερα από 2ms για τη μετάδοση 1 Kbyte πληροφοριών. Το πρωτόκολλο

λειτουργεί αποκλειστικά μέσω κυκλικής επικοινωνίας, όπου κάθε συσκευή πεδίου ανταλλάσσει δεδομένα εισόδου και εξόδου με τον master σε τακτά χρονικά διαστήματα, που αναφέρονται ως cycle time. Η επικοινωνία είναι είτε peer-to-peer, multi-cast ή κυκλικό master/slave χρησιμοποιώντας token .
Πρωτόκολλο Profibus FMS (Fielbus Message Specification) το οποίο κάνει χρήση ενός peer - to-peer μορφής και επιτρέπει την επικοινωνία μεταξύ των master με γενικό σύνολο 127 συσκευών πάνω στο bus. Είναι σημαντικό να σημειωθεί ότι στο πρωτόκολλο FMS, και οι 127 συσκευές μπορούν να λειτουργήσουν ως κύριοι .

Πρωτόκολλο Profibus PA (Process Automation), είναι μια πιο πρόσφατη έκδοση του DP που έχει σχεδιαστεί έχοντας κατά νου τις εγγενείς απαιτήσεις ασφάλειας βιομηχανικών εγκαταστάσεων Προκειμένου να ικανοποιηθούν αυτές οι απαιτήσεις, τα επίπεδα της έντασης και της τάσης του ηλεκτρικού ρεύματος έχουν μειωθεί. Το πρωτόκολλο λειτουργεί με ταχύτητα επικοινωνίας 31,25 Kbps και μπορεί να καλύψει μέγιστη απόσταση 1.900 μέτρων (αναφέρεται ανά κλάδο) . Εάν εφαρμοστούν επαναλήπτες, η απόσταση μπορεί να επεκταθεί έως και 9.500 μέτρα. Το πρωτόκολλο ακολουθεί μια δομή master/slave

3.6.2 DNP3

Το DNP3 (ή Distributed Network Protocol Version 3) είναι ένα τηλεπικοινωνιακό πρότυπο που καθορίζει τις επικοινωνίες μεταξύ CMS, RTU αλλά και των field device. Το DNP3 δημιουργήθηκε ως ιδιόκτητο πρωτόκολλο από τη Harris Controls Division και σχεδιάστηκε ειδικά για SCADA εφαρμογές.
Σε ένα σύστημα SCADA, το πρωτόκολλο DNP3 χρησιμεύει για τη μετάδοση πληροφοριών από μια σειρά συσκευών πεδίου, όπως αισθητήρες και ενεργοποιητές, σε ένα κεντρικό σύστημα ελέγχου. Αυτά τα δεδομένα στη συνέχεια συλλέγονται, αναλύονται και χρησιμοποιούνται για τους σκοπούς του ελέγχου των βιομηχανικών διεργασιών.
Το πρωτόκολλο είναι ένα master-slave, που σημαίνει ότι μια συσκευή master, επικοινωνεί και ελέγχει μια ή περισσότερες συσκευές. Το πρωτόκολλο παρέχει υποστήριξη τόσο για τη μεταφορά δεδομένων με κλήση όσο και για τη μεταφορά δεδομένων βάσει γεγονότων, επιτρέποντας την αποτελεσματική και αξιόπιστη ανταλλαγή δεδομένων μεταξύ των συσκευών πεδίου και ενός κεντρικού συστήματος ελέγχου.
Το DNP3 υποστηρίζει μια ποικιλία συνδέσεων επικοινωνίας, όπως σειριακές, Ethernet και ασύρματες, και παρέχει υποστήριξη για πολλαπλές ταχύτητες επικοινωνίας, όπως 9600, 19200 και 38400 bps. Το πρωτόκολλο περιλαμβάνει επίσης χαρακτηριστικά όπως η υποστηρίξει μηνυμάτων με χρονοσήμανση για καταγραφή ακολουθίας συμβάντων (SOE), σπάει τα μηνύματα σε πολλαπλά πλαίσια για την παροχή βέλτιστου ελέγχου σφαλμάτων και ταχείες ακολουθίες επικοινωνίας . Επιτρέπει την τοπολογία peer-to-peer ,master-slave και multiple-master .Παρέχει απαντήσεις μόνο για "αλλαγμένα δεδομένα , addressing για πάνω από 65.000 συσκευές σε μία μόνο σύνδεση.



Εικόνα 28 DNP3 τοπολογίες

Από την αρχή της χρήσης του στη βιομηχανία διανομής ηλεκτρικού ρεύματος στην Αμερική, το DNP3 απέκτησε ευρεία αναγνώριση τόσο γεωγραφικά όσο και στον βιομηχανικό τομέα. Το DNP3 έχει υποστηριχτεί από πολλούς προμηθευτές και χρήστες στον τομέα της ηλεκτρικής, υδραυλικής, και άλλων βιομηχανιών στη Βόρεια Αμερική, τη Νότια Αμερική, τη Νότια Αφρική, την Ασία και την Αυστραλία. Στην Ευρώπη, το DNP3 ανταγωνίζεται το πρωτόκολλο IEC 60870-5-101, το οποίο χρησιμοποιείται ευρέως σε αυτήν την περιοχή και έχει κοινή προέλευση με το DNP3. Το DNP3, ωστόσο, έχει επεκταθεί σε ευρύτερες βιομηχανικές εφαρμογές στους τομείς της πετρελαίου και φυσικού αερίου, της ύδρευσης/αποχέτευσης και της ασφάλειας.

3.6.3 IEC 60870-5

Το IEC 60870-5 αναφέρεται σε μια σειρά προτύπων που δημιουργήθηκαν από τη Διεθνή Ηλεκτροτεχνική Επιτροπή, γνωστή και ως IEC, με σκοπό την ανάπτυξη ενός ανοικτού πρωτοκόλλου για τη μετάδοση ελέγχου και πληροφοριών τηλεμετρίας SCADA. Αν και το πρωτόκολλο προορίζεται αρχικά για εφαρμογή στην ηλεκτρική βιομηχανία και διαθέτει data objects που είναι ειδικά σχεδιασμένα για αυτές τις εφαρμογές, διαθέτει επίσης data objects που είναι κατάλληλα για γενικές εφαρμογές SCADA. Παρόλα αυτά, το πρωτόκολλο IEC 60870-5 χρησιμοποιείται κυρίως στην ηλεκτρική βιομηχανία των ευρωπαϊκών χωρών.
Η σειρά προτύπων IEC 60870-5 ολοκληρώθηκε το 1995 με τη δημοσίευση του προφίλ IEC 870-5-101, το οποίο κάλυπτε αρχικά τη μετάδοση σε σχετικά χαμηλό εύρος ζώνης σε κυκλώματα επικοινωνίας. Με την αυξανόμενη χρήση των δικτύων της τεχνολογίας επικοινωνιών, το IEC 60870-5 προβλέπει επίσης επικοινωνίες μέσω δικτύων που χρησιμοποιούν πρωτόκολλα TCP/IP.
Το πρότυπο επικοινωνίας IEC 60870-5-101, αλλιώς γνωστό ως T101, διευκολύνει τόσο τις συνδέσεις επικοινωνίας σημείου προς σημείο όσο και πολλαπλών σημείων που μεταδίδουν επικοινωνίες σειριακών δεδομένων χαμηλού εύρους ζώνης. Παρέχει υποστήριξη για διάφορους ρυθμούς επικοινωνίας, συμπεριλαμβανομένων των 2400, 4800, 9600 και 19200 bps, και προσφέρει τη δυνατότητα επιλογής μεταξύ ισορροπημένης ή μη ισορροπημένης επικοινωνίας σε επίπεδο ζεύξης.

Ισορροπημένη (Balanced) επικοινωνία - περιορίζεται μόνο σε συνδέσεις point-to-point:

- Ο master ή ο slave μπορεί να ξεκινήσει κάποια συναλλαγή

- Υπάρχει καλύτερη αποδοτικότητα της χρήσης του συστήματος επικοινωνιών
- Προκύπτουν προβλήματα σύγκρουσης καθώς δύο σταθμοί μπορούν να εκπέμπουν ταυτόχρονα. Σύγκρουση αποφυγή και αποκατάσταση
- Ωστόσο, μόνο για συνδέσεις point-to-point στο πλαίσιο του T101

Ανισόρροπη (Unbalanced) επικοινωνία - κατάλληλη για multidrop:

- Πρωτεύοντα πλαίσια μπορεί να στείλει μόνο ο master
- Δεν απαιτείται αποφυγή σύγκρουσης(απλούστερη σχεδίαση συστήματος)
- Απλούστερη η λειτουργία του επιπέδου ζεύξης δεδομένων του slave

Το πρωτόκολλο όχι μόνο προσφέρει ένα ευρύ φάσμα υποστήριξης για τύπους δεδομένων, αλλά περιλαμβάνει επίσης δυαδικές, αναλογικές και μετρικές τιμές. Αυτό το εύρος το καθιστά προσαρμόσιμο για πολλές εφαρμογές. Επιπλέον, το πρωτόκολλο διαθέτει πρόσθετα χαρακτηριστικά, όπως η χρονική σήμανση και η μεταφορά δεδομένων που ενεργοποιείται από συμβάντα. Αυτά τα στοιχεία διευκολύνουν την απρόσκοπτη και αξιόπιστη ανταλλαγή δεδομένων σε πραγματικό χρόνο.

3.6.4 IEC 61850

Το IEC 61850 αποτελεί ένα διεθνές πρότυπο που καθορίζει πρωτόκολλα επικοινωνίας για έξυπνες ηλεκτρονικές συσκευές σε ηλεκτρικούς υποσταθμούς και αποτελεί μέρος της Διεθνούς Ηλεκτροτεχνικής Επιτροπής (IEC). Ο αφηρημένος τύπος δεδομένων που ορίζονται στο IEC 61850 μπορούν να αντιστοιχιστούν σε διάφορα πρωτόκολλα. Κάποιες από τις αντιστοιχίσεις αυτές είναι :

- Το πρωτόκολλο MMS (Manufacturing Message Specification), (IEC 61850-8-1) το οποίο υποστηρίζει επικοινωνίες master/slave μέσω IP και χρησιμοποιείται για σκοπούς παρακολούθησης αναλογικών μετρήσεων (Τάση, Ένταση, Ισχύς).
- Το πρωτόκολλο GOOSE (Generic Object Oriented Substation Event), (IEC 61850-8-1) χρησιμοποιεί επικοινωνίες multidrop, βασίζεται σε Ethernet και επιτρέπει στα IEDs που εκτελούν χρέη ελεγκτών πύλης (BCU) να ανταλλάσσουν κρίσιμες πληροφορίες μεταξύ τους, και στα IEDs που εκτελούν χρέη προστασίας να στέλνουν εντολές πτώσης προς το διακοπτικό υλικό αλλά να ενημερώνονται και για την θέση άλλων διακοπτικών στοιχείων, έτσι ώστε να λειτουργούν σωστά τα κυκλώματα αλληλοδεσμεύσεων .
- SMV (Sampled Measured Values) (IEC 61850-9-2) φέρουν τιμές ρεύματος και τάσης των γραμμών ισχύος.

Αυτά τα πρωτόκολλα μπορούν να λειτουργήσουν μέσω δικτύων TCP / IP και LAN στους υποσταθμούς με πολύ υψηλές ταχύτητες, έτσι ώστε ο χρόνος απόκρισης, κάτι που είναι πολύ κρίσιμο κυρίως για τα IEDs προστασίας, να μην ξεπερνά τα τέσσερα χιλιοστά του δευτερολέπτου.

3.6.5 OPC

Το OPC, ή Online Platform Communications, αντιπροσωπεύει μια σειρά προτύπων και προδιαγραφών για την επικοινωνία στον τομέα των βιομηχανικών τηλεπικοινωνιών. Το 1996, η ομάδα που ασχολείται με τη βιομηχανική αυτοματοποίηση ανέπτυξε το αρχικό πρότυπο με την ονομασία OLE for Process Control (Object Linking and Embedded for Process Control). Το OPC χρησιμοποιείται για την πραγματικού χρόνου επικοινωνία δεδομένων μεταξύ διάφορων συσκευών ελέγχου από διάφορους κατασκευαστές. Πρόκειται για μια διεπαφή λογισμικού (software-to-software) που δημιουργεί μια σύνδεση ανάμεσα σε εφαρμογές και συσκευές ελέγχου διαδικασιών. Υπάρχουν αρκετά διαφορετικά πρωτόκολλα OPC τα οποία βασίζονται στις πληροφορίες που θέλει να συλλέξει ο χρήστης,

- **OPC DA (Data Access)**: Αυτό εξυπηρετεί το σκοπό της διαρκούς μετάδοσης δεδομένων και σε πραγματικό χρόνο, επιτρέποντας την απρόσκοπτη επικοινωνία μεταξύ προγραμματιζόμενων λογικών ελεγκτών (PLC), απομακρυσμένων τερματικών μονάδων (RTU), κατανεμημένων συστημάτων ελέγχου (DCS) και διεπαφών ανθρώπου-μηχανής/εποπτικού ελέγχου και Εφαρμογές Απόκτησης Δεδομένων (HMI/SCADA).
- **OPC AE (Alarms & Events)**: Ο σκοπός αυτού, είναι να δηλώνει σημαντικά περιστατικά και να εμφανίζει σημαίες σύμφωνα με τις προδιαγραφές του χρήστη. Η μετάδοση πληροφοριών δεν εξαρτάται από το χρόνο, αλλά από την εμφάνιση συγκεκριμένων γεγονότων.
- **OPC HAD (OPC Historical Data Access)**: Ανάκτηση δικαιωμάτων πρόσβασης σε δεδομένα που είναι αποθηκευμένα σε εφαρμογές SCADA.
- **OPC XML DA (Data Access)**: Παρέχει δεδομένα σε κατάλληλη μορφή χρησιμοποιώντας τη γλώσσα XML με στόχο την επικοινωνία μέσω υπηρεσιών διαδικτύου.
- **OPC DX (Data Exchange)**: Απομακρυσμένος έλεγχος, ανταλλαγή δεδομένων από διακομιστή σε διακομιστή.
- **OPC Complex Data** : Εφαρμογή μέσω Data Access/XML-DA σχεδιασμένη να περιγράφει πολύπλοκες δομές δεδομένων, όπως δομές σελίδας και έγγραφα XML.
- **OPC UA (Unified Architecture)**: Νέα γενιά προτύπων OPC.

Το OPC UA αποτελεί την εξέλιξη των προηγούμενων προτύπων OPC, γνωστών ως OPC Classic. Ένα από τα μειονεκτήματα του OPC Classic είναι ότι βασίζεται στις τεχνολογίες COM και DCOM της Microsoft, περιορίζοντας τη συμβατότητά του σε λειτουργικά συστήματα και δίκτυα των Windows. Το πρότυπο βασίζεται στην αρχιτεκτονική master/slave. Η κύρια μονάδα OPC εκτελεί το κρίσιμο έργο της συλλογής πληροφοριών από διάφορους προγραμματιζόμενους λογικούς ελεγκτές (PLC) και στη συνέχεια τη διανομή τους σε διάφορες εφαρμογές ανάλογα με τις ανάγκες. Αυτές οι εφαρμογές λειτουργούν ως slaves, λαμβάνοντας τα δεδομένα από την κύρια μονάδα OPC. Το OPC υποστηρίζει πολλαπλές μεθόδους επικοινωνίας, συμπεριλαμβανομένης της σειριακής επικοινωνίας και της επικοινωνίας Ethernet, και παρέχει μια ευέλικτη και επεκτάσιμη αρχιτεκτονική που μπορεί να προσαρμοστεί σε ένα ευρύ φάσμα εφαρμογών.

3.6.6 HART

Το 1986, η Rosemount παρουσίασε το πρωτόκολλο Highway Addressable Remote Transducer (HART), το οποίο στη συνέχεια έγινε δημοφιλές από το HART Communication Foundation (HCF). Το πρωτόκολλο HART δημιουργήθηκε για να διευκολύνει την επικοινωνία των συσκευών πεδίου και επίσης να διασφαλίσει τη διαλειτουργικότητα με το σύστημα 4-20 mA που ήταν ήδη σε λειτουργία. Το πρωτόκολλο χρησιμοποιεί διαμόρφωση Frequency Shift Keying (FSK) για την ταυτόχρονη μετάδοση αναλογικών και ψηφιακών σημάτων μέσω του ίδιου ζεύγους καλωδίων.

