Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Ψηφιακός Πολιτισμός, Έξυπνες Πόλεις, IoT και Προηγμένες Ψηφιακές Τεχνολογίες»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**ΑΠΟΜΑΚΡΥΣΜΕΝΗ ΠΡΟΣΒΑΣΗ ΚΑΙ ΤΗΛΕΜΕΤΡΙΑ ΣΕ ΒΙΟΜΗΧΑΝΙΚΕΣ ΕΦΑΡΜΟΓΕΣ** **REMOTE ACCESS AND TELEMETRY IN INDUSTRIAL APPLICATIONS**
Ονοματεπώνυμο Φοιτητή	**ΑΝΤΩΝΙΟΣ ΛΕΒΕΝΤΗΣ**
Πατρώνυμο	**ΘΕΜΕΛΗΣ ΛΕΒΕΝΤΗΣ**
Αριθμός Μητρώου	**ΨΠΟΛ19032**
Επιβλέπων	**ΣΠΥΡΙΔΩΝ ΛΙΒΙΕΡΑΤΟΣ**

Ημερομηνία Παράδοσης **ΟΚΤΩΒΡΙΟΣ 2022**

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Σπυρίδων Λιβιεράτος Καθηγητής	Δημήτριος Βέργαδος Καθηγητής	Άγγελος Μιχάλας Καθηγητής

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΕΙΣΑΓΩΓΗ

Ο όρος «ΑΥΤΟΜΑΤΙΣΜΟΣ» χρησιμοποιήθηκε πρώτη φορά τη δεκαετία του 1940 στην αυτοκινητοβιομηχανία για να περιγράψει την αυξημένη χρήση συσκευών και μηχανημάτων που δρούσαν αυτόματα στις γραμμές παραγωγής των βιομηχανιών. Ο αυτοματισμός γενικότερα είναι η τεχνολογική διαδικασία με σκοπό την παρακολούθηση και τον έλεγχο της παραγωγής αλλά και την παράδοση υπηρεσιών και προϊόντων. Η αυτοματοποίηση διαδικασιών και λειτουργιών παίζει εξαιρετικό ρόλο, δεδομένου ότι αυξάνεται η παραγωγικότητα, βελτιώνεται η ασφάλεια και μειώνεται η πιθανότητα λαθών που προκύπτουν από χειροκίνητες διαδικασίες. Τις αυτοματοποιημένες λύσεις εκτός από την βιομηχανία, τις συναντάμε στις εγκαταστάσεις κατασκευών, στις ανανεώσιμες πηγές ενέργειας, στις καλλιέργειες, στις μεταφορές, στα logistics αλλά και στα έξυπνα σπίτια.

Όπως είναι λογικό, όλα τα αυτόματα συστήματα χρειάζονται επιτήρηση, εποπτεία, συντήρηση αλλά και επιδιόρθωση τυχόν βλαβών. Το χρονικό διάστημα που θα μεσολαβήσει από την εμφάνιση μίας βλάβης μέχρι και την αντιμετώπιση της είναι κρίσιμο, διότι η ζημία που θα υποστεί η επιχείρηση με σταματημένη παραγωγή μπορεί να φανεί καταστροφική. Η πίεση που ασκείται στους μηχανικούς διαφορετικών κλάδων για άμεση αντιμετώπιση των βλαβών είναι μεγάλη. Εκ των πραγμάτων όμως, η μετακίνηση ενός τεχνικού στην τοποθεσία που υπάρχει η βλάβη, μπορεί να διαρκέσει μέρες. Λόγω των προαναφερθέντων ζητημάτων, οι επιχειρήσεις οδηγήθηκαν στην επένδυση κεφαλαίων για απομακρυσμένη υποστήριξη των παραγωγών τους μέσω εφαρμογών τηλεμετρίας. Τα οφέλη μιας άμεσης αντιμετώπισης είναι πολυάριθμα. Μειωμένα κόστη λόγω εξόδων μετακίνησης για επισκευή, συντήρηση ή επίβλεψη ομαλής λειτουργίας των μηχανών αλλά και απομακρυσμένη συλλογή δεδομένων με σκοπό την εξόρυξη κρίσιμων συμπερασμάτων, αποτελούν παράγοντες που έθεσαν την τηλεμετρία ως ένα αναπόσπαστο κομμάτι του βιομηχανικού αυτοματισμού.

Ο στόχος της παρούσας διπλωματικής είναι η αναβάθμιση της περιστροφικής καρτονέτας με την τοποθέτηση ενός βιομηχανικού δρομολογητή (Industrial Router). Με το συγκεκριμένο Router, θα υπάρχει η δυνατότητα άμεσης εποπτείας της μηχανής μέσω κινητού τηλεφώνου, υπολογιστή ή tablet, παρακολουθώντας κάποιους βασικούς δείκτες (KPIs – Key Performance Indicators). Σε περίπτωση τυχόν βλαβών, θα υπάρχει άμεση ενημέρωση αποστέλλοντας email και θα δημιουργείται επίσης αρχείο με τις πιο σημαντικές παραμέτρους. Θα πραγματοποιείται συλλογή δεδομένων με σκοπό την έγκαιρη συντήρηση εξαρτημάτων και την πρόβλεψη βλαβών. Η γνώση που αποκτάται από τα συγκεκριμένα συστήματα αποτελεί ευκαιρία στο να βρεθούν βελτιώσεις για μελλοντικές εφαρμογές. Θα δίνεται επίσης πρόσβαση σε τεχνικούς, ώστε να μπορούν να προγραμματίζουν το PLC (Programmable Logic Controller) και το HMI (Human Machine Interface) της μηχανής απομακρυσμένα.

ΚΕΦΑΛΑΙΟ 1 - ΤΗΛΕΜΕΤΡΙΑ

1.1. Ορισμός

Τηλεμετρία είναι η επιστήμη που επιτρέπει την συλλογή δεδομένων εξ αποστάσεως. Τα δεδομένα αποστέλλονται αυτόματα με τη χρήση διαφορετικού τεχνολογικού τύπου πομποδεκτών, συνήθως μέσω ασύρματων μηχανισμών (π.χ. συστήματα ραδιοσυχνοτήτων, υπερήχων, υπέρυθρων ή GSM δικτύων) ή μέσω ενσύρματων δικτύων (π.χ. Ethernet, σειριακές, PoE καλωδιώσεις ή οπτικές ίνες). Όταν τα μέσα τηλεμετρίας χρησιμοποιούνται στο χώρο της βιομηχανίας με σκοπό τον αυτόματο έλεγχο και για την ανάκτηση δεδομένων, χρησιμοποιείται ο όρος SCADA.

Αποτελεί αναπόσπαστο κομμάτι πολλών τεχνολογικών εφαρμογών όπως:

- Μετεωρολογία
- Βιομηχανία πετρελαίου και αερίου
- Αγώνες μηχανοκίνητων οχημάτων
- Μεταφορές
- Γεωργία
- Διαχείριση υδάτινων πόρων
- Διάστημα και Άμυνα
- Έρευνα πόρων
- Επιστήμη διαστήματος
- Δοκιμές πτήσεων
- Εποπτεία ενέργειας
- Διανομή πόρων
- Ιατρική
- Επικοινωνίες
- Εξόρυξη
- Βιομηχανία

Τηλεμετρία είναι η επιτόπια συλλογή μετρήσεων ή άλλων δεδομένων σε απομακρυσμένα σημεία και η αυτόματη μετάδοσή τους σε εξοπλισμό λήψης (τηλεπικοινωνίες) για παρακολούθηση.[1] Η λέξη προέρχεται από τις ελληνικές ρίζες te, «απομακρυσμένο», και μέτρον, «μέτρο». Τα συστήματα που χρειάζονται εξωτερικές οδηγίες και δεδομένα για να λειτουργήσουν απαιτούν το αντίστοιχο της τηλεμετρίας, τηλεδιοίκηση.[2]

Αν και ο όρος αναφέρεται συνήθως σε μηχανισμούς ασύρματης μεταφοράς δεδομένων (π.χ. χρησιμοποιώντας συστήματα ραδιοφώνου, υπερήχων ή υπερύθρων), περιλαμβάνει επίσης δεδομένα που μεταφέρονται μέσω άλλων μέσων όπως δίκτυο τηλεφώνου ή υπολογιστή, οπτική ζεύξη ή άλλες ενσύρματες επικοινωνίες όπως φορείς γραμμών ηλεκτρικής ενέργειας. Πολλά σύγχρονα συστήματα τηλεμετρίας εκμεταλλεύονται το χαμηλό κόστος και την πανταχού παρουσία των δικτύων GSM χρησιμοποιώντας SMS για τη λήψη και τη μετάδοση δεδομένων τηλεμετρίας.

Ο τηλεμετρητής είναι μια φυσική συσκευή που χρησιμοποιείται στην τηλεμετρία. Αποτελείται από έναν αισθητήρα, μια διαδρομή μετάδοσης και μια συσκευή απεικόνισης, εγγραφής ή ελέγχου. Οι ηλεκτρονικές συσκευές χρησιμοποιούνται ευρέως στην τηλεμετρία και μπορεί να είναι ασύρματες ή ενσύρματες, αναλογικές ή ψηφιακές. Είναι επίσης δυνατές και άλλες τεχνολογίες, όπως μηχανικές, υδραυλικές και οπτικές.[3]

Η τηλεμετρία μπορεί να αντικατασταθεί για να επιτρέψει τη μετάδοση πολλαπλών ροών δεδομένων σε ένα σταθερό πλαίσιο.

1.2. Ιστορία

Η αρχή της βιομηχανικής τηλεμετρίας βρίσκεται στην εποχή του ατμού, αν και ο αισθητήρας δεν ονομαζόταν τηλεμετρητής εκείνη την εποχή.[4] Παραδείγματα είναι οι προσθήκες του James Watt (1736-1819) στις ατμομηχανές του για παρακολούθηση από (σχεδόν) απόσταση, όπως το μανόμετρο υδραργύρου και ο ρυθμιστής fly-ball.[4]

Αν και το αρχικό τηλέμετρο αναφερόταν σε μια συσκευή μέτρησης απόστασης (τηλεμετρητής απόστασης), μέχρι τα τέλη του 19ου αιώνα ο ίδιος όρος είχε χρησιμοποιηθεί ευρέως από ηλεκτρολόγους μηχανικούς εφαρμόζοντας τον σε ηλεκτρικές συσκευές που μετρούν πολλές άλλες ποσότητες εκτός από την απόσταση (για παράδειγμα, στο δίπλωμα ευρεσιτεχνίας ενός «Ηλεκτρικού Τηλεμετρικού Πομπού»[5]). Τα γενικά τηλέμετρα περιλάμβαναν αισθητήρες όπως το θερμοστοιχείο (από το έργο του Thomas Johann Seebeck), το θερμόμετρο αντίστασης (του William Siemens με βάση το έργο του Humphry Davy) και τον ηλεκτρικό μετρητή καταπόνησης (με βάση την ανακάλυψη του Lord Kelvin ότι οι αγωγοί υπό μηχανική καταπόνηση αλλάξτε την αντίστασή τους) και συσκευές εξόδου όπως ο τηλεγραφικός βυθός του Samuel Morse και το ρελέ. Το 1889 αυτό οδήγησε έναν συγγραφέα στις διαδικασίες του Ινστιτούτου Πολιτικών Μηχανικών να προτείνει ότι ο όρος για τον τηλεμετρητή απόστασης θα μπορούσε να αντικατασταθεί με ταχύμετρο.[6]

Στη δεκαετία του 1930 η χρήση ηλεκτρικών τηλεμέτρων αυξήθηκε ραγδαία. Ο ηλεκτρικός μετρητής τάσης χρησιμοποιήθηκε ευρέως στην έρευνα πυραύλων και αεροπορίας και το radiosonde εφευρέθηκε για μετεωρολογικές μετρήσεις. Η έλευση του Β' Παγκοσμίου Πολέμου έδωσε ώθηση στη βιομηχανική ανάπτυξη και στο εξής πολλά από αυτά τα τηλέμετρα έγιναν εμπορικά βιώσιμα.[7]

Συνεχίζοντας την έρευνα πυραύλων, η ραδιοτηλεμετρία χρησιμοποιήθηκε συστηματικά καθώς ξεκινούσε η εξερεύνηση του διαστήματος. Τα διαστημικά σκάφη βρίσκονται σε ένα μέρος όπου δεν είναι δυνατή μια φυσική σύνδεση, αφήνοντας ραδιοφωνικά ή άλλα ηλεκτρομαγνητικά κύματα (όπως τα υπέρυθρα λέιζερ) ως τη μόνη βιώσιμη επιλογή για την τηλεμετρία. Κατά τη διάρκεια διαστημικών αποστολών με πλήρωμα χρησιμοποιείται για την παρακολούθηση όχι μόνο παραμέτρων του οχήματος, αλλά και για την υποστήριξη της υγείας και της ζωής των αστροναυτών.[8] Κατά τη διάρκεια του Ψυχρού Πολέμου η τηλεμετρία βρήκε χρήσεις στην κατασκοπεία. Οι αμερικανικές υπηρεσίες πληροφοριών διαπίστωσαν ότι μπορούσαν να παρακολουθήσουν την τηλεμετρία από τις δοκιμές σοβιετικών πυραύλων κατασκευάζοντας ένα δικό τους τηλεμετρητή για να αναχαιτίσει τα ραδιοφωνικά σήματα και ως εκ τούτου να μάθουν πολλά για τις σοβιετικές δυνατότητες.[9]

1.3. Τύποι τηλεμέτρου

Τα τηλέμετρα είναι οι φυσικές συσκευές που χρησιμοποιούνται στην τηλεμετρία. Αποτελείται από έναν αισθητήρα, μια διαδρομή μετάδοσης και μια συσκευή απεικόνισης, εγγραφής ή ελέγχου. Οι ηλεκτρονικές συσκευές χρησιμοποιούνται ευρέως στην τηλεμετρία και μπορεί να είναι ασύρματες ή ενσύρματες, αναλογικές ή ψηφιακές. Είναι επίσης δυνατές και άλλες τεχνολογίες, όπως μηχανικές, υδραυλικές και οπτικές.[10]

Οι πληροφορίες τηλεμέτρησης μέσω καλωδίων είχαν τις ρίζες τους τον 19ο αιώνα. Ένα από τα πρώτα κυκλώματα μετάδοσης δεδομένων αναπτύχθηκε το 1845 μεταξύ του Χειμερινού Παλατιού του Ρώσου Τσάρου και του αρχηγείου του στρατού. Το 1874, Γάλλοι μηχανικοί κατασκεύασαν ένα σύστημα αισθητήρων καιρού και βάθους χιονιού στο Mont Blanc που μετέδωσε πληροφορίες σε πραγματικό χρόνο στο Παρίσι. Το 1901 ο Αμερικανός εφευρέτης C. Michalke κατοχύρωσε με δίπλωμα ευρεσιτεχνίας το selsyn, ένα κύκλωμα για την αποστολή συγχρονισμένων πληροφοριών περιστροφής σε απόσταση. Το 1906 κατασκευάστηκε ένα σύνολο σεισμικών σταθμών με τηλεμέτρηση στο Αστεροσκοπείο Pulkovo στη Ρωσία. Το 1912, η Commonwealth Edison ανέπτυξε ένα σύστημα τηλεμετρίας για την παρακολούθηση των ηλεκτρικών φορτίων στο ηλεκτρικό της δίκτυο. Η Διώρυγα του Παναμά (ολοκληρώθηκε 1913–1914) χρησιμοποίησε εκτεταμένα συστήματα τηλεμετρίας για την παρακολούθηση των κλειδαριών και της στάθμης του νερού.[11]

Η ασύρματη τηλεμετρία εμφανίστηκε νωρίς στο radiosonde, που αναπτύχθηκε ταυτόχρονα το 1930 από τον Robert Bureau στη Γαλλία και τον Pavel Molchanov στη Ρωσία. Το σύστημα του Molchanov διαμόρφωσε τις μετρήσεις θερμοκρασίας και πίεσης μετατρέποντάς τις σε ασύρματο κώδικα Μορς. Ο γερμανικός πύραυλος V-2 χρησιμοποίησε ένα σύστημα πρωτόγονων

πολυπλεξικών ραδιοφωνικών σημάτων που ονομαζόταν "Messina" για να αναφέρει τέσσερις παραμέτρους πυραύλων, αλλά ήταν τόσο αναξιόπιστος που ο Wernher von Braun ισχυρίστηκε κάποτε ότι ήταν πιο χρήσιμο να παρακολουθεί κανείς τον πύραυλο με κιάλια.

Στις ΗΠΑ και την ΕΣΣΔ, το σύστημα της Μεσσήνης αντικαταστάθηκε γρήγορα με καλύτερα συστήματα. και στις δύο περιπτώσεις, με βάση τη διαμόρφωση θέσης παλμού (PPM).[12] Τα πρώιμα σοβιετικά συστήματα πυραύλων και διαστημικής τηλεμετρίας που αναπτύχθηκαν στα τέλη της δεκαετίας του 1940 χρησιμοποιούσαν είτε PPM (π.χ. το σύστημα τηλεμετρίας Tral που αναπτύχθηκε από την OKB-MEI) είτε διαμόρφωση διάρκειας παλμού (π.χ. το σύστημα RTS-5 που αναπτύχθηκε από το NII-885). Στις Ηνωμένες Πολιτείες, η πρώιμη εργασία χρησιμοποιούσε παρόμοια συστήματα, αλλά αργότερα αντικαταστάθηκαν από τη διαμόρφωση παλμικού κώδικα (PCM) (για παράδειγμα, στον ανιχνευτή Mars Mariner 4). Αργότερα οι σοβιετικοί διαπλανητικοί ανιχνευτές χρησιμοποίησαν πλεονάζοντα ραδιοσυστήματα, μεταδίδοντας τηλεμετρία με PCM σε δεκατιανή ζώνη και PPM σε ζώνη εκατοστών.[13]

1.4. Διάφορες εφαρμογές τηλεμετρίας

1.4.1. Μετεωρολογία

Η τηλεμετρία χρησιμοποιείται από τα μετεωρολογικά μπαλόνια για τη μετάδοση μετεωρολογικών δεδομένων από το 1920.

1.4.2. Βιομηχανία πετρελαίου και φυσικού αερίου

Η τηλεμετρία χρησιμοποιείται για τη μετάδοση της μηχανικής γεώτρησης και των πληροφοριών αξιολόγησης σχηματισμού, σε πραγματικό χρόνο, καθώς γίνεται διάνοιξη φρεατίου. Αυτές οι υπηρεσίες είναι γνωστές ως Μέτρηση κατά τη γεώτρηση και Καταγραφή κατά τη γεώτρηση. Οι πληροφορίες που λαμβάνονται χιλιάδες πόδια κάτω από το έδαφος, κατά τη διάτρηση, αποστέλλονται μέσω της οπής διάτρησης στους αισθητήρες επιφάνειας και στο λογισμικό αποδιαμόρφωσης. Το κύμα πίεσης (sana) μεταφράζεται σε χρήσιμες πληροφορίες μετά τα φίλτρα DSP και θορύβου. Αυτές οι πληροφορίες χρησιμοποιούνται για την αξιολόγηση σχηματισμού, τη βελτιστοποίηση γεωτρήσεων και τη γεωκατεύθυνση.

1.4.3. Αγώνες αυτοκινήτου

Η τηλεμετρία είναι ένας βασικός παράγοντας στους σύγχρονους αγώνες μηχανοκίνητων αγώνων, επιτρέποντας στους μηχανικούς αγώνων να ερμηνεύουν τα δεδομένα που συλλέγονται κατά τη διάρκεια μιας δοκιμής ή αγώνα και να τα χρησιμοποιούν για να συντονίζουν σωστά το αυτοκίνητο για βέλτιστη απόδοση. Συστήματα που χρησιμοποιούνται σε σειρές όπως η Formula 1 έχουν εξελιχθεί σε σημείο που μπορεί να υπολογιστεί ο πιθανός χρόνος γύρου του μονοθεσίου. Παραδείγματα μετρήσεων σε αγωνιστικό αυτοκίνητο περιλαμβάνουν επιταχύνσεις (δυνάμεις G) σε τρεις άξονες, ενδείξεις θερμοκρασίας, ταχύτητα τροχού και μετατόπιση ανάρτησης. Στη Formula 1, η εισαγωγή του οδηγού καταγράφεται επίσης, ώστε η ομάδα να μπορεί να αξιολογήσει την απόδοση του οδηγού και (σε περίπτωση ατυχήματος) η FIA να προσδιορίσει ή να αποκλείσει το σφάλμα οδηγού ως πιθανή αιτία.

Οι μεταγενέστερες εξελίξεις περιλαμβάνουν την αμφίδρομη τηλεμετρία που επιτρέπει στους μηχανικούς να ενημερώνουν τις βαθμονόμηση του αυτοκινήτου σε πραγματικό χρόνο (ακόμα και όταν είναι εκτός πίστας). Στη Formula 1, η αμφίδρομη τηλεμετρία εμφανίστηκε στις αρχές της δεκαετίας του 1990 και αποτελούνταν από μια εμφάνιση μηνυμάτων στο ταμπλό, την οποία η ομάδα μπορούσε να ενημερώσει. Η ανάπτυξή του συνεχίστηκε μέχρι τον Μάιο του 2001, όταν επιτρεπόταν για πρώτη φορά στα αυτοκίνητα. Μέχρι το 2002, οι ομάδες μπορούσαν να αλλάξουν τη χαρτογράφηση του κινητήρα και να απενεργοποιήσουν τους αισθητήρες του κινητήρα από το pit ενώ το μονοθέσιο βρισκόταν στην πίστα. Η συγκεκριμένη τεχνολογία μπορεί να χρησιμοποιηθεί και σε άλλους τύπους αγώνων ή σε αυτοκίνητα δρόμου.

Σύστημα μονόδρομης τηλεμετρίας έχει επίσης εφαρμοστεί σε αγωνιστικά αυτοκίνητα R/C για τη λήψη πληροφοριών από τους αισθητήρες του αυτοκινήτου όπως: RPM κινητήρα, τάση, θερμοκρασίες, γκάζι.

1.4.4. Μεταφορές

Στον κλάδο των μεταφορών, η τηλεμετρία παρέχει σημαντικές πληροφορίες σχετικά με την απόδοση ενός οχήματος ή του οδηγού συλλέγοντας δεδομένα από αισθητήρες εντός του οχήματος. Αυτό πραγματοποιείται για διάφορους λόγους που κυμαίνονται από την παρακολούθηση της συμμόρφωσης του προσωπικού, την αξιολόγηση ασφάλισης έως την προγνωστική συντήρηση.

Η τηλεμετρία χρησιμοποιείται επίσης για τη σύνδεση συσκευών μετρητών κυκλοφορίας με καταγραφείς δεδομένων για τη μέτρηση των ροών κυκλοφορίας και του μήκους και του βάρους των οχημάτων.[14]

1.4.5. Γεωργία

Οι περισσότερες δραστηριότητες που σχετίζονται με υγιείς καλλιέργειες και καλές αποδόσεις εξαρτώνται από την έγκαιρη διαθεσιμότητα δεδομένων καιρού και εδάφους. Ως εκ τούτου, οι ασύρματοι μετεωρολογικοί σταθμοί διαδραματίζουν σημαντικό ρόλο στην πρόληψη ασθενειών και στην άρδευση ακριβείας. Αυτοί οι σταθμοί μεταδίδουν παραμέτρους απαραίτητες για τη λήψη αποφάσεων σε έναν σταθμό βάσης: θερμοκρασία αέρα και σχετική υγρασία, βροχόπτωση και υγρασία των φύλλων (για μοντέλα πρόβλεψης ασθενειών), ηλιακή ακτινοβολία και ταχύτητα ανέμου (για τον υπολογισμό της εξατμισοδιαπνοής), αισθητήρες φύλλων ελλειμματικής τάσης νερού (WDS). και την υγρασία του εδάφους (κρίσιμης σημασίας για τις αποφάσεις άρδευσης).

Επειδή τα τοπικά μικροκλίματα μπορεί να διαφέρουν σημαντικά, τέτοια δεδομένα πρέπει να προέρχονται από το εσωτερικό της καλλιέργειας. Οι σταθμοί παρακολούθησης συνήθως μεταδίδουν δεδομένα με επίγειο ραδιόφωνο, αν και περιστασιακά χρησιμοποιούνται δορυφορικά συστήματα. Η ηλιακή ενέργεια χρησιμοποιείται συχνά για να γίνει ο σταθμός ανεξάρτητος από το ηλεκτρικό δίκτυο.

1.4.6. Διαχείριση νερού

Η τηλεμετρία είναι σημαντική στη διαχείριση του νερού, συμπεριλαμβανομένων της ποιότητας του νερού και των λειτουργιών μέτρησης ρεμάτων. Οι κύριες εφαρμογές περιλαμβάνουν AMR (αυτόματη ανάγνωση μετρητών), παρακολούθηση υπόγειων υδάτων, ανίχνευση διαρροών σε αγωγούς διανομής και επιτήρηση εξοπλισμού. Η ύπαρξη δεδομένων σε σχεδόν πραγματικό χρόνο επιτρέπει γρήγορες αντιδράσεις σε γεγονότα στο πεδίο. Ο έλεγχος τηλεμετρίας επιτρέπει στους μηχανικούς να επέμβουν με στοιχεία όπως αντλίες και ενεργοποιώντας ή απενεργοποιώντας τις αντλίες εξ αποστάσεως ανάλογα με τις περιστάσεις. Η τηλεμετρία λεκανών απορροής είναι μια εξαιρετική στρατηγική για τον τρόπο εφαρμογής ενός συστήματος διαχείρισης νερού. [15]

1.4.7. Άμυνα, εξερεύνηση διαστήματος και πόρων

Η τηλεμετρία χρησιμοποιείται σε πολύπλοκα συστήματα όπως πύραυλοι, RPV, διαστημόπλοια, εξέδρες άντλησης πετρελαίου και χημικά εργοστάσια, καθώς επιτρέπει την αυτόματη παρακολούθηση, ειδοποίηση και τήρηση αρχείων που είναι απαραίτητα για αποτελεσματική και ασφαλή λειτουργία. Διαστημικές υπηρεσίες όπως η NASA, το ISRO, ο Ευρωπαϊκός Οργανισμός Διαστήματος (ESA) και άλλοι φορείς χρησιμοποιούν συστήματα τηλεμετρίας ή/και τηλεχειρισμού για τη συλλογή δεδομένων από διαστημόπλοια και δορυφόρους.

Η τηλεμετρία είναι ζωτικής σημασίας για την ανάπτυξη πυραύλων, δορυφόρων και αεροσκαφών, επειδή το σύστημα μπορεί να καταστραφεί κατά τη διάρκεια ή μετά τη δοκιμή. Οι μηχανικοί χρειάζονται κρίσιμες παραμέτρους του συστήματος για να αναλύσουν (και να βελτιώσουν) την απόδοση του συστήματος. Ελλείψει τηλεμετρίας, αυτά τα δεδομένα συχνά δεν θα ήταν διαθέσιμα.

ΚΕΦΑΛΑΙΟ 2 – ΒΙΟΜΗΧΑΝΙΚΑ ΔΙΚΤΥΑ

2.1. Προκλήσεις στις βιομηχανικές λύσεις δικτύωσης για έλεγχο και αυτοματισμό

2.1.1. Επεκτασιμότητα και ευελιξία

Η δυνατότητα κλιμάκωσης και η ευελιξία διαδραματίζουν βασικούς ρόλους στον έλεγχο και στον αυτοματισμό. Οι τεχνολογικές εξελίξεις που οδηγούν σε εξαιρετικά ανεπτυγμένες συσκευές Ethernet έχουν βελτιώσει σημαντικά τον εξοπλισμό αυτοματοποίησης διεργασιών και τη μεταφορά δεδομένων. Οι συσκευές Ethernet προσφέρουν τέτοια πλεονεκτήματα επειδή επιτρέπουν την πρόσβαση στα δεδομένα οπουδήποτε. Το εξειδικευμένο προσωπικό μπορεί να έχει πρόσβαση, να ελέγχει, να παρακολουθεί και να διαχειρίζεται απομακρυσμένες καταστάσεις έκτακτης ανάγκης σε πραγματικό χρόνο. Η επεκτασιμότητα και η ευελιξία που προσφέρει η κατασκευή ενός βιομηχανικού δικτύου είναι ιδιαίτερα σημαντικές για τεχνολογίες όπως συστήματα μηχανικής όρασης, καθώς επιτρέπει την πραγματοποίηση επεξεργασίας μικτών μοντέλων εντός του συστήματος.

Προϊόντα και απαιτήσεις λύσης βιομηχανικής δικτύωσης Ethernet για δυνατότητα κλιμάκωσης και ευελιξίας:

- Βιομηχανικοί διακόπτες Ethernet
- Μετατροπείς πολυμέσων ινών Ethernet
- Βιομηχανικοί διακομιστές ασύρματων συσκευών
- Διακομιστές συσκευών Serial-to-Ethernet
- Προϊόντα ενσωματωμένα με σειριακό, Lan και WLAN (IEEE802.11)
- Διαμορφώσεις θύρας εξοπλισμένες με τεχνολογίες ινών, SFP, χαλκού Gigabit ή 10 / 100MB και PoE

2.1.2. Αξιοπιστία

Η αξιοπιστία έχει αναπόσπαστο ρόλο στην επιτυχή λειτουργία των βιομηχανικών διαδικασιών παραγωγής και αυτοματισμού. Παραδείγματα τομέων όπου η αξιοπιστία είναι ιδιαίτερα σημαντική περιλαμβάνουν τα μηχανήματα CNC, τη βιομηχανία εμφιάλωσης και τα συστήματα όρασης μηχανών όπου η αποτελεσματική και συνεχής λειτουργία είναι απαραίτητη όταν λειτουργεί σε σκληρά περιβάλλοντα ή δονήσεις. Χωρίς αξιοπιστία, οι βιομηχανίες αυτοματισμού ενδέχεται να αντιμετωπίσουν σημαντικό χρόνο διακοπής λειτουργίας. Μια τέτοια διακοπή στην παραγωγή μπορεί να είναι επιζήμια, καθώς μπορεί να οδηγήσει σε απρόβλεπτα και ελαττωματικά προϊόντα. Ως εκ τούτου, οι εγκαταστάσεις χρειάζονται εξοπλισμό δικτύωσης βιομηχανικής ποιότητας ανθεκτικό σε ζημιές από δονήσεις και σκληρά περιβάλλοντα για να διασφαλίζεται η συνεχής λειτουργία και να αποφεύγεται ο χρόνος διακοπής λειτουργίας.

Βιομηχανικές λύσεις δικτύωσης Ethernet και απαιτήσεις των προϊόντων για αξιοπιστία:

- Προϊόντα βιομηχανικής δικτύωσης που πέρασαν πιστοποιήσεις ειδικά σχεδιασμένα και αναπτυγμένα για τα σκληρά περιβάλλοντα που υπάρχουν στη βιομηχανική βιομηχανία αυτοματισμού.
- Εξοπλισμός βιομηχανικής δικτύωσης που περιέχει ενσωματωμένη υψηλή προστασία EFT και ESD για την παροχή δεδομένων μετάδοσης μεταξύ του εξοπλισμού και του δικτύου χωρίς διακοπή.

2.1.3. Ανθεκτικό και μακράς διαρκείας

Ο εξοπλισμός που χρησιμοποιείται στην κατασκευή και τον αυτοματισμό της διαδικασίας πρέπει να αντέχει σε σκληρά βιομηχανικά περιβάλλοντα, όπως ακραίες αλλαγές θερμοκρασίας, δονήσεις και έκθεση σε χημικές ουσίες που μπορεί να προκαλέσουν διάβρωση. Αυτό σημαίνει ότι ο εξοπλισμός πρέπει να έχει στιβαρό και μακράς διαρκείας σχεδιασμό, γι’ αυτό οι εγκαταστάσεις πρέπει να εφαρμόζουν ένα ισχυρό δίκτυο βιομηχανικού αυτοματισμού. Βιομηχανικές εφαρμογές όπου η ανθεκτικότητα είναι σημαντική περιλαμβάνουν τις βιομηχανίες εμφιάλωσης και ανακύκλωσης

χαρτιού, καθώς και κατά τη δημιουργία συστημάτων μηχανικής όρασης ή τη δημιουργία ενός αποτελεσματικού και αξιόπιστου δικτύου διαχείρισης υλικών.

Βιομηχανικές λύσεις δικτύωσης Ethernet και απαιτήσεις των προϊόντων για ανθεκτικότητα:

- IP30 / 40/50/67 ονομαστική αδιάβροχη κατοικία
- Ανθεκτικό μεταλλικό περίβλημα
- Ευρεία ανοχή θερμοκρασίας λειτουργίας
- Στεγανοποίηση κραδασμών
- Υψηλή MTBF και θορύβου

2.1.4. Αυτοπροστατεύομενο δίκτυο

Λόγω των σκληρών περιβαλλόντων στα οποία λειτουργούν οι περισσότερες εγκαταστάσεις αυτοματισμού κατασκευής και επεξεργασίας, είναι απαραίτητο ένα ισχυρό δίκτυο. Τα ισχυρά δίκτυα μπορούν να βοηθήσουν στην προστασία των συστημάτων και του δικτύου από αποτυχία σε περίπτωση απρόβλεπτων συμβάντων που μπορεί να οδηγήσουν σε διακοπή λειτουργίας. Όπως αναφέρθηκε προηγουμένως, ο χρόνος διακοπής λειτουργίας μπορεί να καταστεί επιζήμιος για τέτοιες εγκαταστάσεις, καθώς μπορεί να οδηγήσει σε απρόσμενα και ελαττωματικά προϊόντα που μπορούν να καταστρέψουν πολλές βιομηχανίες. Η διασφάλιση της συνεπούς και συνεχούς λειτουργίας των συστημάτων και της παραγωγής χρησιμοποιώντας ένα ισχυρό δίκτυο μπορεί να βοηθήσει στην αποφυγή τέτοιων προβλημάτων. Η παραγωγή της βιομηχανίας εμφιάλωσης και η τεχνολογία μηχανικής όρασης είναι μόνο μερικά παραδείγματα όπου η εφεδρική υποστήριξη δικτύου είναι υψίστης σημασίας.

Βιομηχανικά προϊόντα και απαιτήσεις λύσης δικτύωσης Ethernet για περιττά δίκτυα αυτοπροστασίας:

- Διαχειριζόμενοι διακόπτες Ethernet
- Διακομιστές σειριακών συσκευών
- Προϊόντα που υποστηρίζουν χαρακτηριστικά απόλυσης
- Προϊόντα με ενσωματωμένο πρωτόκολλο πλεονασμού δικτύου για την παροχή αδιάλειπτης δικτύωσης 24/7 παρέχοντας τοπολογία δικτύου πλεονασμού δακτυλίου για την εκ νέου δρομολόγηση της επικοινωνίας δεδομένων πίσω στη διαδρομή.

2.1.5. Απλοποίηση της συνδεσιμότητας

Οι εγκαταστάσεις αυτοματισμού κατασκευής και επεξεργασίας πρέπει να έχουν τη δυνατότητα διαχείρισης απομακρυσμένων δικτύων σε πραγματικό χρόνο. Η δημιουργία ενός ισχυρού βιομηχανικού δικτύου που επιτρέπει τέτοιες δυνατότητες, ωστόσο, μπορεί να γίνει εξαιρετικά δύσκολη για πολλούς μηχανικούς και σχεδιαστές δικτύων σε τέτοιες βιομηχανίες. Είναι σημαντικό να απλοποιήσουμε τη συνδεσιμότητα για να δημιουργήσετε ένα ισχυρό βιομηχανικό δίκτυο.

Προϊόντα και απαιτήσεις λύσης βιομηχανικής δικτύωσης Ethernet για απλοποίηση της συνδεσιμότητας:

- Διαχειριζόμενοι διακόπτες Ethernet
- Βιομηχανικές ασύρματες συσκευές
- Βιομηχανικοί σειριακοί διακομιστές συσκευών
- Οι βιομηχανικές συσκευές που είναι προεγκατεστημένες με μια ευκολία στη χρήση διεπαφή διαδικτυακής κονσόλας επιτρέπουν εύκολη προσαρμογή, γρήγορη ρύθμιση και ανάπτυξη.

2.2. PROFIBUS

Η ιστορία του PROFIBUS ξεκίνησε με ένα κοινό έργο της ένωσης PROFIBUS και της γερμανικής κυβέρνησης το 1987. Σε αυτήν την προσπάθεια, 21 εταιρείες και ιδρύματα συνδύασαν τις προσπάθειές τους για τη δημιουργία ενός στρατηγικού έργου για το fieldbus. Ο στόχος τους ήταν να σταθεροποιήσουν ένα δίαυλο πεδίου bitserial που θα τυποποιήσει μια διεπαφή συσκευής πεδίου.

Ως εκ τούτου, οι σχετικές εταιρείες μέλη της ZVEI, η Κεντρική Ένωση Ηλεκτρικής Βιομηχανίας, συμφώνησαν να υποστηρίξουν μια τεχνική ιδέα αμοιβαίου ενδιαφέροντος για την κατασκευή και τον αυτοματισμό διεργασιών.

Το πρώτο βήμα ήταν η προδιαγραφή του σύνθετου πρωτοκόλλου επικοινωνίας PROFIBUS FMS (Fieldbus Message Specification), που σχεδιάστηκε για τις απαιτήσεις εργασιών επικοινωνίας.

Ένα βήμα παραπέρα το 1993 ήταν το συμπέρασμα της προδιαγραφής μιας απλούστερης και ταχύτερης παραλλαγής επικοινωνίας, του PROFIBUS-DP (Αποκεντρωμένο Περιφερειακό). Αυτό το πρωτόκολλο είναι τώρα διαθέσιμο σε τρεις λειτουργικές εκδόσεις, DP-V0, DP-V1 και DP-V2.

Με βάση αυτά τα δύο πρωτόκολλα επικοινωνίας, μαζί με την ανάπτυξη διαφόρων προφίλ προσανατολισμένων εφαρμογών και μια σειρά από συσκευές που αναπτύσσονται ταχέως, το PROFIBUS προχώρησε αρχικά στον αυτοματισμό κατασκευής και από το 1995, στον αυτοματισμό της διαδικασίας με την εισαγωγή του PROFIBUS-PA. Σήμερα, το PROFIBUS είναι το κορυφαίο bus πεδίου στον κόσμο.

Το PROFIBUS είναι ένα πρότυπο ανοικτού και ανεξάρτητου πεδίου δικτύου προμηθευτών των οποίων η διασύνδεση μεταξύ τους επιτρέπει μεγάλο αριθμό εφαρμογών σε διαδικασίες, κατασκευή και αυτοματισμό κτιρίων. Αυτό το πρότυπο είναι εγγυημένο σύμφωνα με τα πρότυπα EN 50170 και EN 50254. Από τον Ιανουάριο του 2000, το PROFIBUS καθιερώθηκε σταθερά με το πρότυπο IEC 61158, παράλληλα με άλλα επτά πεδία. Το IEC 61158 χωρίζεται σε επτά μέρη, με το όνομα 61158-1 και 61158-6, το οποίο περιλαμβάνει τις προδιαγραφές του μοντέλου OSI. Αυτή η έκδοση επεκτάθηκε για να συμπεριλάβει το DPV-2. Σε όλο τον κόσμο οι χρήστες μπορούν πλέον να χρησιμοποιούν για αναφορά ένα διεθνές πρότυπο ανοιχτού πρωτοκόλλου, του οποίου η ανάπτυξη επιδιώκει και εξακολουθεί να επιδιώκει μείωση κόστους, ευελιξία, αξιοπιστία, ασφάλεια, λειτουργικότητα, προσανατολισμό προς το μέλλον, για να ταιριάζει στις πιο διαφορετικές εφαρμογές και προμηθευτές.

Σήμερα εκτιμάται ότι περίπου 30 εκατομμύρια κόμβοι έχουν εγκατασταθεί με τεχνολογία PROFIBUS και πάνω από 1000 εγκαταστάσεις με τεχνολογία PROFIBUS-PA. Υπάρχουν 24 περιφερειακοί οργανισμοί (RPA) και 35 κέντρα ικανοτήτων που ειδικεύονται στο PROFIBUS (PCCs) στρατηγικά επισημαίνονται σε πολλές χώρες για να προσφέρουν υποστήριξη στους χρήστες. Στη Βραζιλία, υπάρχει η μόνη PCC στη Λατινική Αμερική, που λειτουργεί σε συνεργασία με την FIPAI στη Σχολή Μηχανικών του Σάο Κάρλος - USP.

Όσον αφορά την επικοινωνία, οι προγραμματιζόμενοι ελεγκτές, όπως PLCs και PCs, διατηρούν αμοιβαία επαφή και επιτρέπουν τη μεταφορά μεγάλων πακέτων δεδομένων μέσω πολλών ισχυρών λειτουργιών. Επιπλέον, η αποτελεσματική ενσωμάτωση με τα υπάρχοντα συστήματα εταιρικής επικοινωνίας όπως το Intranet, το Internet και το Ethernet είναι απολύτως υποχρεωτική. Αυτή η απαίτηση ενεργοποιείται από τα πρωτόκολλα PROFIBUS FMS και PROFINet.

Η αρχιτεκτονική PROFIBUS χωρίζεται σε τρεις κύριες παραλλαγές:

2.2.1. PROFIBUS DP

Το PROFIBUS-DP είναι η λύση υψηλής ταχύτητας PROFIBUS. Αναπτύχθηκε ειδικά για επικοινωνία μεταξύ συστημάτων αυτοματισμού και αποκεντρωμένου εξοπλισμού. Προσανατολισμένος στα συστήματα ελέγχου των οποίων η βελτίωση είναι συσκευές κατανεμημένες I / O, το PROFIBUS-DP αντικαθιστά τα συμβατικά συστήματα μετάδοσης 4 έως 20 mA, HART ή 24-Volt και χρησιμοποιεί RS-485 φυσικό μέσο ή οπτικές ίνες. Απαιτεί λιγότερο από 2 m για τη μετάδοση 1 kbyte εισόδου και εξόδου και χρησιμοποιείται ευρέως κρίσιμος έλεγχος χρόνου.

Επί του παρόντος, το 90% των εφαρμογών που περιλαμβάνουν Profibus slaves χρησιμοποιούν PROFIBUS DP. Αυτή η παραλλαγή έχει τρεις εκδόσεις: DP-V0, DP-V1 e DP-V2. Κάθε έκδοση σχεδιάστηκε σύμφωνα με την τεχνολογική πρόοδο και τη ζήτηση για εφαρμογές καθ' όλη τη διάρκεια του χρόνου.

2.2.2. Λειτουργικότητα των συσκευών

DPV2: Περιλαμβάνει τα χαρακτηριστικά του DPV0 και DPV1 και προσθέτει λειτουργίες για τον έλεγχο μηχανών, κυκλικού συγχρονισμού και χρονικού προσδιορισμού.

DPV1: Acyclic Data Exchange μεταξύ PC ή PLC και slave συσκευές και παραμετροποίηση μέσω ειδικών εργαλείων.

DPV0: Περιλαμβάνει τις βασικές λειτουργίες όπως κυκλική επικοινωνία μεταξύ master και slave, GSD διαμόρφωση και διαγνωστικά.

2.2.3. PROFIBUS-PA

Το PROFIBUS PA είναι η λύση που πληροί τις απαιτήσεις αυτοματισμού διεργασίας, όπου τα συστήματα αυτοματισμού και τα συστήματα ελέγχου διεργασίας συνδέονται με εξοπλισμό πεδίου, όπως πομπούς πίεσης και θερμοκρασίας, μετατροπείς, τοποθετήσεις κ.λπ.

Υπάρχουν πιθανά οφέλη από τη χρήση αυτής της τεχνολογίας, των οποίων τα λειτουργικά πλεονεκτήματα περιλαμβάνουν τη μετάδοση αξιόπιστων πληροφοριών, τη θεραπεία μεταβλητής κατάστασης, ασφαλές σύστημα αστοχίας, εξοπλισμό αυτόματης διάγνωσης, εύρος εξοπλισμού, μέτρηση υψηλής ανάλυσης, ενσωμάτωση με διακριτό έλεγχο σε υψηλές ταχύτητες, εφαρμογές σε οποιοδήποτε τμήμα κ.λπ. Εκτός από τα οικονομικά οφέλη που σχετίζονται με τις εγκαταστάσεις (μείωση έως και 40%, σε ορισμένες περιπτώσεις, σε σύγκριση με τα συμβατικά συστήματα), το κόστος συντήρησης (μείωση έως και 25% σε ορισμένες περιπτώσεις, έναντι συμβατικών συστημάτων) και μικρότερα ο χρόνος εκκίνησης συμβάλλει στη σημαντική αύξηση της λειτουργικότητας και της ασφάλειας.

Το PROFIBUS PA επιτρέπει τη μέτρηση και τον έλεγχο μέσω δύο απλών γραμμών καλωδίων. Επιτρέπει επίσης την τροφοδοσία εξοπλισμού πεδίου σε εγγενώς ασφαλείς περιοχές, εκτός από τη συντήρηση και τη σύνδεση / αποσύνδεση εξοπλισμού ακόμη και κατά τη διάρκεια της λειτουργίας, χωρίς να παρεμβαίνει σε άλλους σταθμούς δυνητικά εκρηκτικών περιοχών. Το PROFIBUS PA αναπτύχθηκε σε συνεργασία με τους χρήστες NAMUR, τον κλάδο ελέγχου και επεξεργασίας, σύμφωνα με τις ειδικές απαιτήσεις της περιοχής εφαρμογής, και συγκεκριμένα:

Το αρχικό προφίλ εφαρμογής για αυτοματοποίηση διεργασιών και διαλειτουργικότητα εξοπλισμού πεδίου από διαφορετικούς κατασκευαστές.

Προσθήκη και αφαίρεση σταθμών bus ακόμη και σε εγγενώς ασφαλείς περιοχές, χωρίς επιρροή σε άλλους σταθμούς.

Διαφανής επικοινωνία μέσω ζεύξεων μεταξύ του διαύλου αυτοματοποίησης PROFIBUS PA και του διαύλου βιομηχανικού αυτοματισμού PROFIBUS-DP.

Πηγή ισχύος και μετάδοση δεδομένων μέσω του ίδιου ζεύγους καλωδίων, με βάση την τεχνολογία IEC 61158-2.

Οι συνδέσεις των πομπών, μετατροπέων και θέσεων σε ένα δίκτυο PROFIBUS DP πραγματοποιούνται από έναν ζεύκτη DP / PA. Το διασταυρούμενο ζεύγος καλωδίων χρησιμοποιείται σε κάθε πηγή ισχύος εξοπλισμού και επικοινωνία για κάθε εξοπλισμό, η οποία διευκολύνει την εγκατάσταση και οδηγεί σε χαμηλό κόστος υλικού, λιγότερο χρόνο εκκίνησης, χωρίς προβλήματα συντήρησης, χαμηλό κόστος λογισμικού μηχανικής και υψηλή επιχειρησιακή εμπιστοσύνη.

Η αρχιτεκτονική και η φιλοσοφία του πρωτοκόλλου PROFIBUS εγγυώνται σε κάθε σταθμό που συμμετέχει στην ανταλλαγή κυκλικών δεδομένων επαρκή χρόνο για την εκτέλεση της εργασίας επικοινωνίας εντός καθορισμένου χρονικού διαστήματος. Για το σκοπό αυτό, χρησιμοποιούν τη διαδικασία μετάβασης διακριτικών που χρησιμοποιείται από τους κύριους σταθμούς bus για να επικοινωνούν μεταξύ τους και τη διαδικασία master slave για να επικοινωνούν με τους slaves. Το μήνυμα διακριτικού, ένα ειδικό πλαίσιο για έναν κύριο που περνά το δικαίωμα πρόσβασης σε άλλο, πρέπει να κυκλοφορεί μία φορά για κάθε κύριο εντός του μέγιστου καθορισμένου, ρυθμιζόμενου χρόνου περιστροφής. Στο PROFIBUS, η διαδικασία μετάδοσης διακριτικών χρησιμοποιείται μόνο για επικοινωνία μεταξύ κύριων στοιχείων.

2.3. PROFInet

Το PROFInet είναι ένα δίκτυο τυποποιημένο από το PROFIBUS International συμβατό με τα IEC 61158-5 και IEC 61158-6. Είναι ένα από τα δεκατέσσερα βιομηχανικά δίκτυα Ethernet. Βασικά, υπάρχουν δύο τύποι PROFInet: PROFInet IO και PROFInet CBA. Το PROFInet IO χρησιμοποιείται σε εφαρμογές σε πραγματικό

χρόνο χωρίς κρίσιμο χρόνο, όπως η μετατροπή στο δίκτυο PROFIBUS-DP.

Το PROFInet είναι μια ολοκληρωμένη έννοια αυτοματισμού που προέκυψε ως αποτέλεσμα της τάσης του αυτοματισμού για επαναχρησιμοποιήσιμα και αρθρωτά μηχανήματα σε εγκαταστάσεις με κατανεμημένη νοημοσύνη. Τα χαρακτηριστικά του ανταποκρίνονται στις ιδιαιτερότητες της τεχνολογίας αυτοματισμού:

- Συνεπής επικοινωνία μεταξύ των διαφόρων επιπέδων διαχείρισης από το πεδίο μέσω των εταιρικών επιπέδων χρησιμοποιώντας το Ethernet.
- Περιλαμβάνει έναν μεγάλο αριθμό πρωτοκόλλων και κατασκευαστών ανοιχτού συστήματος.
- Χρησιμοποιεί πρότυπα πληροφορικής.
- Ενσωμάτωση με συστήματα PROFIBUS χωρίς αλλαγές.

Το PROFInet ορίστηκε συμβατό με το Layer ISO / IEC8802-3 και το DataLink Layer, συμβατό με το TCP / UDP / IP / Ethernet του ISO / IEC8802-3. Ο κύριος στόχος του είναι η εφαρμογή της έννοιας των αντικειμένων που χρησιμοποιούνται ήδη και δοκιμάστηκαν σε λογισμικό τεχνολογίας αυτοματισμού. Σύμφωνα με αυτήν την ιδέα, οι μηχανές και τα εργοστάσια μπορούν να χωριστούν σε τεχνολογικές ενότητες, καθένα από αυτά με τα χαρακτηριστικά τους, τα μηχανικά και ηλεκτρικά-ηλεκτρονικά χαρακτηριστικά και το λογισμικό εφαρμογών. Στη συνέχεια, κάθε μονάδα ενθυλακώνεται σύμφωνα με τα στοιχεία PROFInet και μπορεί να προσεγγιστεί μέσω καθολικών διεπαφών, εκτός από τη διασύνδεση με διάφορες εφαρμογές. Η έννοια των συστατικών θα πρέπει να θεωρείται ως η ιδέα της επαναχρησιμοποίησης μονάδων λογισμικού.

Σε αυτό το πλαίσιο, το PROFInet χρησιμοποιεί στοιχεία COM (Component Object Model), ενώ η επέκτασή του, το DCOM (Distoned Component Object Model) για κατανεμημένα συστήματα. Επομένως, όλα τα αντικείμενα είναι πανομοιότυπα και μοιάζουν. Αυτός ο τύπος κατανεμημένου συστήματος αυτοματισμού επιτρέπει αρθρωτά έργα και εγκαταστάσεις που υποστηρίζουν την επαναχρησιμοποίηση εξαρτημάτων μηχανημάτων και εγκαταστάσεων. Αυτό εξασφαλίζει διαλειτουργικότητα και μειωμένα προβλήματα. Η ενοποίηση των τμημάτων PROFIBUS και του PROFInet γίνεται με την εφαρμογή διακομιστών μεσολάβησης, εξασφαλίζοντας έτσι στον χρήστη τη μέγιστη προστασία στις επενδύσεις. Επιπλέον, η τεχνολογία Proxy επιτρέπει την ενοποίηση με άλλα πεδία.

Το PROFInet διαθέτει τρία διαφορετικά μοντέλα λειτουργίας, δύο από αυτά για εργασία σε πραγματικό χρόνο.

Το πρώτο μοντέλο βασίζεται σε καθαρή αρχιτεκτονική TCP / IP, χρησιμοποιώντας Ethernet στα επίπεδα 1 και 2, IP στο επίπεδο 3 και TTCP ή UDP στα επίπεδα 4. Αυτή η αρχιτεκτονική ονομάζεται non-RT, επειδή πλησιάζει ο χρόνος επεξεργασίας 100 μ. Η εξαιρετική εφαρμογή του χρόνου επικοινωνίας είναι για διαμόρφωση δικτύου ή επικοινωνία με τους πληρεξούσιους, χρησιμοποιώντας το PROFInet CBA. Οι διακομιστές μεσολάβησης είναι μετατροπείς πρωτοκόλλων (για παράδειγμα, PROFInet σε PROFIBUS-DP ή PROFInet σε HART, FF κ.λπ.).

Το δεύτερο μοντέλο βασίζεται στο Soft Real Time (SRT) του οποίου η δυνατότητα είναι να είναι ένα άμεσο κανάλι μεταξύ του επιπέδου Ethernet και της εφαρμογής. Με την εξάλειψη πολλών επιπέδων πρωτοκόλλου, υπάρχει μείωση του μήκους των μεταδιδόμενων τηλεγραφημάτων, τα οποία απαιτούν μικρότερο χρόνο μετάδοσης δεδομένων στο δίκτυο. Σε αυτήν την περίπτωση, μπορούν να χρησιμοποιηθούν και οι δύο τύποι PROFInet και CBA.

Το τρίτο μοντέλο βασίζεται στην έννοια του ισόχρονου πραγματικού χρόνου (IRT), για κρίσιμο χρόνο απόκρισης, μικρότερο από 1 ms. Ένα τυπικό παράδειγμα αυτής της εφαρμογής είναι για τον

έλεγχο της κίνησης των ρομπότ, των οποίων ο χρόνος ενημέρωσης πρέπει να είναι σύντομος. Σε αυτήν την περίπτωση, χρησιμοποιείται μόνο το PROFInet IO.

2.4. Modbus RTU και TCP

Το Modbus RTU είναι ένα ανοιχτό σειριακό πρωτόκολλο που προέρχεται από την αρχιτεκτονική master / slave που αναπτύχθηκε αρχικά από τη Modicon (τώρα Schneider Electric). Είναι ένα ευρέως αποδεκτό πρωτόκολλο σειριακού επιπέδου λόγω της ευκολίας χρήσης και της αξιοπιστίας του. Το Modbus RTU χρησιμοποιείται ευρέως στα συστήματα διαχείρισης κτιρίων (BMS) και στα συστήματα βιομηχανικού αυτοματισμού (IAS).

Τα μηνύματα Modbus RTU είναι μια απλή δομή 16-bit με CRC (Cyclic-Redundant Checksum). Η απλότητα αυτών των μηνυμάτων είναι να διασφαλιστεί η αξιοπιστία. Λόγω αυτής της απλότητας, η βασική δομή μητρώου 16 bit Modbus RTU μπορεί να χρησιμοποιηθεί για τη συσκευασία σε κινούμενο σημείο, πίνακες, κείμενο ASCII, ουρές και άλλα μη σχετικά δεδομένα.

Αυτό το πρωτόκολλο χρησιμοποιεί κυρίως σειριακές διεπαφές RS-232 ή RS-485 για επικοινωνίες και υποστηρίζεται από σχεδόν κάθε εμπορικό πρόγραμμα λογισμικού SCADA, HMI, OPC Server και απόκτησης δεδομένων στην αγορά. Αυτό καθιστά πολύ εύκολη την ενσωμάτωση συμβατού εξοπλισμού Modbus σε νέες ή υπάρχουσες εφαρμογές παρακολούθησης και ελέγχου.

Στη σημερινή εποχή της σύνδεσης στο Διαδίκτυο και των Υπηρεσιών Ιστού, το μη συνδεδεμένο μήνυμα της Modbus και η απλή δομή επικοινωνίας αιτήματος-απόκρισης είναι σχεδόν περίεργα. Σχεδόν τόσο παλιά όσο και ο πρώτος προγραμματιζόμενος λογικός ελεγκτής, το Modicon 084, το οποίο εκείνες τις ημέρες ονομάστηκε PC για προγραμματιζόμενο ελεγκτή.

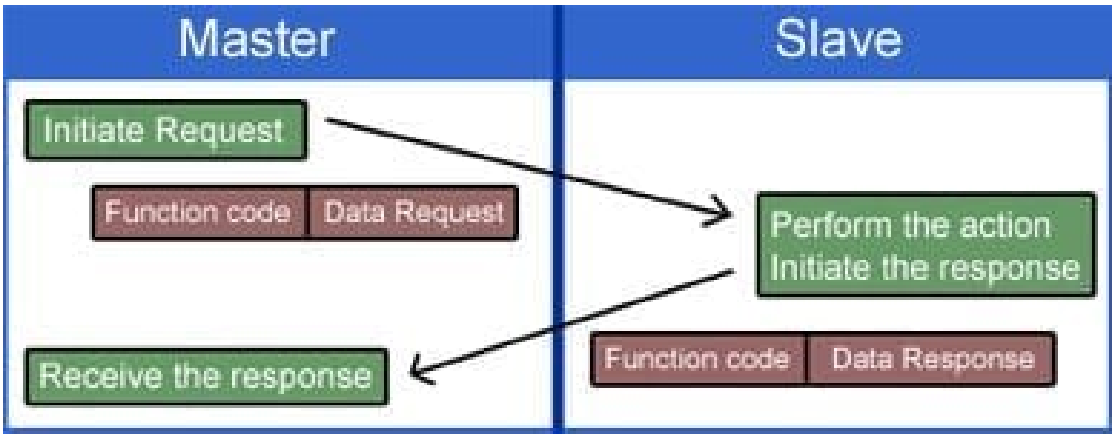
Το Modbus RTU είναι ένα ανοιχτό πρότυπο, που σημαίνει ότι οι κατασκευαστές μπορούν να το ενσωματώσουν στον εξοπλισμό τους χωρίς να χρειάζεται να πληρώσουν δικαιώματα. Είναι το πιο διαδεδομένο πρωτόκολλο επικοινωνίας στον βιομηχανικό αυτοματισμό και είναι πλέον το πιο συχνά διαθέσιμο μέσο σύνδεσης βιομηχανικών ηλεκτρονικών συσκευών.

Το Modbus χρησιμοποιείται ευρέως από πολλούς κατασκευαστές σε πολλές βιομηχανίες. Το Modbus χρησιμοποιείται συνήθως για τη μετάδοση δεδομένων από όργανα ελέγχου σε ελεγκτή λογικής ή σύστημα αρχειοθέτησης δεδομένων. Στην αυτοματοποίηση κτιρίων, για παράδειγμα, η θερμοκρασία και η υγρασία συχνά κοινοποιούνται σε έναν υπολογιστή για μακροχρόνια αποθήκευση. Το Modbus χρησιμοποιείται συχνά για τη σύνδεση ενός εποπτικού υπολογιστή με μια απομακρυσμένη μονάδα τερματικού (RTU) σε συστήματα εποπτείας ελέγχου και απόκτησης δεδομένων (SCADA).

Η απλότητα είναι ο λόγος που το Modbus είναι τόσο διαδεδομένο. Δεν έβλαψε επίσης ότι το Modbus δημιουργήθηκε από έναν από τους μεγαλύτερους κατασκευαστές PLC εκείνη την εποχή και το έκανε ανοιχτό και ευρέως διαθέσιμο. Το Modbus απαιτεί επίσης πολύ λίγο στον χώρο του επεξεργαστή κώδικα ή RAM. Αν και αυτό δεν είναι τόσο σημαντικό σήμερα, λαμβάνοντας υπόψη τους ισχυρούς επεξεργαστές και την τεχνολογία που έχουμε στη διάθεσή μας, ήταν πολύ σημαντικό τα πρώτα χρόνια της βιομηχανικής αυτοματοποίησης όταν οι επεξεργαστές χρησιμοποίησαν τεχνολογία 8-bit και πόροι όπως η RAM και η ROM ήταν εξαιρετικά ακριβά και σπάνια.

Ο έλεγχος μηνυμάτων είναι ένας άλλος λόγος για τον οποίο το Modbus ήταν τόσο δημοφιλές. Ο έλεγχος CRC και LRC σημαίνει ότι τα σφάλματα μετάδοσης ελέγχονται με ακρίβεια 99%.

Το πρωτόκολλο Modbus RTU χρησιμοποιεί τεχνική master / slave για επικοινωνία μεταξύ συσκευών. Δηλαδή, κάθε εφαρμογή που χρησιμοποιεί το πρωτόκολλο Modbus RTU θα έχει Modbus master και τουλάχιστον ένα Modbus slave. Ένα Modbus master είναι συνήθως ένας κεντρικός υπολογιστής εποπτείας που εκτελεί λογισμικό που θα επικοινωνεί με μία ή περισσότερες συσκευές Modbus slave.



Σχήμα 1. Βασική επικοινωνία master – slave σε Modbus protocol

Το Modbus επιτρέπει την επικοινωνία master / slave μεταξύ συσκευών που συνδέονται μέσω λεωφορείων ή δικτύων. Στο μοντέλο OSI, το Modbus βρίσκεται στο επίπεδο 7. Το Modbus προορίζεται να είναι ένα πρωτόκολλο αίτησης / απάντησης και παρέχει υπηρεσίες που καθορίζονται από τους κωδικούς λειτουργίας. Οι κωδικοί λειτουργίας του Modbus είναι στοιχεία των PDU αιτήματος / απάντησης του Modbus (Μονάδα δεδομένων πρωτοκόλλου).

Για να δημιουργήσετε τη μονάδα δεδομένων εφαρμογής Modbus, ο πελάτης πρέπει να ξεκινήσει μια συναλλαγή Modbus. Είναι η συνάρτηση που ενημερώνει τον διακομιστή σχετικά με τον τύπο ενέργειας που πρέπει να εκτελέσει. Η μορφή ενός αιτήματος που ξεκίνησε από ένα Master καθορίζεται από το πρωτόκολλο εφαρμογής Modbus. Στη συνέχεια, το πεδίο κωδικού λειτουργίας κωδικοποιείται σε ένα byte. Μόνο οι κωδικοί που κυμαίνονται από 1 έως 255 θεωρούνται έγκυροι, ενώ οι 128-255 προορίζονται για αποκρίσεις εξαιρέσεων. Όταν ο master στέλνει ένα μήνυμα στο slave, είναι το πεδίο κωδικού λειτουργίας που ενημερώνει τον διακομιστή για το είδος της ενέργειας που πρέπει να εκτελέσει.

Για τον καθορισμό πολλαπλών ενεργειών, ορισμένες λειτουργίες θα έχουν προσθέσει κωδικούς δευτερεύουσας λειτουργίας. Για παράδειγμα, ο master μπορεί να διαβάσει τις καταστάσεις ON / OFF μιας ομάδας διακριτικών εξόδων ή εισόδων. Θα μπορούσε επίσης να διαβάσει / γράψει τα περιεχόμενα δεδομένων μιας ομάδας καταχωρητών Modbus. Όταν ο master λαμβάνει την απόκριση του slave, το πεδίο κωδικού λειτουργίας χρησιμοποιείται από τον slave για να υποδείξει είτε μια απάντηση χωρίς σφάλματα είτε μια απόκριση εξαίρεσης. Ο slave αντηχεί στο αίτημα του αρχικού κώδικα λειτουργίας σε περίπτωση κανονικής απόκρισης.

Όπως όλα τα άλλα σχετικά με το Modbus, η αναπαράσταση των δεδομένων είναι απλή. Στην πραγματικότητα, τα δεδομένα παρουσιάζονται πιο απλά στο Modbus από οποιοδήποτε άλλο βιομηχανικό πρωτόκολλο που θα βρείτε ποτέ. Το μικρότερο κομμάτι αποστέλλεται και λαμβάνεται πρώτα. Όλες οι συσκευές εντός του δικτύου πρέπει να ερμηνεύουν αναλόγως κάθε μεταδιδόμενο byte με αυτόν τον τρόπο.

Δεν υπάρχουν μέθοδοι αυτόματης αναγνώρισης των τιμών baud. Ο ίδιος ρυθμός baud πρέπει να χρησιμοποιείται από τους slave και master που είναι συνδεδεμένοι στο bus. Δεν καθορίζεται συγκεκριμένος ρυθμός baud από το Modbus: οι τυπικοί ρυθμοί baud είναι 9600 ή 19200.

Υπάρχουν μόνο δύο τύποι δεδομένων στο Modbus: πηνία και καταχωρητές. Τα πηνία είναι απλά μεμονωμένα κομμάτια. Τα bit μπορούν να είναι ON (1) ή μπορούν να είναι OFF (0). Ορισμένα πηνία αντιπροσωπεύουν εισόδους, που σημαίνει ότι περιέχουν την κατάσταση ορισμένων φυσικών διακριτών εισόδων. Ή αντιπροσωπεύουν εξόδους, που σημαίνει ότι διατηρούν την κατάσταση κάποιου φυσικού διακριτού σήματος εξόδου. Οι καταχωρητές είναι απλώς 16-bit υπογεγραμμένα δεδομένα μητρώου. Οι καταχωρητές μπορούν να έχουν τιμή από 0 έως 65535 (0 έως δεκαεξαδικό

FFFF). Δεν υπάρχει αναπαράσταση για αρνητικές τιμές, καμία αναπαράσταση για τιμές μεγαλύτερες από 65535 και καμία αναπαράσταση για πραγματικά δεδομένα όπως το 200.125.

Τα μητρώα ομαδοποιούνται σε Μητρώα Εισόδου και Μητρώα Συμμετοχής. Όπως τα πηνία εισόδου, τα μητρώα εισόδου αναφέρουν την κατάσταση κάποιας εξωτερικής εισόδου ως τιμή μεταξύ 0 και 65535. Η αρχική πρόθεση ενός καταχωρητή εισόδου ήταν να αντικατοπτρίζει την αξία ορισμένων αναλογικών εισόδων. Είναι μια ψηφιακή αναπαράσταση ενός αναλογικού σήματος όπως τάσης ή ρεύματος. Οι περισσότερες συσκευές Modbus σήμερα δεν είναι συσκευές εισόδου / εξόδου και οι καταχωρητές εισόδου λειτουργούν απλά πανομοιότυπα με τους καταχωρητές κατοχής.

Τα Holding Registers σχεδιάστηκαν αρχικά ως προσωρινή αποθήκευση προγραμμάτων για συσκευές όπως οι ελεγκτές Modbus. Σήμερα, τα Holding Registers λειτουργούν ως αποθήκευση δεδομένων για συσκευές.

Τα πακέτα Modbus RTU προορίζονται μόνο για αποστολή δεδομένων. Δεν έχουν τη δυνατότητα αποστολής παραμέτρων όπως όνομα σημείου, ανάλυση, μονάδες κ.λπ. Εάν απαιτείται η δυνατότητα αποστολής τέτοιων παραμέτρων, θα πρέπει να διερευνήσει ένα BACnet, EtherNet / IP ή άλλα σύγχρονα πρωτόκολλα.

Οι τυπικές διευθύνσεις κόμβου Modbus RTU είναι 1-255, με 0 να προορίζονται για μηνύματα μετάδοσης και μόνο εγγραφή. Ωστόσο, η διεύθυνση 0 χρησιμοποιείται σπάνια, καθώς δεν υπάρχει επιβεβαίωση ότι το μήνυμα ελήφθη σωστά στον δευτερεύοντα κόμβο. Αυτό δεν έχει μεγάλη επίδραση εάν το φυσικό σας στρώμα είναι RS-232 καθώς μόνο ένας κόμβος μπορεί να εφαρμοστεί ούτως ή άλλως. Το RS-485 περιορίζει τον αριθμό των κόμβων σε 32, αν και ορισμένα προγράμματα οδήγησης θα σας επιτρέψουν να επεκτείνετε το ποσό.

Οι συσκευές Serial Modbus slave αναγνωρίζονται από έναν αριθμό σταθμού που προηγείται της γενικής δομής μηνυμάτων. Γενικά, υποστηρίζονται έως και 32 σταθμοί, καθώς αυτό είναι το όριο που επιβάλλουν τα περισσότερα σειριακά προγράμματα οδήγησης RS485. Δεν υπάρχει όριο λογισμικού στον αριθμό των σταθμών που θα μπορούσαν να υποστηριχθούν. Οι έγκυρες διευθύνσεις slave εκχωρούνται στην περιοχή από 1 έως 255 με τον αριθμό σταθμού 0 δεσμευμένο για μηνύματα μετάδοσης, μηνύματα που υποβάλλονται σε επεξεργασία από όλους τους Slave.

Υπάρχουν πολλές τυπικές μεταφορές που χρησιμοποιούνται για τη μετακίνηση μηνυμάτων πρωτοκόλλου Modbus: RS232 και RS485. Μπορείτε να χρησιμοποιήσετε άλλους, αλλά αυτά είναι τα συνηθισμένα.

Το RS485 είναι διάδοχος του RS232. Λειτουργεί με παρόμοιο τρόπο όσον αφορά τα bit συγχρονισμού που συγχρονίζουν τη μεταφορά bit από σταθμό αποστολής σε σταθμό λήψης. Υπάρχουν, ωστόσο, δύο καθοριστικά χαρακτηριστικά που κάνουν το RS485 διαφορετικό από το RS232. Το πρώτο είναι η ικανότητα οδήγησης πολλών προορισμών. Οι πομποί RS485 μπορούν να σηματοδοτήσουν ηλεκτρικά έως και 32 συσκευές προορισμού. Αυτό καθιστά το RS485 τον προτιμώμενο τρόπο μεταφοράς σειριακών μηνυμάτων Modbus.

Το άλλο καθοριστικό χαρακτηριστικό του RS485 είναι η αυξημένη θωράκιση. Το RS485 δεν χρησιμοποιεί το ηλεκτρικό κοινό ως αναφορά για το ηλεκτρικό σήμα του. Αντ' αυτού, το RS485 χρησιμοποιεί ένα ζεύγος καλωδίων και οδηγεί ένα σήμα ρυθμίζοντας ένα δυναμικό τάσης στο ζεύγος. Με αυτόν τον τρόπο, οποιοσδήποτε περιβαλλοντικός ηλεκτρικός θόρυβος επηρεάζει και τα δύο καλώδια εξίσου και το δυναμικό στα δύο καλώδια δεν αλλάζει.

Ένας μηχανισμός κωδικοποίησης περιγράφει πώς σχηματίζονται μοτίβα bit από τις τιμές ελέγχου και δεδομένων που κωδικοποιούνται στο πακέτο. Τόσο ο αποστολέας όσο και ο παραλήπτης πρέπει να χρησιμοποιούν την ίδια κωδικοποίηση για να κατανοήσουν σωστά τα περιεχόμενα των δεδομένων. Υπάρχουν δύο μηχανισμοί για την κωδικοποίηση μηνυμάτων Modbus: ASCII και RTU.

Η κωδικοποίηση RTU είναι ο πολύ πιο κοινός μηχανισμός κωδικοποίησης που χρησιμοποιείται στο Modbus. Το RTU σημαίνει απλώς ότι οι τιμές κωδικοποιούνται ως τυπικό δυαδικό big-endian. Αυτό σημαίνει ότι στην περίπτωση των τιμών 16-bit, το Most Significant Byte (MSB) κωδικοποιείται πριν από το Least Significant byte (LSB). Μια τιμή 8-bit όπως το δεκαδικό 41 (29 hex) κωδικοποιείται απλά ως 0010 1001. Ενώ μια τιμή 16-bit όπως το δεκαδικό 300 (12C hex) κωδικοποιείται ως 0000 0001 0010 1100. Το MSB του 01 κωδικοποιείται και μεταδίδεται πριν από το LSB του 2C.

Η πιο βασική διαφορά μεταξύ Modbus RTU και Modbus TCP (Επίσης γνωστή ως Modbus IP, Modbus EtherNet και Modbus TCP / IP) είναι ότι το Modbus TCP εκτελείται σε φυσικό επίπεδο Ethernet και το Modbus RTU είναι ένα πρωτόκολλο σειριακού επιπέδου. Το Modbus TCP χρησιμοποιεί επίσης μια κεφαλίδα 6-byte για να επιτρέπει τη δρομολόγηση.

Το Modbus RTU master είναι ένα μόνο master bus. Στέλνει ένα μήνυμα σε μια υποτελή συσκευή RTU και λαμβάνει μια απάντηση. Το Modbus RTU περιορίζεται σε ένα μόνο κύριο. Μόνο ένα σύνολο σημάτων μπορεί να βρίσκεται στον σύνδεσμο RS485 ανά πάσα στιγμή. Είτε μεταδίδεται το μόνο RTU master είτε μεταδίδεται μία από τις συσκευές RTU Client.

Με την εισαγωγή του Modbus TCP, όλα απλοποιήθηκαν και ήταν ευκολότερα. Με το Modbus TCP, οι ελεγκτές μπορούν πολύ πιο αποτελεσματικά να χρησιμοποιούν το εύρος ζώνης στο Ethernet για να είναι το master σε εκατοντάδες συσκευές Modbus TCP. Το Modbus TCP επιτρέπει πολλαπλούς πελάτες. Όπου το RS485 είχε ηλεκτρικό περιορισμό 32 συσκευών, το Ethernet είναι απεριόριστο. Η λειτουργική μνήμη RAM είναι ο μόνος πρακτικός περιορισμός. Με το Modbus TCP, υπάρχει η δυνατότητα για έναν σχεδιαστή δικτύου να χρησιμοποιεί πολλαπλούς clients / masters εάν το επιθυμούν.

Με το Modbus TCP (Ethernet), πρέπει να ασχοληθείτε με έναν ακριβό διακόπτη. Με το Modbus RTU (σειριακό), μπορείτε απλώς να συνδέσετε όλες τις συσκευές μαζί. Συσκευές με παλιούς επεξεργαστές 8-bit και λίγη μνήμη μπορούν εύκολα να κάνουν σειριακό Modbus, αλλά θα χρειαστείτε μια πιο ακριβή πλατφόρμα για να κάνετε Ethernet.

2.6. EtherCAT

Το EtherCAT σημαίνει "Ethernet for Control Automation Technology." Είναι ένα πρωτόκολλο που φέρνει τη δύναμη και την ευελιξία του ethernet σε:

- βιομηχανικό αυτοματισμό
- έλεγχο κίνησης
- συστήματα ελέγχου σε πραγματικό χρόνο
- συστήματα απόκτησης δεδομένων

Αναπτύχθηκε τη δεκαετία του 1970 στο Palo Alto Research Center (PARC) της Xerox, το Ethernet σχεδιάστηκε ως διεπαφή δικτύου χαμηλού κόστους και ανεκτικό σε σφάλματα τόσο για τοπικά όσο και για δίκτυα ευρείας περιοχής. Κατά τη στιγμή της εφεύρεσής της, υπήρχαν άλλα δίκτυα, όπως TokenBus, TokenRing, ARCNET, CDDI και μια ποικιλία λιγότερο γνωστών ή ιδιόκτητων διεπαφών δικτύου.

Το EtherCAT αναπτύχθηκε αρχικά από την Beckhoff Automation, έναν σημαντικό κατασκευαστή PLCs (Programmable Logic Controllers) που χρησιμοποιείται σε βιομηχανικούς αυτοματισμούς και συστήματα ελέγχου σε πραγματικό χρόνο.

Είχαν αναπτύξει τη δική τους έκδοση του Fieldbus που ονομάζεται "LightBus" στα τέλη της δεκαετίας του 1980, για να αντιμετωπίσουν το πρόβλημα του εύρους ζώνης άλλων διεπαφών. Πρόσθετες εργασίες σε αυτό το πρωτόκολλο οδήγησαν τελικά στην εφεύρεση του EtherCAT.

Ο Beckhoff εισήγαγε τον EtherCAT στον κόσμο το 2003. Και μετά το 2004, δώρισαν τα δικαιώματα στο ETG (EtherCAT Technology Group), οι οποίοι είναι υπεύθυνοι για την προώθηση του προτύπου. Το ETG έχει μια πολύ ενεργή ομάδα προγραμματιστών και χρηστών. Το EtherCAT είναι τυποποιημένο σύμφωνα με το IEC 61158. Τα συστήματα ελέγχου αυτοματισμού εργοστασίων είναι εξ ορισμού συστήματα σε πραγματικό χρόνο. Η ενεργοποίηση και απενεργοποίηση των μηχανών απαιτεί πολύ χαμηλό λανθάνοντα χρόνο.

Αλλά σε ένα συμβατικό σύστημα ethernet, δεν υπάρχει συγκεκριμένο πρωτόκολλο για αυτό και όλα τα δεδομένα είναι ουσιαστικά «ίδια». Αυτό λειτουργεί καλά με τους υπολογιστές γραφείου που μοιράζονται εύρος ζώνης δικτύου για πρόσβαση σε διακομιστές και εκτυπωτές, αλλά όχι τόσο καλά με εφαρμογές σε πραγματικό χρόνο.

Η συσκευή EtherCAT MASTER είναι η μόνη που επιτρέπεται να μεταδίδει δεδομένα σε όλο το δίκτυο. Ο master στέλνει μια σειρά δεδομένων σε όλο το bus, εξαλείφοντας τις συγκρούσεις δεδομένων ενός συστήματος ethernet και βελτιστοποιώντας την ταχύτητα ως αποτέλεσμα.

Τα πλαίσια EtherCAT είναι ενσωματωμένα σε ένα τυπικό πλαίσιο Ethernet και αναγνωρίζονται στο πεδίο EtherType με την τιμή 0x88A4. Ο master είναι η μόνη συσκευή σε ένα τμήμα EtherCAT που επιτρέπεται να στέλνει μηνύματα - οι slave μπορούν να προσθέσουν δεδομένα και να στείλουν το πλαίσιο μαζί, αλλά δεν μπορούν να δημιουργήσουν νέα μηνύματα από μόνα τους.

Αυτά τα καρέ λαμβάνονται από τις δευτερεύουσες συσκευές EtherCAT (κόμβους) στους οποίους απευθύνεται. Οι εξαρτημένες συσκευές επεξεργάζονται δεδομένα και προσθέτουν ό, τι ζητήθηκε από τον κύριο και στείλτε το πλαίσιο στον επόμενο κόμβο του δακτυλίου.

Ο επόμενος κόμβος κάνει ακριβώς το ίδιο πράγμα, λαμβάνοντας τα δεδομένα που προορίζονται για αυτόν, βάζοντας τα απαιτούμενα δεδομένα πίσω στο πλαίσιο EtherCAT και στέλνοντάς τα στον επόμενο κόμβο.