Το πρωτόκολλο HART ακολουθεί το μοντέλο OSI, και εστιάζει συγκεκριμένα στο πρώτο, το δεύτερο και το έβδομο επίπεδο. Οι 3 τύποι εντολών ή μηνυμάτων στο επίπεδο εφαρμογής (Επίπεδο 3, OSI) είναι γενικές εντολές που πρέπει να εφαρμόσουν όλες οι συσκευές HART, κοινές εντολές για τις περισσότερες συσκευές πεδίου και μοναδικές ειδικές εντολές για μεμονωμένες συσκευές πεδίου. Το επίπεδο διασύνδεσης δεδομένων του δικτύου HART (Επίπεδο 2, OSI) είναι υπεύθυνο για τη μετάδοση των byte δεδομένων (8-bit) αξιόπιστα και ασύγχρονα, τα οποία είναι οργανωμένα σε πλαίσια και ακολουθούν τη μέθοδο master-slave. Η πρόσβαση στο δίκτυο ρυθμίζεται από κανόνες χρονισμού διαύλου και διαιτησίας. Το φυσικό επίπεδο (Επίπεδο 1, OSI) του δικτύου HART χρησιμοποιεί το πρότυπο Bell 202 της κωδικοποίησης FSK για τη μετάδοση ψηφιακών δεδομένων στα 1200 bit/sec. Αυτό επιτυγχάνεται με την υπέρθεση των σημάτων FSK σε ένα αναλογικό σήμα 4-20 mA.

Υπάρχουν δύο τρόποι σύνδεσης που είναι διαθέσιμοι για συσκευές που χρησιμοποιούν το πρωτόκολλο HART: point-to-point και multidrop. Στην επικοινωνία από σημείο σε σημείο, τα κλασικά σήματα 4-20 mA χρησιμοποιούνται για τη μετάδοση μεταβλητών διεργασίας, ενώ τα ψηφιακά σήματα χρησιμοποιούνται για τη μετάδοση δεδομένων που σχετίζονται με πρόσθετες μεταβλητές, διαμόρφωση και παραμέτρους συσκευής μέσω του πρωτοκόλλου HART. Ο έλεγχος μπορεί να επιτευχθεί με τη χρήση αναλογικών σημάτων 4-20 mA, τα οποία είναι αδιαπέραστα από τα σήματα HART. Τα σήματα που χρησιμοποιούνται στην ψηφιακή επικοινωνία επιτρέπουν την ανάκτηση συμπληρωματικών μεταβλητών και δεδομένων που είναι απαραίτητα για εργασίες όπως συνήθεις λειτουργίες, έκδοση εντολών, εκτέλεση συντήρησης και διάγνωση προβλημάτων. Αντίθετα, στη ρύθμιση multidrop , ένα μοναδικό ζεύγος αγωγών μαζί με μια προαιρετική πηγή τροφοδοσίας επαρκούν για έως και 15 συσκευές που βρίσκονται στο πεδίο. Σε αυτή τη ρύθμιση, όλες οι μεταβλητές διεργασίας μεταφέρονται ψηφιακά.

Η εγκατάσταση συσκευών πεδίου που χρησιμοποιούν την τεχνολογία HART είναι μια απλή και αποτελεσματική διαδικασία. Το πρωτόκολλο HART επιτρέπει την απρόσκοπτη επικοινωνία μεταξύ διαφόρων συσκευών χρησιμοποιώντας μια γραμμή συνεστραμμένου ζεύγους, η οποία έχει ως αποτέλεσμα τη μείωση του αριθμού των καλωδίων που απαιτούνται για την εγκατάσταση. Χρησιμοποιώντας το πρωτόκολλο, οι χρήστες μπορούν να αποκτήσουν πρόσβαση σε όλες τις πληροφορίες που σχετίζονται με τη συσκευή. Αυτό περιλαμβάνει δεδομένα μετρήσεων που μπορούν να χρησιμοποιηθούν για σκοπούς όπως η επαλήθευση ή ο υπολογισμός του μεγέθους της εγκατάστασης και της χρήσης ενέργειας.

Η συμπερίληψη δύο master σταθμών στο σύστημα επιτρέπει την επικοινωνία με δευτερεύουσες συσκευές, ενισχύοντας έτσι την ευελιξία και τις δυνατότητες του συστήματος. [10] [11].

3.6.7 TCP/IC

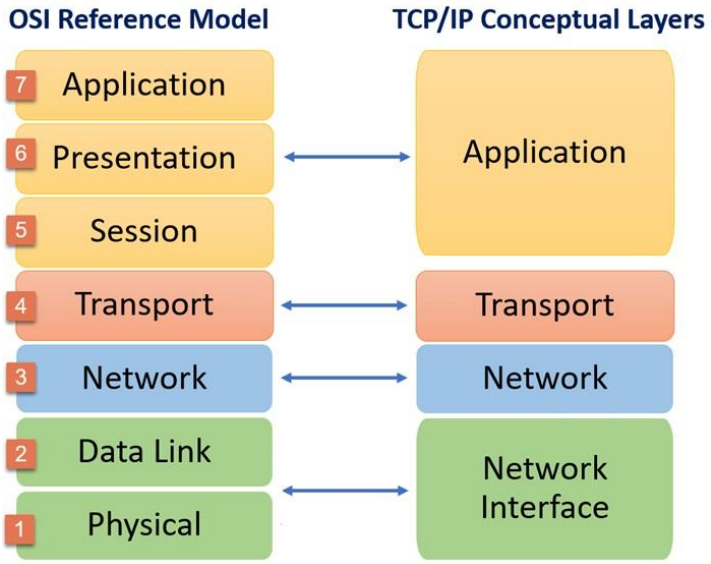
Το TCP/IP ή αλλιώς Πρωτόκολλο Ελέγχου Μετάδοσης/Πρωτόκολλο Διαδικτύου, είναι μια σειρά πρωτοκόλλων που είναι υπεύθυνα για την επικοινωνία δικτύου μεταξύ διαφόρων στοιχείων, συμπεριλαμβανομένων συσκευών πεδίου, προγραμματιζόμενων λογικών ελεγκτών (PLC) και διεπαφών ανθρώπου-μηχανής (HMI). Συγκεκριμένα, το TCP είναι υπεύθυνο για τη διαχείριση δεδομένων, ενώ το IP διευκολύνει την πραγματική μεταφορά δεδομένων μεταξύ των στοιχείων.

Κάθε φορά που μεταδίδονται πληροφορίες μέσω του Διαδικτύου μέσω μιας εφαρμογής, όπως δεδομένα από ένα PLC στο HMI, το TCP τις αναλύει σε πακέτα. Σε κάθε πακέτο εκχωρείται ένας σειριακός αριθμός, διεύθυνση παραλήπτη και άλλες πληροφορίες ελέγχου σφαλμάτων . Τα πακέτα αυτά στέλνονται μέσα στο δίκτυο. Από εδώ και πέρα είναι δουλειά του IP να τα μεταφέρει στο HMI του μακρινού παραλήπτη. Στο τέλος του δέκτη, το TCP λαμβάνει τα πακέτα και τα επαληθεύει για τυχόν σφάλματα. Εάν εντοπιστεί σφάλμα, το TCP ζητά την εκ νέου αποστολή του συγκεκριμένου πακέτου. Μόλις ληφθούν σωστά όλα τα πακέτα, το TCP χρησιμοποιεί τους σειριακούς αριθμούς για να επανασυναρμολογήσει το αρχικό μήνυμα.

Το Πρωτόκολλο Διαδικτύου (IP) χρησιμεύει ως αγωγός για τα πακέτα δεδομένων, να ταξιδεύουν από το σημείο προέλευσης στο σημείο προορισμού. Το IP το επιτυγχάνει αυτό ρυθμίζοντας την κυκλοφορία του δικτύου και διασφαλίζοντας την ακριβή παράδοση των πακέτων. Καταχωρίζοντας δεδομένα σε πακέτα, το Διαδίκτυο μπορεί να εξυπηρετήσει πολλούς χρήστες ταυτόχρονα χρησιμοποιώντας τα ίδια κανάλια επικοινωνίας. Αυτά τα πακέτα δεν απαιτείται να αποσταλούν ομόφωνα και μια γραμμή επικοινωνίας μπορεί να μεταφέρει πολλά πακέτα από τη μια θέση στην άλλη.

Κατά τη μετάδοση, τα πακέτα δεδομένων αποστέλλονται από το ένα σημείο στο άλλο. Εάν μια σύνδεση διακοπεί, ο δρομολογητής που ελέγχει τη ροή δεδομένων μπορεί να βρει μια εναλλακτική διαδρομή. Συνήθως για μια μόνο μεταβίβαση δεδομένων τα διαφορετικά πακέτα ακολουθούν διαφορετικές διαδρομές [12].

Το πρωτόκολλο TCP/IP αποτελείται από τέσσερα επίπεδα. Το επίπεδο διασύνδεσης δεδομένων (Data link layer) περιέχει πρωτόκολλα όπως το IP σειριακής γραμμής (Serial Line IP-SLIP) ή πρωτόκολλα IEEE 802.X. Το επίπεδο δικτύου (Network layer) βρίσκεται το πρωτόκολλο IP. Το επίπεδο μεταφοράς το TCP και το UDP (User Datagram Protocol) και στο επίπεδο εφαρμογών του OSI μοντέλου, συναντάμε πρωτόκολλα όπως το File Transfer Protocol (FTP) για τη μεταφορά αρχείων και το Simple Mail Transfer Protocol (SMTP) για την αποστολή ηλεκτρονικών μηνυμάτων. Ας δούμε τώρα τη συσχέτισή τους με το μοντέλο EPA [4, 13].

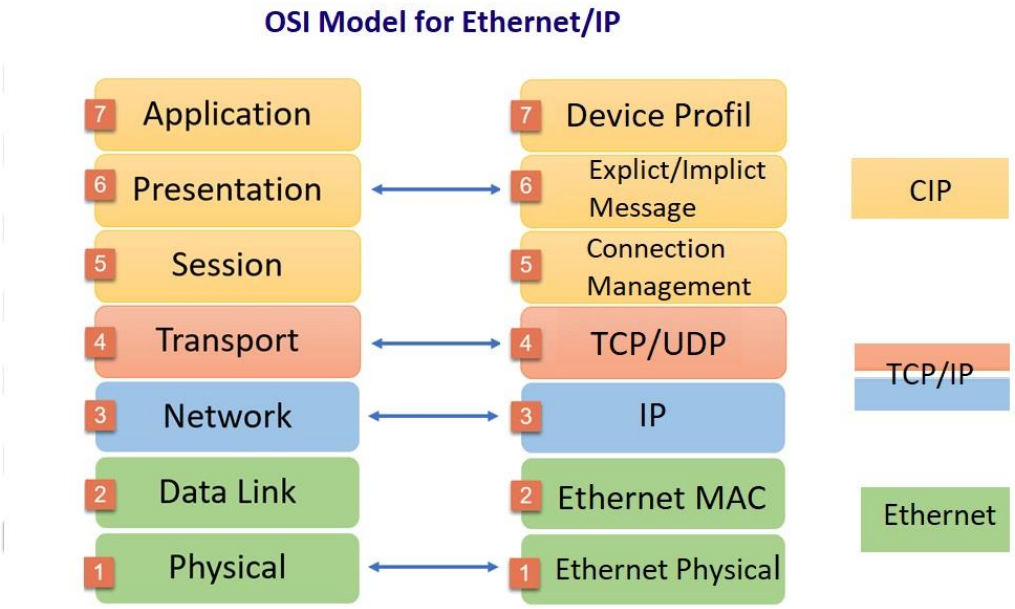


Εικόνα 29 Σύγκριση μεταξύ TCP/IP έναντι Μοντέλου OSI

Το TCP/IP παρέχει αξιόπιστη επικοινωνία με τη χρήση ενός συνδυασμού μηχανισμών ελέγχου ροής και ανίχνευσης σφαλμάτων, διασφαλίζοντας ότι τα δεδομένα μεταδίδονται με ακρίβεια και αποτελεσματικότητα μεταξύ των διαφόρων στοιχείων ενός συστήματος SCADA. Το πρωτόκολλο υποστηρίζει επίσης πολλαπλές συνδέσεις επικοινωνίας, συμπεριλαμβανομένων ενσύρματων και ασύρματων δικτύων, και παρέχει μια ευέλικτη και κλιμακούμενη αρχιτεκτονική που μπορεί να προσαρμοστεί σε ένα ευρύ φάσμα εφαρμογών.

3.6.8 EtherNet/IP

Το Ethernet/IP (Industrial Protocol) επιλέχθηκε ως η επίσημη ονομασία για το πρότυπο Industrial Ethernet. Μοιράζεται πολλές λειτουργικές ομοιότητες με το 802.3 και αποτελείται από έναν συνδυασμό κοινώς διαθέσιμων εμπορικών προϊόντων Ethernet 802.3. Ωστόσο, η βασική διάκριση μεταξύ Ethernet/IP και του τυπικού Ethernet 802.3 που χρησιμοποιείται σε υπολογιστές βρίσκεται μόνο στο επίπεδο λογισμικού, το οποίο είναι μοναδικό στα συστήματα SCADA. Συγκεκριμένα, τα δύο πρωτόκολλα διαφέρουν μόνο στο CIP (Πρωτόκολλο Ελέγχου και Πληροφοριών) που χρησιμοποιούν. Αυτό το πρωτόκολλο λειτουργεί πάνω από το τυπικό Transmission Control Protocol (TCP) και το User Datagram Protocol (UDP) του προτύπου 802.3 για να παρέχει μια ενιαία μέθοδο ανταλλαγής δεδομένων από εφαρμογές. Στο παρακάτω σχήμα, παρουσιάζεται η προαναφερόμενη αρχιτεκτονική δικτύου[14-16].



Εικόνα 30 Σύγκριση μεταξύ ETHERNET/IP έναντι Μοντέλου OSI

Επιπλέον, το CIP λειτουργεί με τα ίδια πρότυπα με το παλαιότερα διαδεδομένο DeviceNet και ControlNet, καθιστώντας το πλήρως συμβατό και με τα δύο. Αυτό σημαίνει ότι η επιλογή ενός προϊόντος Ethernet/IP όχι μόνο παρέχει δυνατότητες CIP, αλλά παρέχει επίσης πρόσβαση στις δυνατότητες DeviceNet και ControlNet. Είναι σημαντικό να σημειωθεί ότι αυτό δεν είναι περιοριστικό, καθώς η εφαρμογή ενός συστήματος SCADA μπορεί να βασίζεται αποκλειστικά στα πρωτόκολλα TCP/IP και UDP, ενώ εξακολουθεί να μπορεί να ενσωματωθεί με συστήματα CIP.

Το Ethernet έχει το μοναδικό χαρακτηριστικό ότι είναι ένα δίκτυο με ενεργή υποδομή. Σε αντίθεση με τα συνηθισμένα βιομηχανικά δίκτυα, που συνήθως έχουν περιορισμένη χωρητικότητα και τρόπους σύνδεσης, το δίκτυο EtherNet/IP προσφέρει τη δυνατότητα σύνδεσης σχεδόν απεριόριστου αριθμού συσκευών σε λειτουργία point-to-point. Επιπλέον, υποστηρίζει διάφορες τοπολογίες, όπως γραμμικές και δακτυλίου, παρέχοντας ευελιξία στη σχεδίαση δικτύων που μπορούν να προσαρμοστούν στις ανάγκες.

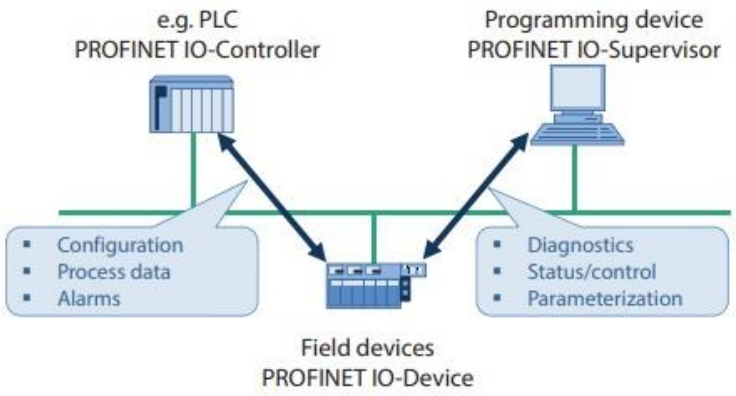
Η συμμόρφωση με τα πρότυπα IEEE Ethernet δίνει τη δυνατότητα επιλογής ταχυτήτων δικτύου, από 10 Mbps έως 1 Gbps, και διαφορετικές τεχνολογίες σύνδεσης, όπως χαλκός, οπτική ίνα και ασύρματη σύνδεση. Επιπλέον, η εξάρτηση από τα πρότυπα IEEE επιτρέπει την ενσωμάτωση νέων εξελίξεων, όπως το Single Pair Ethernet.

Τέλος, τα συστήματα EtherNet/IP μπορούν να παραμετροποιηθούν για να λειτουργούν είτε ως σχέση master/slave είτε ως κατανεμημένη αρχιτεκτονική ελέγχου με peer-to-peer επικοινωνίες [17-19].

3.6.9 Profinet

Το Profinet (Process Field Net) είναι ένα βιομηχανικό πρωτόκολλο επικοινωνίας που βασίζεται στο βιομηχανικό Ethernet, σχεδιασμένο για τη συλλογή δεδομένων από και τον έλεγχο του εξοπλισμού σε βιομηχανικά συστήματα, με εξαιρετική ακρίβεια στην παράδοση

δεδομένων υπό αυστηρούς χρονικούς περιορισμούς. Αυτό το πρότυπο διατηρείται και υποστηρίζεται από τον οργανισμό Profibus και Profinet International.
Υπάρχουν δύο παραλλαγές του Profinet, το Profinet I/O (Input Output) και το Profinet CBA (Component Based Automation). Το Profinet IO χρησιμοποιεί το υλικό και λογισμικό του κλασσικού Ethernet για να καθορίσει ένα δίκτυο με σκοπό την ανταλλαγή δεδομένων, alarm και διαγνωστικών μηνυμάτων μεταξύ των PLC και των άλλων συσκευών του βιομηχανικού δικτύου. Ενώ το Profinet CBA επικεντρώνεται σε κατανεμημένα συστήματα αυτοματισμού
Το Profinet IO ακολουθεί το μοντέλο παρόχου-καταναλωτή (Provider-Consumer) για την ανταλλαγή δεδομένων, όπου το ρόλο των provider έχουν οι I/O Devices ενώ το ρόλο των consumers οι συσκευές I/O Controllers. Συγκεκριμένα το πρωτόκολλο Profinet I/O καθορίζει 3 είδη συσκευών που συνδέονται στο δίκτυο και αυτά είναι τα εξής :



Εικόνα 31

- **I/O Controller**, οι οποίοι τυπικά είναι τα PLCs τα οποία εκτελούν τα προγράμματα αυτοματισμού και ελέγχου των διεργασιών. Ο I/O Controller δίνει τα δεδομένα εξόδου στις διαμορφωμένες συσκευές IO ως πάροχος και είναι ο καταναλωτής των δεδομένων εισόδου των συσκευών IO.
- **I/O Devices**, είναι οι συσκευές που εφαρμόζονται στο πεδίο και ελέγχονται από τους I/O Controllers μέσω του Profinet IO (συγκρίσιμη με τη λειτουργία ενός slave στο PROFIBUS). Τέτοιες συσκευές έχουν την δυνατότητα να είναι remote I/O modules, drives, αισθητήρες, επενεργητές κλπ.
- **I/O Supervisor**, αυτό μπορεί να είναι μια συσκευή προγραμματισμού (PD), προσωπικός υπολογιστής (PC) ή ανθρώπινη μηχανή (HMI) , με σκοπό να θέτει παραμέτρους και να λαμβάνει διαγνωστικά μηνύματα από τις I/O Devices

Το πρωτόκολλο Profinet I/O χρησιμοποιεί 3 διαφορετικά κανάλια επικοινωνίας για την ανταλλαγή δεδομένων μεταξύ I/O Controller και I/O Devices:

- Το βασικό TCP/IP κανάλι είναι χρήσιμο για την παραμετροποίηση, την διαμόρφωση (configuration) και για τις κυκλικές ενέργειές ανάγνωσης/εγγραφής.
- Το κανάλι που αναφέρεται ως RT ή Real Time χρησιμοποιείται συνήθως για τη μετάδοση τυπικών δεδομένων μετ' επιστροφής και μηνυμάτων συναγερμού. Οι

επικοινωνίες RT παρακάμπτουν τα τυπικά επίπεδα TCP/IP του δικτύου Ethernet για να επισπεύσουν την ανταλλαγή δεδομένων μεταξύ των PLC και των field devices σε χρόνο που κυμαίνεται μεταξύ 1-10 ms.

- Το τρίτο κανάλι είναι το Isochronous Real Time (IRT) και αποτελεί το κανάλι πολύ υψηλής ταχύτητας που χρησιμοποιείται για εφαρμογές motion control.

Η ταχύτητα μεταφοράς δεδομένων πάνω σε ένα δίκτυο Profinet I/O μεταξύ ενός controller και των devices είναι της τάξης των 100 Mbits/s όπως και το Fast Ethernet με την απόσταση μεταξύ των συσκευών να είναι πάνω από 100m. Εξαιτίας της υψηλής ταχύτητας μεταφοράς δεδομένων και του χρόνου απόκρισης (response time) που είναι < 1ms το δίκτυο Profinet IO είναι ιδανικό για εφαρμογές όπου απαιτούνται υψηλές ταχύτητες μεταφοράς δεδομένων.
Το Profinet CBA διακρίνεται από τα ανταγωνιστικά πρωτόκολλα (Modbus TCP, EtherNet/IP κ.λπ.) μέσω της πλήρους ενσωμάτωσης των τυποποιημένων λειτουργιών και αρχών της τεχνολογίας πληροφοριών αλλά πλέον δεν υποστηρίζεται και χρησιμοποιείται πολύ σπάνια στην πράξη [20-24].

ΚΕΦΑΛΑΙΟ 4^{Ο}

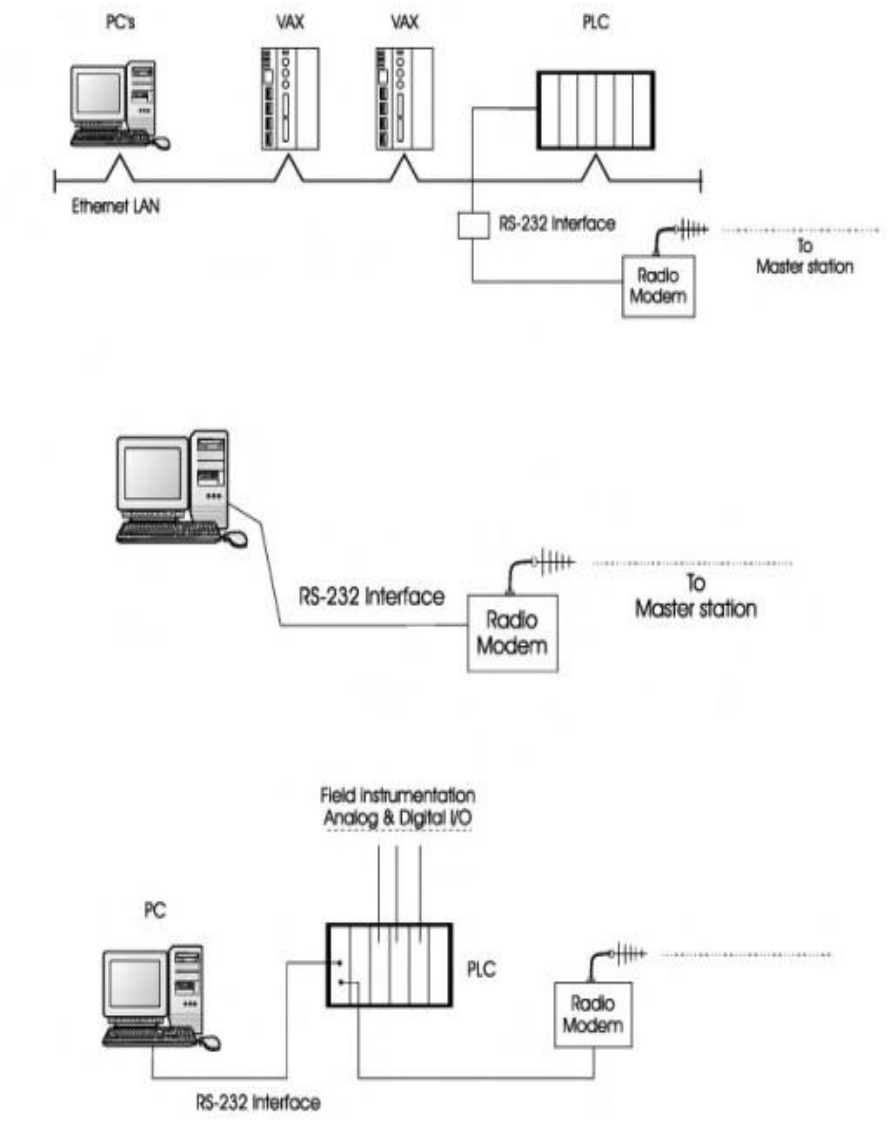
4.1 Κεντρικός Σταθμός Παρακολούθησης

Προκειμένου να ελέγχονται οι βιομηχανικές διαδικασίες με ασφάλεια και αποτελεσματικότητα, είναι απολύτως απαραίτητο να υιοθετηθούν κάποια ανθρώπινα μέσα για την παρακολούθηση των δυναμικών αλλαγών των ελεγχόμενων μεταβλητών και άλλων μεταβλητών και την παρέμβαση κατά την έναρξη, την κανονική λειτουργία και τη διακοπή αυτών των διαδικασιών. Επιπλέον, είναι επίσης απαραίτητο η προαναφερθείσα συσκευή να επιτρέπει τη ρύθμιση και τη συντήρηση των τοπικών μονάδων ελέγχου. Αυτό γίνεται εφικτό μέσω του Κεντρικού Σταθμού Παρακολούθησης (CMS).

Εικόνα 32 Κεντρικός σταθμός παρακολούθησης SCADA

Ο Κεντρικός Σταθμός Παρακολούθησης ή κύριος σταθμός είναι ο κεντρικός κόμβος εντολών και ελέγχου στα συστήματα SCADA, υπεύθυνος για την εποπτεία και τη διαχείριση ολόκληρου του δικτύου. Συλλέγει δεδομένα από απομακρυσμένες συσκευές πεδίου και RTU/PLC, παρέχει δυνατότητες παρακολούθησης και ελέγχου σε πραγματικό χρόνο και διευκολύνει την αποτελεσματική απόκτηση δεδομένων.

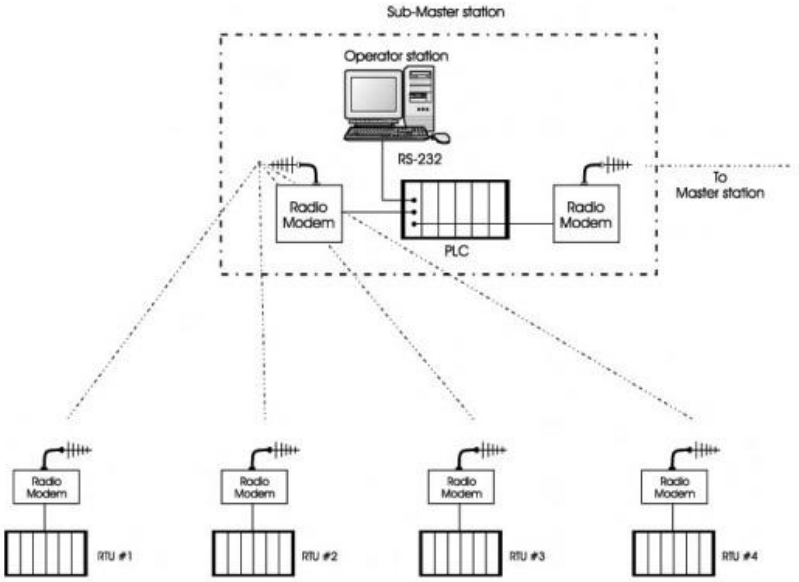
Οι κύριοι σταθμοί SCADA διαφέρουν σε μέγεθος από μικρά control rooms σε υποσταθμούς έως τεράστιους κεντρικούς σταθμούς SCADA. Ο κεντρικός σταθμός έχει δύο βασικές λειτουργίες: πρώτον, να λαμβάνει περιοδικά δεδομένα από τα RTU και τους υποσταθμούς master, και δεύτερον, να ελέγχει απομακρυσμένες συσκευές μέσω του χειριστή σταθμού. Υπάρχουν πολλοί δυνατοί συνδυασμοί συστημάτων, όπως φαίνεται στο παρακάτω διάγραμμα.



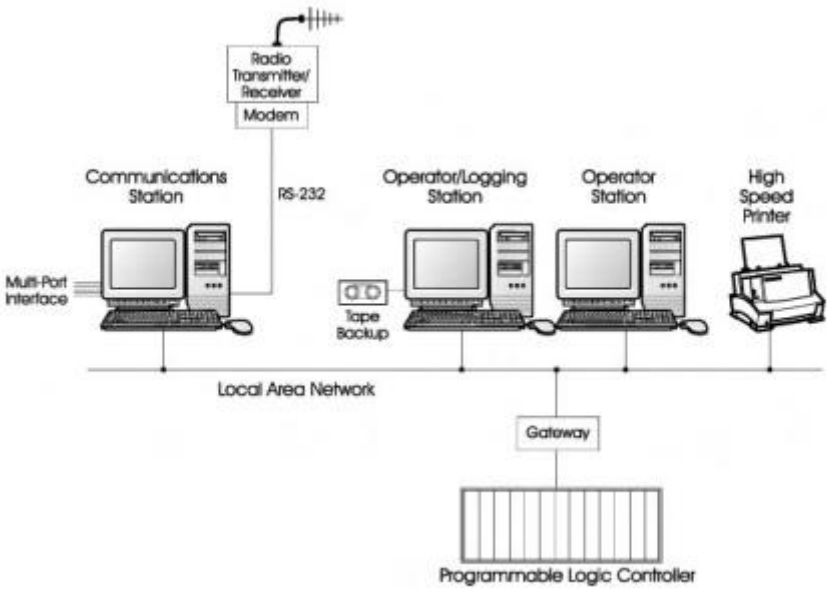
Εικόνα 33 Διάφορες προσεγγίσεις για τον κύριο σταθμό

Μπορεί επίσης να απαιτηθεί η δημιουργία ενός sub-master σημείου ελέγχου. Αυτό είναι απαραίτητο για τον έλεγχο των περιοχών εντός ενός συγκεκριμένου περιορισμένου τμήματος. Ο υπο-κύριος σταθμός εξυπηρετεί μια ποικιλία λειτουργιών, συμπεριλαμβανομένων, ενδεικτικά, των εξής:

- Διαδικασία λήψης πληροφοριών από απομακρυσμένες τερματικές μονάδες (RTU) σε μια συγκεκριμένη περιοχή.
- Καταγραφή και εμφάνιση αυτών σε τοπικό σταθμό-χειριστή
- Μεταφορά των πληροφοριών πίσω στον κεντρικό σταθμό.
- Να προωθεί αιτήματα ελέγχου από τον κεντρικό σταθμό στις RTU εντος ζώνης του.



Εικόνα 34 Αρχιτεκτονική sub-master



Εικόνα 35 Τυπική δομή του κεντρικού σταθμού

Ο κεντρικός σταθμός διαθέτει τα ακόλουθα τυπικά χαρακτηριστικά:

- **Καθιέρωση επικοινωνιών**, η οποία περιλαμβάνει τη διαμόρφωση κάθε RTU,

την προετοιμασία κάθε RTU με παραμέτρους I/O και τη λήψη προγραμμάτων ελέγχου και απόκτησης δεδομένων στο RTU

-**Λειτουργία της ζεύξης επικοινωνιών**, η διαδικασία περιλαμβάνει έναν αριθμό εργασιών, όπως τον εντοπισμό δεδομένων σε κάθε RTU και τη μεταφορά τους σε RTU, την καταγραφή συναγερμών και συμβάντων στον σκληρό δίσκο και την εμφάνισή τους στην οθόνη του χειριστή, εάν απαιτείται. Επιπλέον, περιλαμβάνει την αυτόματη σύνδεση εισόδων και εξόδων σε διαφορετικό RTU.

- **Διαγνωστικά**, συμπεριλαμβανομένων ακριβών διαγνωστικών πληροφοριών σχετικά με βλάβες RTU και πιθανά ζητήματα, καθώς και την πρόβλεψη πιθανών προβλημάτων, όπως υπερφόρτωση δεδομένων.

Συνολικά, ο κεντρικός σταθμός αποτελείται από μια συλλογή υπολογιστών, διακομιστές, περιφερειακές συσκευές και συστήματα εισόδου/εξόδου που συνδράμουν τον χειριστή στην παρακολούθηση της κατάστασης του πεδίου και την εκτέλεση ελέγχου στις κατάλληλες στιγμές. Τα στοιχεία του κεντρικού σταθμού μπορούν να κατηγοριοποιηθούν σε στοιχεία υλικού και λογισμικού.