Η ταχύτητα αυξάνεται από το συμβατικό ethernet όχι μόνο επειδή υπάρχει μόνο μία συσκευή αποστολής δεδομένων, αλλά και λόγω μιας τεχνικής που ονομάζεται «επεξεργασία εν κινήσει». Στο συμβατικό ethernet, κάθε συσκευή πρέπει να διαβάσει την κεφαλίδα κάθε μηνύματος για να προσδιορίσει εάν τα δεδομένα προορίζονται για αυτό, στη συνέχεια να καταπιούν τα δεδομένα και να τα επεξεργαστούν με κάποιο τρόπο. Αλλά με την επεξεργασία εν κινήσει, ο κόμβος διαβάζει την κεφαλίδα και στέλνει τα δεδομένα ταυτόχρονα, εξοικονομώντας χρόνο και βελτιώνοντας την απόδοση.

Τέλος, σε αντίθεση με το συμβατικό ethernet, το EtherCAT επιτρέπει τα εισερχόμενα και εξερχόμενα δεδομένα από περισσότερες από μία συσκευές στο δίκτυο να συνδυάζονται σε μεμονωμένα καρέ. Αυτό βελτιστοποιεί ξανά την ταχύτητα.

Είναι ενδιαφέρον, εάν ένας συγκεκριμένος κόμβος δεν έχει την ισχύ επεξεργασίας για το χειρισμό των δεδομένων, η ταχύτητα του διαύλου μπορεί να ρυθμιστεί από τον master, διασφαλίζοντας ότι δεν θα χαθούν δεδομένα από οποιαδήποτε συσκευή στο δίκτυο.

Μία από τις πιο σημαντικές πτυχές του EtherCAT είναι το κατανεμημένο ρολόι. Κάθε κόμβος σφραγίζει χρονικά τα δεδομένα κατά τη λήψη και, στη συνέχεια, τα σφραγίζει ξανά όταν τα στέλνει στον επόμενο κόμβο. Έτσι, όταν ο master λαμβάνει πίσω τα δεδομένα από τους κόμβους, μπορεί εύκολα να προσδιορίσει την καθυστέρηση κάθε κόμβου. Κάθε μετάδοση δεδομένων από τον κύριο λαμβάνει μια χρονική σήμανση εισόδου / εξόδου από κάθε κόμβο, καθιστώντας το EtherCAT πολύ πιο ντετερμινιστικό και ακριβές στον άξονα T από ό, τι μπορεί να είναι το ethernet.

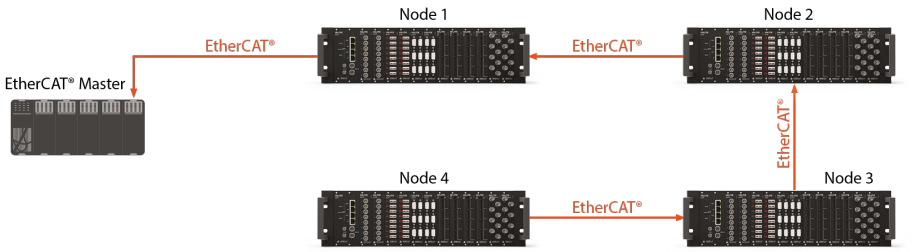
Ακόμα και πριν αρχίσει να λειτουργεί το EtherCAT, ο master στέλνει μια εκπομπή σε όλους τους υποτελείς κόμβους του δικτύου, οι οποίοι την παραλαμβάνουν όταν τη λαμβάνουν και όταν την στέλνουν πίσω. Ο master θα το κάνει αυτόματα όσες φορές χρειάζεται για να μειώσει το jitter και να διατηρήσει συγχρονισμένους τους κόμβους των slaves μεταξύ τους.

Αυτή η ακρίβεια χρονισμού είναι εξαιρετικά σημαντική σε εφαρμογές ελέγχου πραγματικού χρόνου και αυτοματισμού εργοστασίου. Επιτρέπει επιπλέον στα συστήματα DAQ όπως αυτά που διατίθενται από την Dewesoft να ενσωματώνονται τόσο εύκολα σε συστήματα ελέγχου.

Το ενσωματωμένο κατανεμημένο ρολόι της EtherCAT παρέχει εξαιρετική απόδοση "jitter" πολύ μικρότερη από ένα μικροδευτερόλεπτο (1 μs), το οποίο είναι ισοδύναμο με το IEEE 1588 PTP (Precision Time Protocol), χωρίς την ανάγκη επιπλέον υλικού.

Εάν η έξοδος του τελευταίου κόμβου δεν είναι συνδεδεμένη με το master, τα δεδομένα επιστρέφονται αυτόματα προς την άλλη κατεύθυνση μέσω του πρωτοκόλλου EtherCAT. Η χρονική σήμανση διατηρείται.

Αυτή η ανοχή σφαλμάτων σημαίνει ότι τα δίκτυα EtherCAT δεν χρειάζεται να τακτοποιηθούν σε σχήμα δακτυλίου όπως τα παραπάνω σχήματα, αλλά μπορούν να διαμορφωθούν με διάφορους τρόπους, όπως τοπολογία δέντρου, τοπολογία δακτυλίου, τοπολογία γραμμής, τοπολογία αστεριών και ακόμη και συνδυασμοί.



Σχήμα 2. Βασική επικοινωνία master – slave σε Modbus protocol

Φυσικά, πρέπει να υπάρχει μια διαδρομή μεταξύ των slave και του master. Εάν τα αποσυνδέσετε κυριολεκτικά δεν μπορούν να λειτουργήσουν, αλλά το θέμα είναι ότι η τοπολογία του δικτύου είναι πολύ ευέλικτη και ανέχεται αστοχίες σε εξαιρετικό βαθμό.

Διακόπτες, όπως και στα συστήματα ethernet, δεν απαιτούνται από τα συστήματα EtherCAT. Είναι πιθανά μήκη καλωδίου έως 100 μέτρα (328 πόδια) μεταξύ των κόμβων. Το LVDS (διαφορική σηματοδότηση χαμηλής τάσης) στις γραμμές χαλκού συνεστραμμένου ζεύγους λειτουργεί σε υψηλές ταχύτητες και με πολύ χαμηλή κατανάλωση ισχύος. Είναι επίσης δυνατό να χρησιμοποιήσετε καλώδια οπτικών ινών για να αυξήσετε την ταχύτητα και να προσθέσετε γαλβανική απομόνωση μεταξύ συσκευών.

Με λίγες εξαιρέσεις, τα συστήματα που χρησιμοποιούν EtherCAT χωρίζονται σε δύο ομάδες:

- Έλεγχος
- Μέτρηση

Οι συσκευές ελέγχου, όπως PLC, είναι κύριες στο δίκτυο EtherCAT, ενώ οι συσκευές μέτρησης ήταν ιστορικά slave.

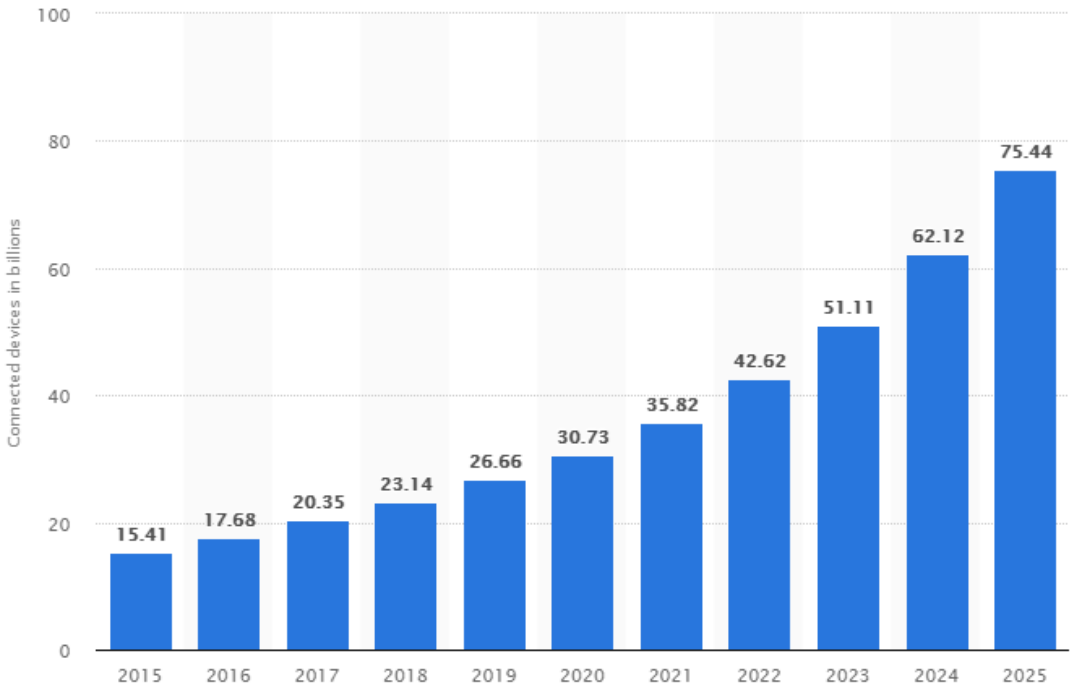
Ωστόσο, ο τρίτος τύπος συσκευής εφευρέθηκε από την Dewesoft: ένα σύστημα DAQ που συνδυάζει την απόκτηση δεδομένων υψηλής ταχύτητας σε έναν κεντρικό υπολογιστή παράλληλα με τα δεδομένα ταχύτητας EtherCAT σε PLC ή λογισμικό / υλικό κύριου ελεγκτή.

Μέχρι πρόσφατα, όταν οι μηχανικοί ήθελαν δεδομένα σε πραγματικό χρόνο από ένα σύστημα DAQ, θα έπαιρναν τις διάφορες αναλογικές εξόδους (ξεχωριστή έξοδο για καθένα από το αναλογικό κανάλι εισόδου) από το σύστημα DAQ και θα τις έφεραν στον ελεγκτή PLC. Αυτό απαιτούσε πολλές αναλογικές εισόδους καθώς και περιττή μετατροπή από αναλογικά σε ψηφιακά δεδομένα.

ΚΕΦΑΛΑΙΟ 3 - ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ

3.1. Εισαγωγή

Το IoT, είναι ουσιαστικά ένα οικοσύστημα φυσικών συσκευών, οχημάτων, συσκευών και άλλων πραγμάτων που έχουν τη δυνατότητα να συνδέουν, να συλλέγουν και να ανταλλάσσουν δεδομένα μέσω ενσύρματου και ασύρματου δικτύου, με λίγο ή καθόλου άνθρωπο σε άνθρωπο ή παρέμβαση από άνθρωπο σε υπολογιστή. Επιτρέποντας την ολοκλήρωση και την ανταλλαγή δεδομένων μεταξύ φυσικών συσκευών και υπολογιστή, αυτό το νέο κύμα τεχνολογίας εστιάζει στο να κάνει την ανθρώπινη ζωή πιο απλοποιημένη και άνετη με το σωστό συνδυασμό αποτελεσματικότητας και παραγωγικότητας (Kozioł, Moya, Yu, Van Phan, & Xu, 2017).

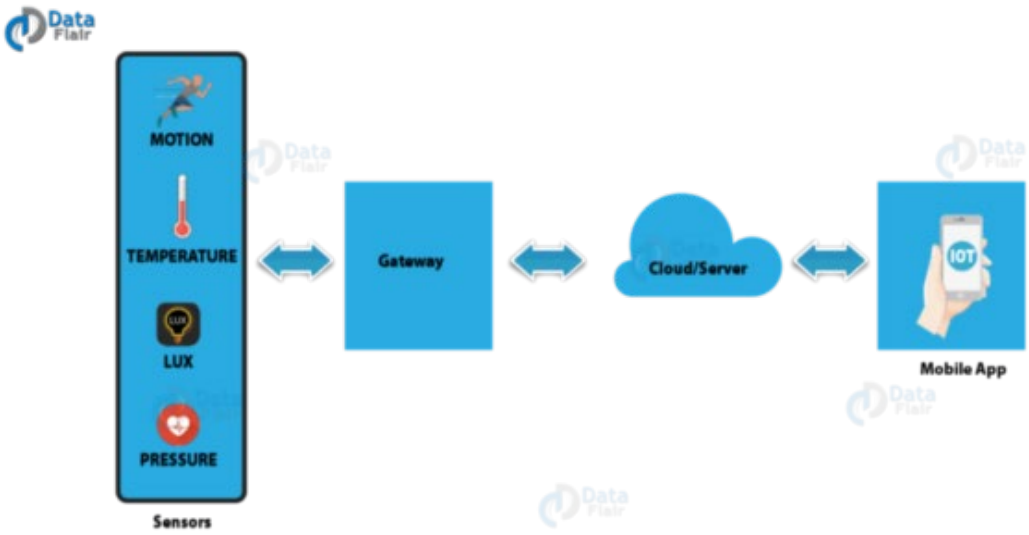


Σχήμα 3. Έρευνα της Statista σχετικά με της συνδεδεμένες στο IoT έξυπνες συσκευές ανά έτος (Hassan, Hu, Lan, Seneviratne, Khalifa, & Das, 2018)

Για να είμαστε πιο συγκεκριμένοι, εκμεταλλευόμενοι τεχνολογίες αιχμής, όπως Μηχανική εκμάθηση, Machine-to-Machine (M2M) Communication and Artificial Intelligence (AI), το IoT στοχεύει στην επέκταση της συνδεσιμότητας πέρα από τις τυπικές υποστηριζόμενες από το Internet φυσικές συσκευές (smartphone, tablet, επιτραπέζιους υπολογιστές, και φορητούς υπολογιστές) σε ένα ευρύ φάσμα φυσικών συσκευών και καθημερινών αντικειμένων που δεν υποστηρίζονται από το Διαδίκτυο, όπως καφετιέρες, πλυντήρια ρούχων, κλειδαριές πόρτας κ.λπ. (Martins, και συν., 2018).

3.2. Πώς λειτουργεί το IoT

Δεδομένου ότι ο μηχανισμός των συσκευών IoT είναι εξαιρετικά τεχνικός, οπότε για πολλούς είναι αρκετά συγκεχυμένο πώς λειτουργεί ένα σύστημα IoT. Λοιπόν, όπως και οποιοδήποτε άλλο σύστημα έχει προκαθορισμένα βήματα και στοιχεία για να το κάνει να λειτουργεί, έτσι το IoT έχει το δικό του. Ένα πλήρες σύστημα IoT αποτελείται από τέσσερα ξεχωριστά συστατικά που συνεργάζονται για να παρέχουν την επιθυμητή έξοδο (Hajny, Dzurenda, & Malina, 2016).



Σχήμα 4. Τρόπος λειτουργίας του IoT (Hakima, 2010)

1. Αισθητήρες / συσκευές

Πρώτα απ' όλα, οι αισθητήρες ή οι συσκευές συλλέγουν πολύ λεπτά δεδομένα από το περιβάλλον. Τα δεδομένα που συλλέχθηκαν θα μπορούσαν να είναι τόσο απλά όσο μια γεωγραφική τοποθεσία ή τόσο περίπλοκη όσο τα βασικά για την υγεία ασθενή.

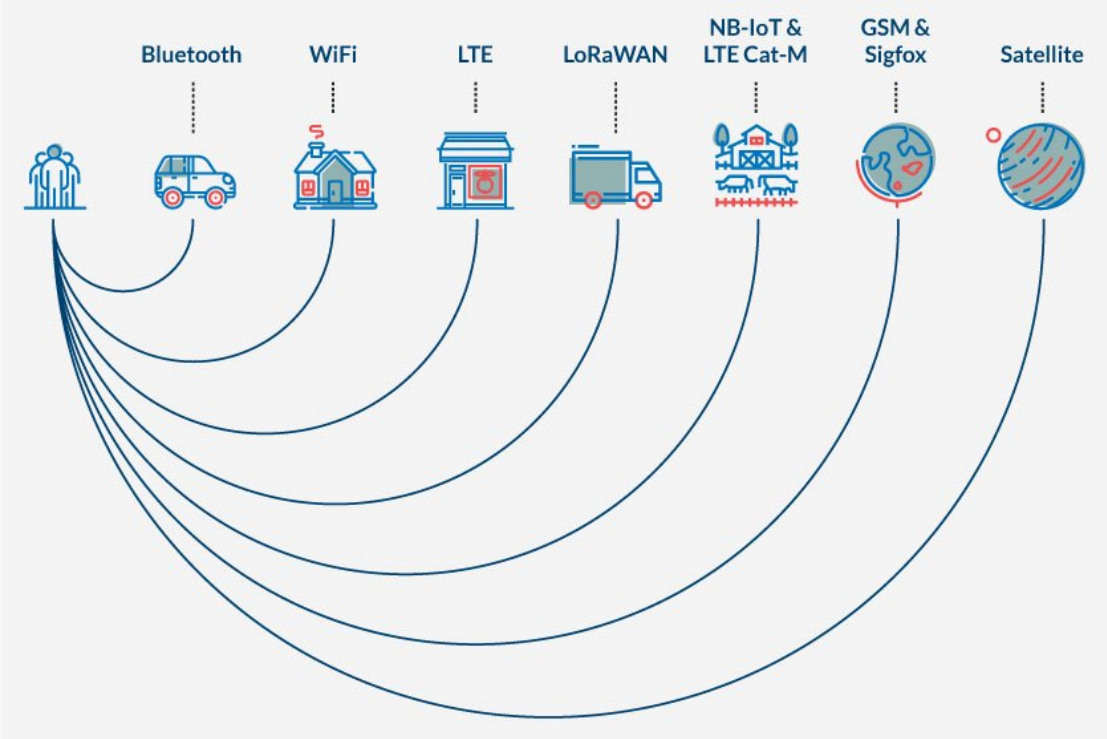
Για να πάρει τις πιο ευαίσθητες αλλαγές στα δεδομένα, μπορεί κανείς να συνδυάσει πολλούς αισθητήρες μαζί για να είναι ένα μέρος μιας συσκευής που είναι ικανή να κάνει κάτι περισσότερο από απλή αίσθηση πραγμάτων. Για παράδειγμα, το κινητό τηλέφωνο είναι μια συσκευή με αρκετούς ενσωματωμένους αισθητήρες όπως GPS, Κάμερα, Επιταχυνσιόμετρο, χωρίς τα οποία το τηλέφωνο δεν μπορεί να ανιχνεύσει πράγματα (Jovanov, 2019).

Σχήμα 5. Διασυνδεδεμένοι αισθητήρες και συσκευές στο IoT (Hajny, Dzurenda, & Malina, 2016)

Έτσι, είτε πρόκειται για αυτόνομο αισθητήρα είτε για συσκευή με πολλαπλούς αισθητήρες, το πρώτο βήμα περιλαμβάνει τη συλλογή όλων των λεπτών λεπτομερειών από το περιβάλλον (Hakima, 2010).

2. Συνδεσιμότητα

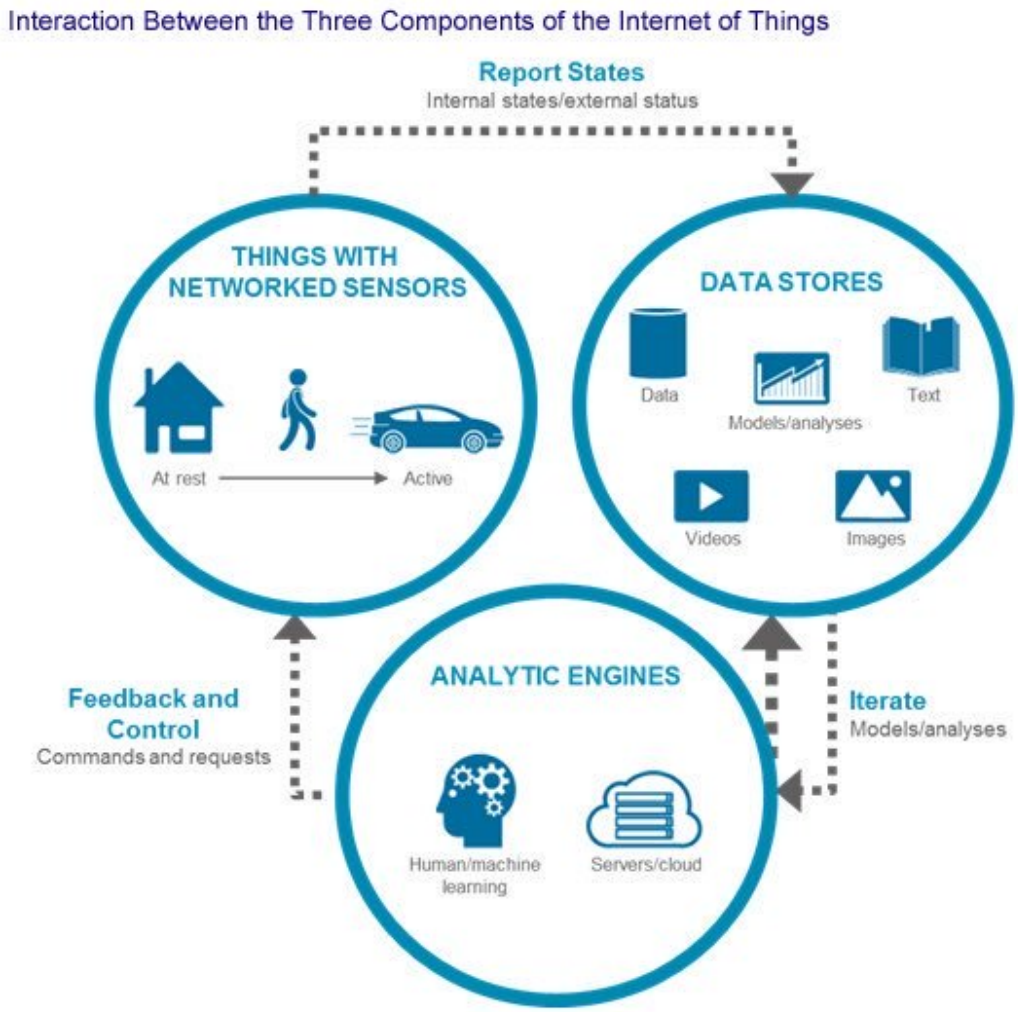
Μόλις συλλεχθούν τα δεδομένα, αποστέλλονται σε μια υποδομή cloud, δηλαδή μια πλατφόρμα IoT, με τη βοήθεια ενός μέσου. Σε αυτό το σημείο λειτουργούν αρκετές τεχνολογίες ασύρματης και ενσύρματης δικτύωσης, όπως Bluetooth, Wi-Fi, Δίκτυα κινητής τηλεφωνίας, LPWAN, Ethernet κ.λπ. Ενώ καθεμία από αυτές τις επιλογές συνδεσιμότητας αντιπροσωπεύει μια αντιστάθμιση μεταξύ της κατανάλωσης ισχύος, του εύρους σύνδεσης και του εύρους ζώνης, η επιλογή της καλύτερης για τη μετάδοση δεδομένων στο cloud εξαρτάται αποκλειστικά από το επίπεδο πολυπλοκότητας και τις συγκεκριμένες απαιτήσεις μιας εφαρμογής IoT (Byrne, O'Sullivan, & Sullivan, 2016).



Σχήμα 6. Συνδεσιμότητα στο IoT (Jovanov, 2019)

3. Επεξεργασία δεδομένων

Μόλις τα δεδομένα φτάσουν στην υποδομή cloud, αποθηκεύονται, αναλύονται και επεξεργάζονται με ασφάλεια χρησιμοποιώντας μια μηχανή Big Data Analytics Engine για καλύτερη λήψη αποφάσεων. Αυτή η ανάλυση μπορεί να είναι τόσο απλή όσο ο έλεγχος εάν η ένδειξη θερμοκρασίας σε ένα AC ή θερμαντήρα βρίσκεται εντός αποδεκτού εύρους ή τόσο περίπλοκη όσο η αναγνώριση των εισβολέων στο σπίτι σας με τη βοήθεια καμερών παρακολούθησης. Τα επεξεργασμένα δεδομένα στη συνέχεια χρησιμοποιούνται για την εκτέλεση άμεσων, έξυπνων ενεργειών που μετατρέπουν τις συνηθισμένες φυσικές μας συσκευές σε εξαιρετικά έξυπνες συσκευές (Sun, Liu, & Zhang, 2017).



Σχήμα 7. Επεξεργασία δεδομένων στο IoT (Kozioł, Moya, Yu, Van Phan, & Xu, 2017)

4. Διεπαφή χρήστη

Το τελευταίο βήμα περιλαμβάνει την ειδοποίηση του τελικού χρήστη σχετικά με τη δράση μέσω email, κειμένου, ειδοποίησης ή ήχου ειδοποίησης που ενεργοποιείται στην εφαρμογή IoT. Ανάλογα με την πολυπλοκότητα του συστήματος IoT, ο χρήστης μπορεί στη συνέχεια είτε να αφήσει ανέπαφη την αυτόματη ενέργεια που εκτελείται, να κάνει προληπτικό έλεγχο στο σύστημα IoT του, είτε να εκτελέσει χειροκίνητα μια ενέργεια για να πυροδοτήσει ή να επηρεάσει το σύστημα. Για παράδειγμα, εάν ο χρήστης εντοπίσει κάποιες αλλαγές σε ένα συγκεκριμένο δωμάτιο, μπορεί να προσαρμόσει από απόσταση τη θερμοκρασία δωματίου μέσω μιας εφαρμογής IoT που είναι εγκατεστημένη στο τηλέφωνό του (Yoo, Song, Cho, & Kim, 2007).

Σχήμα 8. Τύπος διεπαφής χρήστη στο IoT (Zodik, 2015)

3.3. Οφέλη του IoT

Ενώ ο απώτερος στόχος του IoT είναι να αυτοματοποιήσει την ανθρώπινη ζωή ώστε να γίνει πιο παράλογα αποτελεσματική και παραγωγική, υπάρχουν αμέτρητα οφέλη του IoT τόσο για τις επιχειρήσεις όσο και για τους καταναλωτές. Παρακάτω αναφέρονται μερικά μόνο από αυτά:

1. Πρόσβαση σε δεδομένα υψηλής ποιότητας

Όλοι, ειδικά οι έμποροι και οι επιχειρηματίες, αγαπούν τα δεδομένα και με την εφεύρεση συσκευών IoT, οι εταιρείες έχουν πλέον μεγαλύτερη πρόσβαση σε δεδομένα που σχετίζονται με τους πελάτες

και τα προϊόντα τους από ποτέ. Μπορούν να επωφεληθούν από αυτές τις επιχειρησιακές ιδέες σε πραγματικό χρόνο για να παρακολουθούν τη συμπεριφορά των καταναλωτών, να παρέχουν καλύτερες εμπειρίες πελατών και να λαμβάνουν πιο έξυπνες επιχειρηματικές αποφάσεις. Τεχνικά, όσο περισσότερες πληροφορίες έχουμε, τόσο πιο εύκολο είναι να λάβουμε τη σωστή απόφαση (McCann & Bryson, 2009).

2. Καλύτερη παρακολούθηση και διαχείριση

Όποια και αν είναι η βιομηχανία, το IoT κάνει την παρακολούθηση και τη διαχείριση εύκολη για τους οργανισμούς. Από το να παρακολουθούμε το απόθεμα ανά είδος έως την παρακολούθηση της οδικής κυκλοφορίας και των καιρικών συνθηκών έως την ειδοποίηση των ενδιαφερόμενων αρχών για τυχόν ύποπτη συμπεριφορά, το IoT φέρνει επανάσταση στον τρόπο με τον οποίο παρακολουθούμε και διαχειριζόμαστε τα περιουσιακά στοιχεία της επιχείρησής μας. Στην πραγματικότητα, το IoT δεν αφορά μόνο τα έξυπνα σπίτια, αλλά τώρα αφορά επίσης έξυπνα γραφεία, έξυπνη αποθήκη και έξυπνα οτιδήποτε άλλο (Land, Bhattarcharya, Georgiev, Forlivesi, & Kawsar, 2015).

3. Αποτελεσματική χρήση πόρων

Είτε πρόκειται για το σπίτι, το γραφείο, το ξενοδοχείο ή το αυτοκίνητο, το IoT διευκολύνει την αποτελεσματική αξιοποίηση των περιουσιακών στοιχείων για βελτιωμένη παραγωγικότητα. Αξιοποιώντας τη δύναμη της αλληλεπίδρασης μεταξύ μηχανών και μηχανών, ένα σύστημα IoT συλλέγει δεδομένα σε πραγματικό χρόνο με τη βοήθεια αισθητήρων και ενεργοποιητών, ώστε να μπορείτε να τα χρησιμοποιήσετε περαιτέρω για να βελτιώσετε την αποτελεσματικότητα της διαδικασίας και να ελαχιστοποιήσει κανείς την ανθρώπινη παρέμβαση. Ως βασικό παράδειγμα, εάν κάποια από τις οικιακές συσκευές ειδοποιεί για την ολοκλήρωση της εργασίας, δεν χρειάζεται να ανησυχούμε για την αναποτελεσματική κατανάλωση ηλεκτρικής ενέργειας (Wei, 2014).

4. Αυτοματισμός και έλεγχος

Ο αυτοματισμός έχει αποτελέσει σπουδαία ανάγκη και το IoT είναι γνωστό για τον ίδιο λόγο. Δεδομένου ότι οι περισσότερες συσκευές IoT συνδέονται μεταξύ τους μέσω ασύρματης υποδομής, είναι σε θέση να λειτουργούν μόνες τους με μικρή ή καθόλου χειροκίνητη παρέμβαση. Για παράδειγμα, οι οικιακές συσκευές όπως κλιματιστικό, πλυντήρια, φούρνοι και ψυγεία μπορούν να λειτουργούν αυτόματα και μπορούμε ακόμη και να τις παρακολουθούμε και να τις ελέγχουμε από απόσταση (Ometov, και συν., 2016).

5. Άνεση και ευκολία

Ζούμε σε έναν κόσμο με γρήγορο ρυθμό όπου οι πολυάσχολοι άνθρωποι δεν ενδιαφέρονται καν για μικρά πράγματα, όπως η ενεργοποίηση / απενεργοποίηση των φώτων και η ανάγνωση μετρητών ενέργειας, και εδώ έρχεται το IoT. Η διασύνδεση των συσκευών και η συγκέντρωση δεδομένων παρέχει τον πλήρη έλεγχο όλων των συσκευών που είναι συνδεδεμένες μεταξύ τους μέσω του συστήματος IoT. Εφόσον μπορούμε να ελέγχουμε όλες τις συσκευές μας μόνο μέσω μιας κεντρικής συσκευής όπως το τηλέφωνό μας, αυτό οδηγεί σε μεγαλύτερη άνεση (Fernández-Caramés & Fraga-Lamas, 2018).

6. Εξοικονομεί χρόνο και χρήμα

Η ιδέα του IoT περιστρέφεται γύρω από το να γίνουν περισσότερα σε λιγότερο χρόνο, αυτοματοποιώντας εργασίες και απαιτώντας ελάχιστη ή καθόλου ανθρώπινη παρέμβαση. Επιτρέποντάς μας να ολοκληρώσουμε δύσκολες εργασίες γρηγορότερα και με τη βέλτιστη αξιοποίηση της ενέργειας, το IoT όχι μόνο εξοικονομεί πολύτιμο χρόνο, αλλά και χρήμα. Για παράδειγμα, εάν η ηλεκτρονική συσκευή της κουζίνας έχει τη δυνατότητα να απενεργοποιηθεί μετά την ολοκλήρωση της εργασίας, αυτό εξοικονομεί χρόνο και προσπάθειες που απαιτούνται για τη μη αυτόματη απενεργοποίηση της συσκευής, καθώς και επιπλέον δαπάνες που προκαλούνται από την περιττή χρήση ηλεκτρικής ενέργειας (Jovanov, 2019).

3.4. Βασικά συστατικά ενός συστήματος IoT

Hardware

Η καρδιά του IoT είναι δισεκατομμύρια διασυνδεδεμένων συσκευών, γενικά, αισθητήρων και ενεργοποιητών, που επιτρέπει σε κάποιον να αισθανθεί (και μερικές φορές να ελέγχει) τον φυσικό κόσμο γύρω τους. Εκτός από την απαίτηση συνδεσιμότητας δικτύου για τη μετάδοση των δεδομένων που συλλέγουν, αυτές οι συσκευές χρειάζονται επίσης ορισμένες βασικές δυνατότητες επεξεργασίας και αποθήκευσης, οι οποίες παρέχονται συχνά από έναν μικροελεγκτή, ένα σύστημα on-a-chip (SoC) ή μια Gateway προγραμματιζόμενη από το πεδίο πίνακας (FPGA) (Liu & Sun, 2016).

Ενσωματωμένος προγραμματισμός

Οι συσκευές IoT είναι "ενσωματωμένες" συσκευές. Μπορεί να έχουν κατασκευαστεί πρωτότυπα ώστε να χρησιμοποιούν πλατφόρμες μικροελεγκτών, όπως το Arduino, με προσαρμοσμένες πλακέτες κυκλωμάτων (PCB) που αναπτύχθηκαν σε μεταγενέστερο στάδιο. Το πρωτότυπο με αυτές τις πλατφόρμες απαιτεί δεξιότητες σχεδιασμού κυκλώματος, προγραμματισμό μικροελεγκτή και βαθιά κατανόηση των πρωτοκόλλων επικοινωνίας υλικού όπως σειριακό, I2C ή SPI που χρησιμοποιούνται για τη δημιουργία επικοινωνίας μεταξύ του μικροελεγκτή και των συνδεδεμένων αισθητήρων και ενεργοποιητών. Τα ενσωματωμένα προγράμματα αναπτύσσονται συχνά χρησιμοποιώντας C ++ ή C. Ωστόσο, το Python και το JavaScript (για UI και πλατφόρμες) γίνονται πιο δημοφιλή για τον σχεδιασμό συστημάτων IoT (Hajny, Dzurenda, & Malina, 2016).

Ασφάλεια

Η ασφάλεια είναι μια από τις πιο κρίσιμες ανησυχίες στο IoT, που σχετίζεται στενά με την ηθική των δεδομένων, το απόρρητο και την ευθύνη. Πρέπει να είναι ενσωματωμένο σε κάθε βήμα του σχεδιασμού του συστήματος. Με εκατομμύρια νέες συσκευές συνδεδεμένες κάθε μέρα, ο αριθμός των πιθανών (και πραγματικών) φορέων επίθεσης αυξάνεται καθημερινά. Με πολλά διακυβευόμενα, οι δεξιότητες μηχανικής ασφαλείας, συμπεριλαμβανομένης της αξιολόγησης απειλών, της ηθικής εισβολής, της κρυπτογράφησης, της διασφάλισης αρχιτεκτονικών και εφαρμογών δικτύου, παρακολούθησης συμβάντων, καταγραφής δραστηριοτήτων και πληροφοριών για απειλές καθίστανται κρίσιμες για την αποστολή (Kozioł, Moya, Yu, Van Phan, & Xu, 2017).

Δικτύωση και Ενσωμάτωση στο Cloud

Ο σχεδιασμός και η διαχείριση του δικτύου είναι ουσιαστικής σημασίας στο IoT, λόγω του τεράστιου όγκου των συνδεδεμένων συσκευών και λόγω του αντίκτυπου που μπορούν να έχουν οι αποφάσεις σχεδιασμού δικτύου σε αναπτυγμένα συστήματα IoT σε κλίμακα.

Η συνδεσιμότητα επιτρέπει στις συσκευές να επικοινωνούν με άλλες συσκευές, καθώς και με εφαρμογές και υπηρεσίες που εκτελούνται στο cloud. Παρόλο που το cloud computing και το IoT είναι δύο πολύ διαφορετικές τεχνολογίες, η ροή δεδομένων σε πραγματικό χρόνο και η ενσωμάτωση cloud είναι καθοριστικής σημασίας για την ορθή λειτουργία του IoT. Η υποδομή Cloud χρησιμοποιείται για αποθήκευση δεδομένων, επεξεργασία και ανάλυση, καθώς και για την εφαρμογή της επιχειρηματικής λογικής σε εφαρμογές IoT (Thierer, 2015).

Ανάλυση δεδομένων και πρόβλεψη

Ο αριθμός των συσκευών IoT που μεταδίδουν δεδομένα αυξάνεται καθημερινά, γεγονός που μετατρέπει τα μεγάλα δεδομένα σε τεράστια δεδομένα. Οι προγραμματιστές θα πρέπει να απορροφήσουν, να αποθηκεύσουν και να ζητήσουν με ασφάλεια και αξιοπιστία τις τεράστιες ποσότητες ετερογενών δεδομένων που προέρχονται από αυτές τις συσκευές. Πολλές συσκευές IoT δημιουργούν δεδομένα ευαίσθητα σε καθυστέρηση ή χρόνο, επομένως είναι επίσης χρήσιμο να φιλτράρουμε ή να απορρίψουμε άσχετα δεδομένα του δικτύου κάποιου αντί να στέλνουμε τα πάντα στους διακομιστές (Hassan, Hu, Lan, Seneviratne, Khalifa, & Das, 2018).

AI και μηχανική εκμάθηση

Για να αποδώσουμε αξία και να κατανοήσουμε τον τεράστιο όγκο δεδομένων που δημιουργούνται από συσκευές IoT, η μηχανική εκμάθηση και το AI είναι χρήσιμα εργαλεία σε ένα σύστημα IoT. Αυτές οι τεχνικές, με τις οποίες κάποιος διδάσκει μια μηχανή να μάθει εκθέτοντάς την σε τόνους

δεδομένων σχετικά με μια κατάσταση, μπορούν να εφαρμοστούν σε πραγματικό χρόνο, τόσο για τη ροή δεδομένων αισθητήρα για προγνωστική ανάλυση όσο και για τη λήψη αποφάσεων αυτόνομα σε απάντηση στα εισερχόμενα δεδομένα. Η μηχανική εκμάθηση μπορεί επίσης να εφαρμοστεί σε ιστορικά δεδομένα για τον εντοπισμό προτύπων ή ανωμαλιών στα δεδομένα που μπορεί να επιτρέπουν σε όλους να λαμβάνουν σημαντικές αποφάσεις (Di Serio, και συν., 2018).