4.1 Υλικό κύριου σταθμού

Το υλικό σε έναν κεντρικό σταθμό αποτελείται από τον υπολογιστή και τους διακομιστές (servers) των συστημάτων που χρησιμοποιούνται για την εκτέλεση διάφορων εργασιών που πρέπει να πραγματοποιηθούν από τον κεντρικό σταθμό. Η επιλογή των διακομιστών υπολογιστών προβλέπεται να γίνεται με βάση τις απαιτήσεις που έχει ο κύριος σταθμός.

4.1.1 Συστήματα διακομιστών του κεντρικού σταθμού

Ο κεντρικός σταθμός SCADA αποτελείται από μια σειρά διακομιστικών συστημάτων, καθένα εξειδικευμένο για μια συγκεκριμένη λειτουργία. Οι διακομιστές συνδέονται μεταξύ τους μέσω ενός διπλού πλεονάζοντος LAN υψηλής ταχύτητας. Τα δεδομένα από κάθε διακομιστή είναι προσβάσιμα μέσω του πελάτη-εξυπηρετητή. Κάθε σύστημα διακομιστή διαθέτει εξειδικευμένες δυνατότητες και χαρακτηριστικά που το καθιστούν κατάλληλο για μια συγκεκριμένη εφαρμογή. Ανάμεσα σε αυτά περιλαμβάνονται υψηλής απόδοσης επεξεργαστές, αυξημένη μνήμη RAM, πλεονασμός στα τροφοδοτικά, δίκτυα υψηλής ταχύτητας και μνήμες RAM υψηλής απόδοσης. Τα διαθέσιμα συστήματα διακομιστών υπολογιστών σε έναν κεντρικό σταθμό SCADA περιλαμβάνουν:

1. SCADA Server: Έχει την ευθύνη για όλες τις βασικές λειτουργίες SCADA, της συλλογής και εμφάνισης δεδομένων και εκτέλεσης εντολών ελέγχου από το κεντρικό σταθμό.

2. Application Server : Ο διακομιστής εφαρμογών εμπεριέχει τις ενότητες λογισμικού εφαρμογών που απαιτούνται για το συγκεκριμένο σύστημα SCADA.
Για το σύστημα παραγωγής SCADA, το λογισμικό εφαρμογών περιλαμβάνει αυτόματο έλεγχο παραγωγής, οικονομική φορτοδιανομή, δέσμευση μονάδων, βραχυπρόθεσμη πρόβλεψη φορτίου και άλλες λειτουργίες. Το σύστημα μετάδοσης SCADA διαθέτει διάφορα συστήματα διαχείρισης ενέργειας (EMS), τα οποία περιλαμβάνουν, μεταξύ άλλων, τον επεξεργαστή

διαμόρφωσης/τοπολογίας δικτύου, ανάλυση έκτακτης ανάγκης, ισορροπημένη τριφασική ισχύ και βέλτιστη ροή ισχύος. Εν τω μεταξύ, το σύστημα διανομής SCADA διαθέτει δυνατότητα διαχείρισης τάσης, διαχείριση φορτίου, έλεγχο συντελεστή ισχύος, διανομή αμφίδρομης επικοινωνίας και πολλά άλλα. Για συστήματα μικρότερης κλίμακας, το λογισμικό εφαρμογής μπορεί να εγκατασταθεί απευθείας στον διακομιστή SCADA. Επιπλέον, εκτός από τους προαναφερθέντες διακομιστές, υπάρχουν αρκετοί άλλοι τύποι διακομιστών που υπάρχουν στο συγκεκριμένο σύστημα.

3. ISR ή HIM server : Αυτός ο διακομιστής υποστηρίζει την αποθήκευση και ανάκτηση πληροφοριών καθώς και τις λογιστικές δραστηριότητες για το σύστημα, συμπεριλαμβανομένων των στιγμιοτύπων δεδομένων σε πραγματικό χρόνο, καταγραφής, ανάκτησης ιστορικών πληροφοριών και παραγωγής εκθέσεων.

4.Development server : Αυτός ο διακομιστής χειρίζεται την ανάπτυξη και τις αλλαγές στο λογισμικό του συστήματος, συμπεριλαμβανομένης της ανάπτυξης νέων προγραμμάτων, οθονών και βάσεων δεδομένων.

5.Network management server (NMS) : Αυτός ο διακομιστής παρακολουθεί και διαχειρίζεται τον εξοπλισμό που είναι συνδεδεμένος στο τοπικό δίκτυο του κεντρικού σταθμού.

6. Video projection system (mimic board) : Ένα σύστημα προβολής βίντεο, κινεί τις οθόνες των μιμητικών πινάκων σε έναν μεγάλο κεντρικό σταθμό. Οι κύριοι σταθμοί είναι εξοπλισμένοι με οθόνες LCD τελευταίας τεχνολογίας που μπορούν να εμφανίζουν την περιοχή ελέγχου με ποικίλο τρόπο σύμφωνα με ανάλογα με τις απαιτήσεις των χειριστών, και ένα ξεχωριστό σύστημα προβολής βίντεο χειρίζεται αυτή τη λειτουργία.

7. CFE (communication front end)/FEP (front-end processor): Το Communication front end (CFE) είναι η διασύνδεση του κεντρικού υπολογιστή με ένα δίκτυο ή περιφερειακές συσκευές. Το CFE χρησιμοποιείται για την αποφόρτιση του κεντρικού υπολογιστή από τις λειτουργίες επικοινωνίας, όπως η διαχείριση των περιφερειακών συσκευών, μετάδοση και λήψη μηνυμάτων, συναρμολόγηση και αποσυναρμολόγηση πακέτων, και ανίχνευση και διόρθωση σφαλμάτων. Το CFE, που συχνά αναφέρεται ως FEP (front-end processor) επικοινωνεί με τις περιφερειακές συσκευές χρησιμοποιώντας αργές σειριακές διεπαφές, συνήθως μέσω δικτύων επικοινωνίας. Η επικοινωνία του FEP με τον κεντρικό υπολογιστή γίνεται χρησιμοποιώντας μια παράλληλη διασύνδεση υψηλής ταχύτητας διεπαφή.

8. **Inter-Control Center Communications Protocol (ICCP):** Πρωτόκολλο επικοινωνίας μεταξύ κέντρων ελέγχου (ICCP) ,υποστηρίζει τη μετάδοση δεδομένων μεταξύ του master και της ανώτερης ιεραρχίας. Ο ICCP υποστηρίζει επίσης την ανταλλαγή δεδομένων μεταξύ των εγκαταστάσεων με την κατώτερη ιεραρχία.

9. Dispatcher Training Simulater (DTS) server : Ένας διακομιστής που έχει σχεδιαστεί για προσομοίωση εκπαίδευσης αποστολέα (DTS) μπορεί να βρεθεί σε έναν πρωτεύοντα κεντρικό σταθμό, συχνά σε περιφερειακό επίπεδο. Ο διακομιστής DTS χρησιμοποιείται για την εκπαίδευση των χειριστών συστήματος που είναι υπεύθυνοι για τη διαχείριση του συστήματος.

4.1.2 Λογισμικό κεντρικού σταθμού

Το λογισμικό που χρησιμοποιείται στους κεντρικούς σταθμούς μπορεί να αναλυθεί σε τρία κύρια τμήματα: το λειτουργικό σύστημα, το σωστά διαμορφωμένο λογισμικό SCADA και το λογισμικό εφαρμογής SCADA. Επιπλέον, υπάρχει υλικολογισμικό που απαιτείται, όπως το BIOS, το οποίο χρησιμεύει ως ενδιάμεσος μεταξύ του υλικού του υπολογιστή και του λειτουργικού συστήματος. Το λειτουργικό σύστημα μπορεί να αποτελείται από διάφορες επιλογές, όπως DOS, Windows 95/98/2000/10, Windows NT, LINUX και UNIX. Ο όρος λογισμικό συστήματος SCADA αναφέρεται σε λογισμικό που συντάσσεται από τον προμηθευτή του συγκεκριμένου συστήματος SCADA και στη συνέχεια προσαρμόζεται από έναν μεμονωμένο χρήστη.

4.2 Λογισμικό SCADA

Στα σύγχρονα συστήματα SCADA, τα προγράμματα των κεντρικών σταθμών δεν αναπτύσσονται από την αρχή. Αντίθετα, αποτελούνται από προϋπάρχοντα στοιχεία λογισμικού που διευκολύνουν τυποποιημένες μεθόδους διασύνδεσης. Αντί να παράγουν ήδη διαμορφωμένες λύσεις, οι κατασκευαστές δημιουργούν προσαρμόσιμες πλατφόρμες που μπορούν να προσαρμοστούν για να ταιριάζουν στις συγκεκριμένες ανάγκες και απαιτήσεις κάθε μεμονωμένης περίπτωσης. Με τη διαμόρφωση, τη συμπλήρωση ή τη διασύνδεση τμημάτων αυτών των βασικών πλατφορμών, δημιουργείται η απόλυτη λύση ξεχωριστά για κάθε πρόβλημα. Αυτή η εργασία μπορεί να γίνει από τον ίδιο τον κατασκευαστή της πλατφόρμας ή από έναν ξεχωριστό ενοποιητή συστήματος (system integrator) ή τελικό χρήστη. Ως αποτέλεσμα, το κέντρο ελέγχου (και κατ' επέκταση ολόκληρο το σύστημα SCADA) μπορεί να κατασκευαστεί κατά παραγγελία για κάθε εφαρμογή, επιλέγοντας κάθε φορά από ένα σύνολο υπαρχόντων εξαρτημάτων τα εξαρτήματα που χρειάζονται για να καλύψουν τις ανάγκες της συγκεκριμένης εφαρμογής.

Η επεξεργασία τεράστιων ποσοτήτων δεδομένων είναι απαραίτητη προϋπόθεση για τα σύγχρονα συστήματα SCADA ώστε να δίνουν ακριβείς εντολές ελέγχου. Είναι σημαντικό να έχουμε κατά νου ότι το ανθρώπινο μυαλό έχει περιορισμένη ικανότητα να χειρίζεται μεγάλες ποσότητες πληροφοριών, αλλά είναι ικανό να λαμβάνει οξυδερκείς και περίπλοκες αποφάσεις. Επομένως, το λογισμικό που χρησιμοποιείται σε αυτά τα συστήματα πρέπει να παρέχει στους διαχειριστές συστημάτων κατανοητές και αξιόπιστες πληροφορίες σχετικά με την κατάσταση του συστήματος.

Υπάρχουν δύο κύριες ταξινομήσεις για το λογισμικό SCADA: ιδιόκτητο και ανοιχτού κώδικα. Το ιδιόκτητο λογισμικό δημιουργείται από εταιρείες για διασύνδεση με το μεμονωμένο υλικό τους και διατίθεται στο εμπόριο ως προϋπάρχουσα λύση. Το πρωταρχικό πρόβλημα με αυτές τις λύσεις είναι η εξάρτησή τους από το σύστημα του προμηθευτή. Αντίθετα, τα συστήματα ανοικτού κώδικα είναι δημοφιλή λόγω της ικανότητάς τους να επιτυγχάνουν διαλειτουργικότητα εντός του συστήματος. Η δια λειτουργικότητα αφορά την ικανότητα να συνδυάζονται διάφοροι εξοπλισμοί από διάφορους κατασκευαστές σε ένα κοινό σύστημα. Συνδυάζονται με όλες τις σειρές PLC της Siemens και μπορούν επίσης να συνδυαστούν με PLC άλλων εταιρειών σε υπάρχοντα συστήματα. Εγκαθίστανται στον υπολογιστή ή στον πίνακα ελέγχου, ανάλογα με την εφαρμογή. Υπάρχει μια ποικιλία από πίνακες ελέγχου (HMI) που καλύπτουν κάθε απαίτηση και ανάγκη.

4.2.1 Κύριες λειτουργίες του λογισμικού SCADA

- Απόκτηση Δεδομένων σε πραγματικό χρόνο(Real-time data acquisition): PLC (Programmable Logic Controllers), RTUs (Remote Terminal Units) και αισθητήρες.
- Οπτικοποίηση Δεδομένων (Data Visualization): Προσφέρει μια γραφική διεπαφή χρήστη για την οπτικοποίηση των δεδομένων που έχουν αποκτηθεί σε πραγματικό χρόνο, χρησιμοποιώντας εργαλεία όπως γραφήματα, διαγράμματα και μετρητές.
- Συναγερμός (Alarmimg): Διαχείριση συναγερμών (ενεργοποιήσει τους) βάσει προκαθορισμένων συνθηκών, όπως υψηλά/χαμηλά όρια ή τάσεις. Το σύστημα διαχείρισης συναγερμών θα πρέπει επίσης να παρέχει ένα μέσο για την αναγνώριση, σίγαση και παρακολούθηση των συναγερμών.
- Αναφορά (Reporting): Δημιουργία αναφορών με βάση τα δεδομένα που συλλέγονται, όπως ημερήσιες, εβδομαδιαίες, μηνιαίες ή ετήσιες αναφορές.
- Αποθήκευση Δεδομένων (Data Storage): Η δυνατότητα αποθήκευσης των συγκεντρωθέντων δεδομένων σε μια βάση δεδομένων, μαζί με την ικανότητα ανάκτησης και ανάλυσης ιστορικών δεδομένων.
- Απομακρυσμένη Πρόσβαση (Remote Access): Δυνατότητες απομακρυσμένης πρόσβασης, επιτρέποντας στους χρήστες να παρακολουθούν και να ελέγχουν τις βιομηχανικές διεργασίες από οποιαδήποτε τοποθεσία.
- Ενσωμάτωση με άλλα συστήματα: Ενσωμάτωση με άλλα συστήματα, όπως συστήματα ERP (Enterprise Resource Planning), MES (Manufacturing Execution Systems) και ιστορικές βάσεις δεδομένων.
- Διαχείριση χρηστών: Έλεγχος της πρόσβαση των χρηστών στο σύστημα SCADA και τις λειτουργίες τους, με βάση τους ρόλους και τα δικαιώματα τους.
- Εξέλιξη (Trending): Δυνατότητα εξέλιξης των δεδομένων με την πάροδο του χρόνου, επιτρέποντας στους χρήστες να εντοπίζουν μοτίβα και να εντοπίζουν πιθανά προβλήματα.
- Έλεγχος (Control): Η δυνατότητα ελέγχου βιομηχανικών διεργασιών, όπως η εκκίνηση και η διακοπή διεργασιών, η προσαρμογή σημείων ρύθμισης και η ενεργοποίηση συμβάντων.
- Ασφάλεια (Security): Παροχή ισχυρών μέτρων ασφαλείας για την προστασία του συστήματος SCADA και των δεδομένων του από μη εξουσιοδοτημένη πρόσβαση και απειλές στον κυβερνοχώρο.

Αυτά είναι μερικά από τα βασικά χαρακτηριστικά του λογισμικού SCADA. Τα συγκεκριμένα χαρακτηριστικά ενός λογισμικού SCADA μπορεί να διαφέρουν ανάλογα με τον προμηθευτή και τις απαιτήσεις της βιομηχανικής διαδικασίας που παρακολουθείται και ελέγχεται.

4.2.2 Επιλογές λογισμικού

Υπάρχουν πληθώρα επιλογών λογισμικού για συστήματα SCADA, καλύπτοντας τόσο εμπορικές όσο και ανοικτές λύσεις. Το λογισμικό SCADA διακρίνεται συνήθως σε δύο κατηγορίες, το ιδιόκτητο και το ανοικτού κώδικα. Οι εταιρείες αναπτύσσουν ιδιόκτητο λογισμικό για να αλληλεπιδρούν με το δικό τους υλικό, το οποίο προσφέρουν ως "έτοιμες λύσεις". Το βασικό πρόβλημα με αυτές τις λύσεις είναι η έντονη εξάρτηση από τον προμηθευτή του συστήματος. Αντίθετα, τα συστήματα ανοικτού κώδικα έχουν αποκτήσει δημοτικότητα λόγω της δυνατότητας προσφοράς δια λειτουργικότητας στο σύστημα. Η δια λειτουργικότητα αφορά τη δυνατότητα συνδυασμού διάφορου εξοπλισμού από διάφορους κατασκευαστές σε ένα κοινό σύστημα .Η επιλογή του λογισμικού SCADA εξαρτάται από διάφορους παράγοντες, συμπεριλαμβανομένου του μεγέθους και της πολυπλοκότητας της βιομηχανικής διαδικασίας, του επιπέδου προσαρμογής που απαιτείται και των περιορισμών του προϋπολογισμού.

Ορισμένες δημοφιλείς εμπορικές επιλογές λογισμικού SCADA περιλαμβάνουν:

Αρ.	Λογισμικό SCADA	Υποστηριζόμενο λειτουργικό σύστημα	Χαρακτηριστικά	Υποστηριζόμενο πρωτόκολλο
1	AVEVA Intouch	Windows , Linux	Ασφαλής, εποπτικός έλεγχος σε πραγματικό χρόνο, χειρισμός πολύπλοκων λειτουργιών	OPC UA, MQTT, DNP3, MODBUS
2	FactoryTalkview	Windows	Πολλαπλοί χρήστες και διακομιστές μπορούν να χρησιμοποιηθούν, δοκιμή των στοιχείων της εφαρμογής	OPC, ODBC, DDE
3	CimplCity	Windows	Ασφαλέστερη, συγκεντρωτική λειτουργία, απομακρυσμένη πρόσβαση για τον έλεγχο και την πρόσβαση στις πληροφορίες.	OPC UA, MODBUS
4	Simatic WinCC V7	Windows	Είναι κατάλληλο για κάθε εφαρμογή. Αρχειοθέτηση δεδομένων με υψηλή απόδοση . Ενσωματωμένος διακομιστής MS SQL	OPC client & server, ODBC server, OPC UA, OPC classic
5	GENESIS64	Windows ,Cloud	Ασφάλεια συστήματος, αρχειοθέτηση και διατήρηση, παρακολούθηση σε πραγματικό χρόνο	OPC Classic, OPC UA BACnet, Modbus, SNMP, Ethernet
6	VTSCADA	Windows ,Linux	Πρόγραμμα προβολής ιστορικών δεδομένων, Διαισθητική πλοήγηση στη σελίδα,	OPC client & server, ODBC server, OPC UA, OPC classic
7	inVIEW IIOT Platform	Cloud	Απομακρυσμένη πρόσβαση, API & ενσωμάτωση, ανάλυση επιδόσεων μηχανών	MQTT, OPC UA, MODBUS

8	AggreGate SCADA/HMI	Linux ,MAC	Φιλικό προς το Cloud, υποστήριξη SQL	BACnet, DNP3, OPC UA, OPC, KNX, Modbus

1. AVEVA

Αυτό το λογισμικό SCADA είναι κατάλληλο τόσο για μεγάλες όσο και για μικρές βιομηχανίες και μπορεί να συμβάλει στη βελτίωση της αξιοπιστίας των μηχανημάτων και της λειτουργικής αποδοτικότητας. Με τη χρήση αυτού του λογισμικού, είναι δυνατόν να εφαρμόσουμε το πλαίσιο σε πραγματικό χρόνο, να δημιουργήσουμε συναγερμούς, να καταγράψουμε συμβάντα και δεδομένα, προσφέροντας έτσι τη δυνατότητα για τη δημιουργία ενός κοινού ροής πληροφοριών[7].

2. FactoryTalk View

Αυτό το SCADA λογισμικό είναι κατάλληλο για προηγμένες βιομηχανικές εφαρμογές και μπορεί να χρησιμοποιηθεί από διακριτικές εφαρμογές έως παρτίδες. Η Rockwell Automation ανέπτυξε αυτό το λογισμικό, και με τη χρήση του, μπορούμε να ενσωματώσουμε πολλούς χρήστες και διακομιστές για εφαρμογές HMI. Παρέχει όλα τα απαραίτητα εργαλεία για τη δημιουργία κατάλληλων εφαρμογών παρακολούθησης διεργασιών και εποπτικού ελέγχου. Με αυτό το λογισμικό, μπορούμε να παρακολουθούμε τα δεδομένα σε πραγματικό χρόνο. Επιπλέον, διαθέτει σύνδεση με βάση δεδομένων SQL και αντικείμενο πλέγματος δεδομένων, παρέχοντας έτσι κατάλληλες πληροφορίες για τη λήψη αποφάσεων παραγωγής[8].

3. CIMPLICITY SCADA

Αυτό το λογισμικό SCADA είναι κατάλληλο για μεγάλες βιομηχανίες μεταποίησης και προσφέρει ταχύτερη απόκριση, μείωση του κόστους και υψηλή κερδοφορία. Χρησιμοποιώντας αυτό το λογισμικό, μπορούμε να ελέγχουμε τη διαδικασία μας από απομακρυσμένες τοποθεσίες[8].

4. SIMATIC WinCC V7

Αυτό το λογισμικό SCADA προσφέρει έναν βελτιωμένο τρόπο παρακολούθησης της βιομηχανικής διαδικασίας. Διαθέτει αρκετές λειτουργίες υψηλής απόδοσης, οι οποίες είναι πολύ χρήσιμες για την παρακολούθηση της αυτοματοποιημένης διαδικασίας. Με τη χρήση αυτού του λογισμικού, είμαστε σε θέση να παρακολουθούμε τη λειτουργία του εργοστασίου μέσω του διαδικτύου[8].

5. GENESIS64

Πρόκειται για ένα προηγμένο λογισμικό SCADA που έχει σχεδιαστεί για το λειτουργικό σύστημα της Microsoft. Μπορούμε να αξιοποιήσουμε αυτό το λογισμικό SCADA σε διάφορες εφαρμογές, εκμεταλλευόμενοι τις τεχνολογίες 64-bit και OPC UA που περιλαμβάνει. Μέσω της χρήσης αυτών των τεχνολογιών αιχμής, οι χειριστές είναι πλέον σε θέση να ενσωματώνουν απρόσκοπτα και να εκτελούν παραγωγικές δραστηριότητες σε πραγματικό

χρόνο, όλα από ένα ενοποιημένο ταμπλό. Όχι μόνο αυτό, αλλά αυτό το σύστημα είναι επίσης πλήρως συμβατό με τους κανονισμούς ISA 18.2, επιτρέποντας ολοκληρωμένη διαχείριση συναγερμών σε πραγματικό χρόνο σε ολόκληρο το σύστημα. Επιπλέον, αυτό το λογισμικό διασφαλίζει ότι τα δεδομένα από συσκευές όπως αισθητήρες, μετρητές και επεξεργαστές μπορούν να μεταδοθούν με ασφάλεια και σε πραγματικό χρόνο.[8].

6. VTSCADA

Αυτό το λογισμικό SCADA είναι κατάλληλο για εξαιρετικά προσαρμοσμένες εφαρμογές βιομηχανικής παρακολούθησης και ελέγχου. Μεταξύ των πολυάριθμων πλεονεκτημάτων που προσφέρει, αυτό το λογισμικό διαθέτει την ικανότητα να εκτελεί ένα ευρύ φάσμα εργασιών, συμπεριλαμβανομένης της δημιουργίας αντιγράφων ασφαλείας συστήματος, δημιουργία αναφορών, έλεγχος έκδοσης εφαρμογής, ειδοποιήσεις συναγερμού, διαχείριση δημοσκοπήσεων και πολλές άλλες δυνατότητες. Λόγω της ανοιχτής αρχιτεκτονικής του και της εκτεταμένης σειράς προγραμμάτων οδήγησης συσκευών, μπορεί να επικοινωνήσει αποτελεσματικά με την πλειοψηφία των PLC και των RTU. Επιπλέον, με τη λειτουργία προβολής ιστορικών δεδομένων, είναι δυνατή η δημιουργία γραφημάτων με βάση προηγούμενα δεδομένα και η εξαγωγή τους όπως απαιτείται. Επιπλέον, υπάρχουν διαχωρισμένες οθόνες για κάθε RTU.[8].

7. inVIEW IIOT Platform

Μπορούμε να αξιοποιήσουμε αυτό το λογισμικό SCADA για απομακρυσμένο εποπτικό έλεγχο, καθώς μπορούμε να το χρησιμοποιήσουμε για την παρακολούθηση πραγματικών διαδικασιών μέσω προγραμμάτων περιήγησης στο διαδίκτυο. Επίσης, μπορούμε να το χρησιμοποιήσουμε για τη συλλογή δεδομένων από συσκευές IoT και από εξοπλισμό αυτοματισμού. Αυτό το λογισμικό είναι κατάλληλο τόσο για βιομηχανικό, οικιακό, όσο και για υποδομές αυτοματισμού. Ένα από τα κύρια χαρακτηριστικά του είναι η δυνατότητα πρόσβασης σε δεδομένα σε πραγματικό χρόνο και η δυνατότητα εισαγωγής και εξαγωγής δεδομένων. Με την απομακρυσμένη πρόσβαση στις μηχανές, μπορούμε να ελέγξουμε βιομηχανικές συσκευές όπως PLC, HMI, ρομπότ και άλλες[8].

8. AggreGate SCADA/HMI

Χρησιμοποιώντας αυτό το λογισμικό SCADA, είμαστε σε θέση να παρακολουθούμε τη λειτουργία των μηχανημάτων, των διαδικασιών και των εγκαταστάσεων. Μπορούμε να εφαρμόσουμε αυτό το λογισμικό για τον έλεγχο σε πολλούς βιομηχανικούς τομείς. Το λογισμικό διαθέτει έναν δημιουργό διεπαφής χρήστη (UI builder) που λειτουργεί σε πολλές πλατφόρμες, και με αυτόν τον τρόπο μπορούμε να δημιουργήσουμε μια βελτιωμένη ανθρώπου-μηχανής διεπαφή. Επιπλέον, διαθέτει λειτουργία στατιστικού ελέγχου διεργασιών, η οποία μας επιτρέπει να πραγματοποιήσουμε λεπτομερή ανάλυση των δεδομένων. Τέλος, αυτό το λογισμικό SCADA υποστηρίζει τον προγραμματισμό χρησιμοποιώντας γλώσσες PLC, όπως η λογική σκάλας, τα λειτουργικά διαγράμματα με τετράγωνα τμήματα, τα διαδοχικά λειτουργικά διαγράμματα και το δομημένο κείμενο[8].

Από την άλλη πλευρά, οι επιλογές λογισμικού SCADA ανοικτού κώδικα περιλαμβάνουν:

Αρ.	Λογισμικό SCADA	Υποστηριζόμενο λειτουργικό σύστημα	Χαρακτηριστικά	Υποστηριζόμενο πρωτόκολλο
1	Fernhill SCADA	Windows , Linux, MAC	Υποστηρίζει ανοικτές διεπαφές όπως OPC, UA, ODBC. Δυνατότητα πρόσβασης API, εργαλεία εισαγωγής, εργαλείο διαμόρφωσης.	MQTT, OPC Classic, OPC UA, and ODBC
2	TatsoftFactory studio	Windows , Linux, MAC	Μοντελοποίηση δεδομένων σε πραγματικό χρόνο, καταγραφή δεδομένων, διαδρομή ελέγχου, συναγερμοί και συμβάντα	OPC/MQTT
3	RapidSCADA	Windows , MAC	Παρακολούθηση σε πραγματικό χρόνο, οπτικοποίηση δεδομένων, ενσωμάτωση υλικού	MODBUS, OPC, SNMP, SMTP, MQTT
4	IgnitionSCADA	Windows , Linux, MAC , Cloud	Ενσωματωμένο OPC UA Ενσωμάτωση υλικού Ενσωμάτωση HMI Ετικέτες SQL Παρακολούθηση σε πραγματικό χρόνο, Υποστηρίζει Oracle, MS SQL, MYSQL κ.λπ.	Modbus, UDP, and TCP
5	OpenSCADA	Windows ,Linux	Δυνατότητα σύνδεσης με OPC Client, S7 MPI, S7 PPI, Profinet, Modbus RTU, Modbus TCP/IP.	Modbus, OPC-UA, HTTP
6	VTSCADALight	Windows ,Linux	Παρακολούθηση της υγείας των σταθμών εργασίας/εξυπηρετητών, δυνατότητα πλεονασμού και δημιουργίας αντιγράφων ασφαλείας του συστήματος, αναφορά στατιστικών στοιχείων και διαχείριση συναγερμών.	OPC, ODBC, SQL queries, Historian, and SOAP
7	SZARP	Windows ,Linux	Το SZARP υποστηρίζει κινητές συσκευές, καλύτερη διεπαφή χρήστη	MODBUS (TCP & client-server)
8	SCADA BR	Linux,MAC	Μπορεί να χρησιμοποιηθεί για οικιακό και κτιριακό αυτοματισμό, γραφική αναπαράσταση δεδομένων, σύστημα δικαιωμάτων χρήστη	MODBUS TCP/IP, OPC, DNP3, IEC, HTTP, Serial ASCII

1. Fernhill SCADA

Μπορούμε να χρησιμοποιήσουμε αυτό το λογισμικό SCADA για την παρακολούθηση και τον έλεγχο των διαδικασιών μας, είναι κατάλληλο για ευρύ φάσμα βιομηχανικών διεργασιών, από την υδροηλεκτρική έως την παραγωγή κρασιού. Αυτό το SCADA αποτελεί εξαιρετική λύση όσον αφορά την αρχιτεκτονική πελάτη-εξυπηρετητή. Επιπλέον, παρέχει διάφορες διεπαφές πρόσβασης σε δεδομένα, όπως το .net API, το Java API, το OPC Classic, το OPC UA και το ODBC. Αυτό το λογισμικό SCADA επιφέρει επίσης βελτιωμένα μέτρα ασφαλείας, διασφαλίζοντας την προστασία του εξοπλισμού μας από μη εξουσιοδοτημένη πρόσβαση[8].

2. Tatsoft Factory Studio

Χρησιμοποιώντας αυτό το εργαλείο, θα μπορούμε να αναπτύξουμε βιομηχανικές εφαρμογές με ασφάλεια και απόδοση. Το λογισμικό διαθέτει πολλά χαρακτηριστικά, όπως το μεσίτη MQTT, τη διαδρομή ελέγχου και πολλά άλλα. Μπορούμε να δημιουργήσουμε σενάρια προγραμματισμού σε C, VB.Net, JavaScript και Python. Επιπλέον, περιλαμβάνει πολλούς ενσωματωμένους οδηγούς πρωτοκόλλων για PLC, DCS, και υποστηρίζει επίσης άλλα βιομηχανικά πρότυπα[8].

3. Rapid SCADA

Το λογισμικό που αναφέρεται εδώ είναι προσβάσιμο ως ανοιχτού κώδικα και χρησιμοποιείται στη τομέα του βιομηχανικού αυτοματισμού. Έρχεται με μια σειρά εργαλείων, τα οποία επιταχύνουν την άμεση επίβλεψη και διαχείριση, καθιστώντας το ιδανικό για τεράστια και διάσπαρτα συστήματα βιομηχανικού αυτοματισμού. Επιπλέον, το λογισμικό μπορεί εύκολα να ενσωματωθεί με εξωτερικές βάσεις δεδομένων σε πραγματικό χρόνο. Τα βασικά χαρακτηριστικά του αποτελούνται από μια μονάδα αυτόματου ελέγχου, μια μονάδα ταχείας πύλης, απομακρυσμένη αντιμετώπιση προβλημάτων και άλλα χρήσιμα εργαλεία[8].

4. Ignition SCADA

Το συγκεκριμένο λογισμικού μπορεί να εφαρμοστεί σε μεγάλες βιομηχανίες και αποτελεί μια διαδικτυακή λύση που επιτρέπει τον απομακρυσμένο έλεγχο των διαδικασιών. Χρησιμοποιώντας αυτό το λογισμικό, μπορούμε να παρακολουθούμε δεδομένα από διάφορες τοποθεσίες[8].

5. OpenSCADA

Αυτό το είδος του λογισμικού SCADA προσφέρει αρθρωτότητα και επεκτασιμότητα, επιτρέποντας τον έλεγχο και την απεικόνιση βιομηχανικών διαδικασιών. Παρέχει βελτιωμένο έλεγχο των μονάδων και δίνει πρόσβαση στη βάση δεδομένων. Επιπλέον, διαθέτει διάφορες μεθόδους επικοινωνίας, όπως MODBUS και OPC-UA, για τη σύνδεση με

το εξωτερικό περιβάλλον. Η συλλογή δεδομένων από εξωτερικές πηγές, όπως ελεγκτές και αισθητήρες, είναι επίσης εφικτή[8].