3.5. Τα πρότυπα και τα πλαίσια IoT

Υπάρχουν διάφορα αναδυόμενα πρότυπα IoT, όπως τα εξής (Anderson & Rainie, 2014):

- Το IPv6 μέσω ασύρματων δικτύων προσωπικής περιοχής χαμηλής κατανάλωσης (6LoWPAN) είναι ένα ανοικτό πρότυπο που καθορίζεται από τη Δύναμη Μηχανικής Διαδικτύου (IETF). Το πρότυπο 6LoWPAN επιτρέπει σε οποιοδήποτε ραδιοφωνικό σταθμό χαμηλής κατανάλωσης να επικοινωνεί με το Διαδίκτυο, συμπεριλαμβανομένων των 804.15.4, Bluetooth Low Energy (BLE) και Z-Wave (για οικιακή αυτοματοποίηση).
- Το ZigBee είναι ένα ασύρματο δίκτυο χαμηλής κατανάλωσης δεδομένων χαμηλής ταχύτητας που χρησιμοποιείται κυρίως σε βιομηχανικές εγκαταστάσεις. Το ZigBee βασίζεται στο πρότυπο 802.15.4 του Ινστιτούτου Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών (IEEE). Η ZigBee Alliance δημιούργησε το Dotdot, την παγκόσμια γλώσσα για το IoT, που επιτρέπει σε έξυπνα αντικείμενα να λειτουργούν με ασφάλεια σε οποιοδήποτε δίκτυο και να κατανοούν ο ένας τον άλλον.
- Το LiteOS είναι ένα λειτουργικό σύστημα (OS) παρόμοιο με Unix για ασύρματα δίκτυα αισθητήρων. Το LiteOS υποστηρίζει smartphones, φορητά, έξυπνες εφαρμογές κατασκευής, έξυπνα σπίτια και το διαδίκτυο των οχημάτων (IoV). Το λειτουργικό σύστημα λειτουργεί επίσης ως έξυπνη πλατφόρμα ανάπτυξης συσκευών.
- Το OneM2M είναι ένα στρώμα υπηρεσιών Machine-to-Machine το οποίο μπορεί να ενσωματωθεί σε λογισμικό και υλικό για τη σύνδεση συσκευών. Ο παγκόσμιος οργανισμός τυποποίησης, OneM2M, δημιουργήθηκε για την ανάπτυξη επαναχρησιμοποιήσιμων προτύπων που επιτρέπουν την επικοινωνία μεταξύ εφαρμογών IoT σε διαφορετικές κατακόρυφες περιοχές.
- Η Υπηρεσία Διανομής Δεδομένων (DDS) αναπτύχθηκε από την ομάδα διαχείρισης αντικειμένων (OMG) και είναι ένα πρότυπο IoT για επικοινωνία M2M σε πραγματικό χρόνο, κλιμακούμενη και υψηλής απόδοσης.
- Το Advanced Message Queuing Protocol (AMQP) είναι ένα δημοσιευμένο πρότυπο ανοιχτού κώδικα για ασύγχρονα μηνύματα μέσω καλωδίου. Το AMQP επιτρέπει κρυπτογραφημένα και διαλειτουργικά μηνύματα μεταξύ οργανισμών και εφαρμογών. Το πρωτόκολλο χρησιμοποιείται σε μηνύματα πελάτη-διακομιστή και στη διαχείριση συσκευών IoT.
- Το Πρωτόκολλο Περιορισμένης Εφαρμογής (CoAP) είναι ένα πρωτόκολλο που σχεδιάστηκε από το IETF που καθορίζει τον τρόπο με τον οποίο μπορούν να λειτουργήσουν συσκευές χαμηλής κατανάλωσης, περιορισμένης χρήσης υπολογιστών στο IoT.
- Το ευρύ δίκτυο ευρείας περιοχής (LoRaWAN) είναι ένα πρωτόκολλο για δίκτυα WAN που έχουν σχεδιαστεί για να υποστηρίζουν τεράστια δίκτυα, όπως έξυπνες πόλεις, με εκατομμύρια συσκευές χαμηλής κατανάλωσης.

Τα πλαίσια του Διαδικτύου περιλαμβάνουν τα ακόλουθα (Stallings, 2007):

- Amazon Web Services (AWS) Το IoT είναι μια πλατφόρμα υπολογιστικού cloud για το IoT που κυκλοφορεί από την Amazon. Αυτό το πλαίσιο έχει σχεδιαστεί για να επιτρέπει στις έξυπνες συσκευές να συνδέονται εύκολα και να αλληλοεπιδρούν με ασφάλεια με το cloud AWS και άλλες συνδεδεμένες συσκευές.
- Το Arm Mbed IoT είναι μια πλατφόρμα για την ανάπτυξη εφαρμογών για IoT με βάση τους μικροελεγκτές βραχίονα. Ο στόχος της πλατφόρμας Arm Mbed IoT είναι να παρέχει ένα

κλιμακωτό, συνδεδεμένο και ασφαλές περιβάλλον για συσκευές IoT ενσωματώνοντας εργαλεία και υπηρεσίες Mbed.

- Η Azure IoT Suite της Microsoft είναι μια πλατφόρμα που αποτελείται από ένα σύνολο υπηρεσιών που επιτρέπει στους χρήστες να αλληλοεπιδρούν και να λαμβάνουν δεδομένα από τις συσκευές IoT τους, καθώς και να εκτελούν διάφορες λειτουργίες πάνω σε δεδομένα όπως πολυδιάστατη ανάλυση, μετασχηματισμό και συνάθροιση και να απεικονίζουν αυτές τις λειτουργίες με έναν τρόπο που είναι κατάλληλος για τις επιχειρήσεις.
- Το Brillo / Weave της Google είναι μια πλατφόρμα για την ταχεία εφαρμογή εφαρμογών IoT. Η πλατφόρμα αποτελείται από δύο κύρια συστήματα: το Brillo, ένα λειτουργικό σύστημα Android για την ανάπτυξη ενσωματωμένων συσκευών χαμηλής κατανάλωσης και το Weave, ένα πρωτόκολλο επικοινωνίας με γνώμονα το IoT που χρησιμεύει ως γλώσσα επικοινωνίας μεταξύ της συσκευής και του cloud.
- Η Calvin είναι μια πλατφόρμα IoT ανοιχτής πηγής που εκδίδεται από την Ericsson και έχει σχεδιαστεί για τη δημιουργία και τη διαχείριση κατανεμημένων εφαρμογών που επιτρέπουν στις συσκευές να μιλούν μεταξύ τους. Η Calvin περιλαμβάνει ένα πλαίσιο ανάπτυξης για προγραμματιστές εφαρμογών, καθώς και ένα περιβάλλον χρόνου εκτέλεσης για το χειρισμό της τρέχουσας εφαρμογής.

3.6. Εφαρμογές Διασύνδεσης καταναλωτών και επιχειρήσεων

Υπάρχουν πολυάριθμες πραγματικές εφαρμογές του IoT, που κυμαίνονται από τον καταναλωτή IoT και την επιχείρηση IoT έως τη βιομηχανική και βιομηχανική χρήση του Διαδικτύου (IoT). Οι εφαρμογές του Διαδικτύου καλύπτουν πολλές κατακόρυφες καταστάσεις, όπως η αυτοκινητοβιομηχανία, οι τηλεπικοινωνίες και η ενέργεια.

Στον τομέα των καταναλωτών, για παράδειγμα, τα έξυπνα σπίτια που είναι εξοπλισμένα με έξυπνους θερμοστάτες, έξυπνες συσκευές και συνδεδεμένα συστήματα θέρμανσης, φωτισμού και ηλεκτρονικών συσκευών μπορούν να ελέγχονται εξ αποστάσεως μέσω υπολογιστών και smartphones (Tao, 2001).

Τα wearables με αισθητήρες και λογισμικό μπορούν να συλλέγουν και να αναλύουν τα δεδομένα των χρηστών, αποστέλλοντας μηνύματα σε άλλες τεχνολογίες σχετικά με τους χρήστες, με σκοπό να διευκολύνουν τη ζωή των χρηστών. Τα wearables χρησιμοποιούνται επίσης για δημόσια ασφάλεια - για παράδειγμα, βελτιώνοντας τους χρόνους απόκρισης των πρώτων ανταποκριτών σε καταστάσεις έκτακτης ανάγκης, παρέχοντας βελτιστοποιημένες διαδρομές σε μια τοποθεσία ή παρακολουθώντας τα ζωτικά σήματα των εργατών ή των πυροσβεστών σε χώρους που απειλούν τη ζωή (Mann, 1998).

Στην υγειονομική περίθαλψη, το IoT προσφέρει πολλά οφέλη, συμπεριλαμβανομένης της ικανότητας για πιο στενή παρακολούθηση των ασθενών χρησιμοποιώντας μια ανάλυση των δεδομένων που παράγονται. Τα νοσοκομεία συχνά χρησιμοποιούν συστήματα IoT για να ολοκληρώσουν καθήκοντα όπως διαχείριση αποθεμάτων τόσο για φαρμακευτικά όσο και για ιατρικά εργαλεία.

Η θερμοκρασία μπορεί να ρυθμιστεί αυτόματα - για παράδειγμα, ενεργοποιώντας το κλιματιστικό αν οι αισθητήρες ανιχνεύσουν μια αίθουσα συνεδριάσεων γεμάτη ή στρέφοντας τη θερμότητα εάν όλοι στο γραφείο έχουν πάει στο σπίτι (Anderson & Rainie, 2014).

Στη γεωργία, τα έξυπνα συστήματα καλλιέργειας που βασίζονται στο IoT μπορούν να συμβάλλουν στην παρακολούθηση, για παράδειγμα, του φωτός, της θερμοκρασίας, της υγρασίας και της υγρασίας του εδάφους των καλλιεργήσιμων περιοχών χρησιμοποιώντας συνδεδεμένους αισθητήρες. Το IoT είναι επίσης σημαντικό εργαλείο για την αυτοματοποίηση των συστημάτων άρδευσης.

Σε μια έξυπνη πόλη, οι αισθητήρες και οι εφαρμογές του IoT, όπως τα έξυπνα φώτα του δρόμου και οι έξυπνοι μετρητές, μπορούν να βοηθήσουν στην ελάφρυνση της κυκλοφορίας, στη διατήρηση της ενέργειας, στην παρακολούθηση και αντιμετώπιση περιβαλλοντικών προβλημάτων και στη βελτίωση της υγιεινής (Svanberg & Evans, 2014).

3.7. Ασφάλεια και προστασία της ιδιωτικής ζωής στο IoT

Το 2016, μία από τις πιο διαβόητες πρόσφατες επιθέσεις στο IoT αφορούσε το Mirai, ένα botnet που διείσδυσε στον πάροχο υπηρεσιών domain name Dyn, και οδήγησε πολλές ιστοσελίδες για μεγάλο χρονικό διάστημα σε μια από τις μεγαλύτερες κατανεμημένες επιθέσεις άρνησης υπηρεσίας (DDoS). Οι επιτιθέμενοι απέκτησαν πρόσβαση στο δίκτυο χρησιμοποιώντας συσκευές που δεν τηρούσαν τα πρωτόκολλα ασφαλείας (Yoo, Song, Cho, & Kim, 2007).

Επειδή οι συσκευές IoT είναι στενά συνδεδεμένες, το μόνο που ο χάκερ πρέπει να κάνει είναι να εκμεταλλευτεί ένα τρωτό σημείο για να χειριστεί όλα τα δεδομένα, καθιστώντας το ακατάλληλο (Svanberg & Evans, 2014).

Οι χάκερ δεν είναι η μόνη απειλή για το IoT. το ιδιωτικό απόρρητο αποτελεί άλλη σημαντική μέριμνα για τους χρήστες του Διαδικτύου.

Πέρα από τη διαρροή προσωπικών δεδομένων, το IoT θέτει σε κίνδυνο την υποδομή ζωτικής σημασίας, συμπεριλαμβανομένης της ηλεκτρικής ενέργειας, των μεταφορών και των χρηματοπιστωτικών υπηρεσιών (Svanberg & Evans, 2014).

3.8. Ιστορία του IoT

Ο Kevin Ashton, συνιδρυτής του Κέντρου Auto-ID στο Ινστιτούτο Τεχνολογίας της Μασαχουσέτης (MIT), ανέφερε για πρώτη φορά το IoT σε μια παρουσίαση που έκανε στην Procter & Gamble (P & G) το 1999. Το βιβλίο του καθηγητή του MIT Neil Gershenfeld, «Όταν τα πράγματα αρχίζουν να σκέφτονται» - “When things start thinking”, εμφανίστηκε επίσης το 1999. Δεν χρησιμοποίησε τον ακριβή όρο, αλλά παρείχε ένα σαφές όραμα για την κατεύθυνση του IoT (Stallings, 2007). Η σύγκλιση συνέβαλε στη διάσπαση των ορίων μεταξύ επιχειρησιακής τεχνολογίας (OT) και τεχνολογίας της πληροφορίας (IT), επιτρέποντας την ανάλυση μη δομημένων δεδομένων που δημιουργήθηκαν από μηχανές για γνώση. Παρόλο που ο Ashton έκανε την πρώτη αναφορά στο IoT, η ιδέα των συνδεδεμένων συσκευών υπήρξε διαθέσιμη από τη δεκαετία του '70, με τα ενσωματωμένα διαδικτυακά συστήματα monikers και την διάχυτη πληροφορική (Yoo, Song, Cho, & Kim, 2007).

Η πρώτη συσκευή στο διαδίκτυο, για παράδειγμα, ήταν μια μηχανή οπτάνθρακα στο πανεπιστήμιο Carnegie Mellon στις αρχές της δεκαετίας του 1980. Χρησιμοποιώντας το διαδίκτυο, οι προγραμματιστές μπορούσαν να ελέγξουν την κατάσταση του μηχανήματος. Το IoT εξελίχθηκε από την επικοινωνία Machine-to-Machine (M2M), δηλαδή τις μηχανές που συνδέονται μεταξύ τους μέσω ενός δικτύου χωρίς ανθρώπινη αλληλεπίδραση. Το M2M αναφέρεται στη σύνδεση μιας συσκευής με το cloud, τη διαχείριση και τη συλλογή δεδομένων.

Πηγαίνοντας το M2M στο επόμενο επίπεδο, το IoT είναι ένα δίκτυο αισθητήρων με δισεκατομμύρια έξυπνες συσκευές που συνδέουν άτομα, συστήματα και άλλες εφαρμογές για τη συλλογή και την ανταλλαγή δεδομένων. Αποτελώντας την βάση του συστήματος, το M2M προσφέρει τη συνδεσιμότητα που επιτρέπει την ύπαρξη του IoT (Tao, 2001).

Το IoT είναι επίσης μια φυσική επέκταση του ελέγχου εποπτείας και απόκτησης δεδομένων (SCADA), μιας κατηγορίας προγραμμάτων εφαρμογών λογισμικού για τον έλεγχο της διαδικασίας, τη συλλογή δεδομένων σε πραγματικό χρόνο από απομακρυσμένες τοποθεσίες καθώς και τον έλεγχο του εξοπλισμού και των συνθηκών. Τα συστήματα SCADA περιλαμβάνουν εξαρτήματα υλικού και λογισμικού. Η εξέλιξη του SCADA είναι τέτοια, ώστε τα συστήματα τελευταίας γενιάς να έχουν αναπτυχθεί σε συστήματα IoT πρώτης γενιάς (Hakima, 2010).

ΚΕΦΑΛΑΙΟ 4 – ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ (CYBERSECURITY)

4.1. Τι είναι η κυβερνοασφάλεια

Η κυβερνοασφάλεια είναι η πρακτική της προστασίας κρίσιμων συστημάτων και ευαίσθητων πληροφοριών από ψηφιακές επιθέσεις. Γνωστά και ως ασφάλεια τεχνολογίας πληροφοριών (IT), τα μέτρα κυβερνοασφάλειας έχουν σχεδιαστεί για την καταπολέμηση απειλών κατά δικτυωμένων συστημάτων και εφαρμογών, είτε αυτές οι απειλές προέρχονται από το εσωτερικό είτε από το εξωτερικό ενός οργανισμού.

Το 2020, το μέσο κόστος μιας παραβίασης δεδομένων ήταν 3,86 εκατομμύρια USD παγκοσμίως και 8,64 εκατομμύρια USD στις Ηνωμένες Πολιτείες. Αυτά τα κόστη περιλαμβάνουν τα έξοδα ανακάλυψης και αντιμετώπισης της παραβίασης, το κόστος διακοπής λειτουργίας και τα χαμένα έσοδα και τη μακροπρόθεσμη ζημιά στη φήμη μιας επιχείρησης και της επωνυμίας της. Οι εγκληματίες του κυβερνοχώρου στοχεύουν προσωπικά αναγνωρίσιμα στοιχεία πελατών (PII) - ονόματα, διευθύνσεις, εθνικούς αριθμούς αναγνώρισης (π.χ. αριθμούς κοινωνικής ασφάλισης στις ΗΠΑ, φορολογικοί κωδικοί στην Ιταλία), πληροφορίες πιστωτικών καρτών - και στη συνέχεια πωλούν αυτά τα αρχεία σε υπόγειες ψηφιακές αγορές. Τα διακυβευμένα PII συχνά οδηγούν σε απώλεια της εμπιστοσύνης των πελατών, ρυθμιστικά πρόστιμα και ακόμη και νομικές ενέργειες.

Η πολυπλοκότητα του συστήματος ασφαλείας, που δημιουργείται από διαφορετικές τεχνολογίες και την έλλειψη εσωτερικής τεχνογνωσίας, μπορεί να αυξήσει αυτό το κόστος. Ωστόσο, οι οργανισμοί με μια ολοκληρωμένη στρατηγική κυβερνοασφάλειας, που διέπεται από βέλτιστες πρακτικές και αυτοματοποιούνται χρησιμοποιώντας προηγμένα αναλυτικά στοιχεία, τεχνητή νοημοσύνη (AI) και μηχανική μάθηση, μπορούν να καταπολεμήσουν τις απειλές στον κυβερνοχώρο πιο αποτελεσματικά και να μειώσουν τον κύκλο ζωής και τον αντίκτυπο των παραβιάσεων όταν συμβαίνουν.

4.2. Τομείς κυβερνοασφάλειας

Μια ισχυρή στρατηγική κυβερνοασφάλειας διαθέτει επίπεδα προστασίας για την άμυνα έναντι του εγκλήματος στον κυβερνοχώρο, συμπεριλαμβανομένων των επιθέσεων στον κυβερνοχώρο που επιχειρούν να αποκτήσουν πρόσβαση, να αλλάξουν ή να καταστρέψουν δεδομένα, εκβιάζουν χρήματα από χρήστες ή τον οργανισμό ή στοχεύουν στη διακοπή της κανονικής επιχειρηματικής λειτουργίας. Τα αντίμετρα πρέπει να αφορούν:

Ασφάλεια υποδομής ζωτικής σημασίας - πρακτικές για την προστασία των συστημάτων υπολογιστών, των δικτύων και άλλων περιουσιακών στοιχείων στα οποία βασίζεται η κοινωνία για την εθνική ασφάλεια, την οικονομική υγεία ή/και τη δημόσια ασφάλεια. Το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) έχει δημιουργήσει ένα πλαίσιο κυβερνοασφάλειας για να βοηθήσει οργανισμούς σε αυτόν τον τομέα, ενώ το Υπουργείο Εσωτερικής Ασφάλειας των ΗΠΑ (DHS) παρέχει πρόσθετη καθοδήγηση.

Ασφάλεια δικτύου - μέτρα ασφαλείας για την προστασία ενός δικτύου υπολογιστών από εισβολείς, συμπεριλαμβανομένων τόσο των ενσύρματων όσο και των ασύρματων (Wi-Fi) συνδέσεων.

Ασφάλεια εφαρμογών - διαδικασίες που βοηθούν στην προστασία των εφαρμογών που λειτουργούν εντός των εγκαταστάσεων και στο cloud. Η ασφάλεια θα πρέπει να ενσωματώνεται στις εφαρμογές στο στάδιο του σχεδιασμού, λαμβάνοντας υπόψη τον τρόπο χειρισμού των δεδομένων, τον έλεγχο ταυτότητας χρήστη κ.λπ.

Ασφάλεια στο cloud - συγκεκριμένα, αληθινός εμπιστευτικός υπολογισμός που κρυπτογραφεί δεδομένα cloud σε κατάσταση ηρεμίας (στην αποθήκευση), σε κίνηση (καθώς ταξιδεύουν προς, από και μέσα στο cloud) και σε χρήση (κατά την επεξεργασία) για την υποστήριξη του απορρήτου των πελατών, των επιχειρηματικών απαιτήσεων και της κανονιστικής συμμόρφωσης πρότυπα.

Ασφάλεια πληροφοριών - μέτρα προστασίας δεδομένων, όπως ο Γενικός Κανονισμός Προστασίας Δεδομένων ή ο GDPR, που προστατεύουν τα πιο ευαίσθητα δεδομένα σας από μη εξουσιοδοτημένη πρόσβαση, έκθεση ή κλοπή.

Εκπαίδευση τελικού χρήστη - δημιουργία ευαισθητοποίησης για την ασφάλεια σε ολόκληρο τον οργανισμό για την ενίσχυση της ασφάλειας τελικού σημείου. Για παράδειγμα, οι χρήστες μπορούν να εκπαιδευτούν να διαγράφουν ύποπτα συνημμένα email, να αποφεύγουν τη χρήση άγνωστων συσκευών USB κ.λπ.

Ανάκτηση καταστροφών / σχεδιασμός επιχειρηματικής συνέχειας - εργαλεία και διαδικασίες για την αντιμετώπιση απρογραμμάτιστων συμβάντων, όπως φυσικές καταστροφές, διακοπές ρεύματος ή περιστατικά ασφάλειας στον κυβερνοχώρο, με ελάχιστη διακοπή σε βασικές λειτουργίες.

Ασφάλεια αποθήκευσης - Το IBM FlashSystem® προσφέρει σταθερή ανθεκτικότητα δεδομένων με πολλές διασφαλίσεις. Αυτό περιλαμβάνει κρυπτογράφηση και αμετάβλητα και μεμονωμένα αντίγραφα δεδομένων. Αυτά παραμένουν στην ίδια δεξαμενή, ώστε να μπορούν γρήγορα να αποκατασταθούν για να υποστηρίξουν την ανάκτηση, ελαχιστοποιώντας τον αντίκτυπο μιας επίθεσης στον κυβερνοχώρο.

4.3. Επικίνδυνοι μύθοι για την ασφάλεια στον κυβερνοχώρο

Ο όγκος των περιστατικών κυβερνοασφάλειας αυξάνεται σε ολόκληρο τον κόσμο, αλλά εξακολουθούν να υπάρχουν παρανοήσεις, συμπεριλαμβανομένης της ιδέας ότι:

Οι κυβερνοεγκληματίες είναι ξένοι. Στην πραγματικότητα, οι παραβιάσεις της κυβερνοασφάλειας είναι συχνά αποτέλεσμα κακόβουλων εμπιστευτικών πληροφοριών, που εργάζονται για τον εαυτό τους ή σε συνεννόηση με εξωτερικούς χάκερ. Αυτοί οι μυημένοι μπορούν να είναι μέρος καλά οργανωμένων ομάδων, που υποστηρίζονται από έθνη-κράτη.

Οι κίνδυνοι είναι γνωστοί. Στην πραγματικότητα, η επιφάνεια κινδύνου εξακολουθεί να επεκτείνεται, με χιλιάδες νέα τρωτά σημεία να αναφέρονται σε παλιές και νέες εφαρμογές και συσκευές. Και οι ευκαιρίες για ανθρώπινο λάθος - ειδικά από αμελείς υπαλλήλους ή εργολάβους που προκαλούν ακούσια παραβίαση δεδομένων - συνεχίζουν να αυξάνονται.

Οι φορείς επίθεσης περιέχονται. Οι εγκληματίες του κυβερνοχώρου βρίσκουν συνεχώς νέους φορείς επιθέσεων - συμπεριλαμβανομένων συστημάτων Linux, λειτουργικής τεχνολογίας (OT), συσκευών Internet of Things (IoT) και περιβαλλόντων cloud.

Ο κλάδος μου είναι ασφαλής. Κάθε κλάδος έχει το μερίδιό του σε κινδύνους για την ασφάλεια στον κυβερνοχώρο, με τους αντιπάλους του κυβερνοχώρου να εκμεταλλεύονται τις ανάγκες των δικτύων επικοινωνίας σε σχεδόν κάθε κρατικό και ιδιωτικό οργανισμό. Για παράδειγμα, οι επιθέσεις ransomware (βλ. παρακάτω) στοχεύουν περισσότερους τομείς από ποτέ, συμπεριλαμβανομένων τοπικών κυβερνήσεων και μη κερδοσκοπικών οργανισμών, ενώ έχουν επίσης αυξηθεί οι απειλές σε αλυσίδες εφοδιασμού, ιστότοπους ".gov" και κρίσιμες υποδομές.

4.4. Συνήθεις απειλές στον κυβερνοχώρο

Αν και οι επαγγελματίες της κυβερνοασφάλειας εργάζονται σκληρά για να καλύψουν τα κενά ασφαλείας, οι επιτιθέμενοι αναζητούν πάντα νέους τρόπους για να ξεφύγουν από την προσοχή του IT, να αποφύγουν τα αμυντικά μέτρα και να εκμεταλλευτούν τις αναδυόμενες αδυναμίες. Οι πιο πρόσφατες απειλές για την ασφάλεια στον κυβερνοχώρο δίνουν μια νέα στροφή στις «γνωστές» απειλές, αξιοποιώντας περιβάλλοντα εργασίας από το σπίτι, εργαλεία απομακρυσμένης πρόσβασης και νέες υπηρεσίες cloud. Αυτές οι εξελισσόμενες απειλές περιλαμβάνουν:

Κακόβουλο λογισμικό

Ο όρος "κακόβουλο λογισμικό" αναφέρεται σε παραλλαγές κακόβουλου λογισμικού—όπως ιούς τύπου worm, ιούς, Trojans και λογισμικό υποκλοπής spyware—που παρέχουν μη εξουσιοδοτημένη πρόσβαση ή προκαλούν ζημιά σε έναν υπολογιστή. Οι επιθέσεις κακόβουλου λογισμικού είναι όλο και πιο «χωρίς αρχεία» και έχουν σχεδιαστεί για να παρακάμπτουν γνωστές μεθόδους ανίχνευσης, όπως εργαλεία προστασίας από ιούς, που σαρώνουν για κακόβουλα συνημμένα αρχεία.

Ransomware

Το Ransomware είναι ένας τύπος κακόβουλου λογισμικού που κλειδώνει αρχεία, δεδομένα ή συστήματα και απειλεί να διαγράψει ή να καταστρέψει τα δεδομένα - ή να κάνει ιδιωτικά ή ευαίσθητα

δεδομένα στο κοινό - εκτός εάν καταβληθούν λύτρα στους κυβερνοεγκληματίες που εξαπέλυσαν την επίθεση. Πρόσφατες επιθέσεις ransomware έχουν στοχεύσει πολιτείες και τοπικές κυβερνήσεις, οι οποίες είναι πιο εύκολο να παραβιαστούν από τους οργανισμούς και υπό πίεση να πληρώσουν λύτρα προκειμένου να αποκατασταθούν εφαρμογές και ιστότοποι στους οποίους βασίζονται οι πολίτες.

Phishing / κοινωνική μηχανική

Το ηλεκτρονικό ψάρεμα (phishing) είναι μια μορφή κοινωνικής μηχανικής που εξαπατά τους χρήστες να παρέχουν τα δικά τους PII ή ευαίσθητες πληροφορίες. Στις απάτες ηλεκτρονικού ψαρέματος, τα μηνύματα ηλεκτρονικού ταχυδρομείου ή τα μηνύματα κειμένου φαίνεται να προέρχονται από μια νόμιμη εταιρεία που ζητά ευαίσθητες πληροφορίες, όπως δεδομένα πιστωτικής κάρτας ή στοιχεία σύνδεσης. Το FBI έχει σημειώσει για μια αύξηση του phishing που σχετίζεται με την πανδημία, που συνδέεται με την ανάπτυξη της εξ αποστάσεως εργασίας.

Εσωτερικές απειλές

Οι νυν ή πρώην υπάλληλοι, οι επιχειρηματικοί εταίροι, οι εργολάβοι ή οποιοσδήποτε είχε πρόσβαση σε συστήματα ή δίκτυα στο παρελθόν μπορεί να θεωρηθεί απειλή από εσωτερικές πληροφορίες εάν κάνουν κατάχρηση των αδειών πρόσβασής τους. Οι εσωτερικές απειλές μπορεί να είναι αόρατες σε παραδοσιακές λύσεις ασφαλείας, όπως τα τείχη προστασίας και τα συστήματα ανίχνευσης εισβολής, τα οποία εστιάζουν σε εξωτερικές απειλές.

Κατανεμημένες επιθέσεις άρνησης υπηρεσίας (DDoS).

Μια επίθεση DDoS επιχειρεί να καταρρεύσει έναν διακομιστή, έναν ιστότοπο ή ένα δίκτυο υπερφορτώνοντάς τον με κίνηση, συνήθως από πολλαπλά συντονισμένα συστήματα. Οι επιθέσεις DDoS κατακλύζουν τα εταιρικά δίκτυα μέσω του απλού πρωτοκόλλου διαχείρισης δικτύου (SNMP), που χρησιμοποιείται για μόντεμ, εκτυπωτές, διακόπτες, δρομολογητές και διακομιστές.

Προηγμένες επίμονες απειλές (APT)

Σε ένα APT, ένας εισβολέας ή μια ομάδα εισβολέων διεισδύουν σε ένα σύστημα και παραμένουν απαρατήρητοι για μεγάλο χρονικό διάστημα. Ο εισβολέας αφήνει ανέπαφα τα δίκτυα και τα συστήματα, έτσι ώστε ο εισβολέας να μπορεί να κατασκοπεύει την επιχειρηματική δραστηριότητα και να κλέβει ευαίσθητα δεδομένα αποφεύγοντας την ενεργοποίηση αμυντικών αντιμέτρων. Η πρόσφατη παραβίαση των κυβερνητικών συστημάτων των Ηνωμένων Πολιτειών από την Solar Winds είναι ένα παράδειγμα APT.

Επιθέσεις Man-in-the-Middle

Το Man-in-the-Middle είναι μια επίθεση υποκλοπής, όπου ένας κυβερνοεγκληματίας παρακολουθεί και αναμεταδίδει μηνύματα μεταξύ δύο μερών για να κλέψει δεδομένα. Για παράδειγμα, σε ένα μη ασφαλές δίκτυο Wi-Fi, ένας εισβολέας μπορεί να υποκλέψει δεδομένα που διαβιβάζονται μεταξύ της συσκευής του επισκέπτη και του δικτύου.

4.5. Βασικές τεχνολογίες και βέλτιστες πρακτικές κυβερνοασφάλειας

Οι ακόλουθες βέλτιστες πρακτικές και τεχνολογίες μπορούν να βοηθήσουν τους οργανισμούς να εφαρμόσει ισχυρή ασφάλεια στον κυβερνοχώρο που μειώνει την ευπάθειά σας σε επιθέσεις στον κυβερνοχώρο και προστατεύει τα κρίσιμα πληροφοριακά σας συστήματα, χωρίς να παρεμβαίνει στην εμπειρία του χρήστη ή του πελάτη:

Η διαχείριση ταυτότητας και πρόσβασης (IAM) καθορίζει τους ρόλους και τα δικαιώματα πρόσβασης για κάθε χρήστη, καθώς και τους όρους υπό τους οποίους του παραχωρούνται ή του αρνούνται τα προνόμιά του. Οι μεθοδολογίες IAM περιλαμβάνουν απλή σύνδεση, η οποία επιτρέπει σε έναν χρήστη να συνδεθεί σε ένα δίκτυο μία φορά χωρίς να εισαγάγει εκ νέου διαπιστευτήρια κατά την ίδια περίοδο λειτουργίας. πολυπαραγοντικός έλεγχος ταυτότητας, που απαιτεί δύο ή περισσότερα διαπιστευτήρια πρόσβασης. προνομιούχους λογαριασμούς χρηστών, οι οποίοι παρέχουν δικαιώματα διαχειριστή μόνο σε ορισμένους χρήστες· και διαχείριση κύκλου ζωής χρήστη, η οποία διαχειρίζεται την ταυτότητα κάθε χρήστη και τα δικαιώματα πρόσβασης από την αρχική εγγραφή έως τη συνταξιοδότηση. Τα εργαλεία IAM μπορούν επίσης να δώσουν στους

επαγγελματίες σας στον τομέα της κυβερνοασφάλειας βαθύτερη ορατότητα σε ύποπτη δραστηριότητα σε συσκευές τελικού χρήστη, συμπεριλαμβανομένων των τελικών σημείων στα οποία δεν μπορούν να έχουν φυσική πρόσβαση. Αυτό βοηθά στην επιτάχυνση της έρευνας και των χρόνων απόκρισης για την απομόνωση και τον περιορισμό της ζημιάς μιας παραβίασης.

Μια ολοκληρωμένη πλατφόρμα ασφάλειας δεδομένων προστατεύει ευαίσθητες πληροφορίες σε πολλαπλά περιβάλλοντα, συμπεριλαμβανομένων των υβριδικών περιβαλλόντων multicloud. Οι καλύτερες πλατφόρμες ασφάλειας δεδομένων παρέχουν αυτοματοποιημένη, σε πραγματικό χρόνο ορατότητα των τρωτών σημείων δεδομένων, καθώς και συνεχή παρακολούθηση που τους ειδοποιεί για τρωτά σημεία και κινδύνους δεδομένων πριν γίνουν παραβιάσεις δεδομένων. Θα πρέπει επίσης να απλοποιήσουν τη συμμόρφωση με τους κανονισμούς περί απορρήτου δεδομένων της κυβέρνησης και του κλάδου. Τα αντίγραφα ασφαλείας και η κρυπτογράφηση είναι επίσης ζωτικής σημασίας για την ασφάλεια των δεδομένων.

Πληροφορίες ασφαλείας και διαχείριση συμβάντων (SIEM) συγκεντρώνει και αναλύει δεδομένα από συμβάντα ασφαλείας για να ανιχνεύσει αυτόματα ύποπτες δραστηριότητες χρήστη και να ενεργοποιήσει μια προληπτική ή επανορθωτική απόκριση. Σήμερα, οι λύσεις SIEM περιλαμβάνουν προηγμένες μεθόδους ανίχνευσης, όπως ανάλυση συμπεριφοράς χρηστών και τεχνητή νοημοσύνη (AI). Η SIEM μπορεί να ιεραρχήσει αυτόματα την απόκριση σε απειλές στον κυβερνοχώρο σύμφωνα με τους στόχους διαχείρισης κινδύνου του οργανισμού σας. Και πολλοί οργανισμοί ενσωματώνουν τα εργαλεία SIEM τους με πλατφόρμες ενορχήστρωσης, αυτοματοποίησης και απόκρισης (SOAR) ασφαλείας που αυτοματοποιούν και επιταχύνουν περαιτέρω την απόκριση των οργανισμών σε περιστατικά ασφάλειας στον κυβερνοχώρο και επιλύουν πολλά περιστατικά χωρίς ανθρώπινη παρέμβαση.

4.6. Στρατηγική ασφάλειας μηδενικής εμπιστοσύνης

Οι επιχειρήσεις σήμερα συνδέονται όπως ποτέ πριν. Τα συστήματα, οι χρήστες και τα δεδομένα σας ζουν και λειτουργούν σε διαφορετικά περιβάλλοντα. Η περιμετρική ασφάλεια δεν είναι πλέον επαρκής, αλλά η εφαρμογή ελέγχων ασφαλείας σε κάθε περιβάλλον δημιουργεί πολυπλοκότητα. Το αποτέλεσμα και στις δύο περιπτώσεις είναι υποβαθμισμένη προστασία για τα σημαντικότερα περιουσιακά σας στοιχεία. Μια στρατηγική μηδενικής εμπιστοσύνης προϋποθέτει συμβιβασμό και ρυθμίζει στοιχεία ελέγχου για την επικύρωση κάθε χρήστη, συσκευής και σύνδεσης στην επιχείρηση για αυθεντικότητα και σκοπό. Για να είναι επιτυχής η εκτέλεση μιας στρατηγικής μηδενικής εμπιστοσύνης, οι οργανισμοί χρειάζονται έναν τρόπο να συνδυάζουν πληροφορίες ασφαλείας προκειμένου να δημιουργήσουν το πλαίσιο (ασφάλεια συσκευής, τοποθεσία, κ.λπ.) που ενημερώνει και επιβάλλει ελέγχους επικύρωσης.

ΚΕΦΑΛΑΙΟ 5 – PROGRAMMABLE LOGIC CONTROLLERS (PLC)

5.1. Γενική περιγραφή

Η μηχανική ελέγχου εξελίχθηκε με την πάροδο του χρόνου. Στο παρελθόν, οι άνθρωποι ήταν η κύρια μέθοδος ελέγχου ενός συστήματος. Πιο πρόσφατα, η ηλεκτρική ενέργεια χρησιμοποιήθηκε για έλεγχο και ο πρώιμος ηλεκτρικός έλεγχος βασίστηκε σε ρελέ. Αυτά τα ρελέ επιτρέπουν την ενεργοποίηση και απενεργοποίηση ισχύος χωρίς μηχανικό διακόπτη. Είναι κοινό να χρησιμοποιείτε ρελέ για να λαμβάνετε απλές λογικές αποφάσεις ελέγχου. Η ανάπτυξη υπολογιστών χαμηλού κόστους έφερε την πιο πρόσφατη επανάσταση, τον προγραμματιζόμενο λογικό ελεγκτή (PLC). Η έλευση του PLC ξεκίνησε τη δεκαετία του 1970 και έχει γίνει η πιο κοινή επιλογή για ελέγχους κατασκευής. Τα PLC έχουν κερδίσει δημοτικότητα στο εργοστάσιο και πιθανότατα θα παραμείνουν κυρίαρχα για κάποιο χρονικό διάστημα. Τα περισσότερα από αυτά οφείλονται στα πλεονεκτήματα που προσφέρουν.

- Οικονομικό για τον έλεγχο σύνθετων συστημάτων.
- Ευέλικτη και μπορεί να εφαρμοστεί ξανά για τον έλεγχο άλλων συστημάτων γρήγορα και εύκολα.
- Οι υπολογιστικές ικανότητες επιτρέπουν πιο εξελιγμένο έλεγχο.
- Τα βοηθήματα λήψης προβλημάτων διευκολύνουν τον προγραμματισμό και μειώνουν το χρόνο διακοπής.
- Τα αξιόπιστα εξαρτήματα καθιστούν πιθανό να λειτουργήσουν για χρόνια πριν από την αποτυχία.

5.2. Programmable Logic Controllers

Ένας προγραμματιζόμενος ελεγκτής λογικής (PLC) ή ένας προγραμματιζόμενος ελεγκτής είναι ένας ψηφιακός υπολογιστής που χρησιμοποιείται για αυτοματοποίηση ηλεκτρομηχανολογικών διεργασιών, όπως έλεγχος μηχανημάτων σε εργοστασιακές γραμμές συναρμολόγησης, βόλτες διασκέδασης ή φωτιστικά. Τα PLC χρησιμοποιούνται σε πολλές βιομηχανίες και μηχανήματα. Σε αντίθεση με τους υπολογιστές γενικής χρήσης, το PLC έχει σχεδιαστεί για πολλαπλές ρυθμίσεις εισόδου και εξόδου, εκτεταμένα εύρη θερμοκρασίας, ανοσία στον ηλεκτρικό θόρυβο και αντίσταση σε κραδασμούς και κρούσεις. Τα προγράμματα για τον έλεγχο της λειτουργίας του μηχανήματος συνήθως αποθηκεύονται σε εφεδρική μπαταρία ή μη πτητική μνήμη. Ένα PLC είναι ένα παράδειγμα ενός συστήματος σκληρού πραγματικού χρόνου, καθώς τα αποτελέσματα εξόδου πρέπει να παραχθούν σε απόκριση σε συνθήκες εισόδου εντός περιορισμένου χρόνου, διαφορετικά θα προκύψει ακούσια λειτουργία.