6. VTScadaLight

Αυτό το λογισμικό SCADA είναι κατάλληλο για υψηλά προσαρμοσμένη βιομηχανική παρακολούθηση. Παρέχει μια βελτιωμένη αρχιτεκτονική που περιλαμβάνει όλα τα χαρακτηριστικά του λογισμικού HMI SCADA, όπως οθόνες διεργασιών, διαχείριση συναγερμών και συμβάντων, και προβολή ιστορικών δεδομένων. Ένα από τα πιο αξιοσημείωτα χαρακτηριστικά αυτού του λογισμικού είναι η ανοιχτή αρχιτεκτονική του, η οποία επιτρέπει την απρόσκοπτη επικοινωνία με μια ποικιλία προγραμματιζόμενων λογικών ελεγκτών (PLC) και απομακρυσμένων τερματικών μονάδων (RTU). Επιπλέον, η επισήμανση τόσο των αναλογικών όσο και των ψηφιακών σημάτων, καθώς και των συνδέσεων συσκευών, διασφαλίζει ότι η ποιότητα αυτού του λογισμικού παραμένει σταθερά υψηλή για μεγάλο χρονικό διάστημα. [8].

7. SZARP

Είναι ένα λογισμικό SCADA ανοικτού κώδικα, όπου μπορούμε να το περιγράψουμε ως λογισμικό που διαθέτει μια σημαντική συλλογή διαδικασιών/εφαρμογών. Κάθε διεργασία σε αυτό θα είχε μια ξεχωριστή εργασία η οποία θα επιτελούνταν τέλεια[8].

8. SCADA BR

Αφορά ανοικτού κώδικα λογισμικό που μπορεί να χρησιμοποιηθεί για εφαρμογές εποπτικού ελέγχου. Με αυτό το λογισμικό, είναι δυνατή η πραγματικού χρόνου απεικόνιση των δεδομένων και η καταγραφή τους σε μια βάση δεδομένων. Μπορούμε να αποκτήσουμε πρόσβαση σε αυτό το λογισμικό από έναν υπολογιστή ή κινητό, και διαθέτει μηχανές σεναρίων για τον έλεγχο αυτοματισμών και παρτίδων [8].

4.3 HMI

Η διεπαφή ανθρώπου-μηχανής (HMI) είναι συνδεδεμένη με το σύστημα παρακολούθησης και είναι το παράθυρο για να εργαστούν οι χειριστές του συστήματος στην αίθουσα ελέγχου. Στον τομέα των συστημάτων SCADA, η διεπαφή ανθρώπου-μηχανής (HMI) χρησιμεύει ως πύλη για αλληλεπίδραση και διαχείριση. Ενώ το σύστημα SCADA παρέχει τη λειτουργική ραχοκοκαλιά του συστήματος, οι εταιρείες μπορούν να αξιοποιήσουν τη δύναμη αυτής της λειτουργικότητας μέσω του HMI. Μέσω γραφικών διαγραμμάτων προσομοίωσης και σελίδων καταγραφής συμβάντων, το HMI εμφανίζει όλες τις ελεγχόμενες διαδικασίες. Εν τω μεταξύ, δεδομένα σε πραγματικό χρόνο για διάφορα διαγράμματα , γραφήματα και οθόνες συναγερμού παρέχονται από την άμεση επικοινωνία μεταξύ του HMI και του υπολογιστή παρακολούθησης SCADA. Σε ορισμένες περιπτώσεις, το HMI συλλέγει επίσης εξωτερικά δεδομένα, δημιουργεί αναφορές και στέλνει ειδοποιήσεις. Συνήθως αποτελούνται από γραμμικά σχέδια, σχηματικά σύμβολα ή φωτογραφίες που περιέχουν κινούμενα σύμβολα, τα διαγράμματα προσομοίωσης αντιπροσωπεύουν στοιχεία διαδικασίας.

Η παρακολούθηση των εργοστασιακών διεργασιών πραγματοποιείται μέσω της χρήσης HMI, ή διεπαφής ανθρώπου-μηχανής. Οι χειριστές έχουν τη δυνατότητα να διαχειρίζονται τις λειτουργίες των εγκαταστάσεων χρησιμοποιώντας πληκτρολόγια και οθόνες αφής για την έκδοση εντολών. Για παράδειγμα, ένας χειριστής μπορεί να προσδιορίσει εάν μια αντλία ρευστού είναι ή όχι λειτουργική βλέποντας ένα σύμβολο ενεργοποίησης/απενεργοποίησης και παρακολουθεί τη ροή του ρευστού μέσω ενός σωλήνα χρησιμοποιώντας ένα ροόμετρο. Μέσω της γραφικής διεπαφής, μπορούν να εκτελέσουν πολλές λειτουργίες, όπως η απενεργοποίηση της αντλίας με ένα μόνο κλικ ή άγγιγμα. Κατά συνέπεια, ο ρυθμός ροής μειώνεται και εμφανίζεται δυναμικά σε πραγματικό χρόνο στην οθόνη. Εντός του HMI, ένα λογισμικό «ιστορικού» ενσωματώνεται για την αποθήκευση χρονολογικών δεδομένων και συμβάντων σε μια βάση δεδομένων, η οποία μπορεί να χρησιμοποιηθεί για πρόσθετες πληροφορίες. Αυτά τα δεδομένα προέρχονται από τον διακομιστή συλλογής δεδομένων.

Λειτουργίες λογισμικού HMI:

- Μηχανισμοί ελέγχου πρόσβασης
- Οπτικοποίηση και έλεγχος
- Τυποποιημένες οθόνες συστήματος
- Ιστορική εξέλιξη, απεικόνιση εξέλιξης, εξέλιξη σε πραγματικό χρόνο
- Καταγραφές και αναφορές, υπολογιζόμενες τιμές, δημιουργία αναφορών φύλλου εργασίας,
- Αναφορές ως μηχανισμός ανταλλαγής δεδομένων
- Επεξεργασία συναγερμών

4.4 Κεντρική Βάση Δεδομένων

Μια κεντρική βάση δεδομένων, γνωστή και ως ιστορικός, είναι ένα κρίσιμο στοιχείο ενός συστήματος SCADA (Supervisory Control and Data Acquisition). Χρησιμεύει ως κεντρικό αποθετήριο για όλα τα δεδομένα που συλλέγονται από διάφορες βιομηχανικές διεργασίες, όπως αισθητήρες, PLC (προγραμματιζόμενοι λογικοί ελεγκτές) και άλλες συσκευές. Το Historian έχει σχεδιαστεί για να αποθηκεύει δεδομένα σε μορφή χρονοσειράς, επιτρέποντας στους χρήστες να αναλύουν και να συγκρίνουν δεδομένα με την πάροδο του χρόνου. Η πρωταρχική λειτουργία του Historian είναι να παρέχει αξιόπιστα και ακριβή δεδομένα για σκοπούς ανάλυσης, αναφοράς και αντιμετώπισης προβλημάτων. Μπορεί επίσης να παρέχει δυνατότητες απεικόνισης δεδομένων και υποβολής εκθέσεων σε πραγματικό χρόνο, καθιστώντας το πολύτιμο εργαλείο για την παρακολούθηση και τον έλεγχο βιομηχανικών διεργασιών. Εκτός από την αποθήκευση δεδομένων, το Historian μπορεί επίσης να παρέχει δυνατότητες συγκέντρωσης, συμπίεσης και δημιουργίας αντιγράφων ασφαλείας δεδομένων, διασφαλίζοντας ότι τα δεδομένα είναι ασφαλή και διαθέσιμα όταν χρειάζεται. Ορισμένα Historians περιλαμβάνουν επίσης προηγμένες δυνατότητες ανάλυσης και

μηχανικής μάθησης, επιτρέποντας στους χρήστες να αποκτήσουν βαθύτερες γνώσεις σχετικά με τις βιομηχανικές διαδικασίες τους.

Συνολικά, η κεντρική βάση δεδομένων ή το Historian σε ένα σύστημα SCADA είναι ένα βασικό εργαλείο που επιτρέπει στους χρήστες να συλλέγουν, να αποθηκεύουν και να αναλύουν δεδομένα από διάφορες βιομηχανικές διεργασίες, παρέχοντάς τους τις γνώσεις που χρειάζονται για τη λήψη τεκμηριωμένων αποφάσεων και τη βελτιστοποίηση των λειτουργιών τους

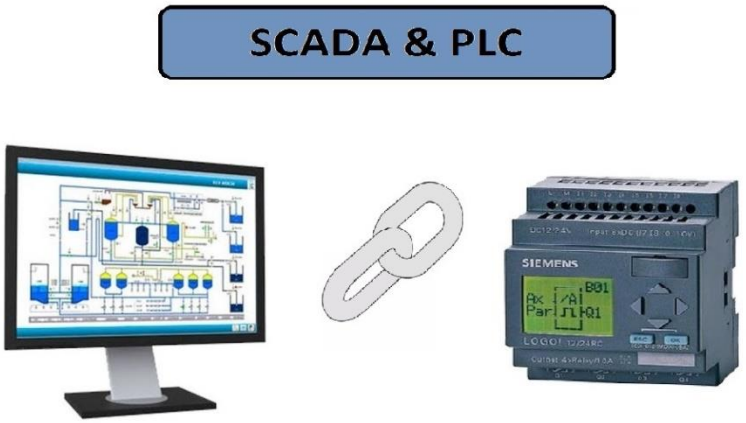
4.5 Τείχος προστασίας

Ο δρομολογητής τείχους προστασίας σε ένα σύστημα SCADA είναι το πιο κρίσιμο στοιχείο όσον αφορά την ασφάλεια του συστήματος και των δεδομένων. σταθερότητα της ροής δεδομένων. Ένα τείχος προστασίας μπορεί να εφαρμόσει διάφορους κανόνες για να προστατεύσει τις εσωτερικές συσκευές του συστήματος SCADA και να αποτρέψει ευάλωτες επιθέσεις. Μπορεί να διατηρεί το σύστημα λειτουργικό με λογαριασμούς που απαιτούνται μόνο από τον πελάτη και τον χειριστή συντήρησης, ενώ απαγορεύει οποιαδήποτε ασυνήθιστη κίνηση. Αυτό μπορεί να επιτευχθεί μέσω πελατών VPN και ισχυρών πιστοποιητικών. Δεν πρέπει να εφαρμόζεται προώθηση θυρών, καθώς αυτό δεν αποτελεί καλή πρακτική. Ο διαχειριστής δικτύου σε έναν σταθμό παραγωγής ηλεκτρικής ενέργειας φέρει την ευθύνη για την εγκατάσταση ενός τείχους προστασίας που παρέχει έλεγχο πρόσβασης και μέτρα ασφαλείας στον κυβερνοχώρο. Για να θεωρείται αποτελεσματικό, το τείχος προστασίας πρέπει να πληροί τόσο τα εθνικά όσο και τα βιομηχανικά πρότυπα ασφάλειας, καθώς και να συμμορφώνεται με τις βέλτιστες πρακτικές ασφαλείας εντός του πεδίου. Ένας δρομολογητής τείχους προστασίας μπορεί να παρέχει μια ποικιλία υπηρεσιών, όπως δρομολόγηση επιπέδου 3 και InterVLAN, εφαρμογή ασφαλούς σύνδεσης με LACP και διαμορφώσεις VPN και IPSEC. Μπορεί επίσης να διαχειρίζεται απομακρυσμένες συνδέσεις, να ελέγχει τις ροές κίνησης δεδομένων και την πρόσβαση των χρηστών, να διασφαλίζει την ασφάλεια των δεδομένων και να διευκολύνει ασφαλή σενάρια πελάτη-προς-πελάτη.

ΚΕΦΑΛΑΙΟ 5^{Ο}

5.1 SCADA & PLC

Η σχέση μεταξύ των συστημάτων SCADA (Supervisory Control and Data Acquisition) και των PLC (Programmable Logic Controllers) είναι βασικό στοιχείο της λειτουργίας των συστημάτων βιομηχανικού αυτοματισμού και ελέγχου. Αυτά τα δύο στοιχεία συνεργάζονται ώστε να παρακολουθούν και να ελέγχουν τις διαδικασίες σε ένα βιομηχανικό περιβάλλον.



Τα PLC ενεργούν ως οι πρωταρχικοί ελεγκτές σε αυτή τη σχέση. Είναι υπεύθυνοι για την εκτέλεση της λογικής ελέγχου, τη διαχείριση των συσκευών και του εξοπλισμού και τη διασφάλιση του ελέγχου του συστήματος σε πραγματικό χρόνο. Τα PLC λαμβάνουν σήματα εισόδου από αισθητήρες τα οποία επεξεργάζονται βάσει μιας προ-προγραμματισμένης λογικής και στέλνουν σήματα εξόδου σε ενεργοποιητές ή άλλες συσκευές. Σαρώνουν και ενημερώνουν συνεχώς τις εισόδους και τις εξόδους τους σύμφωνα με τη λογική ελέγχου που έχει προγραμματιστεί σε αυτά.

Τα συστήματα SCADA, από την άλλη πλευρά, χρησιμεύουν ως το κεντρικό εποπτικό επίπεδο. Συλλέγουν δεδομένα από πολλαπλά PLC, συνήθως μέσω δικτύου, χρησιμοποιώντας πρωτόκολλα επικοινωνίας όπως OPC, Modbus, Profibus ή Ethernet/IP. Τα συστήματα SCADA παρέχουν μια γραφική διεπαφή, γνωστή ως διεπαφή ανθρώπου-μηχανής (HMI), η οποία επιτρέπει στους χειριστές να παρακολουθούν και να ελέγχουν ολόκληρο το σύστημα. Μέσω του HMI, οι χειριστές μπορούν να απεικονίζουν τις μεταβλητές της διεργασίας, να παρακολουθούν την κατάσταση του συστήματος και να λαμβάνουν συναγερμούς ή ειδοποιήσεις.

Το σύστημα SCADA παρέχει πρόσθετες λειτουργίες πέραν του ελέγχου σε πραγματικό χρόνο. Μπορεί να αποθηκεύει δεδομένα για ανάλυση, να παράγει αναφορές και να εκτελεί ιστορικές τάσεις. Τα συστήματα SCADA προσφέρουν λειτουργίες όπως καταγραφή δεδομένων, συναγερμούς και αναφορές για να βοηθήσουν τους χειριστές και τους διαχειριστές στη λήψη τεκμηριωμένων αποφάσεων. Παρέχουν επίσης τη δυνατότητα στους χειριστές να στέλνουν εντολές ή σήματα ελέγχου σε PLC για να τροποποιούν τη συμπεριφορά του συστήματος όταν είναι απαραίτητο.

Συνοπτικά, τα PLC και τα συστήματα SCADA αποτελούν μια συμβιωτική σχέση στον βιομηχανικό αυτοματισμό. Τα PLC αναλαμβάνουν τον έλεγχο σε πραγματικό χρόνο και τη διαχείριση των συσκευών, ενώ τα συστήματα SCADA συλλέγουν δεδομένα, παρέχουν δυνατότητες οπτικοποίησης και παρακολούθησης και προσφέρουν προηγμένες λειτουργίες για την ανάλυση δεδομένων και τη διαχείριση του συστήματος. Μαζί, επιτρέπουν την

αποδοτική και αποτελεσματική παρακολούθηση, τον έλεγχο και την αυτοματοποίηση των βιομηχανικών διεργασιών.

5.1.1 Λειτουργία PLC σε βιομηχανικά περιβάλλοντα

Η λειτουργία προγραμματιζόμενων λογικών ελεγκτών (PLC) σε βιομηχανικό περιβάλλον είναι μια κρίσιμη πτυχή της σύγχρονης κατασκευής και παραγωγής. Με την ικανότητα να αυτοματοποιούν και να ελέγχουν ένα ευρύ φάσμα διαδικασιών, τα PLC έχουν φέρει επανάσταση στον τρόπο λειτουργίας των εργοστασίων και άλλων βιομηχανικών εγκαταστάσεων. Είτε είναι ο έλεγχος της ροής των υλικών μέσω μιας γραμμής παραγωγής, η παρακολούθηση και η ρύθμιση της θερμοκρασίας και της πίεσης σε μια μονάδα χημικής επεξεργασίας ή η ρύθμιση της ταχύτητας και της θέσης της ρομποτικής σε μια γραμμή συναρμολόγησης, τα PLC διαδραματίζουν αναπόσπαστο ρόλο στη διατήρηση αποδοτικών και αποτελεσματικών βιομηχανικών λειτουργιών . Μπορεί να προκύψουν προκλήσεις κατά τη λειτουργία ηλεκτρικών κυκλωμάτων με μεταγωγούς και Η/Υ σε βιομηχανικές περιοχές λόγω δυσμενών συνθηκών. Ωστόσο, οι προγραμματιζόμενοι λογικοί ελεγκτές (PLC) έχουν σχεδιαστεί ειδικά για να λειτουργούν σε τέτοια περιβάλλοντα με κατάλληλες προδιαγραφές. Το βιομηχανικό περιβάλλον περιλαμβάνει μια σειρά από στοιχεία και παράγοντες.

- Διάφορες φυσικές και μηχανικές πτυχές του περιβάλλοντος μπορεί να έχουν αντίκτυπο στον εξοπλισμό, συμπεριλαμβανομένων των κραδασμών, των φορτίων από κρούσεις, της υγρασίας και της θερμοκρασίας.
- Οι χημικοί ρύποι, που περιλαμβάνουν αέρια, ατμούς και λεπτά σωματίδια σκόνης, έχουν τη δυνατότητα να καταστρέψουν τους αγωγούς και τα ηλεκτρικά κυκλώματα προκαλώντας διάβρωση.
- Οι παρεμβολές σε κυκλώματα και καλωδιώσεις, το θερμοηλεκτρικό EMF, τα δυναμικά βολταϊκών συνδέσεων, ο ηλεκτροστατικός θόρυβος και οι ηλεκτρομαγνητικές παρεμβολές (όπως η ηλεκτροσυγκόλληση) είναι όλοι οι τύποι ηλεκτρικού θορύβου που μπορεί να προκύψουν.

5.1.2 Πλεονεκτήματα / Μειονεκτήματα της χρήσης των PLC

Αναλυτικότερα τα πλεονεκτήματα των προγραμματιζόμενων λογικών ελεγκτών είναι τα εξής:

- Μειωμένο κόστος υλοποίησης του αυτοματισμού
- Χρόνος υλοποίησης του αυτοματισμού
- Ελαχιστοποιημένο κόστος συντήρησης
- Οι αυτοματοποιημένες τροποποιήσεις παρέχουν μεγάλη ευελιξία
- Τεράστιες δυνατότητες επέκτασης του αυτοματισμού
- Δημιουργία εύκολων έξυπνων/πολύπλοκων διεργασιών
- Δυνατότητα σύνδεσης σε κεντρικό σύστημα υπολογιστών ή εταιρικό δίκτυο.
- Απαιτείται ελάχιστος χώρος
- Μικρότερη κατανάλωση ενέργειας.

- Απλή και εύχρηστη γλώσσα προγραμματισμού

Ο αυτοματισμός PLC προσφέρει τεράστιες δυνατότητες. Πολύπλοκη και έξυπνη επεξεργασία μπορεί να δημιουργηθεί εύκολα, κάτι που είναι δύσκολο να επιτευχθεί στον κλασικό αυτοματισμό. Επιπλέον, μπορούν να συνδεθούν ασύρματα με συστήματα SCADA σε απομακρυσμένες εφαρμογές, όπως μονάδες επεξεργασίας νερού. Φυσικά, μια εφαρμογή ή ένα προϊόν έχει πάντα τα μειονεκτήματά του. Για προγραμματιζόμενους λογικούς ελεγκτές, έχει ως εξής:

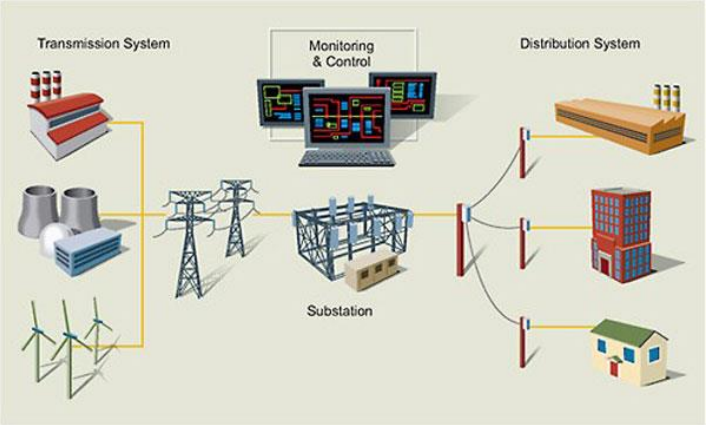
- Κοστοβόρα για πολύ μικρές και απλές εφαρμογές
- Απαίτηση εξειδικευμένου προσωπικού για την εγκατάσταση, τον προγραμματισμό και την λειτουργία του.
- Σε περίπτωση που προκληθεί ζημιά και δεν μπορεί να αποκατασταθεί, θα παρέχεται ακριβής αντικατάσταση.
- Τυχόν σοβαρά σφάλματα στο πρόγραμμα λειτουργίας του PLC.
- Δεν είναι δυνατή η αποθήκευση μεγάλων ποσοτήτων δεδομένων.
- Ο περιορισμός όσον αφορά την ποσότητα των I/O .
- Η ικανότητα αντοχής στις ηλεκτρονικές παρεμβολές είναι ένας κρίσιμος παράγοντας που πρέπει να ληφθεί υπόψη στις ηλεκτρονικές συσκευές

- Μπορεί να προκληθεί ζημιά στα συστήματα αυτοματισμού απο την υπερφόρτωση δικτύου. Ένα τέτοιο αποτέλεσμα είναι πιο πιθανό εάν τα πρωτόκολλα επικοινωνίας μεταξύ του προγραμματιζόμενου λογικού ελεγκτή (PLC) και του εταιρικού δικτύου δεν είναι ανεξάρτητα και υπάρχει συνεχής εισροή επικοινωνίας μεταξύ τους.

5.2 Εφαρμογές συστημάτων SCADA

Τα συστήματα SCADA (Supervisory Control and Data Acquisition) χρησιμοποιούνται σε ένα ευρύ φάσμα βιομηχανιών και εφαρμογών όπου υπάρχει ανάγκη παρακολούθησης και ελέγχου των βιομηχανικών διεργασιών. Ακολουθούν ορισμένα συνηθισμένα παραδείγματα για το πού χρησιμοποιούνται τα συστήματα SCADA:

Παραγωγή και διανομή ηλεκτρικής ενέργειας: Τα συστήματα SCADA χρησιμοποιούνται συνήθως σε εγκαταστάσεις παραγωγής και διανομής ηλεκτρικής ενέργειας για την παρακολούθηση και τον έλεγχο της ροής της ηλεκτρικής ενέργειας. Αυτό περιλαμβάνει τον έλεγχο του εξοπλισμού των σταθμών παραγωγής ηλεκτρικής ενέργειας, την παρακολούθηση των γραμμών μεταφοράς και τη διαχείριση των υποσταθμών.



Εικόνα 36 Δικτύο διανομής ηλεκτρικής ενέργειας

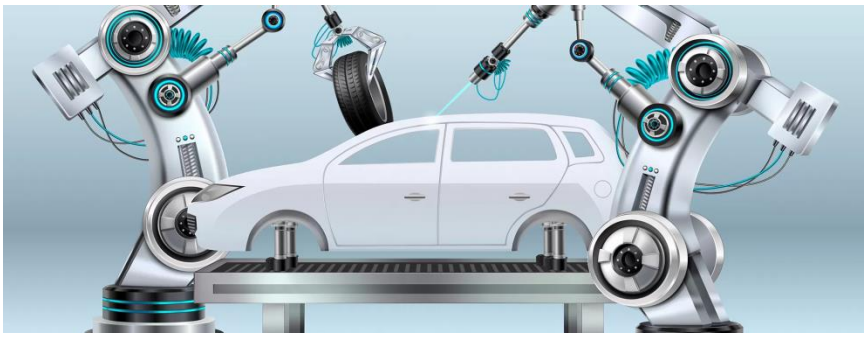
Διαχείριση νερού και λυμάτων: Τα συστήματα SCADA αναπτύσσονται σε δίκτυα ύδρευσης, δεξαμενές, αντλιοστάσια και εγκαταστάσεις επεξεργασίας λυμάτων. Παρακολουθούν τα επίπεδα νερού, την πίεση, τους ρυθμούς ροής και τις ποιοτικές παραμέτρους. Τα συστήματα SCADA συμβάλλουν στη βελτιστοποίηση της διανομής νερού, στον εντοπισμό διαρροών, στον έλεγχο των αντλιών και στη διασφάλιση της συμμόρφωσης με τους περιβαλλοντικούς κανονισμούς [25].

Εικόνα 37

Πετρέλαιο και φυσικό αέριο: Τα συστήματα SCADA χρησιμοποιούνται επίσης και στη βιομηχανία πετρελαίου και φυσικού αερίου για την παρακολούθηση και τον έλεγχο αγωγών, φρεατίων και λοιπού εξοπλισμού. Αυτό περιλαμβάνει την παρακολούθηση των ρυθμών ροής, της πίεσης και της θερμοκρασίας, καθώς και τον έλεγχο αντλιών και βαλβίδων.

Εικόνα 38

Βιομηχανία: Τα συστήματα SCADA παίζουν καθοριστικό ρόλο στον βιομηχανικό αυτοματισμό. Παρακολουθούν και ελέγχουν διαδικασίες παραγωγής, όπως γραμμές συναρμολόγησης, ρομποτικά συστήματα, λειτουργίες συσκευασίας και ποιοτικό έλεγχο. Παρέχοντας δεδομένα σε πραγματικό χρόνο σχετικά με την απόδοση των μηχανών, τους ρυθμούς παραγωγής και τις μετρήσεις ποιότητας, τα συστήματα SCADA επιτρέπουν στους χειριστές να μεγιστοποιούν την αποδοτικότητα και να αντιμετωπίζουν άμεσα τυχόν προβλήματα που προκύπτουν.[26].

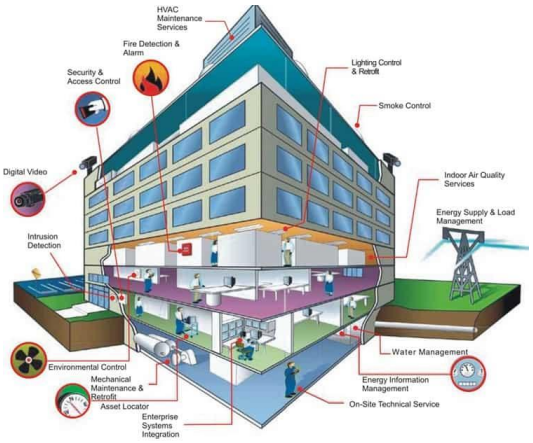


Εικόνα 39

Μεταφορές: Τα συστήματα SCADA χρησιμοποιούνται στις υποδομές μεταφορών, συμπεριλαμβανομένης της διαχείρισης της κυκλοφορίας, των σιδηροδρομικών συστημάτων, των αεροδρομίων και των θαλάσσιων λιμένων. Παρακολουθούν τη ροή της κυκλοφορίας, ελέγχουν τους φωτεινούς σηματοδότες, διαχειρίζονται τα σιδηροδρομικά συστήματα σηματοδότησης, ρυθμίζουν τις λειτουργίες των αεροδρομίων και επιβλέπουν τη διακίνηση φορτίων και οχημάτων [27].

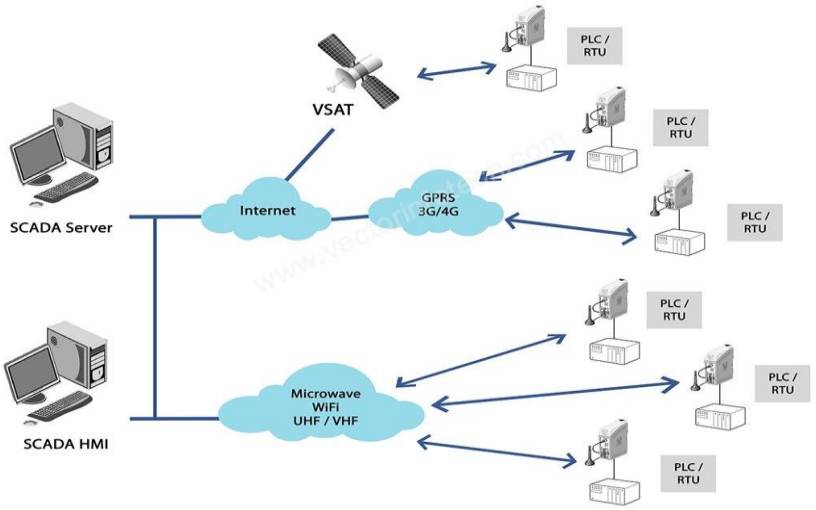
Εικόνα 40

Αυτοματισμοί κτιρίων: Τα συστήματα SCADA χρησιμοποιούνται σε μεγάλα κτίρια, όπως νοσοκομεία, πανεπιστήμια, συγκροτήματα γραφείων και εμπορικά κέντρα. Επιπρόσθετα, παρακολουθούν και ελέγχουν τα συστήματα HVAC (θέρμανσης, εξαερισμού και κλιματισμού), τον φωτισμό, τον έλεγχο πρόσβασης, τους συναγερμούς πυρκαγιάς και άλλες υπηρεσίες κτιριακών μονάδων. Τα συστήματα SCADA επιτρέπουν τη διαχείριση της ενέργειας, την άνεση των ενοίκων και την ασφάλεια[28].



Εικόνα 41 BMS (Building Management System) είναι ένα σύγχρονο σύστημα που επιτρέπει τον έλεγχο και τη διαχείριση όλων των τεχνικών συστημάτων του κτιρίου [29]

Τηλεπικοινωνίες: Τα συστήματα SCADA χρησιμοποιούνται στον τομέα των τηλεπικοινωνιών για την παρακολούθηση και τη διαχείριση της υποδομής του δικτύου, συμπεριλαμβανομένων των σταθμών βάσης, των δρομολογητών, των μεταγωγέων και των καλωδίων οπτικών ινών. Παρέχουν δεδομένα σε πραγματικό χρόνο σχετικά με την απόδοση του δικτύου, το φορτίο κίνησης και την υγεία του εξοπλισμού. Τα συστήματα SCADA συμβάλλουν στη διασφάλιση της αξιοπιστίας του δικτύου, στον εντοπισμό βλαβών και στη διευκόλυνση των δραστηριοτήτων συντήρησης.



Εικόνα 42

5.3 Ασφάλεια

Η ασφάλεια αποτελεί κρίσιμο ζήτημα στα συστήματα SCADA, καθώς χρησιμοποιούνται συχνά για τον έλεγχο κρίσιμων υποδομών, όπως σταθμοί παραγωγής ενέργειας και εγκαταστάσεις επεξεργασίας νερού. Η χρήση πρωτοκόλλων επικοινωνίας στα συστήματα SCADA αποτελεί επίσης μια πιθανή ευπάθεια, καθώς τα πρωτόκολλα αυτά μπορούν να αξιοποιηθούν από επιτιθέμενους για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε συστήματα ελέγχου.

Προγενέστερα, ένα παραδοσιακό σύστημα SCADA ήταν ένα κλειστό δίκτυο με σειριακές συνδέσεις (όπως το RS-232) και υλοποιήσεις πρωτοκόλλου fieldbus, που περιείχε μόνο αξιόπιστες συσκευές με ελάχιστη ή καθόλου σύνδεση με τον έξω κόσμο. Πολλά από αυτά τα συστήματα είναι ηλικίας δεκαετιών και έχουν ελάχιστη έως καθόλου ασφάλεια (π.χ. ξεπερασμένα λειτουργικά συστήματα, απαρχαιωμένο λογισμικό προστασίας από ιούς). Τέτοια συστήματα είναι ασφαλή επειδή έχουν τοπικό έλεγχο και περιορισμένη συνδεσιμότητα.