Σχήμα 9. Κατασκευές PLC Allen Bradley

5.3. Ιστορία

Το PLC εφευρέθηκε ως απάντηση στις ανάγκες της αμερικανικής αυτοκινητοβιομηχανίας. Οι προγραμματιζόμενοι λογικοί ελεγκτές υιοθετήθηκαν αρχικά από την αυτοκινητοβιομηχανία όπου η αναθεώρηση λογισμικού αντικατέστησε την επανασύρματη σύνδεση των ενσύρματων πινάκων ελέγχου όταν άλλαξαν τα μοντέλα παραγωγής.

Πριν από το PLC, ο έλεγχος, ο προσδιορισμός αλληλουχίας και η λογική αλληλοσύνδεσης ασφαλείας για την κατασκευή αυτοκινήτων είχαν επιτευχθεί χρησιμοποιώντας εκατοντάδες ή χιλιάδες ρελέ, χρονόμετρα έκκεντρου και αλληλουχίες τυμπάνου και αποκλειστικούς ελεγκτές κλειστού βρόχου. Η διαδικασία για την ενημέρωση τέτοιων εγκαταστάσεων για την ετήσια αλλαγή μοντέλου ήταν πολύ χρονοβόρα και δαπανηρή, καθώς οι ηλεκτρολόγοι έπρεπε να επανασυνδέουν μεμονωμένα κάθε ρελέ.

Οι ψηφιακοί υπολογιστές, ως προγραμματιζόμενες συσκευές γενικής χρήσης, σύντομα εφαρμόστηκαν για τον έλεγχο των βιομηχανικών διεργασιών. Οι πρώτοι υπολογιστές απαιτούσαν εξειδικευμένους προγραμματιστές και αυστηρό λειτουργικό περιβαλλοντικό έλεγχο για θερμοκρασία, καθαριότητα και ποιότητα ισχύος. Η χρήση υπολογιστή γενικής χρήσης για τον έλεγχο της διαδικασίας απαιτείται για την προστασία του υπολογιστή από τις συνθήκες στο δάπεδο της εγκατάστασης. Ένας υπολογιστής βιομηχανικού ελέγχου θα έχει πολλά χαρακτηριστικά: θα ανέχεται το περιβάλλον του καταστήματος, θα υποστηρίζει διακριτή (bit-form) είσοδο και έξοδο με έναν εύκολα επεκτάσιμο τρόπο, δεν θα απαιτούσε χρόνια εκπαίδευσης και θα επέτρεπε τη λειτουργία του προς παρακολούθηση. Ο χρόνος απόκρισης οποιουδήποτε συστήματος υπολογιστή πρέπει να είναι αρκετά γρήγορος για να είναι χρήσιμος για έλεγχο. η απαιτούμενη ταχύτητα ποικίλλει ανάλογα με τη φύση της διαδικασίας. Το 1968, η GM Hydramatic (το τμήμα αυτόματης μετάδοσης της General Motors) υπέβαλε αίτημα για πρόταση ηλεκτρονικής αντικατάστασης συστημάτων ρελέ. Η πρόταση που κέρδισε προήλθε από τους Bedford Associates of Bedford, Massachusetts. Το πρώτο PLC, ορίστηκε το 084 επειδή ήταν το ογδόντα τέταρτο έργο της Bedford Associates, ήταν το αποτέλεσμα. Η Bedford Associates ξεκίνησε μια νέα εταιρεία αφιερωμένη στην ανάπτυξη, την κατασκευή, την πώληση και τη συντήρηση αυτού του νέου προϊόντος: Modicon, το οποίο αντιπροσωπεύει το Modular Digital Controller. Ένας από τους ανθρώπους που εργάστηκαν σε αυτό το έργο ήταν ο Dick Morley, ο οποίος θεωρείται «πατέρας» του PLC. Η μάρκα Modicon πωλήθηκε το 1977 στην Gould Electronics και αργότερα εξαγοράστηκε από τη γερμανική εταιρεία AEG και στη συνέχεια από τη γαλλική Schneider Electric , ο τρέχων κάτοχος.

Ένα από τα πρώτα 084 μοντέλα που κατασκευάστηκε τώρα εκτίθεται στα κεντρικά γραφεία της Modicon στο North Andover της Μασαχουσέτης. Παρουσιάστηκε στη Modicon από την GM, όταν η μονάδα αποσύρθηκε μετά από σχεδόν είκοσι χρόνια αδιάλειπτης υπηρεσίας. Η Modicon χρησιμοποίησε το 84 moniker στο τέλος της γκάμας προϊόντων του μέχρι το 984 να εμφανιστεί. Η αυτοκινητοβιομηχανία εξακολουθεί να είναι ένας από τους μεγαλύτερους χρήστες PLC.

5.4. Ανάπτυξη

Τα πρώτα PLC σχεδιάστηκαν για να αντικαταστήσουν τα λογικά συστήματα ρελέ. Αυτά τα PLC προγραμματίστηκαν σε "κλίμακα λογικής", που μοιάζει έντονα με ένα σχηματικό διάγραμμα της λογικής ρελέ. Αυτή η σημειογραφία του προγράμματος επιλέχθηκε για τη μείωση των απαιτήσεων κατάρτισης για τους υπάρχοντες τεχνικούς. Άλλα πρώιμα PLC χρησιμοποίησαν μια μορφή προγραμματισμού λίστας οδηγιών, βασισμένη σε λογική επίλυση στοίβας.

Τα σύγχρονα PLC μπορούν να προγραμματιστούν με διάφορους τρόπους, από τη λογική κλίμακας έως τις πιο παραδοσιακές γλώσσες προγραμματισμού όπως τη BASIC και τη C. Μια άλλη μέθοδος είναι η State Logic, μια γλώσσα προγραμματισμού πολύ υψηλού επιπέδου που έχει σχεδιαστεί για τον προγραμματισμό PLC βάσει διαγραμμάτων μετάβασης κατάστασης.

Πολλά πρώιμα PLC δεν είχαν συνοδευτικά τερματικά προγραμματισμού που ήταν ικανά γραφικής αναπαράστασης της λογικής, και έτσι η λογική αντιπροσωπεύθηκε αντ' αυτού ως μια σειρά λογικών εκφράσεων σε κάποια έκδοση της μορφής Boolean, παρόμοια με την άλγεβρα Boolean. Καθώς εξελίχθηκαν τα τερματικά προγραμματισμού, έγινε πιο συνηθισμένο να χρησιμοποιείται η λογική της σκάλας, για τους προαναφερθέντες λόγους και επειδή ήταν μια γνωστή μορφή που χρησιμοποιείται για ηλεκτρομηχανικούς πίνακες ελέγχου. Υπάρχουν νεότερες μορφές όπως το State Logic και το Function Block (το οποίο μοιάζει με τον τρόπο με τον οποίο απεικονίζεται η λογική κατά τη χρήση ψηφιακών ολοκληρωμένων κυκλωμάτων λογικής), αλλά εξακολουθούν να μην είναι τόσο δημοφιλή όσο η λογική της κλίμακας. Ένας πρωταρχικός λόγος για αυτό είναι ότι τα PLC επιλύουν τη λογική με μια προβλέψιμη και επαναλαμβανόμενη ακολουθία και η λογική της σκάλας επιτρέπει στον προγραμματιστή (το άτομο που γράφει τη λογική) να βλέπει τυχόν προβλήματα με το χρονοδιάγραμμα της ακολουθίας λογικής πιο εύκολα από ό, τι θα ήταν δυνατό σε άλλα μορφές.

5.5. Λειτουργικότητα

Η λειτουργικότητα του PLC έχει εξελιχθεί με τα χρόνια και περιλαμβάνει διαδοχικό έλεγχο ρελέ, έλεγχο κίνησης, έλεγχο διαδικασίας, κατανεμημένα συστήματα ελέγχου και δικτύωση. Ο χειρισμός δεδομένων, η αποθήκευση, η ισχύς επεξεργασίας και οι δυνατότητες επικοινωνίας ορισμένων σύγχρονων PLC είναι περίπου ισοδύναμες με τους επιτραπέζιους υπολογιστές. Ο προγραμματισμός τύπου PLC σε συνδυασμό με απομακρυσμένο υλικό I / O, επιτρέπει σε έναν επιτραπέζιο υπολογιστή γενικής χρήσης να επικαλύπτει ορισμένα PLC σε ορισμένες εφαρμογές. Όσον αφορά την πρακτικότητα αυτών των ελεγκτών λογικής που βασίζονται σε επιτραπέζιους υπολογιστές, είναι σημαντικό να σημειωθεί ότι δεν έχουν γίνει γενικά αποδεκτές στη βαριά βιομηχανία, επειδή οι επιτραπέζιοι υπολογιστές λειτουργούν σε λιγότερο σταθερά λειτουργικά συστήματα από ό, τι τα PLC και επειδή το υλικό του επιτραπέζιου υπολογιστή συνήθως δεν έχει σχεδιαστεί στα ίδια επίπεδα ανοχής στη θερμοκρασία, την υγρασία, τους κραδασμούς και τη μακροζωία με τους επεξεργαστές που χρησιμοποιούνται σε PLC. Εκτός από τους περιορισμούς υλικού της λογικής που βασίζεται σε επιτραπέζιους υπολογιστές, λειτουργικά συστήματα όπως τα Windows δεν προσφέρονται για εκτέλεση ντετερμινιστικής λογικής, με αποτέλεσμα η λογική να μην ανταποκρίνεται πάντοτε σε αλλαγές στην κατάσταση λογικής ή στην κατάσταση εισαγωγής με την εξαιρετική συνέπεια στο χρονισμό αναμένεται από PLC. Παρόλα αυτά, τέτοιες εφαρμογές λογικής επιφάνειας εργασίας βρίσκουν χρήση σε λιγότερο κρίσιμες καταστάσεις, όπως αυτοματοποίηση εργαστηρίου και χρήση σε μικρές εγκαταστάσεις όπου η εφαρμογή είναι λιγότερο απαιτητική και κρίσιμη, επειδή είναι γενικά πολύ λιγότερο δαπανηρές από τις PLC.

Τα τελευταία χρόνια, μικρά προϊόντα που ονομάζονται PLR (προγραμματιζόμενα λογικά ρελέ), καθώς και με παρόμοια ονόματα, έχουν γίνει πιο κοινά και αποδεκτά. Αυτά μοιάζουν πολύ με PLC και χρησιμοποιούνται στη βιομηχανία φωτός όπου εμπλέκονται μόνο μερικά σημεία εισόδου / εξόδου (δηλ. Μερικά σήματα που εισέρχονται από τον πραγματικό κόσμο και μερικά εξερχόμενα) και απαιτείται χαμηλό κόστος. Αυτές οι μικρές συσκευές κατασκευάζονται συνήθως σε ένα κοινό φυσικό μέγεθος και σχήμα από πολλούς κατασκευαστές και φέρουν την επωνυμία των κατασκευαστών μεγαλύτερων PLC για να συμπληρώσουν τη χαμηλή γκάμα προϊόντων τους. Τα δημοφιλή ονόματα περιλαμβάνουν τον ελεγκτή PICO, το NANO PLC και άλλα ονόματα που υποδηλώνουν πολύ μικρούς ελεγκτές. Τα περισσότερα από αυτά έχουν μεταξύ 8 και 12 ψηφιακές εισόδους, 4 και 8 ψηφιακές εξόδους και έως και 2 αναλογικές εισόδους. Το μέγεθος είναι συνήθως περίπου 4 "πλάτος, ύψος 3" και βάθος 3 ". Οι περισσότερες τέτοιες συσκευές περιλαμβάνουν μια μικρή οθόνη LCD μεγέθους γραμματοσήμου για προβολή απλοποιημένης λογικής σκάλας (μόνο ένα πολύ μικρό μέρος του προγράμματος είναι ορατό σε μια δεδομένη στιγμή) και κατάσταση των σημείων I / O και συνήθως αυτές οι οθόνες συνοδεύονται από ένα 4-way rocker push-plus συν τέσσερα ακόμη ξεχωριστά κουμπιά, παρόμοια με τα πλήκτρα του τηλεχειριστηρίου VCR και χρησιμοποιούνται για πλοήγηση και επεξεργασία της λογικής. Τα περισσότερα διαθέτουν ένα μικρό βύσμα για σύνδεση μέσω RS-232 ή RS-485 σε έναν προσωπικό υπολογιστή, έτσι ώστε οι προγραμματιστές να μπορούν να χρησιμοποιούν απλές εφαρμογές Windows για προγραμματισμό αντί να υποχρεούνται να χρησιμοποιούν το μικροσκοπικό LCD και το μπουτόν για αυτόν τον σκοπό.

Σε αντίθεση με τα κανονικά PLC που είναι συνήθως αρθρωτά και πολύ επεκτάσιμα, τα PLR συνήθως δεν είναι αρθρωτά ή επεκτάσιμα, αλλά η τιμή τους μπορεί να είναι δύο τάξεις μεγέθους μικρότερη από ένα PLC και εξακολουθούν να προσφέρουν στιβαρό σχεδιασμό και ντετερμινιστική εκτέλεση της λογικής.

5.6. Σύγκριση PLC με άλλα συστήματα ελέγχου

Τα PLC είναι καλά προσαρμοσμένα σε μια σειρά εργασιών αυτοματισμού. Πρόκειται συνήθως για βιομηχανικές διαδικασίες στην κατασκευή όπου το κόστος ανάπτυξης και συντήρησης του συστήματος αυτοματισμού είναι υψηλό σε σχέση με το συνολικό κόστος της αυτοματοποίησης και όπου αναμένονται αλλαγές στο σύστημα κατά τη διάρκεια της λειτουργίας του. Τα PLC περιέχουν συσκευές εισόδου και εξόδου συμβατές με βιομηχανικές πιλοτικές συσκευές και χειριστήρια. Απαιτείται λίγος ηλεκτρικός σχεδιασμός και το πρόβλημα σχεδιασμού επικεντρώνεται στην έκφραση της επιθυμητής ακολουθίας λειτουργιών. Οι εφαρμογές PLC είναι συνήθως εξαιρετικά προσαρμοσμένα συστήματα, οπότε το κόστος μιας συσκευασμένης PLC είναι χαμηλό σε σύγκριση με το κόστος ενός συγκεκριμένου σχεδιασμένου σχεδιασμού ελεγκτή. Από την άλλη πλευρά, στην περίπτωση μαζικών προϊόντων, τα προσαρμοσμένα συστήματα ελέγχου είναι οικονομικά. Αυτό οφείλεται στο χαμηλότερο κόστος των εξαρτημάτων, τα οποία μπορούν να επιλεχθούν βέλτιστα αντί μιας «γενικής» λύσης, και όπου οι μη επαναλαμβανόμενες χρεώσεις μηχανικής κατανέμονται σε χιλιάδες ή εκατομμύρια μονάδες.

Σχήμα 10. Το PLC Allen-Bradley είναι εγκατεστημένο σε έναν πίνακα ελέγχου

Για εργασίες μεγάλου όγκου ή πολύ απλές εργασίες αυτοματοποίησης, χρησιμοποιούνται διαφορετικές τεχνικές. Για παράδειγμα, ένα πλυντήριο πιάτων καταναλωτή θα ελέγχεται από ένα ηλεκτρομηχανικό χρονόμετρο έκκεντρου που κοστίζει μόνο μερικά δολάρια σε ποσότητες παραγωγής.

Ένας σχεδιασμός που βασίζεται σε μικροελεγκτή θα ήταν κατάλληλος όπου θα παράγονται εκατοντάδες ή χιλιάδες μονάδες και έτσι το κόστος ανάπτυξης (σχεδιασμός τροφοδοτικών, υλικού εισόδου / εξόδου και απαραίτητες δοκιμές και πιστοποίηση) μπορεί να διαδοθεί σε πολλές πωλήσεις, και όπου το τέλος- ο χρήστης δεν θα χρειαστεί να αλλάξει τον έλεγχο. Οι εφαρμογές αυτοκινήτων είναι ένα παράδειγμα. εκατομμύρια μονάδες κατασκευάζονται κάθε χρόνο και πολύ λίγοι τελικοί χρήστες αλλάζουν τον προγραμματισμό αυτών των ελεγκτών. Ωστόσο, ορισμένα ειδικά οχήματα όπως τα λεωφορεία διέλευσης χρησιμοποιούν οικονομικά PLC αντί για ειδικά σχεδιασμένα χειριστήρια, επειδή οι όγκοι είναι χαμηλοί και το κόστος ανάπτυξης θα ήταν αντιοικονομικό.

Πολύ περίπλοκος έλεγχος διεργασιών, όπως χρησιμοποιείται στη χημική βιομηχανία, μπορεί να απαιτεί αλγόριθμους και απόδοση πέρα από την ικανότητα ακόμη και PLC υψηλής απόδοσης. Οι έλεγχοι πολύ υψηλής ταχύτητας ή ακριβείας ενδέχεται επίσης να απαιτούν προσαρμοσμένες λύσεις. για παράδειγμα, έλεγχοι πτήσης αεροσκαφών. Οι υπολογιστές μιας πλακέτας που

χρησιμοποιούν ημι-προσαρμοσμένο ή πλήρως ιδιόκτητο υλικό μπορούν να επιλεγούν για πολύ απαιτητικές εφαρμογές ελέγχου, όπου μπορεί να υποστηριχθεί το υψηλό κόστος ανάπτυξης και συντήρησης. Τα "Soft PLC" που εκτελούνται σε επιτραπέζιους υπολογιστές μπορούν να διασυνδεθούν με βιομηχανικό υλικό I / O, ενώ εκτελούν προγράμματα σε μια έκδοση εμπορικών λειτουργικών συστημάτων προσαρμοσμένων για ανάγκες ελέγχου διεργασιών.

Οι προγραμματιζόμενοι ελεγκτές χρησιμοποιούνται ευρέως στον έλεγχο κίνησης, στον έλεγχο θέσης και στον έλεγχο ροπής. Ορισμένοι κατασκευαστές παράγουν μονάδες ελέγχου κίνησης για ενσωμάτωση με PLC έτσι ώστε ο κώδικας G (που περιλαμβάνει μηχανή CNC) να μπορεί να χρησιμοποιηθεί για την καθοδήγηση των κινήσεων του μηχανήματος.

Τα PLC μπορεί να περιλαμβάνουν λογική για έναν αναλογικό βρόχο ελέγχου ανατροφοδότησης μίας μεταβλητής, έναν "αναλογικό, ολοκληρωμένο, παράγωγο" ή "ελεγκτή PID". Ένας βρόχος PID θα μπορούσε να χρησιμοποιηθεί για τον έλεγχο της θερμοκρασίας μιας διαδικασίας κατασκευής, για παράδειγμα. Ιστορικά τα PLC συνήθως είχαν διαμορφωθεί με λίγους αναλογικούς βρόχους ελέγχου. όπου οι διαδικασίες απαιτούσαν εκατοντάδες ή χιλιάδες βρόχους, θα χρησιμοποιήθηκε ένα κατανεμημένο (DCS). Καθώς τα PLC έχουν γίνει πιο ισχυρά, το όριο μεταξύ των εφαρμογών DCS και PLC έχει γίνει λιγότερο διακριτό.

Τα PLC έχουν παρόμοια λειτουργικότητα με τις απομακρυσμένες τερματικές μονάδες. Ένα RTU, ωστόσο, συνήθως δεν υποστηρίζει αλγόριθμους ελέγχου ή βρόχους ελέγχου. Καθώς το υλικό γίνεται γρήγορα πιο ισχυρό και φθηνότερο, τα RTUs, PLC και DCS αρχίζουν ολοένα και περισσότερο να αλληλεπικαλύπτονται με ευθύνες και πολλοί προμηθευτές πωλούν RTU με χαρακτηριστικά τύπου PLC και αντίστροφα. Ο κλάδος έχει τυποποιήσει τη λειτουργική γλώσσα του IEC 61131-3 για τη δημιουργία προγραμμάτων που εκτελούνται σε RTU και PLC, αν και σχεδόν όλοι οι προμηθευτές προσφέρουν επίσης ιδιόκτητες εναλλακτικές λύσεις και συναφή περιβάλλοντα ανάπτυξης.

Τα τελευταία χρόνια τα "Safety" PLC έχουν αρχίσει να γίνονται δημοφιλή, είτε ως αυτόνομα μοντέλα (Pilz PNOZ Multi, Sick κ.λπ.) είτε ως λειτουργικότητα και υλικό με ασφάλεια που προστέθηκε στις υπάρχουσες αρχιτεκτονικές ελεγκτών (Allen Bradley Guardlogix, Siemens F-series κ.λπ.). Αυτά διαφέρουν από τους συμβατικούς τύπους PLC καθώς είναι κατάλληλοι για χρήση σε κρίσιμες για την ασφάλεια εφαρμογές για τις οποίες τα PLC παραδοσιακά συμπληρώθηκαν με ενσύρματα ρελέ ασφαλείας. Για παράδειγμα, ένα Safety PLC μπορεί να χρησιμοποιηθεί για τον έλεγχο της πρόσβασης σε ένα κελί ρομπότ με πρόσβαση παγιδευμένου κλειδιού, ή ίσως για τη διαχείριση της απόκρισης τερματισμού λειτουργίας σε μια στάση έκτακτης ανάγκης σε μια γραμμή παραγωγής μεταφορέων. Τέτοια PLC έχουν συνήθως ένα περιορισμένο σύνολο τακτικών οδηγιών, επαυξημένο με οδηγίες ασφαλείας ειδικά σχεδιασμένες για διασύνδεση με στάσεις έκτακτης ανάγκης, οθόνες φωτός και ούτω καθεξής. Η ευελιξία που προσφέρουν τέτοια συστήματα είχε ως αποτέλεσμα την ταχεία αύξηση της ζήτησης για αυτούς τους ελεγκτές.

5.7. Πλεονεκτήματα των PLC

Οι προγραμματιζόμενοι ελεγκτές είναι κατασκευασμένοι από στοιχεία στερεάς κατάστασης και ως εκ τούτου παρέχουν υψηλή αξιοπιστία.

Είναι ευέλικτα και οι αλλαγές στη σειρά λειτουργίας μπορούν εύκολα να ενσωματωθούν λόγω προγραμματισμού. Μπορεί να έχουν αρθρωτό χαρακτήρα και έτσι είναι δυνατή η επέκταση και η εύκολη εγκατάσταση. Η χρήση του PLC οδηγεί σε σημαντική εξοικονόμηση κόστους υλικού και καλωδίωσης. Είναι συμπαγής και καταλαμβάνουν λιγότερο χώρο.

Εξαλείφουν στοιχεία υλικού όπως χρονοδιακόπτες, μετρητές και βοηθητικά ρελέ. Η παρουσία για χρονομετρητές και μετρητές έχει εύκολη προσβασιμότητα.

Το PLC μπορεί να ελέγξει μια ποικιλία συσκευών και εξαλείφει την ανάγκη για προσαρμοσμένους ελέγχους.

Εύκολες διαγνωστικές εγκαταστάσεις παρέχονται ως μέρος του συστήματος. Η διάγνωση των εξωτερικών συστημάτων γίνεται επίσης πολύ απλή. Έτσι εύκολη συντήρηση / συντήρηση.

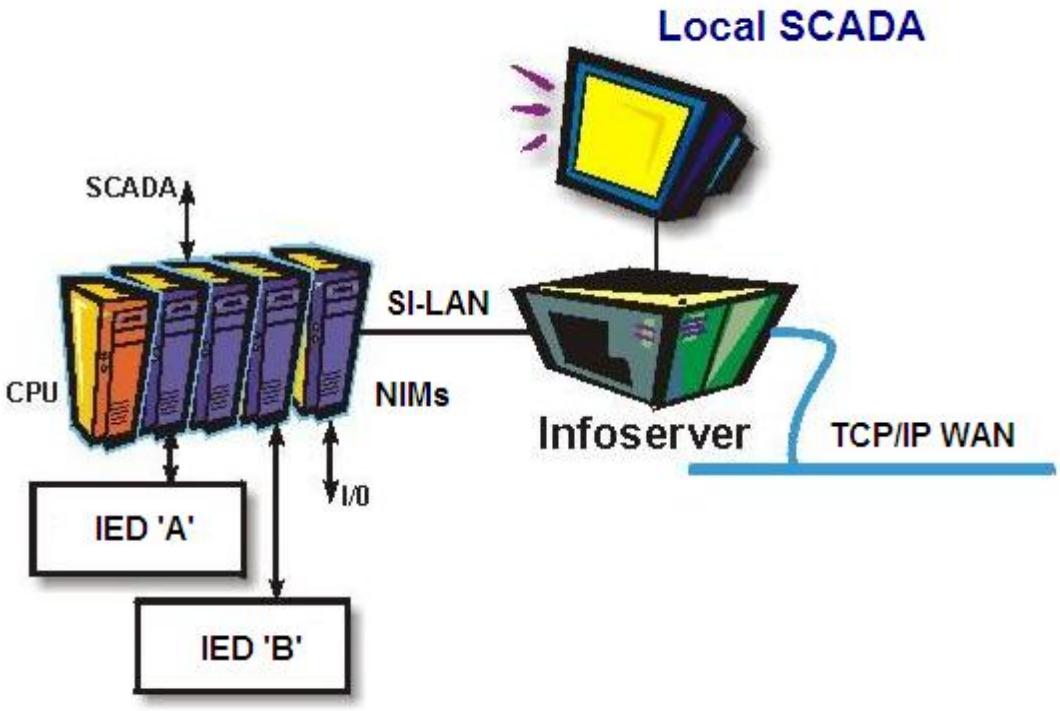
Οι συσκευές προγραμματισμού παρέχουν φιλική προς τον χειριστή διεπαφή με το μηχάνημα. Όντας αποτέλεσμα της τελευταίας τεχνολογίας της τεχνολογίας ηλεκτρονικών, οι προγραμματιζόμενοι ελεγκτές παρέχουν υψηλότερο επίπεδο απόδοσης με υπολογιστές. Μπορούν να ληφθούν και να διατηρηθούν χρήσιμα δεδομένα διαχείρισης.

Έχει απόλυτη προστασία από την απαξίωση και έχει ευρύ πεδίο για την αναβάθμιση.

5.8. Συστήματα SCADA

Το SCADA χρησιμοποιείται ευρέως στη βιομηχανία για τον εποπτικό έλεγχο και την απόκτηση δεδομένων βιομηχανικών διαδικασιών. Τα συστήματα SCADA διεισδύουν τώρα επίσης στα πειραματικά εργαστήρια φυσικής για τους ελέγχους των βοηθητικών συστημάτων όπως η ψύξη, ο εξαερισμός, η κατανομή ισχύος κ.λπ. πείραμα, για να αναφέρουμε μόνο δύο παραδείγματα στο CERN.

Τα συστήματα SCADA έχουν σημειώσει σημαντική πρόοδο τα τελευταία χρόνια όσον αφορά τη λειτουργικότητα, τη δυνατότητα κλιμάκωσης, την απόδοση και το άνοιγμα, έτσι ώστε να είναι μια εναλλακτική λύση στην εσωτερική ανάπτυξη, ακόμη και για πολύ απαιτητικά και πολύπλοκα συστήματα ελέγχου όπως αυτά των πειραμάτων φυσικής.



Σχήμα 11. Δίκτυο SCADA

ΚΕΦΑΛΑΙΟ 6 – ΑΡΧΙΤΕΚΤΟΝΙΚΗ PLC

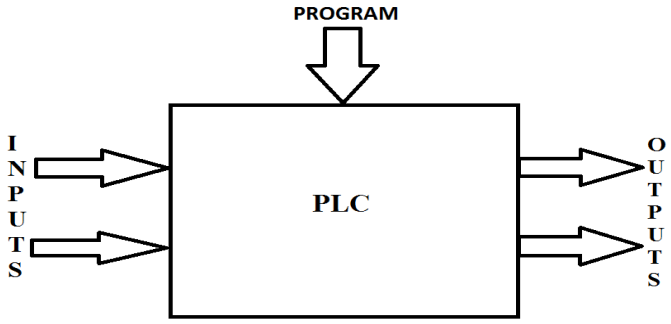
6.1. Εισαγωγή

Ένας προγραμματιζόμενος λογικός ελεγκτής (PLC) είναι μια ειδική μορφή ελεγκτή που βασίζεται σε μικροεπεξεργαστή που χρησιμοποιεί προγραμματιζόμενη μνήμη για την αποθήκευση οδηγιών και για την εφαρμογή λειτουργιών όπως λογική, αλληλουχία, χρονισμός, καταμέτρηση και αριθμητική για τον έλεγχο μηχανών και διαδικασιών. Είναι σχεδιασμένο να λειτουργεί από μηχανικούς με ίσως περιορισμένη γνώση υπολογιστών και υπολογιστικών γλωσσών. Δεν έχουν σχεδιαστεί έτσι ώστε μόνο οι προγραμματιστές υπολογιστών να μπορούν να ρυθμίζουν ή να αλλάζουν τα προγράμματα. Έτσι, οι σχεδιαστές του PLC το έχουν προγραμματίσει ώστε το πρόγραμμα ελέγχου να μπορεί να εισαχθεί χρησιμοποιώντας μια απλή, μάλλον διαισθητική μορφή γλώσσας. Ο όρος λογική χρησιμοποιείται επειδή ο προγραμματισμός ασχολείται πρωτίστως με την υλοποίηση λειτουργιών λογικής και εναλλαγής. Για παράδειγμα, εάν συμβεί Α ή Β, ενεργοποιήστε το C. Εάν συμβεί Α και Β, ενεργοποιήστε το D. Οι συσκευές εισόδου (δηλαδή, αισθητήρες όπως διακόπτες) και οι συσκευές εξόδου (κινητήρες, βαλβίδες κ.λπ.) στο σύστημα που ελέγχεται συνδέονται στο PLC. Στη συνέχεια, ο χειριστής εισάγει μια ακολουθία οδηγιών, ένα πρόγραμμα, στη μνήμη του PLC. Στη συνέχεια, ο ελεγκτής παρακολουθεί τις εισόδους και τις εξόδους σύμφωνα με αυτό το πρόγραμμα και εκτελεί τους κανόνες ελέγχου για τους οποίους έχει προγραμματιστεί. Τα PLC έχουν το μεγάλο πλεονέκτημα ότι ο ίδιος βασικός ελεγκτής μπορεί να χρησιμοποιηθεί με ένα ευρύ φάσμα συστημάτων ελέγχου. Για να τροποποιήσουμε ένα σύστημα ελέγχου και τους κανόνες που πρόκειται να χρησιμοποιηθούν, το μόνο που χρειάζεται είναι ένας χειριστής να πληκτρολογήσει ένα διαφορετικό σύνολο οδηγιών. Δεν χρειάζεται να επανασυνδέσουμε. Το αποτέλεσμα είναι ένα ευέλικτο, οικονομικά αποδοτικό σύστημα που μπορεί να χρησιμοποιηθεί με συστήματα ελέγχου, τα οποία ποικίλλουν αρκετά ευρέως στη φύση και την πολυπλοκότητά τους. Τα PLC είναι παρόμοια με τους υπολογιστές, αλλά ενώ οι υπολογιστές είναι βελτιστοποιημένοι για εργασίες υπολογισμού και εμφάνισης, οι PLC είναι βελτιστοποιημένοι για εργασίες ελέγχου και το βιομηχανικό περιβάλλον.

Τα PLC γενικότερα:

- Είναι ανθεκτικά και σχεδιασμένα για να αντέχουν σε δονήσεις, θερμοκρασία, υγρασία και θόρυβο.
- Είναι διεπαφή για εισόδους και εξόδους ήδη μέσα στον ελεγκτή.
- Προγραμματίζονται εύκολα και έχουν εύκολα κατανοητή γλώσσα προγραμματισμού που αφορά κυρίως τις λειτουργίες λογικής και εναλλαγής.

Το πρώτο PLC αναπτύχθηκε το 1969. Τα PLC χρησιμοποιούνται πλέον ευρέως και επεκτείνονται από μικρές, αυτόνομες μονάδες για χρήση με ίσως 20 ψηφιακές εισόδους/ εξόδους σε αρθρωτά συστήματα που μπορούν να χρησιμοποιηθούν για μεγάλο αριθμό εισόδων/ εξόδων, χειρισμό ψηφιακών ή αναλογικών εισόδων/ εξόδων, και εκτελούν τρόπους ελέγχου αναλογικού-ακέραιου-παραγώγου.



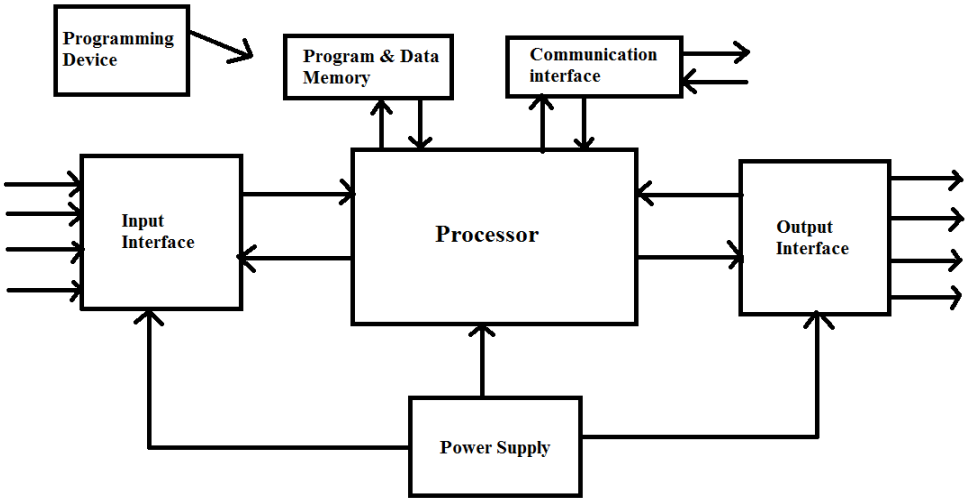
Σχήμα 12. Ένας προγραμματιζόμενος λογικός ελεγκτής

6.2. Το Hardware

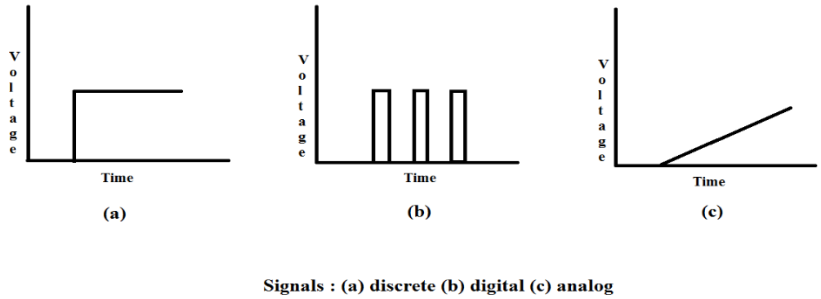
Συνήθως ένα σύστημα PLC έχει τα βασικά λειτουργικά συστατικά της μονάδας επεξεργαστή, της μνήμης, της μονάδας τροφοδοσίας, του τμήματος διεπαφής εισόδου / εξόδου, της διεπαφής επικοινωνίας και της συσκευής προγραμματισμού.

Η μονάδα επεξεργαστή ή η κεντρική μονάδα επεξεργασίας (CPU) είναι η μονάδα που περιέχει τον μικροεπεξεργαστή. Αυτή η μονάδα ερμηνεύει τα σήματα εισόδου και εκτελεί τις ενέργειες ελέγχου σύμφωνα με το πρόγραμμα που είναι αποθηκευμένο στη μνήμη του, μεταδίδοντας τις αποφάσεις ως σήματα δράσης στις εξόδους.

- Η μονάδα τροφοδοσίας απαιτείται για τη μετατροπή της τάσης εναλλασσόμενου ρεύματος στην χαμηλή τάση DC (5 V) που απαιτείται για τον επεξεργαστή και τα κυκλώματα στις ενότητες διεπαφής εισόδου και εξόδου.
- Η συσκευή προγραμματισμού χρησιμοποιείται για την εισαγωγή του απαιτούμενου προγράμματος στη μνήμη του επεξεργαστή. Το πρόγραμμα αναπτύσσεται στη συσκευή και μετά μεταφέρεται στη μονάδα μνήμης του PLC.
- Η μονάδα μνήμης είναι όπου αποθηκεύεται το πρόγραμμα που περιέχει τις ενέργειες ελέγχου που πρέπει να ασκήσει ο μικροεπεξεργαστής και όπου τα δεδομένα αποθηκεύονται από την είσοδο για επεξεργασία και για την έξοδο.



Σχήμα 13. Το σύστημα PLC

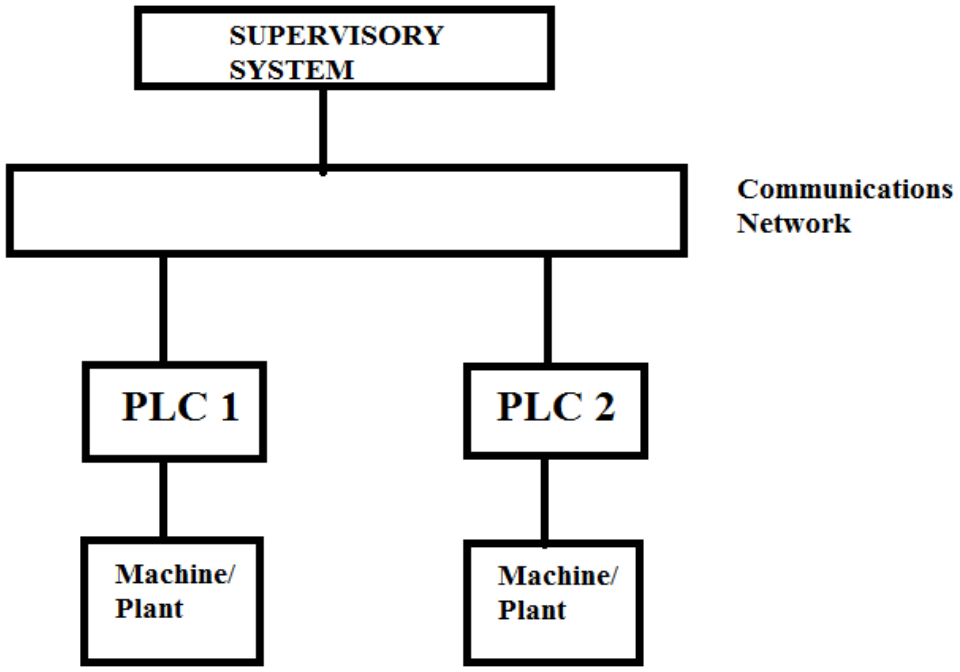


Σχήμα 14. Σήματα

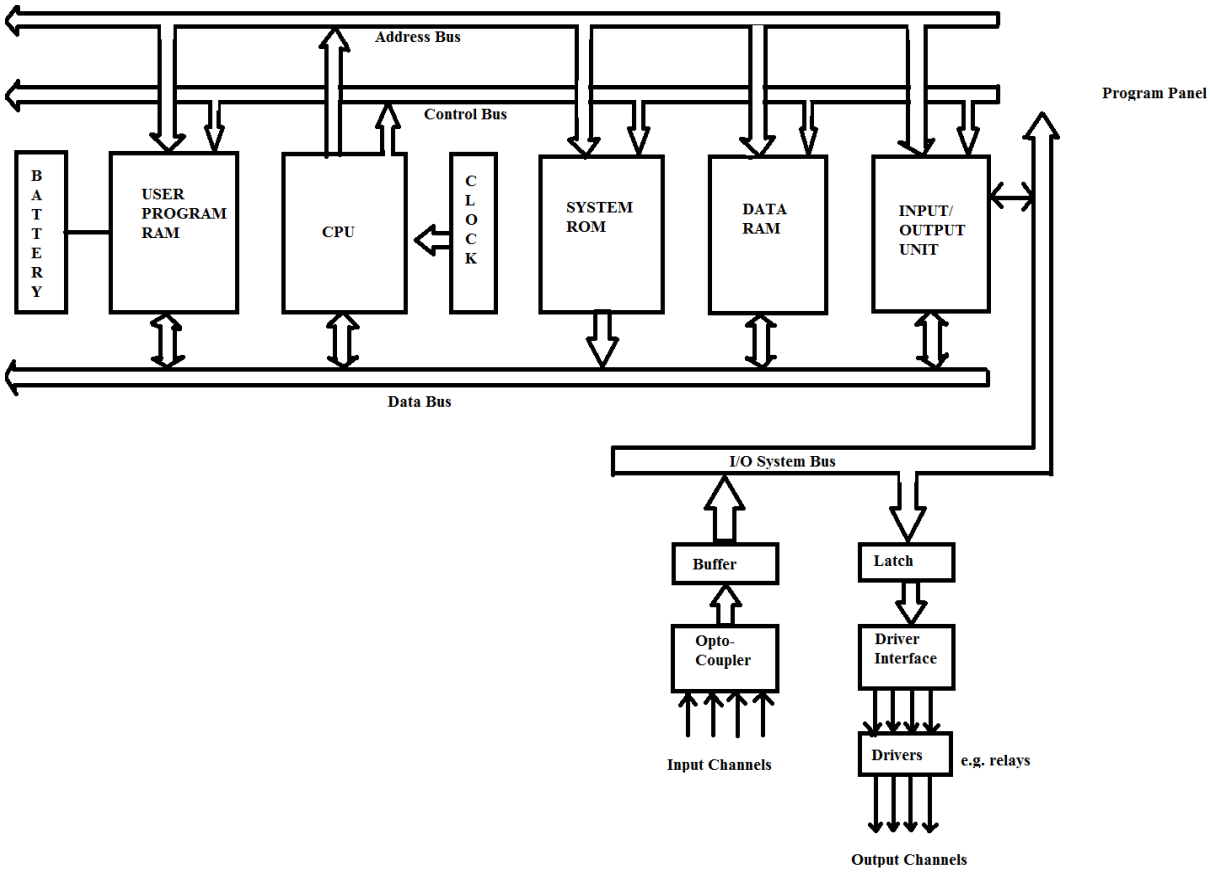
- Οι ενότητες εισόδου και εξόδου είναι όπου ο επεξεργαστής λαμβάνει πληροφορίες από εξωτερικές συσκευές και μεταδίδει πληροφορίες σε εξωτερικές συσκευές. Οι είσοδοι μπορεί επομένως να είναι από διακόπτες, όπως απεικονίζεται με το αυτόματο τρυπάνι, ή άλλους αισθητήρες όπως φωτοηλεκτρικά κύτταρα, όπως στον μηχανισμό μετρητή, αισθητήρες θερμοκρασίας, αισθητήρες ροής ή παρόμοια. Οι έξοδοι μπορεί να είναι σε πηνία εκκίνησης κινητήρα, ηλεκτρομαγνητικές βαλβίδες ή παρόμοια πράγματα. Οι συσκευές εισόδου και εξόδου μπορούν να ταξινομηθούν ως δίνουν σήματα που είναι διακριτά, ψηφιακά ή αναλογικά. Οι συσκευές που παρέχουν διακριτά ή ψηφιακά σήματα είναι αυτές όπου τα σήματα είναι είτε σβηστά ή ενεργοποιημένα. Έτσι ένας διακόπτης είναι μια συσκευή που δίνει ένα διακριτό σήμα, είτε δεν υπάρχει τάση είτε τάση. Οι ψηφιακές συσκευές μπορούν να θεωρηθούν ουσιαστικά ως διακριτές συσκευές που δίνουν μια ακολουθία σημάτων on / off. Οι αναλογικές συσκευές δίνουν σήματα των οποίων το μέγεθος είναι ανάλογο με το μέγεθος της μεταβλητής που παρακολουθείται. Για παράδειγμα, ένας αισθητήρας θερμοκρασίας μπορεί να δώσει τάση ανάλογη με τη θερμοκρασία.
- Η διεπαφή επικοινωνίας χρησιμοποιείται για τη λήψη και μετάδοση δεδομένων σε δίκτυα επικοινωνίας από ή προς άλλα απομακρυσμένα PLC. Ασχολείται με ενέργειες όπως επαλήθευση συσκευής, απόκτηση δεδομένων, συγχρονισμός μεταξύ εφαρμογών χρήστη και διαχείριση σύνδεσης.

6.3. Εσωτερική αρχιτεκτονική

Η βασική εσωτερική αρχιτεκτονική ενός PLC φαίνεται παρακάτω. Αποτελείται από μια κεντρική μονάδα επεξεργασίας (CPU) που περιέχει τον μικροεπεξεργαστή συστήματος, τη μνήμη και το κύκλωμα εισόδου / εξόδου.



Σχήμα 5. Βασικό μοντέλο επικοινωνίας



Σχήμα 16. Αρχιτεκτονική του PLC

Η CPU ελέγχει και επεξεργάζεται όλες τις λειτουργίες εντός του PLC. Διατίθεται με ένα ρολόι που έχει συχνότητα τυπικά μεταξύ 1 και 8 MHz. Αυτή η συχνότητα καθορίζει την ταχύτητα λειτουργίας του PLC και παρέχει το χρόνο και το συγχρονισμό για όλα τα στοιχεία του συστήματος. Οι πληροφορίες στο PLC μεταφέρονται μέσω ψηφιακών σημάτων. Οι εσωτερικές διαδρομές κατά τις οποίες ρέουν τα ψηφιακά σήματα ονομάζονται λεωφορεία. Με τη φυσική έννοια, ένα bus είναι μόνο ένας αριθμός αγωγών κατά μήκος των οποίων μπορούν να ρέουν ηλεκτρικά σήματα. Μπορεί να είναι κομμάτια σε πλακέτα τυπωμένου κυκλώματος ή καλώδια σε καλώδιο κορδέλας. Η CPU χρησιμοποιεί το δίαυλο δεδομένων για την αποστολή δεδομένων μεταξύ των συστατικών στοιχείων, του δίαυλου διευθύνσεων για την αποστολή των διευθύνσεων τοποθεσιών για πρόσβαση σε αποθηκευμένα δεδομένα και του διαύλου ελέγχου για σήματα που σχετίζονται με ενέργειες εσωτερικού ελέγχου. Ο δίαυλος συστήματος χρησιμοποιείται για επικοινωνίες μεταξύ των θυρών εισόδου / εξόδου και της μονάδας εισόδου / εξόδου.

6.4. Η CPU

Η εσωτερική δομή της CPU εξαρτάται από τον σχετικό μικροεπεξεργαστή. Γενικά, οι CPU έχουν τα ακόλουθα:

- Μια αριθμητική και λογική μονάδα (ALU) που είναι υπεύθυνη για τον χειρισμό δεδομένων και τη διεξαγωγή αριθμητικών λειτουργιών προσθήκης και αφαίρεσης και λογικών λειτουργιών AND, OR, NOT και EXCLUSIVE-OR.

- Μνήμη, ονομαζόμενοι καταχωρητές, που βρίσκονται εντός του μικροεπεξεργαστή και χρησιμοποιούνται για την αποθήκευση πληροφοριών που εμπλέκονται στην εκτέλεση του προγράμματος.
- Μια μονάδα ελέγχου που χρησιμοποιείται για τον έλεγχο του χρόνου λειτουργίας.

6.5. Buses

Τα λεωφορεία είναι τα μονοπάτια που χρησιμοποιούνται για επικοινωνία εντός του PLC. Οι πληροφορίες μεταδίδονται σε δυαδική μορφή, δηλαδή ως ομάδα δυαδικών ψηφίων, με λίγο να είναι δυαδικό ψηφίο 1 ή 0, που δείχνει καταστάσεις ενεργοποίησης / απενεργοποίησης. Ο όρος λέξη χρησιμοποιείται για την ομάδα bits που αποτελούν κάποιες πληροφορίες. Έτσι, μια λέξη 8-bit μπορεί να είναι ο δυαδικός αριθμός 00100110. Κάθε ένα από τα δυαδικά ψηφία επικοινωνείται ταυτόχρονα κατά μήκος του δικού του παράλληλου καλωδίου. Το σύστημα διαθέτει τέσσερα λεωφορεία:

- Ο δίαυλος δεδομένων μεταφέρει τα δεδομένα που χρησιμοποιούνται στην επεξεργασία που γίνεται από την CPU. Ένας μικροεπεξεργαστής που ονομάζεται 8-bit έχει έναν εσωτερικό δίαυλο δεδομένων που μπορεί να χειριστεί αριθμούς 8-bit. Έτσι μπορεί να εκτελεί λειτουργίες μεταξύ αριθμών 8-bit και να παρέχει αποτελέσματα ως τιμές 8-bit.
- Ο δίαυλος διευθύνσεων χρησιμοποιείται για τη μεταφορά των διευθύνσεων των τοποθεσιών μνήμης. Για να μπορεί κάθε λέξη να βρίσκεται στη μνήμη, κάθε τοποθεσία μνήμης έχει μια μοναδική διεύθυνση. Ακριβώς όπως τα σπίτια σε μια πόλη λαμβάνουν κάθε μια ξεχωριστή διεύθυνση έτσι ώστε να μπορούν να εντοπιστούν, έτσι κάθε τοποθεσία λέξης έχει μια διεύθυνση έτσι ώστε τα δεδομένα που είναι αποθηκευμένα σε μια συγκεκριμένη τοποθεσία να έχουν πρόσβαση από την CPU, είτε για ανάγνωση δεδομένων που βρίσκονται εκεί είτε για να γράφουν δεδομένα εκεί. Είναι ο δίαυλος διευθύνσεων που μεταφέρει τις πληροφορίες που υποδεικνύουν σε ποια διεύθυνση πρέπει να έχετε πρόσβαση. Εάν ο δίαυλος διευθύνσεων αποτελείται από οκτώ γραμμές, ο αριθμός των λέξεων 8-bit, και συνεπώς ο αριθμός των διακριτών διευθύνσεων, είναι 28 ¼ 256. Με 16 γραμμές διευθύνσεων, είναι δυνατές 65.536 διευθύνσεις.
- Ο δίαυλος ελέγχου μεταφέρει τα σήματα που χρησιμοποιεί η CPU για έλεγχο, όπως για να ενημερώνει τις συσκευές μνήμης εάν πρόκειται να λαμβάνει δεδομένα από δεδομένα εισόδου ή εξόδου και να μεταφέρει σήματα χρονισμού που χρησιμοποιούνται για συγχρονισμό ενεργειών.
- Ο δίαυλος συστήματος χρησιμοποιείται για επικοινωνίες μεταξύ των θυρών εισόδου / εξόδου και της μονάδας εισόδου / εξόδου.

6.6. Μνήμη

Για να λειτουργήσει το σύστημα PLC υπάρχει ανάγκη να έχει πρόσβαση στα δεδομένα που πρόκειται να υποβληθούν σε επεξεργασία και σε οδηγίες, δηλαδή στο πρόγραμμα, που το ενημερώνει για τον τρόπο επεξεργασίας των δεδομένων. Και οι δύο αποθηκεύονται στη μνήμη PLC για πρόσβαση κατά τη διάρκεια της επεξεργασίας. Υπάρχουν πολλά στοιχεία μνήμης σε ένα σύστημα PLC:

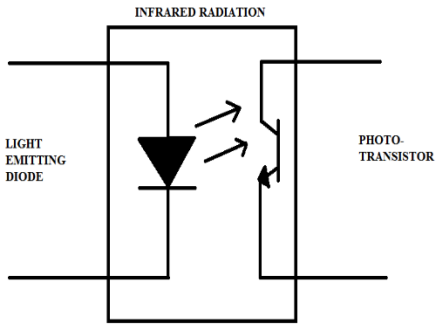
- Η μνήμη μόνο για ανάγνωση συστήματος (ROM) παρέχει μόνιμη αποθήκευση για το λειτουργικό σύστημα και σταθερά δεδομένα που χρησιμοποιεί η CPU.
- Η μνήμη τυχαίας προσπέλασης (RAM) χρησιμοποιείται για το πρόγραμμα του χρήστη.
- Η μνήμη τυχαίας προσπέλασης (RAM) χρησιμοποιείται για δεδομένα. Εδώ αποθηκεύονται πληροφορίες σχετικά με την κατάσταση των συσκευών εισόδου και εξόδου και τις τιμές των χρονομέτρων και των μετρητών και άλλων εσωτερικών συσκευών. Η μνήμη RAM αναφέρεται μερικές φορές ως πίνακας δεδομένων ή πίνακας μητρώου. Μέρος αυτής της μνήμης, δηλαδή ένα μπλοκ διευθύνσεων, θα διατεθεί για τις διευθύνσεις εισόδου και εξόδου και τις καταστάσεις αυτών των εισόδων και εξόδων. Μέρος θα διατεθεί για προκαθορισμένα δεδομένα και μέρος για αποθήκευση τιμών μετρητή, τιμές χρονοδιακόπτη και τα παρόμοια.

- Ενδεχομένως, ως πρόσθετη μονάδα, η διαγράψιμη και προγραμματιζόμενη μνήμη μόνο για ανάγνωση (EPROM) χρησιμοποιείται για την μόνιμη αποθήκευση προγραμμάτων. Τα προγράμματα και τα δεδομένα στη μνήμη RAM μπορούν να αλλάξουν από τον χρήστη. Όλα τα PLC θα έχουν κάποια ποσότητα μνήμης RAM για την αποθήκευση προγραμμάτων που έχουν αναπτυχθεί από τα δεδομένα χρήστη και προγράμματος. Ωστόσο, για να αποφευχθεί η απώλεια προγραμμάτων όταν η τροφοδοσία είναι απενεργοποιημένη, χρησιμοποιείται μια μπαταρία στο PLC για τη διατήρηση των περιεχομένων της RAM για ένα χρονικό διάστημα. Αφού αναπτυχθεί ένα πρόγραμμα στη μνήμη RAM, μπορεί να φορτωθεί σε ένα τσιπ μνήμης EPROM και έτσι να γίνει μόνιμη. Επιπλέον, υπάρχουν προσωρινά αποθέματα buffer για τα κανάλια εισόδου / εξόδου. Η χωρητικότητα αποθήκευσης μιας μονάδας μνήμης καθορίζεται από τον αριθμό των δυαδικών λέξεων που μπορεί να αποθηκεύσει. Έτσι, εάν ένα μέγεθος μνήμης είναι 256 λέξεις, μπορεί να αποθηκεύσει 256 _ 8 ¼ 2048 bit εάν χρησιμοποιούνται λέξεις 8-bit και 256 _ 16 ¼ 4096 bits εάν χρησιμοποιούνται λέξεις 16-bit. Τα μεγέθη μνήμης καθορίζονται συχνά ως προς τον αριθμό των διαθέσιμων θέσεων αποθήκευσης, με το 1K να αντιπροσωπεύει τον αριθμό 210, δηλαδή το 1024. Οι κατασκευαστές παρέχουν τσιπ μνήμης με τις θέσεις αποθήκευσης ομαδοποιημένες σε ομάδες 1, 4 και 8 bit. Μια μνήμη 4K _ 1 έχει 4 _ 1 _ 1024 bit τοποθεσίες. Η μνήμη 4K _ 8 έχει τοποθεσίες 4 _ 8 _ 1024 bit. Ο όρος byte χρησιμοποιείται για μια λέξη μήκους 8 bit. Έτσι, η μνήμη 4K _ 8 μπορεί να αποθηκεύσει 4096 byte. Με ένα δίαυλο διευθύνσεων 16-bit μπορούμε να έχουμε 216 διαφορετικές διευθύνσεις, και έτσι, με λέξεις 8-bit αποθηκευμένες σε κάθε διεύθυνση, μπορούμε να έχουμε 216 _ 8 θέσεις αποθήκευσης και έτσι να χρησιμοποιήσουμε μια μνήμη μεγέθους 216 _ 8/210 ¼ 64K _ 8, που μπορεί να έχει τη μορφή τεσσάρων τσιπ μνήμης 16K _ 8-bit.

6.7. Μονάδα εισόδου / εξόδου

Η μονάδα εισόδου / εξόδου παρέχει τη διασύνδεση μεταξύ του συστήματος και του εξωτερικού κόσμου, επιτρέποντας την πραγματοποίηση συνδέσεων μέσω καναλιών εισόδου / εξόδου σε συσκευές εισόδου όπως αισθητήρες και συσκευές εξόδου όπως κινητήρες και ηλεκτρομαγνητικές βαλβίδες. Μέσω της μονάδας εισόδου / εξόδου εισάγονται προγράμματα από έναν πίνακα προγραμμάτων. Κάθε σημείο εισόδου / εξόδου έχει μια μοναδική διεύθυνση που μπορεί να χρησιμοποιηθεί από την CPU. Είναι σαν μια σειρά σπιτιών κατά μήκος ενός δρόμου. Ο αριθμός 10 μπορεί να είναι το «σπίτι» που χρησιμοποιείται για μια είσοδο από έναν συγκεκριμένο αισθητήρα, ενώ ο αριθμός 45 μπορεί να είναι το «σπίτι» που χρησιμοποιείται για την έξοδο σε έναν συγκεκριμένο κινητήρα.

Τα κανάλια εισόδου / εξόδου παρέχουν λειτουργίες απομόνωσης και ρύθμισης σήματος έτσι ώστε οι αισθητήρες και οι ενεργοποιητές να μπορούν συχνά να συνδέονται απευθείας σε αυτά χωρίς την ανάγκη για άλλα κυκλώματα.



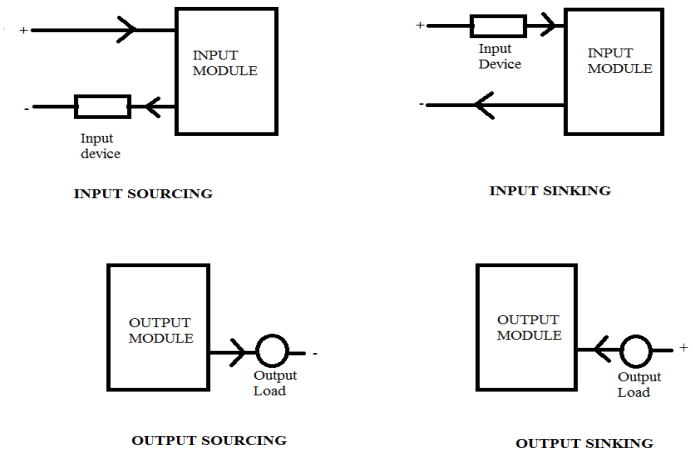
Σχήμα 17. Οπτοαπομονωτής (optoisolator)

Η ηλεκτρική απομόνωση από τον εξωτερικό κόσμο συνήθως γίνεται μέσω οπτοσυζευκτών. Το σχήμα δείχνει την αρχή ενός οπτοαπομονωτή. Όταν ένας ψηφιακός παλμός διέρχεται από τη δίοδο εκπομπής φωτός, παράγεται ένας παλμός υπέρυθρης ακτινοβολίας. Αυτός ο παλμός ανιχνεύεται από το φωτοτρανζίστορ και δημιουργεί τάση σε αυτό το κύκλωμα. Το χάσμα μεταξύ της διόδου εκπομπής φωτός και του φωτοτρανζίστορ δίνει ηλεκτρική απομόνωση, αλλά η διάταξη εξακολουθεί να επιτρέπει έναν ψηφιακό παλμό σε ένα κύκλωμα να δημιουργεί έναν ψηφιακό παλμό σε ένα άλλο κύκλωμα. Οι έξοδοι καθορίζονται ως τύπου ρελέ, τύπου τρανζίστορ ή τύπου triac:

- Με τον τύπο ρελέ, το σήμα από την έξοδο PLC χρησιμοποιείται για τη λειτουργία ενός ρελέ και είναι σε θέση να αλλάζει ρεύματα της τάξης μερικών αμπέρ σε ένα εξωτερικό κύκλωμα. Το ρελέ όχι μόνο επιτρέπει στα μικρά ρεύματα να αλλάζουν πολύ μεγαλύτερα ρεύματα, αλλά επίσης απομονώνει το PLC από το εξωτερικό κύκλωμα. Ωστόσο, τα ρελέ είναι σχετικά αργά στη λειτουργία. Οι έξοδοι ρελέ είναι κατάλληλες για εναλλαγή AC και DC. Μπορούν να αντέξουν σε υψηλά ρεύματα κύματος και μεταβατικά τάσης.
- Ο τύπος εξόδου τρανζίστορ χρησιμοποιεί ένα τρανζίστορ για εναλλαγή ρεύματος μέσω του εξωτερικού κυκλώματος. Αυτό δίνει μια πολύ ταχύτερη εναλλαγή δράσης. Ωστόσο, είναι αυστηρά για εναλλαγή DC και καταστρέφεται από υπέρταση και υψηλή αντίστροφη τάση. Για προστασία, χρησιμοποιείται ασφάλεια ή ενσωματωμένη ηλεκτρονική προστασία. Οι οπτοαπομονωτές χρησιμοποιούνται για την απομόνωση.
- Οι έξοδοι Triac, με οπτοαπομονωτές για απομόνωση, μπορούν να χρησιμοποιηθούν για τον έλεγχο εξωτερικών φορτίων που συνδέονται με το τροφοδοτικό AC. Είναι αυστηρά για λειτουργία AC και καταστρέφεται πολύ εύκολα από υπερβολικό ρεύμα. Οι ασφάλειες περιλαμβάνονται σχεδόν πάντα για την προστασία τέτοιων εξόδων.

6.8. Οι όροι Sourcing και Sinking

Οι όροι sourcing και sinking χρησιμοποιούνται για να περιγράψουν τον τρόπο με τον οποίο οι συσκευές DC συνδέονται σε PLC. Με την προμήθεια, χρησιμοποιώντας τη συμβατική κατεύθυνση ροής ρεύματος από θετική σε αρνητική, μια συσκευή εισόδου λαμβάνει ρεύμα από τη μονάδα εισόδου, δηλαδή, η μονάδα εισόδου είναι η πηγή του ρεύματος. Με το sinking, χρησιμοποιώντας τη συμβατική κατεύθυνση ροής ρεύματος, μια συσκευή εισόδου παρέχει ρεύμα στη μονάδα εισόδου, δηλαδή, η μονάδα εισόδου είναι η μετάβαση για το ρεύμα. Εάν το ρεύμα ρέει από τη μονάδα εξόδου σε ένα φορτίο εξόδου, η μονάδα εξόδου αναφέρεται ως προμήθεια. Εάν το ρεύμα ρέει στη μονάδα εξόδου από ένα φορτίο εξόδου, η μονάδα εξόδου αναφέρεται ως βύθιση.

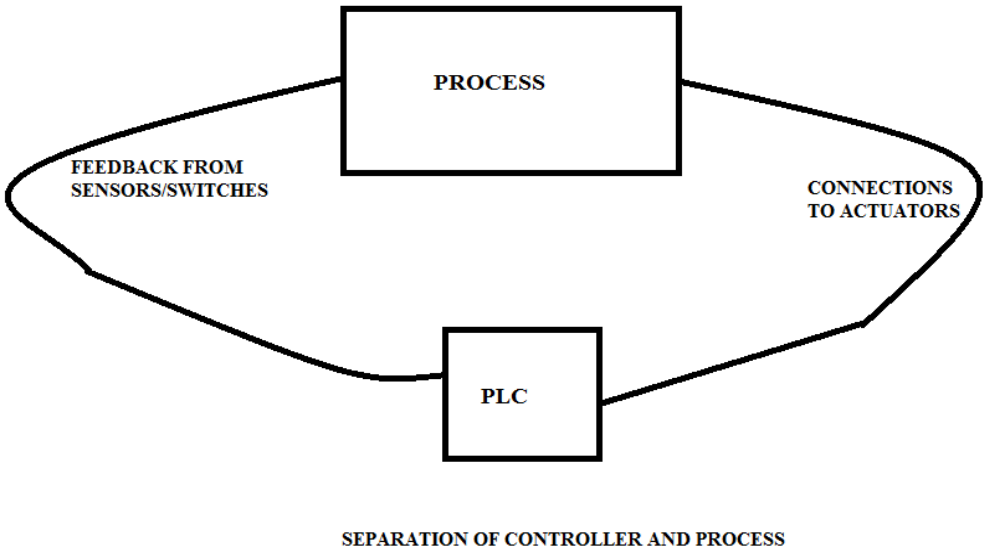


Σχήμα 18. Sourcing και sinking εισόδων/εξόδων

Είναι σημαντικό να γνωρίζουμε τον σχετικό τύπο εισόδου ή εξόδου, ώστε να μπορεί να συνδεθεί σωστά με το PLC. Έτσι, οι αισθητήρες με εξόδους προμήθειας πρέπει να συνδέονται με τις εισόδους PLC βύθισης και οι αισθητήρες με εξόδους βύθισης θα πρέπει να συνδέονται με τις εισόδους PLC προέλευσης. Η διεπαφή με το PLC δεν θα λειτουργεί και ενδέχεται να προκληθεί ζημιά εάν δεν ακολουθηθεί αυτή η οδηγία.

6.9. Συνδέσεις PLC

Όταν μια διαδικασία ελέγχεται από PLC, χρησιμοποιεί εισόδους από αισθητήρες για να λαμβάνει αποφάσεις και να ενημερώνει εξόδους για να οδηγεί ενεργοποιητές. Η διαδικασία είναι μια πραγματική διαδικασία που θα αλλάξει με την πάροδο του χρόνου. Οι ενεργοποιητές θα οδηγήσουν το σύστημα σε νέες καταστάσεις (ή τρόπους λειτουργίας). Αυτό σημαίνει ότι ο ελεγκτής περιορίζεται από τους διαθέσιμους αισθητήρες, εάν δεν υπάρχει διαθέσιμη είσοδος, ο ελεγκτής δεν θα έχει τρόπο να εντοπίσει μια κατάσταση.

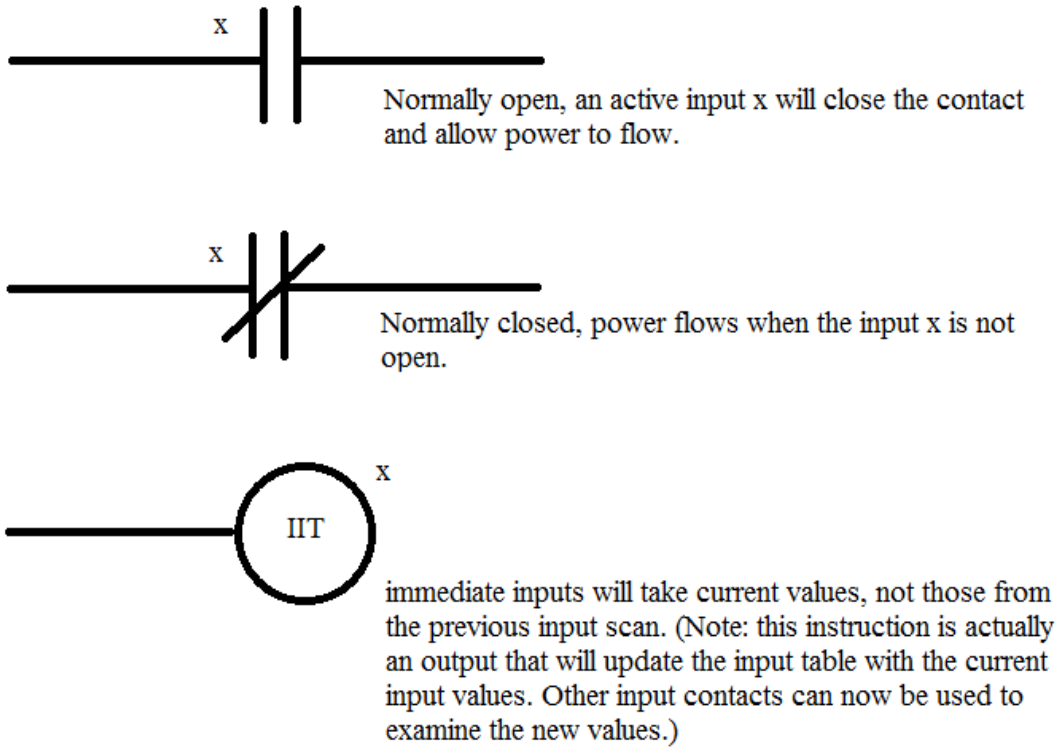


Σχήμα 19. Ο διαχωρισμός του ελεγκτή και της διαδικασίας

Ο βρόχος ελέγχου είναι ένας συνεχής κύκλος των εισόδων ανάγνωσης PLC, επίλυση της λογικής της σκάλας και μετά αλλαγή των εξόδων. Όπως κάθε υπολογιστής, αυτό δεν συμβαίνει άμεσα. Όταν η τροφοδοσία είναι ενεργοποιημένη αρχικά, το PLC κάνει έναν γρήγορο έλεγχο λογικής για να διασφαλίσει ότι το υλικό λειτουργεί σωστά. Εάν υπάρχει πρόβλημα, το PLC θα σταματήσει και θα δείξει ότι υπάρχει σφάλμα. Για παράδειγμα, εάν η εφεδρική μπαταρία PLC είναι χαμηλή και χάθηκε η ισχύς, η μνήμη θα είναι κατεστραμμένη και αυτό θα οδηγήσει σε σφάλμα. Εάν το PLC περάσει τον έλεγχο λογικής, τότε θα σαρώσει (διαβάσει) όλες τις εισόδους. Μετά την αποθήκευση των τιμών εισόδου στη μνήμη, η λογική της σκάλας θα σαρωθεί (επιλυθεί) χρησιμοποιώντας τις αποθηκευμένες τιμές - όχι τις τρέχουσες τιμές. Αυτό γίνεται για την αποφυγή προβλημάτων λογικής όταν αλλάζουν οι είσοδοι κατά τη σάρωση λογικής σκάλας. Όταν ολοκληρωθεί η σάρωση λογικής σκάλας, οι έξοδοι θα σαρωθούν (οι τιμές εξόδου θα αλλάξουν). Μετά από αυτό το σύστημα επιστρέφει για να κάνει έλεγχο λογικής και ο βρόχος συνεχίζεται επ' αόριστόν. Σε αντίθεση με τους κανονικούς υπολογιστές, ολόκληρο το πρόγραμμα θα εκτελείται σε κάθε σάρωση. Οι τυπικοί χρόνοι για κάθε ένα από τα στάδια είναι της τάξης των χιλιοστών του δευτερολέπτου.

6.10. Είσοδοι λογικής σκάλας

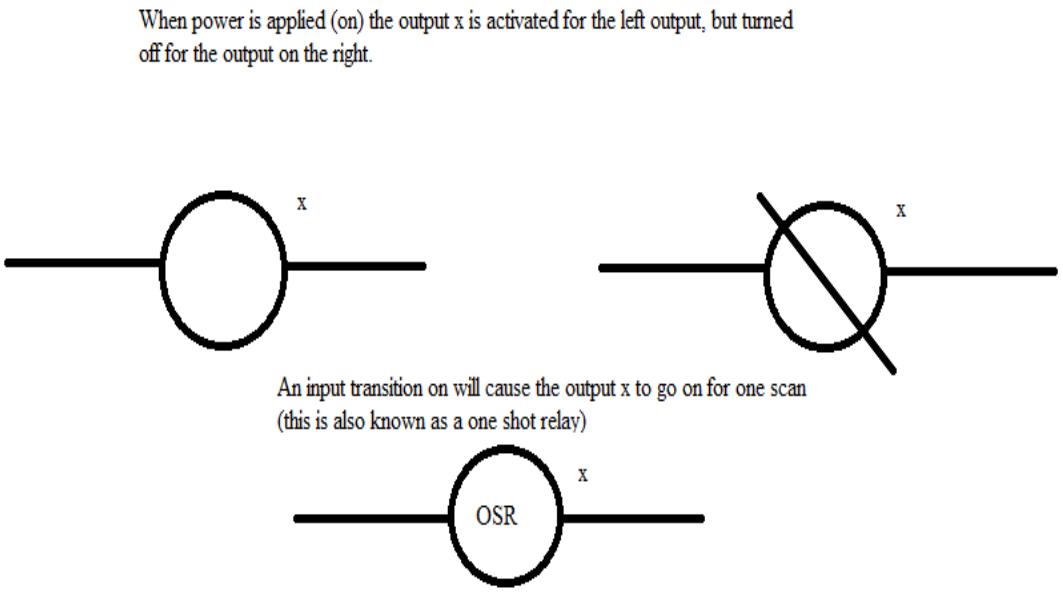
Οι είσοδοι PLC απεικονίζονται εύκολα στη λογική της σκάλας. Εμφανίζονται οι τρεις τύποι εισόδων. Οι δύο πρώτες είναι συνήθως ανοικτές και κανονικά κλειστές εισόδους, που συζητήθηκαν προηγουμένως. Η λειτουργία IIT (Άμεση είσοδος) επιτρέπει την ανάγνωση των εισόδων μετά τη σάρωση εισόδου, ενώ η λογική της σκάλας γίνεται σάρωση. Αυτό επιτρέπει στη λογική της σκάλας να εξετάζει τις τιμές εισόδου συχνότερα από μία φορά σε κάθε κύκλο.



Σχήμα 20. Σύμβολα

6.11. Έξοδος λογικής σκάλας

Στη λογική της κλίμακας υπάρχουν πολλοί τύποι εξόδων, αλλά δεν διατίθενται με συνέπεια σε όλα τα PLC. Ορισμένες από τις εξόδους θα συνδεθούν εξωτερικά με συσκευές εκτός του PLC, αλλά είναι επίσης δυνατή η χρήση τοποθεσιών εσωτερικής μνήμης στο PLC. Η πρώτη είναι μια κανονική έξοδος, όταν ενεργοποιείται η έξοδος θα ενεργοποιηθεί και ενεργοποιεί μια έξοδο. Ο κύκλος με διαγώνια γραμμή είναι κανονικά στην έξοδο. Όταν ενεργοποιηθεί η έξοδος θα απενεργοποιηθεί. Αυτός ο τύπος εξόδου δεν είναι διαθέσιμος σε όλους τους τύπους PLC. Όταν ενεργοποιηθεί αρχικά, η εντολή OSR (One Shot Relay) θα ενεργοποιηθεί για μία σάρωση, αλλά στη συνέχεια θα απενεργοποιηθεί για όλες τις σαρώσεις μετά, έως ότου απενεργοποιηθεί. Οι οδηγίες L (σύρτης) και U (απεμπλοκή) μπορούν να χρησιμοποιηθούν για το κλείδωμα των εξόδων. Όταν μια έξοδος L ενεργοποιείται, η έξοδος θα ενεργοποιηθεί επ' αόριστόν, ακόμη και όταν το πηνίο εξόδου απενεργοποιείται. Η έξοδος μπορεί να απενεργοποιηθεί μόνο χρησιμοποιώντας έξοδο U. Η τελευταία οδηγία είναι το IOT (Άμεση έξοδος) που θα επιτρέπει την ενημέρωση των εξόδων χωρίς να χρειάζεται να περιμένετε να ολοκληρωθεί η σάρωση λογικής σκάλας.



Σχήμα 21. Σύμβολα εξόδου

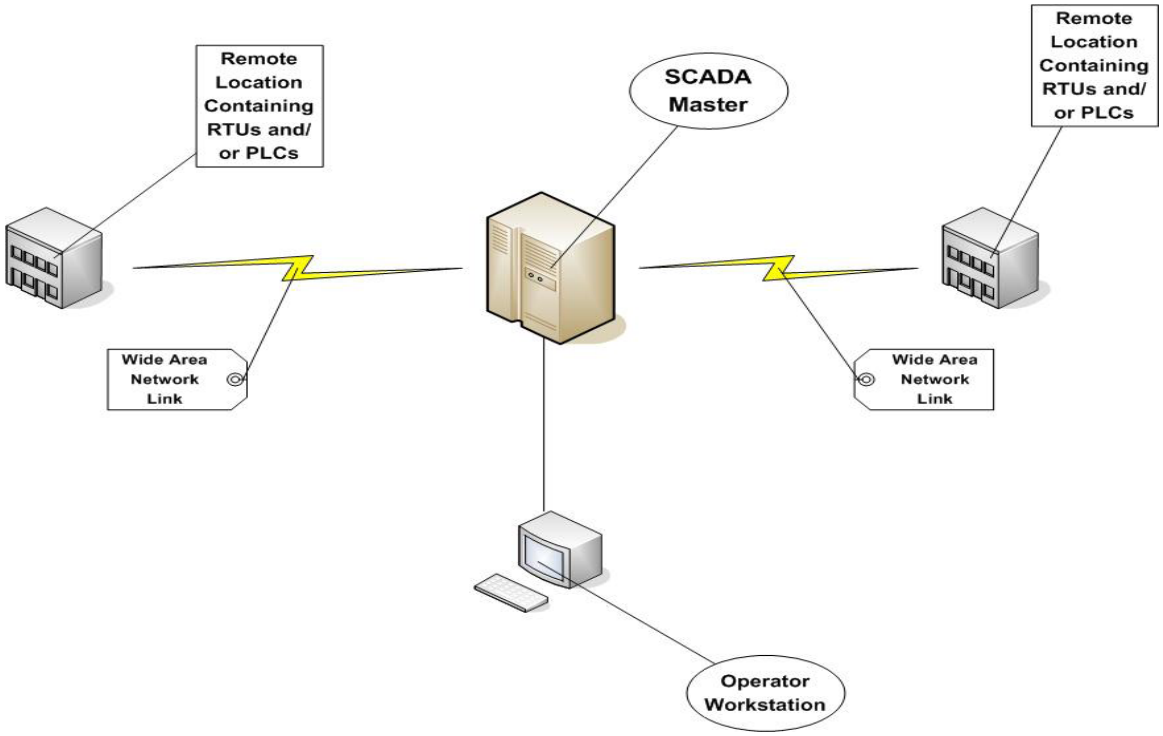
Οι έξοδοι εμφανίζονται επίσης συνήθως χρησιμοποιώντας παρενθέσεις - () - αντί για τον κύκλο. Αυτό συμβαίνει επειδή πολλά από τα συστήματα προγραμματισμού βασίζονται σε κείμενο και δεν μπορούν να σχεδιαστούν κύκλοι.