Σήμερα, τα συστήματα SCADA υιοθετούν γεωγραφικά την τεχνολογία και την αρχιτεκτονική των συστημάτων πληροφορικής. Πρωτόκολλα όπως το Modbus, το Ethernet/IP και το DNP3, που χρησιμοποιούνται για την αυτοματοποίηση και τον έλεγχο του εξοπλισμού βιομηχανικών διεργασιών στα συστήματα SCADA, έχουν όλα τις δικές τους αδυναμίες, οι οποίες εγείρουν ανησυχίες για την ασφάλεια. Για τους παραπάνω λόγους, τα συστήματα SCADA εκτίθενται αναπόφευκτα σε απειλές από άλλα δικτυωμένα συστήματα υπολογιστών, εκτός από απειλές που σχετίζονται με τα δικά τους συστήματα (ιδιόκτητα πρωτόκολλα σχεδιασμένα πριν από δεκαετίες με άγνωστη θέση ασφαλείας και εγγενείς αδυναμίες). . Μέχρι σήμερα, πολλές συμβουλές ευπάθειας έχουν δημοσιευτεί σε τυπικές βάσεις

δεδομένων ευπάθειας, όπως η Common Vulnerability Exposure Database, εστιάζοντας κυρίως στις επιθέσεις Denial of Service (DoS) και Buffer Overflow.
Τα συστήματα SCADA έχουν δημιουργηθεί για να λειτουργούν συνεχώς για παρατεταμένες χρονικές περιόδους χωρίς την ανάγκη επανεκκίνησης. Λόγω του σχεδιασμού τους, αυτά τα συστήματα διαθέτουν συχνά περιορισμένους πόρους, όπως περιορισμένη ισχύ επεξεργασίας ή ταχύτητα σύνδεσης. Ως αποτέλεσμα, η χρήση τεχνικών κατά του κακόβουλου λογισμικού ή/και κρυπτογράφησης επιβάλλει πρόσθετα υπολογιστικά έξοδα και καθυστέρηση δικτύου λόγω των πρόσθετων πακέτων που απαιτούνται. Έχουν επίσης το μειονέκτημα ότι αναπτύσσονται για απομονωμένα δίκτυα, πράγμα που σημαίνει ότι δεν υπάρχει ευαισθητοποίηση σχετικά με την ασφάλεια.
Για την αντιμετώπιση αυτών των προβλημάτων ασφαλείας, πολλά πρωτόκολλα επικοινωνίας που χρησιμοποιούνται σε συστήματα SCADA, συμπεριλαμβανομένων των MODBUS, PROFIBUS, DNP3, IEC 60870-5 και IEC 61850, έχουν σχεδιαστεί με χαρακτηριστικά ασφαλείας, όπως κρυπτογράφηση και πιστοποίηση ταυτότητας. Η χρήση ασφαλών πρωτοκόλλων επικοινωνίας, όπως το Secure Sockets Layer (SSL) και το Transport Layer Security (TLS), μπορεί επίσης να παρέχει ένα πρόσθετο επίπεδο ασφάλειας με την κρυπτογράφηση όλων των δεδομένων που μεταδίδονται μέσω του δικτύου.
Είναι σημαντικό να σημειωθεί ότι η ασφάλεια ενός συστήματος SCADA δεν εξαρτάται αποκλειστικά από το πρωτόκολλο επικοινωνίας που χρησιμοποιείται. Άλλοι παράγοντες, όπως ο σχεδιασμός και η διαμόρφωση του συστήματος, η φυσική ασφάλεια των συσκευών και η διαθεσιμότητα των διορθωτικών προγραμμάτων και των ενημερώσεων, διαδραματίζουν επίσης κρίσιμο ρόλο στη διασφάλιση της ασφάλειας του συστήματος [30].

5.4 Οφέλη και πλεονεκτήματα των συστημάτων SCADA

Προκειμένου να καταστεί η λειτουργία των βιομηχανικών οργανισμών ομαλή και χωρίς προβλήματα, είναι απαραίτητο να βελτιστοποιηθεί η ροή ενέργειας και υλικού με διάφορα μηχανικά μέσα και μέσω της παρακολούθησης της ροής πληροφοριών. . Η επίτευξή του απαιτεί συχνά αντισταθμίσεις μεταξύ ορισμένων οικονομικών και ποιοτικών παραγόντων, οδηγώντας σε κάποια άλλα οφέλη. Φυσικά, αυτά τα οφέλη μπορούν να οικοδομηθούν σε πολλαπλά επίπεδα ανθρώπινου παράγοντα και παραγωγικών διαδικασιών. Παρακάτω παρατίθενται ορισμένα ενδεικτικά πλεονεκτήματα που σχετίζονται κυρίως με την διαδικασία παραγωγής .

- Αυξημένη παραγωγή λόγω της μέγιστης αξιοποίησης όλων των διαθέσιμων πόρων, π.χ. βιομηχανικές μονάδες που λειτουργούν στο ανώτατο όριο
- Η βέλτιστη αξιοποίηση των εσωτερικών πηγών ενέργειας και η μείωση του κόστους εργασίας οδηγούν σε μείωση του κόστους παραγωγής ανά μονάδα προϊόντος.
- Μειωμένο κόστος διαδικασίας παραγωγής ανά μονάδα προϊόντος λόγω βέλτιστης αξιοποίησης της εσωτερικής ενέργειας και μειωμένο κόστος εργασίας Η ποιότητα των παραγόμενων προϊόντων βελτιώνεται καθώς οι συνθήκες λειτουργίας μπορούν

να διατηρηθούν σε μικρότερες ανοχές και τα σφάλματα μπορούν πλέον να εντοπιστούν σε πολύ σύντομο χρονικό διάστημα

- Η μείωση των εξόδων συντήρησης μεμονωμένων μηχανημάτων
- Ευελιξία παραγωγής υπό μεταβαλλόμενες συνθήκες αγοράς

Εικόνα 43 Οπτικοποίηση ελέγχου δεξαμενής μέσω συστήματος SCADA

Τα συστήματα SCADA παρέχουν συγκεκριμένα:

- Η επίτευξη της μέγιστης απόδοσης σε μια βιομηχανική μονάδα επιτυγχάνεται μέσω της παρακολούθησης της παραγωγικής διαδικασίας, η οποία διασφαλίζει την ομαλότητά της.
- Η βελτίωση της επικοινωνίας μεταξύ των βιομηχανικών μονάδων σε όλα τα επίπεδα, ιδιαίτερα μεταξύ παραγωγής και διαχείρισης, είναι ζωτικής σημασίας.
- Οι εργαζόμενοι είναι σε θέση να λαμβάνουν πιο τεκμηριωμένες αποφάσεις και επομένως να εκτελούν τα καθήκοντά τους με μεγαλύτερη επιτυχία.
- Εντοπισμός και χειρισμός σφαλμάτων ταχύτερα, μειώνοντας το κόστος συντήρησης εκτός από τη βελτίωση της απόδοσης .
- Βελτιώσεις σε γενικές συνθήκες ασφάλειας και εργασίας .
- Παρέχετε στη διοίκηση πιο ακριβείς και έγκαιρες πληροφορίες.

Όσον αφορά τον ανθρώπινο παράγοντα, υπάρχουν διάφορα πλεονεκτήματα

- Περιορίζει το ρόλο του ανθρώπινου παράγοντα μόνο στον τομέα του ελέγχου.
- Αναλαμβάνει τη χειρωνακτική εργασία από τις μηχανές.
- Ελαχιστοποιεί τον κίνδυνο εργατικών ατυχημάτων. Οι μηχανές αναλαμβάνουν επικίνδυνες εργασίες.
- Ελαχιστοποιεί το ανθρώπινο λάθος.

Ορισμένα πρακτικά παραδείγματα που αναφέρονται σε γενικές γραμμές στα οφέλη από τη χρήση συστημάτων SCADA σε παραγωγικές διαδικασίες περιλαμβάνουν τα εξής :

- Αυτό επιτρέπει στους διευθυντές και τους μηχανικούς να βλέπουν τις πληροφορίες στους υπολογιστές τους, ανεξάρτητα από το αν η πηγή δεδομένων βρίσκεται κοντά ή μακριά.

- Η δυνατότητα του χρήστη να διαμορφώσει το πλήρες σύστημα παρακολούθησης που απαιτείται ενισχύεται με τη βοήθεια χιλιάδων περιφερειακών συσκευών μέτρησης και ελέγχου που μπορούν να ενσωματωθούν απευθείας στο σύστημα χωρίς πρόσθετο κόστος.
- Η ικανότητα προσαρμογής του συστήματος εποπτείας στις μοναδικές προδιαγραφές του χρήστη βελτιώνεται με την ενσωμάτωση πολυάριθμων περιφερειακών συσκευών μέτρησης και ελέγχου, οι οποίες μπορούν να ενσωματωθούν απρόσκοπτα στο σύστημα χωρίς πρόσθετα έξοδα.
- Οι χειριστές μπορούν να παρακολουθούν και να ελέγχουν τον εξοπλισμό μέσω μιας εύχρηστης γραφικής διεπαφής χρήστη (GUI) χρησιμοποιώντας μια οθόνη PC με Microsoft Windows.
- Οι καταστάσεις έκτακτης ανάγκης (ειδοποιήσεις) μπορούν να ενημερώνονται με ηχογραφημένα μηνύματα που μεταδίδονται αυτόματα μέσω τηλεφώνου, ραδιοφώνου, δικτύου υπολογιστών κ.λπ.
- Με τις προόδους της τεχνολογίας, οποιοσδήποτε χειριστής μπορεί πλέον να αποθηκεύει αβίαστα και να έχει πρόσβαση σε σημαντικά μεγαλύτερες ποσότητες δεδομένων. Επιπλέον, μπορούν να εξετάσουν αρχεία δεδομένων από προηγούμενα γεγονότα για να κάνουν πιο ενημερωμένες συγκρίσεις, να αντλήσουν πιο πειστικά αποτελέσματα και να αντιμετωπίσουν τυχόν προβλήματα που μπορεί να προκύψουν.
- Οι απομακρυσμένες συσκευές μπορούν να ρυθμιστούν εξ αποστάσεως χωρίς να υπάρχει φυσική παρουσία του χρήστη.
- Οι χειριστές είναι πλέον σε θέση να ενσωματώνουν δεδομένα και μετρήσεις σε πραγματικό χρόνο σε συστήματα παρακολούθησης.
- Η δυνατότητα χρήσης προσιτών και φιλικών προς το χρήστη προσωπικών υπολογιστών ως τερματικών συσκευών καθίσταται δυνατή. Σε αντίθεση με τον εξειδικευμένο εξοπλισμό, αυτοί οι υπολογιστές είναι ευκολότεροι και πιο προσιτοί για αναβάθμιση ή τροποποίηση ανάλογα με τις ανάγκες.
- Ταυτόχρονα, επιτρέπει τη χρήση σύγχρονων κοινών πρωτοκόλλων και υλικών δικτύου, καθιστώντας εύκολη και οικονομική την αναβάθμιση, προσαρμογή ή αντικατάσταση. Αυτό επιτυγχάνει αξιόπιστη δικτυακή επικοινωνία μεταξύ υλικού από διαφορετικούς κατασκευαστές.
- Είναι επιτακτική ανάγκη ο προμηθευτής του συστήματος να παρέχει επαρκή τεχνική υποστήριξη και συντήρηση για το σύστημα.

5.5 Προβλήματα και μειονεκτήματα των συστημάτων SCADA

Η διασύνδεση συστημάτων SCADA σε μηχανισμούς παρακολούθησης βιομηχανικών μονάδων μπορεί προφανώς να μας προσφέρει απεριόριστες λύσεις στη διαχείριση ελέγχου παραγωγικής διαδικασίας. Ταυτόχρονα όμως έχουν προκύψει κάποια προβλήματα στην ενσωμάτωσή του σε πολλές σύγχρονες βιομηχανίες. Ενδεικτικά, τα μειονεκτήματα αυτών των συστημάτων είναι:

- Δομικά, τα συστήματα SCADA χαρακτηρίζονται από πολύπλοκα, ακριβά και απαιτητικά υλικά. Η βιομηχανία παραγωγής ηλεκτρονικών ειδών αναγκάζεται σε έναν ατελείωτο κύκλο αναβάθμισης του κατασκευαστικού της εξοπλισμού για να μπορέσει να συμβαδίσει με τη συνεχή εξέλιξη των συστημάτων.
- Ο χειριστής ενδέχεται να επηρεάσει τη λειτουργία ορισμένων περιφερειακών συσκευών.
- Οι μεγάλες βιομηχανικές εγκαταστάσεις απαιτούν πολύπλοκες συνδέσεις που μερικές φορές είναι δύσκολο να υλοποιηθούν.
- Λόγω της πολυπλοκότητας του συστήματος, απαιτείται προσωπικό με εκτενή τεχνική εξειδίκευση, όπως αναλυτές συστημάτων και προγραμματιστές αισθητήρων.
- Δεδομένου ότι το Διαδίκτυο χρησιμεύει ως μέσο επικοινωνίας και διασύνδεσης μεταξύ συσκευών, τα σύγχρονα συστήματα επιτήρησης έχουν αρκετές ευπάθειες ασφαλείας που οδηγούν σε πιθανότητα υποκλοπής και χειραγώγησης των διαδικασιών παραγωγής.

Βιβλιογραφία

1. Mini A. Thomas, J.D.M., *Power System SCADA and Smart Grids*. 2015.
2. Fatima, T.A.Z., *Master Station Architecture of a SCADA System.* IETE Journal of Education, 2015. **43**(2): p. 121-126.
3. Γεώργιος, Χ., *Εργαλεία Μηχανικής Λογισμικού*. 2015: Kallipos.
4. David Bailey, E.W., *Practical SCADA for Industry*. 2003.
5. Gordon Clarke, D.R.a.E.W., *Modern SCADA Protocols*. 2003.
6. Jhaver, A.B.R.N.D., *Supervisory Control and Data Acquisition.* International Journal of Computer Applications, 2014. **102**.
7. AutomationForum.co. *What is the purpose of SCADA in an industrial process?* ; Available from: https://automationforum.co/best-12-free-scada-software/.
8. AutomationForum.co. *Leading 12 SCADA software*. Available from: https://automationforum.co/leading-12-scada-software/.
9. CompuSystems. *SCADA Primer*. Available from: https://ourinstrumentationgroup.com/SCADA_Primer.pdf.
10. Θεοχάρης, Σ.Κ., *Εργαστηριακές Εφαρμογές SCADA*, in *Τμήμα Ηλεκτρονικών Υπολογιστικών Συστημάτων Τ.Ε.* 2015, ΑΕΙ Πειραιά.
11. Μάριος, Κ., *« Πρωτόκολλαβιομηχανικώνδικτύων / δικτύων αυτοματισμού»*. 2006, Πανεπιστήμιο Μακεδονίας.
12. Applications, C.N.T.; Available from: http://conta.uom.gr/conta/ekpaideysh/metaptyxiaka/technologies_diktywn/teaching_m/tcpip/general.htm.
13. K., P. *Αρχιτεκτονική Δικτύων*. 2009; Available from: http://users.sch.gr/pepoudi/site/pages/page38.html.
14. ODVA, *Common Industrial Protocol (CIP) And The Family of CIP Networks.* 2016.
15. Wikipedia, *Common Industrial Protocol.*
16. Co., W.G., *EtherNet/IP and CIP.* 2022.
17. ODVA, *CIP on Ethernet Technology.* Technology Overview Series, 2021.
18. Βελώνη, Α. *Βιομηχανική Πληροφορική*. Available from: https://docplayer.gr/11698218-Viomihaniki-pliroforiki.html.
19. Εμμανουήλ, Κ., *Συστήματα Βιομηχανικού Ελέγχου*, in *ΤΕΙ Πειραιά*. 2014.
20. Wikipedia. *PROFINET*. Available from: https://en.wikipedia.org/wiki/Profinet.
21. Yang Ming, L.G., *Analysis of PROFINET IO Communication Protocol.* 2014.
22. Automation, R.-R.T. *An Introduction to PROFINET IO*. 2023.
23. *PROFINET SYSTEM DESCRIPTION - Technology and Application*. Available from: https://www.profibus.com/index.php?eID=dumpFile&t=f&f=51714&token=4ea5554cbb80a066e805a879116ead2a759c23c3.
24. IDX. *The PROFINET Protocol Family*. Available from: https://www.idx.co.za/protocol/the-profinet-protocol-family/.
25. Forum, T.E. *SCADA Training - T&D Automation*. Available from: https://www.electricityforum.com/electrical-training/scada-training.
26. ΚΑΠΝΟΥΤΖΗΣ, Μ., *¨Η ΕΞΕΛΙΞΗ ΤΩΝ ΑΥΤΟΜΑΤΙΣΜΩΝ ΚΑΙ ΟΙ ΠΡΟΓΡΑΜΜΑΤΙΖΟΜΕΝΟΙ ΛΟΓΙΚΟΙ ΕΛΕΓΚΤΕΣ¨*, in *ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ*. 2021: ΛΑΡΙΣΑ.
27. Πέππας Αθανάσιος, Τ.Α., *«Αυτοματισμοί και αισθητήριες διατάξεις στην αεροπορική βιομηχανία»*, in *ΤΕΙ ΠΕΙΡΑΙΑ*. 2006.
28. nexusintegra, *SCADA systems and industry 4.0.*
29. M&E, H.S. *BMS SOLUTION - FACTORY MANAGEMENT*.
30. Κατσίγιαννης, Κ.Β., *Ασφάλεια Βιομηχανικών Συστημάτων και Εφαρμογών*. 2020, Πανεπιστήμιο Πατρών.

31. Supervisory Control and Data Acquisition, Stuart A. Boyer, ISA The Instrumentation, Systems, and Automation Society; 3rd edition

32. IEEE Standard C37.1-1994, Definition, Specification, and Analysis of System Used for Supervisory Control, Data Acquisition, and Automatic Control

33. Pyramid of automation and industry 4.0 from : https://www.witorg.com/pyramid-of-automation-and-industry-4-0/

34. Leventis A. , REMOTE ACCESS AND TELEMETRY IN INDUSTRIAL APPLICATIONS. 2022 , University of Piraeus