6.12. SCADA

Το SCADA είναι ένα αρκτικόλεξο για τον εποπτικό έλεγχο και την απόκτηση δεδομένων. Τα συστήματα SCADA χρησιμοποιούνται για την παρακολούθηση και τον έλεγχο μιας εγκατάστασης ή εξοπλισμού σε βιομηχανίες όπως τηλεπικοινωνίες, έλεγχος νερού και αποβλήτων, ενέργεια, διύλιση πετρελαίου και φυσικού αερίου και μεταφορά. Αυτά τα συστήματα περιλαμβάνουν τη μεταφορά δεδομένων μεταξύ ενός κεντρικού υπολογιστή SCADA και ενός αριθμού απομακρυσμένων τερματικών μονάδων (RTU) και / ή προγραμματιζόμενων ελεγκτών λογικής (PLC), και του κεντρικού κεντρικού υπολογιστή και των τερματικών χειριστή. Ένα σύστημα SCADA συλλέγει πληροφορίες (όπως όταν έχει σημειωθεί διαρροή σε αγωγό), μεταφέρει τις πληροφορίες πίσω σε μια κεντρική τοποθεσία και στη συνέχεια, ειδοποιεί τον οικιακό σταθμό ότι έχει προκύψει διαρροή, πραγματοποιώντας την απαραίτητη ανάλυση και έλεγχο, όπως προσδιορισμός εάν η διαρροή είναι κρίσιμη και η προβολή των πληροφοριών με λογικό και οργανωμένο τρόπο. Αυτά τα συστήματα μπορεί να είναι σχετικά απλά, όπως αυτά που παρακολουθούν τις περιβαλλοντικές συνθήκες ενός μικρού κτιρίου γραφείων ή πολύ περίπλοκα, όπως ένα σύστημα που παρακολουθεί όλη τη δραστηριότητα σε πυρηνική μονάδα παραγωγής ενέργειας ή τη δραστηριότητα ενός δημοτικού συστήματος νερού. Παραδοσιακά, τα συστήματα SCADA έχουν χρησιμοποιήσει το δημόσιο δίκτυο μεταγωγής (PSN) για σκοπούς παρακολούθησης. Σήμερα πολλά συστήματα παρακολουθούνται χρησιμοποιώντας την υποδομή του εταιρικού τοπικού δικτύου (LAN) / Wide Area Network (WAN). Οι ασύρματες τεχνολογίες αναπτύσσονται ευρέως για σκοπούς παρακολούθησης.

Τα συστήματα SCADA αποτελούνται από:

- Μία ή περισσότερες συσκευές διεπαφής δεδομένων πεδίου, συνήθως RTU ή PLC, οι οποίες διασυνδέονται με συσκευές ανίχνευσης πεδίου και τοπικούς διακόπτες ελέγχου και ενεργοποιητές βαλβίδας
- Ένα σύστημα επικοινωνίας που χρησιμοποιείται για τη μεταφορά δεδομένων μεταξύ συσκευών διεπαφής δεδομένων πεδίου και μονάδων ελέγχου και των υπολογιστών στον κεντρικό κεντρικό υπολογιστή SCADA. Το σύστημα μπορεί να είναι ραδιόφωνο, τηλέφωνο, καλώδιο, δορυφόρος κ.λπ. ή οποιοσδήποτε συνδυασμός αυτών.
- Κεντρικός κεντρικός διακομιστής ή διακομιστές υπολογιστών (μερικές φορές ονομάζεται SCADA Center, master station ή Master Terminal Unit (MTU)
- Μια συλλογή από τυπικά ή / και προσαρμοσμένα λογισμικά [μερικές φορές ονομάζονται λογισμικό Human Machine Interface (HMI) ή Man Machine Interface (MMI)] συστήματα που χρησιμοποιούνται για την παροχή της κεντρικής εφαρμογής κεντρικού υπολογιστή και του τερματικού χειριστή SCADA, την υποστήριξη του συστήματος επικοινωνιών και την παρακολούθηση και ελέγξτε τις συσκευές διεπαφής δεδομένων πεδίου από απόσταση.



Σχήμα 22. Δικτύωση SCADA

6.12.1. Τύποι του SCADA

1. D+R+N (Development +Run + Networking)
2. R+N (Run +Networking)
3. Factory focus

6.12.2. Στοιχεία του SCADA

1. Δυναμική διαδικασία Γραφικό
2. Καλοκαίρι συναγερμού

3. Ιστορικό συναγερμών
4. Τάση σε πραγματικό χρόνο
5. Ιστορική χρονική τάση
6. Ασφάλεια (Ασφάλεια εφαρμογών)
7. Συνδεσιμότητα βάσης δεδομένων
8. Συνδεσιμότητα συσκευών
9. Σενάρια
10. Διαχείριση συνταγών

6.12.3. Κατασκευή του SCADA

Modicon (Telemecanique): Visual look

Allen Bradley: RS View

Siemens: win cc

KPIT: ASTRA

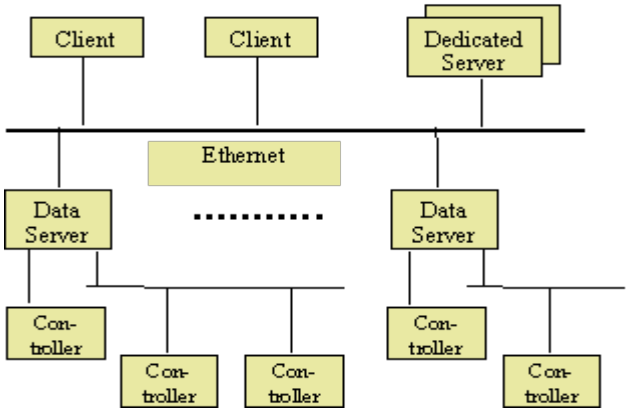
Intelution: Aspic

Wonderware: In touch

6.12.4. Αρχιτεκτονική

Αρχιτεκτονική υλικού:

Μπορεί κανείς να διακρίνει δύο βασικά επίπεδα σε ένα σύστημα SCADA: το "επίπεδο πελάτη" που εξυπηρετεί την αλληλεπίδραση ανθρώπου-μηχανής και το "επίπεδο διακομιστή δεδομένων" που χειρίζεται τις περισσότερες από τις δραστηριότητες ελέγχου δεδομένων διεργασίας. Οι διακομιστές δεδομένων επικοινωνούν με συσκευές στο πεδίο μέσω ελεγκτών διεργασιών. Ελεγκτές διαδικασίας, π.χ. Τα PLC συνδέονται στους διακομιστές δεδομένων είτε απευθείας είτε μέσω δικτύων ή διαύλων πεδίου που είναι ιδιόκτητα (π.χ. Siemens H1) ή μη ιδιοκτησίας (π.χ. Profibus). Οι διακομιστές δεδομένων συνδέονται μεταξύ τους και σε σταθμούς πελατών μέσω ενός Ethernet LAN. Οι διακομιστές δεδομένων και οι σταθμοί πελατών είναι πλατφόρμες NT, αλλά για πολλά προϊόντα οι σταθμοί πελατών μπορεί επίσης να είναι μηχανές W95.



Σχήμα 23. Τυπική αρχιτεκτονική υλικού

Αρχιτεκτονική λογισμικού:

Τα προϊόντα είναι πολλαπλών εργασιών και βασίζονται σε βάση δεδομένων σε πραγματικό χρόνο (RTDB) που βρίσκεται σε έναν ή περισσότερους διακομιστές. Οι διακομιστές είναι υπεύθυνοι για την απόκτηση και τον χειρισμό δεδομένων (π.χ. ελεγκτές δημοσκόπησης, έλεγχος συναγερμών, υπολογισμοί, καταγραφή και αρχειοθέτηση) σε ένα σύνολο παραμέτρων, συνήθως σε αυτές με τις

οποίες συνδέονται. Ωστόσο, είναι δυνατό να υπάρχουν αποκλειστικοί διακομιστές για συγκεκριμένες εργασίες, π.χ. ιστορικός, καταγραφέας δεδομένων, χειριστής συναγερμών.

6.12.5. Επικοινωνία

Εσωτερική επικοινωνία:

Η επικοινωνία μεταξύ διακομιστή-πελάτη και διακομιστή-διακομιστή γίνεται γενικά σε βάση δημοσίευσης-εγγραφής και βάσει συμβάντων και χρησιμοποιεί πρωτόκολλο TCP / IP, δηλαδή, μια εφαρμογή πελάτη εγγράφεται σε μια παράμετρο που ανήκει σε μια συγκεκριμένη εφαρμογή διακομιστή και αλλάζει μόνο όταν αυτή η παράμετρος κοινοποιείται στην εφαρμογή πελάτη.

Πρόσβαση σε συσκευές:

Οι διακομιστές δεδομένων πραγματοποιούν δημοσκοπήσεις στους ελεγκτές με ρυθμό ψηφοφορίας που καθορίζεται από τον χρήστη. Το ποσοστό ψηφοφορίας μπορεί να διαφέρει για διαφορετικές παραμέτρους. Οι ελεγκτές μεταβιβάζουν τις απαιτούμενες παραμέτρους στους διακομιστές δεδομένων. Η χρονική σήμανση των παραμέτρων της διαδικασίας πραγματοποιείται συνήθως στους ελεγκτές και αυτή η χρονική σήμανση αναλαμβάνεται από τον διακομιστή δεδομένων. Εάν το ελεγκτή και το πρωτόκολλο επικοινωνίας που χρησιμοποιούνται υποστηρίζουν ανεπιθύμητη μεταφορά δεδομένων, τότε τα προϊόντα θα το υποστηρίξουν επίσης. Τα προϊόντα παρέχουν προγράμματα οδήγησης επικοινωνίας για τα περισσότερα από τα κοινά PLC και ευρέως χρησιμοποιούμενα λεωφορεία πεδίου, π.χ. Modbus. Από τα τρία λεωφορεία πεδίου που συνιστώνται στο CERN, υποστηρίζονται τόσο το Profibus όσο και το Worldfip, αλλά το CANbus συχνά όχι. Ορισμένα από τα προγράμματα οδήγησης βασίζονται σε προϊόντα τρίτων (π.χ. κάρτες Applicom) και συνεπώς έχουν επιπλέον κόστος που σχετίζεται με αυτά. Ένας μεμονωμένος διακομιστής δεδομένων μπορεί να υποστηρίζει πολλαπλά πρωτόκολλα επικοινωνίας: μπορεί γενικά να υποστηρίζει τόσα πρωτόκολλα όσο διαθέτει υποδοχές για κάρτες διασύνδεσης. Η προσπάθεια που απαιτείται για την ανάπτυξη νέων προγραμμάτων οδήγησης συνήθως κυμαίνεται από 2-6 εβδομάδες ανάλογα με την πολυπλοκότητα και την ομοιότητα με τα υπάρχοντα προγράμματα οδήγησης, και παρέχεται μια εργαλειοθήκη ανάπτυξης προγραμμάτων οδήγησης.

Διασύνδεση:

Διεπαφές εφαρμογών / άνοιγμα:

Αναπτύσσεται η παροχή λειτουργικότητας πελάτη OPC για την πρόσβαση SCADA σε συσκευές με ανοιχτό και τυπικό τρόπο. Φαίνεται ακόμη ότι υπάρχει έλλειψη συσκευών / ελεγκτών, που παρέχουν λογισμικό διακομιστή OPC, αλλά αυτό βελτιώνεται γρήγορα καθώς οι περισσότεροι παραγωγοί ελεγκτών συμμετέχουν ενεργά στην ανάπτυξη αυτού του προτύπου. Τα προϊόντα παρέχουν επίσης:

- Μια διασύνδεση ανοιχτής βάσης δεδομένων (ODBC) με τα δεδομένα στο αρχείο / αρχεία καταγραφής, αλλά όχι στη βάση δεδομένων διαμόρφωσης.
- Μια εγκατάσταση εισαγωγής / εξαγωγής ASCII για δεδομένα διαμόρφωσης.
- Μια βιβλιοθήκη API που υποστηρίζει C, C ++ και Visual Basic (VB) για πρόσβαση σε δεδομένα στα αρχεία καταγραφής και αρχείο RTDB. Το API συχνά δεν παρέχει πρόσβαση στις εσωτερικές λειτουργίες του προϊόντος, όπως χειρισμός συναγερμών, αναφορές, τάσεις κ.λπ. Τα προϊόντα υπολογιστή παρέχουν υποστήριξη για τα πρότυπα της Microsoft, όπως το Dynamic Data Exchange (DDE) που επιτρέπει π.χ. για να οπτικοποιήσουμε δυναμικά δεδομένα σε υπολογιστικό φύλλο EXCEL, Dynamic Link Library (DLL) και Object Linking and Embedding (OLE).

Βάση δεδομένων:

Τα δεδομένα διαμόρφωσης αποθηκεύονται σε μια βάση δεδομένων η οποία είναι λογικά συγκεντρωτική αλλά διανέμεται φυσικά και είναι γενικά ιδιόκτητης μορφής.

Σύστημα (RDBMS) με πιο αργό ρυθμό είτε απευθείας είτε μέσω διασύνδεσης ODBC.

Επεκτασιμότητα:

Η επεκτασιμότητα θεωρείται ως η δυνατότητα επέκτασης του συστήματος ελέγχου με βάση το SCADA προσθέτοντας περισσότερες μεταβλητές διεργασίας, πιο εξειδικευμένους διακομιστές (π.χ. για χειρισμό συναγερμών) ή περισσότερους πελάτες. Τα προϊόντα επιτυγχάνουν επεκτασιμότητα συνδέοντας πολλούς διακομιστές δεδομένων σε πολλούς ελεγκτές. Κάθε διακομιστής δεδομένων έχει τη δική του βάση δεδομένων διαμόρφωσης και RTDB και είναι υπεύθυνος για τον χειρισμό ενός υποσυνόλου των μεταβλητών διεργασίας (απόκτηση, διαχείριση συναγερμών, αρχειοθέτηση).

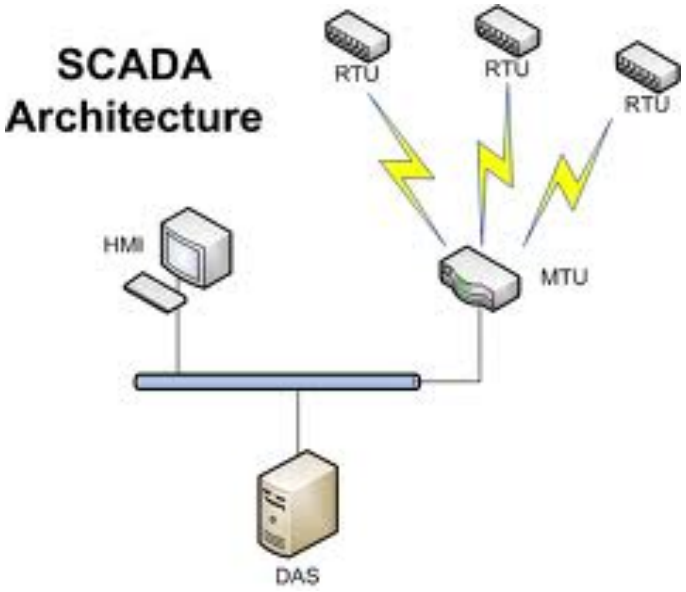
Πλεονασμός:

Τα προϊόντα έχουν συχνά ενσωματωμένο πλεονασμό λογισμικού σε επίπεδο διακομιστή, το οποίο είναι συνήθως διαφανές για τον χρήστη. Πολλά από τα προϊόντα παρέχουν επίσης πιο ολοκληρωμένες λύσεις απολύσεων, εάν απαιτείται.

6.12.6. Υποσύστημα SCADA

Ένα σύστημα SCADA αποτελείται συνήθως από τα ακόλουθα υποσυστήματα:

- Interface διεπαφή ανθρώπου-μηχανής ή HMI που παρουσιάζει δεδομένα διεργασίας σε ανθρώπινο χειριστή που παρακολουθεί και ελέγχει τη διαδικασία.
- Ένα σύστημα εποπτείας (υπολογιστή) για τη συλλογή δεδομένων σχετικά με τη διαδικασία και την αποστολή εντολών στη διαδικασία.
- Απομακρυσμένες τερματικές μονάδες (RTU) που συνδέονται με αισθητήρες κατά τη διαδικασία, μετατροπή σημάτων αισθητήρα σε ψηφιακά δεδομένα και αποστολή ψηφιακών δεδομένων στο εποπτικό σύστημα.
- Προγραμματιζόμενος λογικός ελεγκτής (PLC) που χρησιμοποιείται ως συσκευές πεδίου επειδή είναι πιο οικονομικοί, ευέλικτοι, ευέλικτοι και διαμορφώσιμοι.
- Infrastructure Υποδομή επικοινωνίας που συνδέει το εποπτικό σύστημα με τις απομακρυσμένες τερματικές μονάδες.



Σχήμα 24. Στοιχεία του SCADA

6.11.7. Πιθανά οφέλη του SCADA

Τα οφέλη που μπορεί κανείς να αναμένει από την υιοθέτηση ενός συστήματος SCADA για τον έλεγχο των πειραματικών εγκαταστάσεων φυσικής μπορεί να συνοψιστεί ως εξής:

- Πλούσια λειτουργικότητα και εκτεταμένες εγκαταστάσεις ανάπτυξης. Το ποσό της προσπάθειας που επενδύεται στο προϊόν SCADA ανέρχεται σε 50 έως 100 χρόνια.
- Το ποσό της συγκεκριμένης ανάπτυξης που πρέπει να εκτελεστεί από τον τελικό χρήστη είναι περιορισμένο, ειδικά με κατάλληλη τεχνική.
- Αξιοπιστία και ανθεκτικότητα. Αυτά τα συστήματα χρησιμοποιούνται για κρίσιμες βιομηχανικές διαδικασίες αποστολών όπου η αξιοπιστία και η απόδοση είναι υψίστης σημασίας. Επιπλέον, η συγκεκριμένη ανάπτυξη πραγματοποιείται σε ένα καλά εδραιωμένο πλαίσιο που ενισχύει την αξιοπιστία και την ανθεκτικότητα.
- Τεχνική υποστήριξη και συντήρηση από τον πωλητή.

ΚΕΦΑΛΑΙΟ 7 – ΔΙΑΔΙΚΑΣΙΕΣ ΕΦΑΡΜΟΓΗΣ

7.1. Περιγραφή μηχανής

Η περιστροφική καρτονέτα διαστάσεων 1.500*2.000*2.200, περιλαμβάνεται από σκελετό με ανοδιωμένο αλουμίνιο βαρέως τύπου στο κάτω μέρος και κουβούκλιο ασφαλείας στο επάνω με πολυκαρμπονικά τζάμια και πόρτες. Στο κέντρο της υπάρχει ένας δίσκος, διπλός δώδεκα (12) θέσεων, κινούμενος με μηχανικό διαιρέτη ακριβείας, με ρυθμίσεις όσον αφορά το ύψος του για να διαχειρίζεται διάφορα μεγέθη κουτιών.

Περιγραφή Λειτουργίας:

1. Υπάρχει τροφοδότης κουτιών όπου τοποθετούνται τα κουτιά flat από τον χειριστή και από εκεί τα παραλαμβάνει ένας πνευματικός μηχανισμός με κενό αέρος, τα αναπτύσσει και τα τοποθετεί στον κεντρικό δίσκο με τις μήτρες.

2. Περιστρέφονται βηματικά όπου κατ' αρχήν κλείνονται τα πλαϊνά κάτω FLAPS του κουτιού και στην στάση γίνεται το τελικό κλείσιμο του κουτιού στην κάτω μεριά. Ενδιάμεσα του πρώτου και του δεύτερου σταθμού πριν από το κλείσιμο των κάτω flaps θα τοποθετηθεί εκτυπωτικό.

3. Στην επόμενη θέση γίνεται η τοποθέτηση της οδηγίας με ρυθμιζόμενο τροφοδότη, αποτελούμενο από stacker τοποθέτησης προ διπλωμένης οδηγίας από τον χειριστή και πνευματικό μηχανισμό με κενό αέρος για την παραλαβή των οδηγιών από το stacker και την ορθή τοποθέτηση τους μέσα στα κουτιά.

4. Προχωρώντας γίνεται η τοποθέτηση του φιαλιδίου μέσα στο κουτί με αυτόματο τροφοδότη, ρυθμιζόμενο ως προς το ύψος και το φάρδος για διάφορα μεγέθη φιαλιδίων, αποτελούμενο από μεταφορική ταινία και μηχανισμό τοποθέτησης φιαλιδίων σε κουτί με πνευματικό μηχανισμό.

5. Κατόπιν της πλήρωσης των κουτιών και με φιαλίδια κλείνονται τα πλαϊνά πάνω FLAPS του κουτιού και στην επόμενη περιστροφή γίνεται το τελικό κλείσιμο του κουτιού στην πάνω μεριά.

6. Έπειτα, το κουτί εξέρχεται έτοιμο από την μηχανή.

7.2. Talk2M

Ο οίκος HMS έχει αναπτύξει, από το 2006, ένα IIoT Cloud για απομακρυσμένη διασύνδεση των προϊόντων της. Αποτελεί στην ουσία μια υπηρεσία και λειτουργεί σαν μια γέφυρα που εκμηδενίζει την απόσταση μεταξύ των μηχανών ενός εργοστασίου με τους υπολογιστές, τα κινητά και γενικότερα τα συστήματα απεικόνισης που βρίσκονται σε διάφορα σημεία του πλανήτη.

Το Talk2m είναι διαθέσιμο σε 2 εκδόσεις:

1. Talk2M Free+, ο χρήστης έχει δωρεάν πρόσβαση στο Cloud με την αγορά ενός Ewon.

2. Talk2M Pro, ο χρήστης οφείλει να πληρώνει μια ετήσια συνδρομή για να απολαμβάνει τις υπηρεσίες του.

Υπάρχουν παγκοσμίως servers σε αναμονή ώστε οι υπηρεσίες που προσφέρει το Talk2M να είναι πάντα διαθέσιμες, πιστοποιήσεις ISO καθώς και VPN κανάλια για την ασφαλή μετάδοση των δεδομένων. Υπάρχει η ευελιξία δημιουργίας group χρηστών δίνοντας διαφορετικά δικαιώματα στον καθένα. Για να συνδεθεί ο χρήστης χρησιμοποιεί το προσωπικό user name και κωδικό του. Σε περίπτωση που είναι επιθυμητό, γίνεται και ταυτοποίηση δύο παραγόντων μέσω του προσωπικού τηλεφώνου του χρήστη που ανήκει ο λογαριασμός. Για επιπλέον ασφάλεια, μπορεί να τοποθετηθεί εξωτερικός διακόπτης όπου θα ελέγχει χειροκίνητα την είσοδο ενός χρήστη στο λογαριασμό που απευθύνεται το εκάστοτε Ewon. Αξιοσημείωτο είναι το γεγονός πως οι συνδέσεις αποθηκεύονται λεπτομερώς ώστε να είναι γνωστό το πότε, ποιος και για πόσο έμεινε συνδεδεμένος ένας χρήστης.

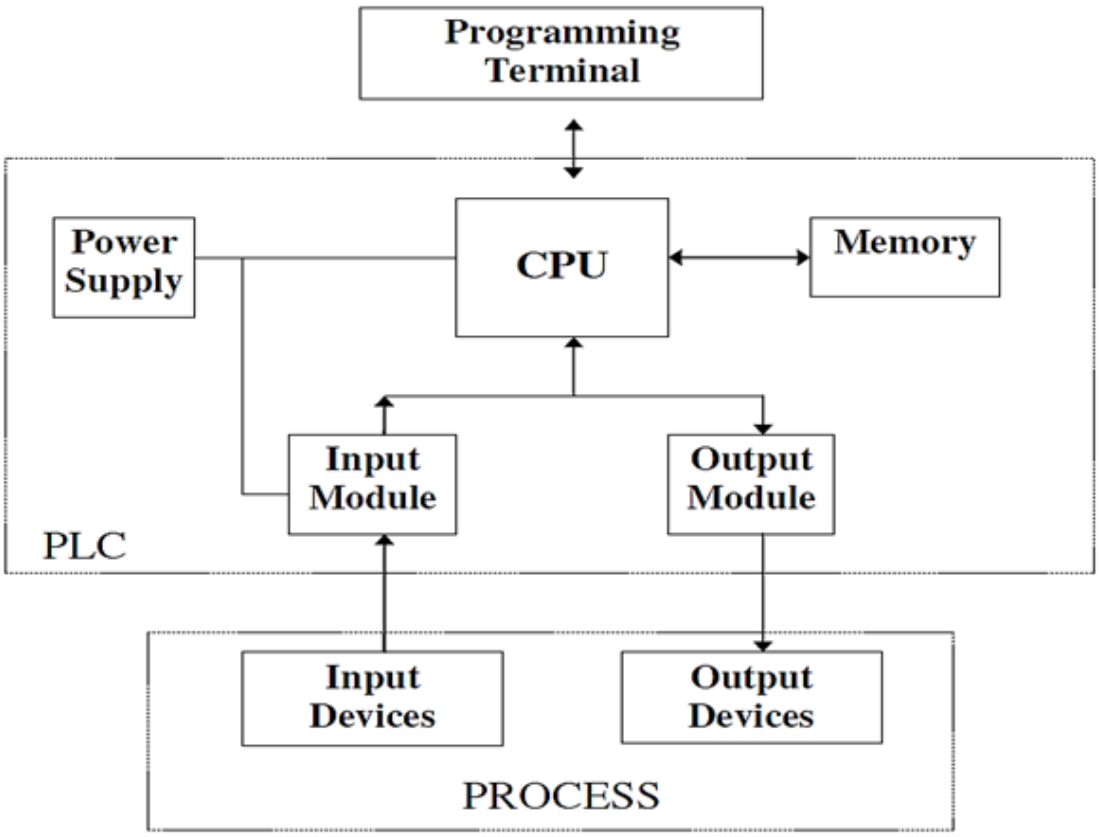
Το Talk2M προσφέρει επίσης και την υπηρεσία DataMailbox, όπου γίνεται αποθήκευση δεδομένων χωρίς να υπάρχει ο κίνδυνος διπλοεγγραφής. Με την συγκεκριμένη υπηρεσία του Talk2M,

διαφορετικές πλατφόρμες μπορούν να αντλήσουν αποθηκευμένα αρχεία μέσω του HTTPS πρωτοκόλλου.

7.3. PLC

Μια επιπλέον υπηρεσία που προσφέρεται από το Cloud του οίκου HMS είναι το M2web το οποίο προσφέρει ασφαλή πρόσβαση από ένα web browser στις απομακρυσμένες συσκευές. Συσκευές όπως HMIs, IP Cameras και οποιοδήποτε άλλο Web Server. Επιτρέπει επίσης την απεικόνιση μέχρι και έξη KPIs της μηχανής για άμεση παρακολούθηση, όποτε και όπου είναι αναγκαίο.

Στην περιστροφική καρτονέτα όλες οι αυτοματοποιημένες διεργασίες εκτελούνται από μία κεντρική μονάδα ελέγχου, το PLC (Programmable Logic Controller ή Προγραμματιζόμενος Λογικός Ελεγκτής). Οι κύριοι στόχοι μιας αυτοματοποιημένης μονάδας είναι να εξασφαλίζεται η ασφάλεια στο περιβάλλον που εκτελούνται οι εργασίες, να αυξάνεται η παραγωγή μειώνοντας το κόστος λειτουργίας και να βελτιώνεται η ποιότητα του εξαγομένου υλικού. Παλαιότερα, για να πραγματοποιηθούν όλα τα παραπάνω χρησιμοποιούνταν οι κλασσικές εγκαταστάσεις αυτοματισμού που αποτελούνταν από τεράστιες σειρές με πολυάριθμα Ρελέ (Relay ή Ηλεκτρονόμος) και επαφές. Πλέον έχουν αντικατασταθεί με τα PLC που απαρτίζονται από τουλάχιστον μία κεντρική μονάδα επεξεργασίας, μία μονάδα τροφοδοσίας, μία μονάδα μνήμης και τις ψηφιακές ή αναλογικές εισόδους και εξόδους.

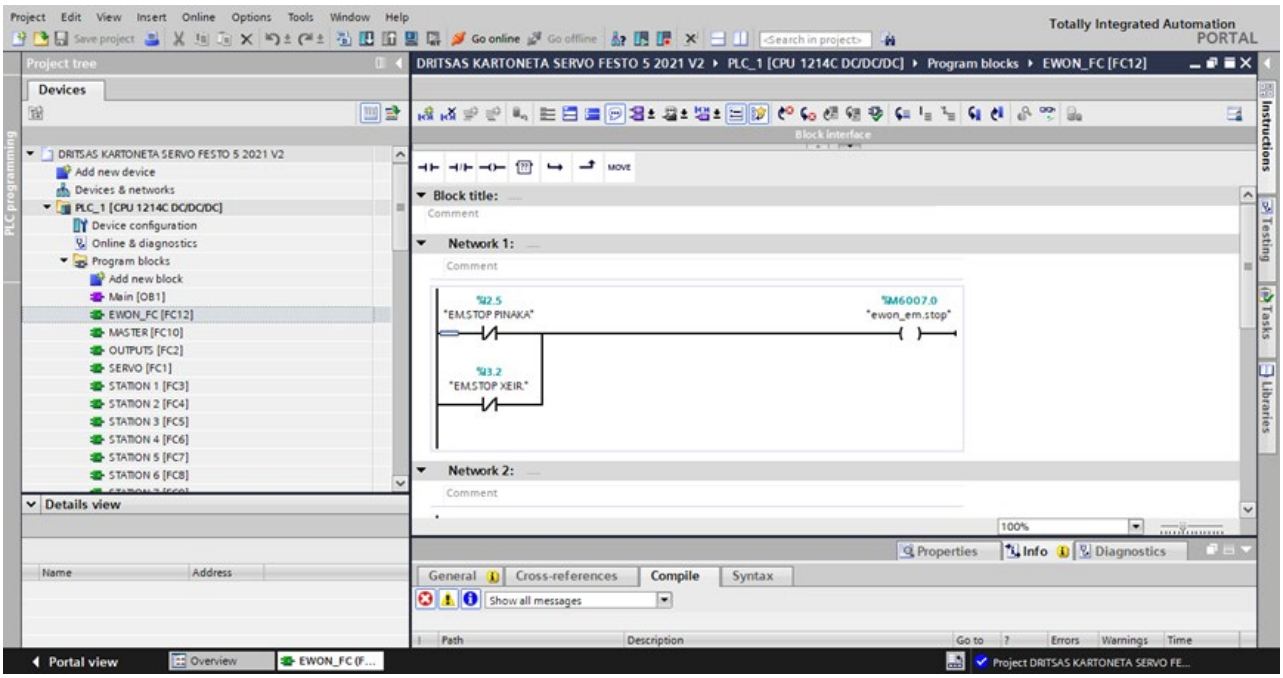


Σχήμα 25. Σχεδιάγραμμα PLC με I/O.

Στην παρούσα μηχανή χρησιμοποιήθηκε το PLC SIMATIC S7 1200 του γερμανικού οίκου Siemens. Το συγκεκριμένο προϊόν αποτελεί μία έξυπνη επιλογή με ενσωματωμένα I/O, θύρες επικοινωνίας και είναι πλήρως επεκτάσιμο με επιπλέον κάρτες I/O. Πιο συγκεκριμένα, στον ηλεκτρολογικό πίνακα

χρησιμοποιήθηκε η CPU 1214C και δύο κάρτες I/O που η κάθε μία διαθέτει 16 ψηφιακές εισόδους και 16 ψηφιακές εξόδους 24VDC/0.5A. Διαθέτει 50 kbyte μνήμη για τα δεδομένα του χρήστη και Load memory 2 Mbyte με δυνατότητα επέκτασης στα 24 Mbyte με την SIMATIC memory card. Επεξεργαστική ισχύ στα 0.1 μs για bit λειτουργίες, 12 μs για word λειτουργίες και 18 μs για floating αριθμητικές λειτουργίες.

Οι συγκεκριμένοι ελεγκτές προγραμματίζονται μέσω της πλατφόρμας του οίκου Siemens που ονομάζεται TIA PORTAL. Η συγκεκριμένη πλατφόρμα είναι διαμορφωμένη με τέτοιο τρόπο ώστε να διευκολύνει το χρήστη με την ανάλυση και τον εντοπισμό των τυχών σφαλμάτων. Επίσης πολύ σημαντικός παράγοντας αποτελεί το γεγονός ότι την ίδια πλατφόρμα την χρησιμοποιούμε για να προγραμματίσουμε την οθόνη (HMI).

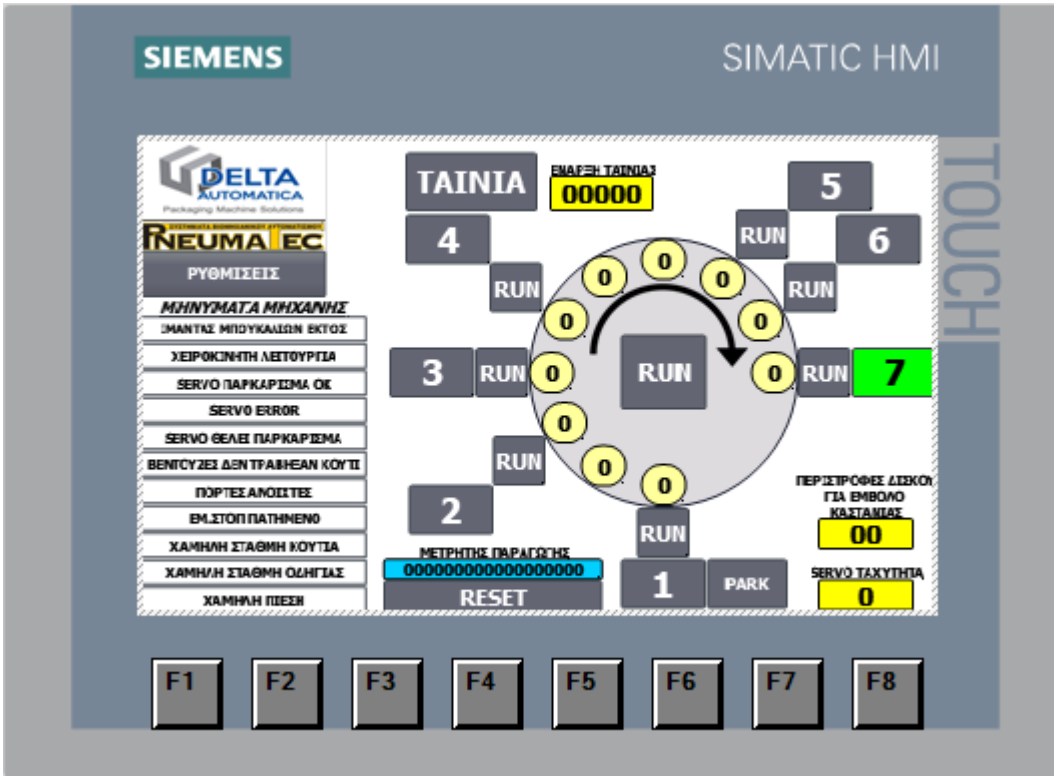


Σχήμα 26. TIA PORTAL SIEMENS

7.4. HMI

Στην πρόσοψη του ηλεκτρολογικού πίνακα της μηχανής, είναι τοποθετημένη η κεντρική οθόνη ή HMI όπως ονομάζεται (Human Machine Interface). Ουσιαστικά, πρόκειται για ένα δίαυλο επικοινωνίας μεταξύ ανθρώπου και μηχανής. Με διάφορες γραφικές απεικονίσεις, ο χρήστης είναι σε θέση να ελέγχει και να χειρίζεται την μηχανή. Ταυτόχρονα η οθόνη οπτικοποιεί τη λειτουργία της μηχανής και διευκολύνει τον χειριστή ως προς την επίβλεψη και την διαχείριση της. Η προσεγμένη και λεπτομερής σχεδίαση των ενδείξεων και των γραφικών, συμβάλουν σημαντικά στην επιτυχημένη αλληλεπίδραση, αντιθέτως μια άστοχη σχεδίαση μπορεί να οδηγήσει σε μη επιθυμητά αποτελέσματα και σε πολλά σφάλματα.

Η οθόνη που χρησιμοποιήθηκε είναι η SIMATIC Basic Panel KTP700 PN του οίκου Siemens. Πρόκειται για μια TFT LED widescreen οθόνη, 7 in, με ανάλυση 800 * 400 pixel. Με τάση τροφοδοσίας 24 VDC, τύπο επεξεργαστή ARM και διαθέσιμη μνήμη για τον χρήστη 10 Mbyte. Διαθέτει επίσης ένα μπάζερ, Ethernet και USB θύρες. Τα HMI του οίκου Siemens προγραμματίζονται επίσης με ίδια πλατφόρμα που προγραμματίζονται και τα PLC, την Tia Portal.



Σχήμα 27. TIA PORTAL SIEMENS

Με την οθόνη, ο χειριστής θα είναι σε θέση ενεργοποιεί την αυτόματη λειτουργία της μηχανής ή να ενημερώνεται για το αν το κουμπί έκτακτης ανάγκης είναι πατημένο, αν η στάθμη των κουτιών ή των οδηγιών είναι σε χαμηλά επίπεδα ή αν υπάρχει χαμηλή πίεση στο υδραυλικό σύστημα αέρος της μηχανής. Επίσης σε ποια θέση βρίσκεται το περιστρεφόμενο τραπέζι, την ταχύτητα του σερβοκινητήρα και τον μετρητή παραγωγής.

7.5. FLEXY 205

Στην εποχή του Industry 4.0, μια ονομασία που δόθηκε να για να περιγράψει την εξέλιξη στην αυτοματοποίηση των παραγωγών και της ανταλλαγής δεδομένων μεταξύ των τεχνολογικών συστημάτων σε ένα βιομηχανικό χώρο, οι δυσκολίες που πρέπει να αντιμετωπιστούν ποικίλουν. Υπάρχουν για παράδειγμα πολύ εξειδικευμένα πρωτόκολλα σε παλαιές μηχανές που δεν μπορούν να παρέχουν δεδομένα ώστε να πραγματοποιηθούν οι κατάλληλες αναλύσεις ή συστήματα που είναι ευάλωτα από άποψη ασφάλειας. Γεγονός που απασχολεί ιδιαίτερα το τμήμα των I.T στις βιομηχανίες.

Οι κατασκευαστές από την πλευρά τους προσπαθούν να προσαρμοστούν σε αυτές τις απαιτήσεις, αναβαθμίζοντας ποιοτικά της μηχανές και τα αυτοματοποιημένα συστήματα γενικότερα. Για να το επιτύχουν παρακολουθούν συνεχώς την λειτουργία της μηχανής, δημιουργούν ειδοποιήσεις για ανεπιθύμητες βλάβες, προγραμματίζουν συντηρήσεις ώστε να μειωθούν επείγοντες καταστάσεις και να αυξηθεί η παραγωγή.

Το Flexy 205, ένας από τους πιο καινοτόμους βιομηχανικούς δρομολογητές, καλύπτει τις ανάγκες των τελικών χρηστών διότι είναι συμβατό και επικοινωνεί με όλα τα πρωτοκόλλα των PLC καθώς και με OPC UA σε μοντέλο client, συλλέγει δεδομένα και τα προωθεί στα ERP και CRM προγράμματα των επιχειρήσεων. Από την πλευρά των κατασκευαστών, τους διευκολύνει διότι μπορούν και προωθούν τα δεδομένα σε άλλες custom εφαρμογές ή πλατφόρμες και σε συστήματα

cloud αλλά και να επεμβαίνουν απομακρυσμένα για βελτιστοποιήσεις και επιδιορθώσεις στα PLC και τα HMI.

Σχήμα 28. Ewon Flexy 205

Η απλή έκδοση του Ewon Flexy 205 περιλαμβάνει τέσσερις θύρες Ethernet όπου η κάθε μία μπορεί να χρησιμοποιηθεί είτε σαν WAN είτε σαν LAN, με την προϋπόθεση πως η WAN θα είναι μία και οι υπόλοιπες τρεις θα είναι LAN. Διατίθενται επίσης δύο θέσεις για κάρτες επέκτασης και μία θύρα για SD κάρτα για διευκόλυνση στο Set up ή και για έξτρα χώρο αποθήκευσης. Οι διαστάσεις του είναι 133 * 122 * 55 mm, λειτουργεί με 24V DC τροφοδοσία και σε περιβάλλον με θερμοκρασία -25°C μέχρι τους 70°C. Με την αγορά ενός προϊόντος δίνεται δωρεάν πρόσβαση στον server Talk2m. Οι κάρτες επέκτασης που διατίθενται είναι οι εξής:

Σχήμα 29. Κάρτα επέκτασης 4G

Σχήμα 30. Κάρτα επέκτασης WiFi

Σχήμα 31. Κάρτα επέκτασης WiFi

Σχήμα 32. Κάρτα επέκτασης USB

Σχήμα 33. Κάρτα επέκτασης Ethernet

Σχήμα 34. Κάρτα επέκτασης Serial

Για την απόκτηση των δεδομένων από τα PLC μέσω της Ewon συσκευής δεν υπάρχει ανάγκη για γραφή περαιτέρω κώδικα στο PLC και η διαδικασία μπορεί να επιτευχθεί ενώ η μηχανή είναι σε λειτουργία. Το Ewon δύναται να ρυθμιστεί μέσω ενός WEB Browser και τα να «τραβήξει» μέχρι και 2500 παραμέτρους με ρυθμό μικρότερο του 1sec. Παράμετροι τύπου String υποστηρίζονται καθώς μπορεί να αποθηκεύσει δεδομένα τοπικά για 1.000.000 χρονικές στιγμές. Επίσης είναι διαθέσιμες και οι ζώνες ωρών για διευκόλυνση.

7.6. ΠΩΣ ΛΕΙΤΟΥΡΓΕΙ Ο ΚΩΔΙΚΑΣ

Αντί να χρησιμοποιήσουμε τον οδηγό Ιστού και να διαμορφώσουμε έτσι τη σύνδεση Talk2M, μπορούμε να την εκκινήσουμε χρησιμοποιώντας κάποιο βασικό σενάριο.

Είναι δυνατό με την εντολή: SetSys PRG"T2MCFG",....

Αυτή η εντολή μπορεί να χρησιμοποιηθεί για την ενεργοποίηση του οδηγού διαμόρφωσης Talk2M από το Basic.

Αυτή η συνάρτηση μπορεί να λάβει 1, 2,3 ή 4 παραμέτρους:

SetSys PRG,"T2MCFG",S1

Το S1 είναι το κλειδί ενεργοποίησης

SetSys PRG,"T2MCFG",S1,S2

Το S1 είναι το κλειδί ενεργοποίησης

Το S2 είναι ο τρόπος σύνδεσης (ως συμβολοσειρά).

Πιθανές τιμές είναι:

"0": Αυτόματος εντοπισμός

"1": UDP

"2": Άμεση σύνδεση TCP (HTTPS).

"3": TCP μέσω διακομιστή μεσολάβησης (HTTPS)

SetSys PRG,"T2MCFG",S1,S2,S3

Το S1 είναι το όνομα eWON όπως ορίζεται στο Talk2M

Το S2 είναι το login του χρήστη Talk2M που έχει πρόσβαση στη διαμόρφωση eWON

Το S3 είναι ο κωδικός πρόσβασης του συγκεκριμένου χρήστη του Talk2M.

SetSys PRG,"T2MCFG",S1,S2,S3,S4

Το S1 είναι το όνομα eWON όπως ορίζεται στο Talk2M

Το S2 είναι το login του χρήστη Talk2M που έχει πρόσβαση στη διαμόρφωση eWON

Το S3 είναι ο κωδικός πρόσβασης του συγκεκριμένου χρήστη του Talk2M.

Το S4 είναι ο τρόπος σύνδεσης (ως συμβολοσειρά).

Πιθανές τιμές είναι:

"0": Αυτόματος εντοπισμός

"1": UDP

"2": Άμεση σύνδεση TCP (HTTPS).

"3": TCP μέσω διακομιστή μεσολάβησης (HTTPS)

Για να εκκινήσουμε τον οδηγό Talk2M μέσω διακομιστή μεσολάβησης χρησιμοποιώντας το κλειδί ενεργοποίησης, χρησιμοποιούμε το ακόλουθο βασικό σενάριο:

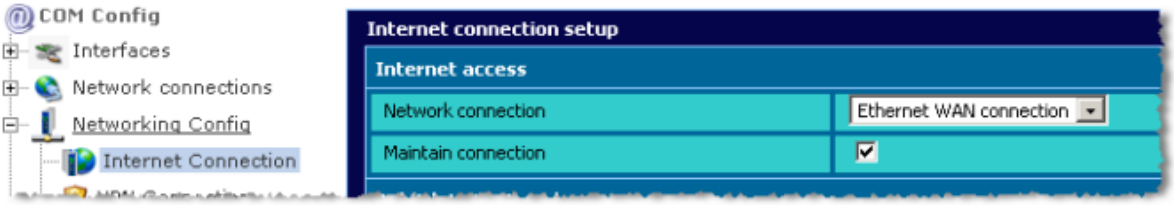
```
SETSYS COM, "LOAD"
SETSYS COM, "WANPxyAddr","10.0.120.24"
SETSYS COM, "WANPxyPort", 8124
SETSYS COM, "WANPxyUsr","abcd\jcn"
SETSYS COM, "WANPxyPass","Mt8ert45"
SETSYS COM, "SAVE"

SetSys PRG,"T2MCFG","CDD81DD701F2516D8D038E95A6A5E3", "3"
```

Για να κάνουμε εναλλαγή για να ενεργοποιήσουμε τη σύνδεση WAN, όταν ο διακόπτης είναι ενεργοποιημένος, το eWON περνά μέσα από το εταιρικό LAN για να συνδεθεί στο Διαδίκτυο (χρησιμοποιώντας το Talk2M για παράδειγμα). Όταν ο διακόπτης είναι OFF, το eWON κλείνει τη διεπαφή WAN και απομονώνεται πλήρως από το εταιρικό LAN.

Ένας διακόπτης τοποθετείται στην υποδοχή ψηφιακής εισόδου του eWON και σε αυτήν την ψηφιακή είσοδο έχει ρυθμιστεί μια ετικέτα που ονομάζεται Switch.

Το eWON έχει ρυθμιστεί για σύνδεση στο Διαδίκτυο "ON WAN".



Ο κώδικας είναι ο ακόλουθος:

```
Rem --- eWON start section: Init Section
ewon_init_section:
    Rem --- eWON user (start)
    ONCHANGE "Switch","goto DoSwitch"
    goto DoSwitch
    Rem --- eWON user (end)
```

```
End
Rem --- eWON end section: Init Section
Rem --- eWON start section: Switch
Rem --- eWON user (start)
DoSwitch:
    If (Switch@<>0) Then
        rem Open Internet connection
        Setsys COM,"load"
        Setsys COM,"WANCnx","2"
        Setsys COM,"WANPermCnx","1"
        Setsys COM,"save"
        Print Time$;" Connection opened"
    else
        rem Close Internet connection
        Setsys COM,"load"
        Setsys COM,"WANCnx","0"
        Setsys COM,"save"
        Print Time$;" Connection closed"
        endif
    end
    Rem --- eWON user (end)
End
Rem --- eWON end section: Switch

```

Όσον αφορά στην εξαγωγή πληροφοριών μόντεμ και κάρτας SIM χρησιμοποιώντας δέσμες ενεργειών, αυτό το παράδειγμα σεναρίου επιτρέπει να δούμε τα GsmIMEI, GsmINSI, GsmCellId, GsmLAC, GsmWlessNet & GsmNetRegTxt που βρίσκονται μέσα στο "estat.htm".

GsmIMEI: Η διεθνής ταυτότητα κινητού εξοπλισμού είναι ένας αριθμός, συνήθως μοναδικός, για τον προσδιορισμό του GSM. Ο αριθμός IMEI χρησιμοποιείται από ένα δίκτυο GSM για την αναγνώριση έγκυρων συσκευών και επομένως μπορεί να χρησιμοποιηθεί για να σταματήσει την πρόσβαση ενός κλεμμένου τηλεφώνου σε αυτό το δίκτυο.

GSMIMSI: Μια διεθνής ταυτότητα συνδρομητή κινητής τηλεφωνίας είναι μια μοναδική αναγνώριση που σχετίζεται με όλους τους χρήστες κινητών τηλεφώνων του δικτύου GSM, UMTS και LTE.

GsmCellId: είναι ένας γενικά μοναδικός αριθμός που χρησιμοποιείται για την αναγνώριση κάθε σταθμού πομποδέκτη βάσης (BTS) ή τομέα ενός BTS εντός ενός κωδικού περιοχής τοποθεσίας (LAC) εάν δεν είναι εντός δικτύου GSM.

GsmLAC: τοπικός κωδικός περιοχής.

GsmWlessNet*: αναφέρει το τρέχον εντοπισμένο ασύρματο δίκτυο. Αυτό μας δίνει μια τιμή από 0 έως 5 που αντιστοιχεί στον τύπο δικτύου.

ΑΓΝΩΣΤΟ = 0

GPRS = 1

EGPRS = 2

WCDMA = 3

HSPA = 4

NO_GPRS = 5

GsmNetRegTxt*: Υποδεικνύει την κατάσταση σύνδεσης δικτύου (Χωρίς δίκτυο, Οικιακό δίκτυο ή Περιαγωγή) ακολουθούμενη από τον τύπο δικτύου που εντοπίστηκε σε παρένθεση (EDGE, GPRS, HSPA, κ.λπ.)

Χρησιμοποιούμε το SETSYS INF "load" για να φορτώσουμε πληροφορίες σχετικά με το eWON.

Το "A$ = GETSYS INF,"GsmIMEI"" χρησιμοποιείται για την εξαγωγή της τιμής που θέλουμε, σε αυτήν την περίπτωση GsmIMEI

Ο κώδικας είναι ο ακόλουθος:

```
GSM_Info:
    Cls
    SETSYS INF,"load"
    A$ = GETSYS INF,"GsmIMEI"
    Print "GsmIMEI : ";A$
    A$ = GETSYS INF,"GsmIMSI"
    Print "GsmIMSI : ";A$
    A$ = GETSYS INF,"GsmCellId"
    Print "GsmCellID : ";A$
    A$ = GETSYS INF,"GsmLAC"
    Print "GsmLAC : ";A$
    A$ = GETSYS INF,"GsmWlessNet"
    Print "GsmWlessNet : ";A$;" UNKNOWN = 0,GPRS = 1,EGPRS = 2,WCDMA =
3,HSPA  = 4,NO_GPRS = 5"
    A$ = GETSYS INF,"GsmNetRegTxt"
    Print "GsmNetRegTxt : ";A$
End
```

Από την άλλη ο κώδικας για να εξάγουμε την ημερομηνία και την ώρα χρησιμοποιώντας το BASIC του eWON είναι ο ακόλουθος:

```
1    Clock:
2    A$ = Time$
3    Print A$
4    H% = Val(A$(12 To 13))
5    M% = Val(A$(15 To 16))
6    D% = Val(A$(1 To 2))
7    Z% = Val(A$(4 To 5))
8    Y% = Val(A$(7 To 10))
9    Print "Current Hour : "; H%
10   Print "Current Minute : "; M%
11   Print "Current Day : "; D%
12   Print "Current Month : "; Z%
13   Print "Current Year : "; Y%
14   END
```

Ο μόνος τρόπος για να προσαρμόσετε το μήνυμα ηλεκτρονικού ταχυδρομείου συναγερμού (SMS) είναι να χειριστείτε όλες τις Ενέργειες συναγερμού με σενάριο.

Πρέπει να κάνουμε 3 μικρές εργασίες:

Λαμβάνουμε το συμβάν συναγερμού με τις οδηγίες χειριστή συμβάντων ONALARM.

Μορφοποιούμε το email όπως θέλουμε δημιουργώντας μια συμβολοσειρά.

Στέλνουμε το email με την οδηγία SendMail.

Με αυτόν τον κώδικα, το συμβάν συναγερμού ενεργοποιείται κάθε φορά που αλλάζει η κατάσταση συναγερμού.

Στη συνέχεια, πρέπει να ελέγξουμε σε ποια κατάσταση συναγερμού βρίσκεται η ετικέτα μας.

Το Init_Section του eWON θα περιέχει:

```
ONALARM "TagTest","GOTO ProcessTagTestAlarm"
```

Δημιουργούμε μια νέα ενότητα:

```
ProcessTagTestAlarm:
    A% = ALSTAT("TagTest")
    PRINT Time$;" TagTest alarm ";A%
    IF (A%=2) THEN
        Rem Send eMail only when the alarm occurs
        N$ = CHR$(10)+CHR$(13) : Rem CRLF
        A$ = "This is my customised alarm eMail for tag TagTest" + N$
        A$ = A$ + "The current value of TagTest is " + STR$(TagTest@) + N$
        A$ = A$ + "The current time is " + TIME$
        SENDMAIL "user@company.com","","TagTest alarm Subject",A$
    ENDIF
END
```

Το eWON εξοπλισμένο με μόντεμ GSM/GPRS μπορεί να λαμβάνει SMS.

Για την αντιμετώπιση του ληφθέντος SMS, η συνάρτηση «ONSMS» πρέπει να χρησιμοποιηθεί σε συνδυασμό με τη συνάρτηση «getsys prg», «SmsRead»». Τα ακόλουθα πεδία πληροφοριών μπορούν στη συνέχεια να εξαχθούν από κάθε λαμβανόμενο SMS:

smsFrom: Συμβολοσειρά που κρατά τον αριθμό τηλεφώνου του αποστολέα

smsDate: Συμβολοσειρά που κρατά την Ημερομηνία λήψης SMS

smsMsg: Συμβολοσειρά που κρατά το μήνυμα SMS

Κάθε φορά που χρησιμοποιείται η λειτουργία «getsys prg, «SmsRead»», το SMS θα διαβάζεται και θα διαγράφεται από την κάρτα Sim.

Το σενάριο που εμφανίζεται παρακάτω θα διαβάζει κάθε SMS και θα στέλνει ένα SMS πίσω στον αποστολέα SMS. Το SMS θα περιέχει τα περιεχόμενα SMS του ληφθέντος SMS.

```
InitSection:
    ONSMS "Goto HSms"
    HSms:
        a% = getsys prg,"SmsRead"
        if (a%<>0) then
            s% = s%+1
            print "SMS Nr: ";s%
            f$ = getsys prg,"smsfrom"
            print "From: ";f$
            print getsys prg,"smsdate"
            a$ = getsys prg,"smsmsg"
            print "Message: ";a$
            b$ = f$+",gsm,0"
            c$ = "Received message: "+a$
            sendsms b$,c$
            goto HSms
        endif
    end

```

Το σενάριο που εμφανίζεται παρακάτω θα ορίσει την τιμή της ετικέτας «Var1» στην τιμή που λαμβάνεται από το SMS. (Παράδειγμα περιεχομένου του ληφθέντος SMS = 1234). Η λειτουργία «LogEvent» χρησιμοποιείται για την παρακολούθηση της ενέργειας που γίνεται μέσω SMS.

```
1    InitSection:
2        ONSMS "Goto HSms"
3        HSms:
4            a% = Getsys Prg,"SmsRead"
5            If (a%<>0) Then
6                f$ = Getsys Prg,"smsfrom"
7                a$ = Getsys Prg,"smsmsg"
8                Var1@ = Val(a$)
9                LOGEVENT "Value of Tag Var1@ changed to:" + a$ + " by GSM number: " + f$
10               Goto Hsms
11           Endif
12       End
```

Το σενάριο που εμφανίζεται παρακάτω θα αναγνωρίσει το συναγερμό της ετικέτας που περιέχεται στο μήνυμα SMS. (Παράδειγμα περιεχομένου του ληφθέντος SMS = Var1). Η λειτουργία «LogEvent» χρησιμοποιείται για την παρακολούθηση της ενέργειας που γίνεται μέσω SMS.

```
1
2    InitSection:
3        ONSMS "Goto HSms"
4        HSms:
5            a% = Getsys Prg,"SmsRead"
6            If (a%<>0) Then
7                f$ = Getsys Prg,"smsfrom"
8                a$ = Getsys Prg,"smsmsg"
9                SETSYS PRG,"RESUMENEXT",1
10               ALMACK a$,""
11               e% = Getsys Prg,"LSTERR"
12               IF e% = -1 Then
13                   LOGEVENT "Acknowledge of alarm " + a$ + " by GSM number: " + f$, 120
14               Else
15                   IF e% = 4 Then
16                       LOGEVENT "Alarm acknowledge failed because specified Tag is unk
17                   Else
18                       LOGEVENT "Alarm acknowledge failed. (SMS Content: " + a$ + " , S
19                   Endif
20               Endif
21               SETSYS PRG,"LSTERR",-1
22               SETSYS PRG,"RESUMENEXT",0
23               Goto HSms
24           Endif
```

Ένα SMS μπορεί να χρησιμοποιηθεί για να «ξυπνήσει» το eWON GSM/GPRS για τη δημιουργία σύνδεσης στο Διαδίκτυο. Το σενάριο που εμφανίζεται παρακάτω θα στείλει ένα μήνυμα μετά τη λήψη SMS.

Στη συνέχεια, η προγραμματισμένη αλληλογραφία θα ενεργοποιήσει την εξερχόμενη σύνδεση στο Διαδίκτυο όπως έχει διαμορφωθεί στις ρυθμίσεις Εξερχόμενης σύνδεσης του eWON. (Παράδειγμα περιεχομένου του ληφθέντος SMS = Σύνδεση).

Η λειτουργία «LogEvent» χρησιμοποιείται για την παρακολούθηση της ενέργειας που γίνεται μέσω SMS.

```
InitSection:
    ONSMS "Goto HSms"
    HSms:
        a% = Getsys Prg,"SmsRead"
        If (a%<>0) Then
            f$ = Getsys Prg,"smsfrom"
            a$ = Getsys Prg,"smsmsg"
            If a$ = "Connect" Then
                Sendmail "MyMail@abc.be","","eWON Wake up by SMS","The eWON online
                LOGEVENT "eWON Wake up by SMS from GSM number: " + f$, 120
            ENDIF
            Goto Hsms
        Endif
    End
```

Τώρα θα δημιουργήσουμε τα αρχεία που θα χρησιμοποιηθούν για την αναφορά. Για να εισαγάγουμε την τρέχουσα τιμή της ετικέτας στην αναφορά, θα χρησιμοποιήσουμε τη σύνταξη TagSSI. Το SSI σημαίνει Συμπερίληψη από την πλευρά του διακομιστή. Αυτή η μέθοδος χρησιμοποιείται για τη δημιουργία τοποθεσιών web στους οποίους ο διακομιστής ενημερώνει μέρη της σελίδας HTML. Για περαιτέρω επεξηγήσεις, ανατρέξτε στον Οδηγό αναφοράς Web eWON (RG-003-0-EN). Το μόνο που πρέπει να γνωρίζει για το παράδειγμά μας εδώ είναι ότι πρέπει να χρησιμοποιήσουμε την ακόλουθη σύνταξη για να συμπεριλάβουμε την τιμή μιας ετικέτας μέσα στην αναφορά: <%#TagSSI,TagName%> Όταν το eWON στέλνει την αναφορά μέσω email ή FTP, eWON θα αναλύσει το αρχείο και θα αντικαταστήσει το <%#TagSSI,TagName%> με την τρέχουσα τιμή της ετικέτας που ονομάζεται "Tagname".

Δημιουργούμε ένα αρχείο κειμένου που ονομάζεται VesselData.txt με το ακόλουθο περιεχόμενο και τοποθετήστε αυτό το αρχείο στον φάκελο /usr του eWON (χρησιμοποιώντας FTP):

```
Values of the vessel sensors at <%#TagSSI,HourInfo%>
Vessel Temperature : <%#TagSSI,VesselTemperature%> °C
Vessel Pressure : <%#TagSSI,VesselPressure%> bar
Vessel Level : <%#TagSSI,VesselLevel%> L
```

Δημιουργούμε ένα αρχείο HTML που ονομάζεται VesselData.html, με το ακόλουθο περιεχόμενο και τοποθετήστε αυτό το αρχείο στον φάκελο /usr του eWON (χρησιμοποιώντας FTP):

```
<html doctype="html">
    <head>
        <meta charset="UTF-8" />
    </head>
    <body>
        <p><strong>Values of the vessel sensors at <%#TagSSI,HourInfo%></strong></p
        <p>Vessel Temperature : <%#TagSSI,VesselTemperature%> °C</p>
        <p>Vessel Pressure : <%#TagSSI,VesselPressure%> bar</p>
        <p>Vessel Level : <%#TagSSI,VesselLevel%> L</p>
    </body>
</html>
```

Στην ενότητα Init:

```
REM Activation of Timer 1 executed each 60 seconds
TSET 1,60
REM Trigger of the GetTime section
ONTIMER 1, "Goto GetTime"
END
```

Στην ενότητα User:

```

GetTime:
    A$ = TIME$
    REM Get the day of the week
    a% = DOW A$
    REM Get the hour value
    b% = VAL(A$(12 TO 13))
    REM Get the minute value
    c% = VAL(A$(15 TO 16))
    REM Check if action must be done
    REM Check Day of the week
    IF ((a% > 0) AND (a% < 6)) THEN
        REM Check hour of the day
        IF ((b% >= 8) AND (b% <= 17)) THEN
            REM Check minute of the hour
            IF (c% = 0) THEN
                HourInfo = b%
                Goto SendVesselData
            ENDIF
        ENDIF
    ENDIF
END

SendVesselData:
    REM Send mail with text file in attachment
    Sendmail "test@test.com", "", "Vessel Sensors Values", "&[$dtUF $fnVesselData.t
    REM Send mail with html file in attachment
    Sendmail "test@test.com", "", "Vessel Sensors Values", "&[$dtUF $fnVesselData.h
END

```

ΣΥΜΠΕΡΑΣΜΑΤΑ

Η κεντρική λύση βασίζεται στον ακόλουθο εξοπλισμό E-Won, το Flexy 205 dual IIoT Gateway και τον δρομολογητή Remote Access. Το eWON Flexy 205 είναι μια νέα προηγμένη πύλη δεδομένων Διαδικτύου, η οποία επιτρέπει στον χρήστη να παρακολουθεί και να συλλέγει KPI (Key Performance Indicators) που είναι πολύ χρήσιμα στην προληπτική συντήρηση. Με καταγραφή δεδομένων, συναγερμούς, ενσωματωμένη διεπαφή ιστού, σενάρια και βελτιωμένη σύνδεση στο διαδίκτυο, το Flexy 205 είναι μια αρθρωτή πύλη Διαδικτύου για εφαρμογές IoT. Αυτός ο εξοπλισμός επιτρέπει

επίσης απομακρυσμένη πρόσβαση VPN για εύκολη αντιμετώπιση προβλημάτων βιομηχανικού εξοπλισμού από απόσταση και μπορεί επίσης να χρησιμεύσει ως εξοπλισμός σε εργαστήρια απομακρυσμένου αυτοματισμού. Εκτός από την απομακρυσμένη πρόσβαση VPN με τις υπηρεσίες απομακρυσμένης σύνδεσης eWON Talk2M, επιτρέπει στο χρήστη να δημιουργεί συναγερμούς και ειδοποιήσεις, καθώς και να διαβάζει δεδομένα από μηχανήματα και εξοπλισμό. Είναι επίσης δυνατό να ενσωματωθούν δεδομένα στο σύστημα του ίδιου του χρήστη ή σε πλατφόρμες cloud χρησιμοποιώντας την εφαρμογή διεπαφής προγραμματισμού Talk2M (API), δέσμες ενεργειών HTTP ή MQTT, που αποτελούν μόνο ορισμένα από τα υποστηριζόμενα πρωτόκολλα.

Ως αποτέλεσμα της κρίσης που δημιουργήθηκε από την πανδημία του κορωνοϊού, οι βιομηχανικές δραστηριότητες αναγκάστηκαν να αλλάξουν τον τρόπο διεξαγωγής τους, λόγω των περιορισμών που επιβάλλονται από τις επικρατούσες συνθήκες. Μεταξύ των προκλήσεων για τη δραστηριότητα είναι η υλοποίηση πρακτικών κλάδων. Στόχος είναι να ενεργοποιηθούν οι βιομηχανικές δραστηριότητες που χρησιμοποιούν τεχνολογίες Διαδικτύου των Πραγμάτων (IoT), μια έννοια που σχετίζεται με την ψηφιακή διασύνδεση εξοπλισμού βιομηχανικού αυτοματισμού μέσω του Διαδικτύου. Η λύση που θα εφαρμοστεί, η απομακρυσμένη εποπτεία βιομηχανικού αυτοματισμού, παρουσιάζεται στα προηγούμενα κεφάλαια. Ο στόχος αυτού του τύπου εποπτείας είναι να καταστεί δυνατή η απομακρυσμένη διασύνδεση σε βιομηχανικό αυτοματισμό μέσω μιας πλατφόρμας, προκειμένου να υποστηριχθούν οι εργαζόμενοι από διαφορετικές πλευρές σε πρακτικές εργασίες αυτοματισμού που πραγματοποιούνται χρησιμοποιώντας PLC, HMI και άλλο εξοπλισμό για το αποτέλεσμα.

Η επένδυση που απαιτείται για τέτοια συστήματα θα εξαρτηθεί από τις φυσικές συνθήκες της βιομηχανίας καθώς και από τον εξοπλισμό που το συνιστά. Όσον αφορά τον εξοπλισμό βιομηχανικού αυτοματισμού, το ιδανικό ως προς τη σύνθεση θα ήταν το εξής:

• Dual IIoT Gateway και δρομολογητής Remote Access Flexy 205 από την E-Won.

• Το PLC.

• Το HMI.

• Σύστημα ελεγκτών και μοτέρ σερβο.

• Αναλογικές είσοδοι και έξοδοι.

• Τεχνολογία IO-LINK (προαιρετικό).

• Αρκετοί βιομηχανικοί διακόπτες για διασύνδεση εξοπλισμού.

• Γραμμή βιομηχανικών διεργασιών για εφαρμογή της του βιομηχανικού αυτοματισμού σε γραμμές παραγωγής. Το κόστος για την αγορά του δρομολογητή Remote Access Flexy 205 από την E-Won είναι περίπου 500,00 €, το οποίο σε αυτή την περίπτωση είναι χαμηλή αξία σε σύγκριση με τον υπόλοιπο εξοπλισμό που αποτελείται ο ηλεκτρολογικός πίνακας.

Υπάρχουν πλεονεκτήματα και μειονεκτήματα στη χρήση απομακρυσμένων εργαστηρίων. Τα πλεονεκτήματα είναι αλληλεπίδραση με τον εξοπλισμό, βαθμονόμηση, ρεαλιστικά δεδομένα, χωρίς περιορισμούς χρόνου και τόπου και μεσαίο κόστος. Τα μειονεκτήματα είναι μόνο οι μικρές πιθανότητες ατυχημάτων όταν η βιομηχανική μηχανή ελέγχεται απομακρυσμένα. Για παράδειγμα μια ελλιπής επικοινωνίας μεταξύ του τεχνικού που ελέγχει τις κινήσεις μιας γραμμής παραγωγής με τον χειριστή της μηχανής, μπορούν να δημιουργήσουν ένα επικίνδυνο περιβάλλον.

• Θα είναι επίσης προσβάσιμο από smartphone, γεφυρώνοντας το χάσμα πρόσβασης για αυτόν τον τύπο τεχνολογίας.

• Το σύστημα επιτρέπει την πρόσβαση σε διάφορες τεχνολογίες που υπάρχουν σε εργοστάσια και βιομηχανίες, ακόμη και αν είναι λίγο παλιά, καθώς αυτή η λύση μπορεί να προσαρμοστεί σε ό,τι θα ήταν επωφελές.

• Οι μηχανικοί συντήρησης με δυσκολίες μετάβασης στον τόπο που υπάρχει η βλάβη, μπορούν έτσι να έχουν ένα πολύ ενδιαφέρον εργαλείο που θα τους επιτρέψει να έχουν πρόσβαση σε όλους τους υπάρχοντες πόρους καθώς και πολύ πρακτικό στη βιομηχανική πραγματικότητα.

Το μέλλον μοιάζει πιο αβέβαιο από ποτέ. Αλλά οι πιο πρόσφατοι μήνες έδειξαν ξεκάθαρα, ίσως σε αντίθεση με ό,τι θα μπορούσαν να μαντέψουν τα πιο απαισιόδοξα μυαλά, ότι υπάρχει σε όλο τον κόσμο, μεγάλη ικανότητα οργάνωσης, ανθεκτικότητας, προσαρμογής και καινοτομίας, που θα επιτρέψει στα ιδρύματα για να ξεπεραστούν οι προκλήσεις που βρίσκονται μπροστά μας, ως αποτέλεσμα της εξάπλωσης του COVID-19. Η δημιουργία μιας πλατφόρμας πρόσβασης και η επίσημη επαλήθευση των προγραμμάτων που εκτελούνται, χρησιμοποιώντας λογισμικό όσο το δυνατόν γρηγορότερα, ώστε να μην χάνεται χρόνος, θα ήταν ένα φανταστικό βήμα προς τα εμπρός προς την υλοποίηση μιας τέτοιας βιομηχανικής πλατφόρμας.

Συνοπτικά, η παρούσα εργασία πραγματεύεται τη συμβολή ενός απομακρυσμένου τρόπου εποπτείας βιομηχανικού αυτοματισμού στην προοπτική των δύο βιώσιμων διαστάσεων της ανάπτυξης, δηλαδή στις πτυχές της οικονομικής και κοινωνικής ολοκλήρωσης. Είναι σημαντικό να σημειωθεί ότι αυτός ο τύπος απομακρυσμένου συστήματος δεν θα αντικαταστήσει κανένα άλλο φυσικό πρόσωπο, αλλά θα πρέπει να θεωρείται μόνο ως συμπληρωματικό εργαλείο, επιτρέποντας στους εργαζόμενους αλλά και στους επενδυτές να πραγματοποιούν καινοτόμες πρακτικές και μεθόδους άμεσης επέμβασης και πρόσβασης σε εξοπλισμό βιομηχανικού αυτοματισμού με βιώσιμο τρόπο.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Amyx, S. (2017). Privacy dangers of wearables and the IoT. Managing Security Issues and the Hidden Dangers of Wearable Technologies. IGI Global, σσ. 131-160.

Anderson, J., & Rainie, H. (2014). The IoT will thrive by 2025. Pew Research Center. Internet & American Life Project.

Asthana, S., Megahed, A., & Strong, R. (2017). A recommendation system for proactive health monitoring using IoT and wearable technologies. 2017 IEEE International Conference on AI & Mobile Services (AIMS) (σσ. 14-21). IEEE.

Byrne, J., O'Sullivan, K., & Sullivan, K. (2016). An IoT and wearable technology hackathon for promoting careers in computer science. IEEE Transactions on Education, σσ. 50-58.

Cho, G., Lee, S., & Cho, J. (2009). Review and reappraisal of smart clothing. International Journal of Human-Computer Interaction, σσ. 582-617.

Di Serio, A., Buckley, J., Barton, J., Newberry, R., Rodencial, M., Dunlop, G., και συν. (2018). Potential of sub-GHz wireless for future IoT wearables and design of compact 915 MHz antenna. Sensors, σ. 22.

Fernández-Caramés, T., & Fraga-Lamas, P. (2018). Towards the Internet of smart clothing: A review on IoT wearables and garments for creating intelligent connected e-textiles. Electronics, σ. 405.

Hajny, J., Dzurenda, P., & Malina, L. (2016). Multi-Device Authentication using Wearables and IoT. SECRYPT, σσ. 483-488.

Hakima, C. (2010). The IoT: Connecting Objects. New York: John Wiley & Sons.

Hall, P., & Hao, Y. (2012). Antennas and propagation for body-centric wireless communications. New York: Artech house.

Hassan, M., Hu, W., Lan, G., Seneviratne, A., Khalifa, S., & Das, S. (2018). Kinetic-powered health wearables: Challenges and opportunities. Computer, σσ. 67-74.

Jovanov, E. (2019). Wearables Meet IoT: Synergistic Personal Area Networks (SPANs). Sensors, σ. 4295.

Kozioł, D., Moya, F., Yu, L., Van Phan, V., & Xu, S. (2017). QoS and service continuity in 3GPP D2D for IoT and wearables. IEEE Conference on Standards for Communications and Networking (CSCN). 233-239: IEEE.

Land, N., Bhattarcharya, S., Georgiev, P., Forlivesi, C., & Kawsar, F. (2015). An early resource characterization of deep learning on wearables, smartphones and internet-of-things devices. Proceedings of the 2015 international workshop on IoT towards applications, (σσ. 7-12).

Liu, J., & Sun, W. (2016). Smart attacks against intelligent wearables in people-centric IoT. IEEE Communications Magazine, σσ. 44-49.

Mann, S. (1998). Wearable computing as means for personal empowerment. Proc. 3rd Int. Conf. on Wearable Computing (ICWC) (σσ. 51-59). ICWC.

Martins, A., Pinheiro, M., Ferreira, A., Almeida, R., Matos, F., Oliveira, J., και συν. (2018). Heterogeneous integration challenges within wafer level fan-out SiP for wearables and IoT. 2018 IEEE 68th Electronic Components and Technology Conference (ECTC) (σσ. 1485-1492). IEEE.

McCann, J., & Bryson, D. (2009). Smart clothes and wearable technology. London: Elsevier.

Metcalf, D., Milliard, S., Gomez, M., & Schwartz, M. (2016). Wearables and the IoT for health: Wearable, interconnected devices promise more efficient and comprehensive health care. IEEE pulse, σσ. 35-39.

Ometov, A., Masek, P., Malina, L., Florea, R., Hosek, J., Andreev, S., και συν. (2016). Feasibility characterization of cryptographic primitives for constrained (wearable) IoT devices. 2016 IEEE

International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops) (σσ. 1-6). IEEE.

Sojuyigbe, S., & Daniel, K. (2015). Wearables/IOT devices: Challenges and solutions to integration of miniature antennas in close proximity to the human body. 2015 IEEE Symposium on Electromagnetic Compatibility and Signal Integrity (σσ. 75-78). IEEE.

Stallings, W. (2007). Data and computer communications. New Delhi: Pearson Education India.

Sun, W., Liu, J., & Zhang, H. (2017). When smart wearables meet intelligent vehicles: Challenges and future directions. IEEE wireless communications, σσ. 58-65.

Svanberg, J., & Evans, J. (2014). Impact of SenseCam on memory, identity and mood in Korsakoff's syndrome: A single case experimental design study. Neuropsychological rehabilitation, σσ. 400-418.

Tao, X. (2001). Smart fibres, fabrics and clothing: fundamentals and applications. London: Elsevier.

Thierer, A. (2015). The IoT and wearable technology: Addressing privacy and security concerns without derailing innovation. New York: Self Publiced.

Wei, J. (2014). How Wearables Intersect with the Cloud and the IoT: Considerations for the developers of wearables. IEEE Consumer Electronics Magazine, σσ. 53-56.

Yoo, H., Song, S., Cho, N., & Kim, H. (2007). Low energy on-body communication for BSN. 4th International Workshop on Wearable and Implantable Body Sensor Networks (BSN 2007) (σσ. 15-20). Berlin: Springer.

Zimmerman, T. (1996). Personal area networks: near-field intrabody communication. IBM systems Journal, σσ. 609-617.

Zodik, G. (2015). Wearables, and IoT. 2015 2nd ACM International Conference on Mobile Software Engineering and Systems (σσ. 129-130). IEEE.

Αλεξόπουλος, Α., Λαγογιάννης, Γ., (2012), Τηλεπικοινωνίες και δίκτυα υπολογιστών, Εκδόσεις: Γιαλός

Αρσένης, Σ., (2009), Σχεδιασμός και υλοποίηση δικτύων – Από μικρά δίκτυα γραφείου μέχρι μεγάλα δίκτυα επιχειρήσεων, Εκδόσεις: Κλειδάριθμος

Βενιέρης, Ι., (2012), Δίκτυα ευρείας ζώνης, Εκδόσεις: Τζιόλας

Καραγιαννίδης, Γ., (2009), Τηλεπικοινωνιακά συστήματα, Εκδόσεις: Τζιόλας

Μαργαρίτη, Σ., Στεργίου, Ε., (2006), Τοπικά και αστικά δίκτυα (LAN-MAN), Εκδόσεις: Εκδόσεις Νέων Τεχνολογιών

Tanenbaum, A., (2003), Δίκτυα υπολογιστών, Εκδόσεις: Κλειδάριθμος

Πρέβες, Ν., (2008), Ασύρματα δίκτυα υπολογιστών, Εκδόσεις: Εκδόσεις Νέων Τεχνολογιών

Kurose, R., (2013), Δικτύωση Υπολογιστών, 6η Έκδοση, Εκδόσεις: Γκιούρδας

Hallberg, B., (2011), Δίκτυα, Εκδόσεις: Γκιούρδας

Stallings, W., (2011), Επικοινωνίες υπολογιστών και δεδομένων, Εκδόσεις: Τζιόλας

Ross, J., (2009), Εισαγωγή στην ασύρματη δικτύωση, Εκδόσεις: Κλειδάριθμος

Stallings, W., (2007), Ασύρματες επικοινωνίες και δίκτυα, Εκδόσεις: Τζιόλας

Forouzan, B., (2005), Πρωτόκολλο TCP/IP, Εκδόσεις: Γκιούρδας

White, C., (2012), Data Communications and Computer Networks: A Business User's Approach, Εκδόσεις: Cengage Learning

Peterson, L., Davie, B., (2011), Computer Networks: A Systems Approach, Εκδόσεις: Elsevier

Gupta, P., (2006), Data Communications And Computer Networks, Εκδόσεις: PHI Learning

Kizza, J., (2005), Computer Network Security, Εκδόσεις: Springer

Halsall, F., (2005), Computer Networking and the Internet, Εκδόσεις: Pearson Education

Mansfield, K., Antonakos, J., (2009), Computer Networking for LANS to WANS: Hardware, Software and Security, Εκδόσεις: Cengage Learning

Stewart, K., Adams, A., Reid, A., Lorenz, J., (2008), Designing and Supporting Computer Networks, Εκδόσεις: Cisco Press

Duck, M., Rea, R., (2003), Data Communications and Computer Networks: For Computer Scientists and Engineers, Εκδόσεις: Pearson Education

Shinder, D., (2001), Computer Networking Essentials, Εκδόσεις: Cisco Press

Comer, D., (2009), Computer Networks and Internets, Εκδόσεις: Prentice Hal

Mir, N., (2006), Computer and Communication Networks, Εκδόσεις: Pearson Education

Abbasi, A., Holz, T., Zambon, E., & Etalle, S. (2017, December). ECFI: Asynchronous control flow integrity for programmable logic controllers. In *Proceedings of the 33rd Annual Computer Security Applications Conference* (pp. 437-448).

Alphonsus, E. R., & Abdullah, M. O. (2016). A review on the applications of programmable logic controllers (PLCs). *Renewable and Sustainable Energy Reviews*, *60*, 1185-1205.

Alves, T., Das, R., & Morris, T. (2018). Embedding encryption and machine learning intrusion prevention systems on programmable logic controllers. *IEEE Embedded Systems Letters*, *10*(3), 99-102.

Aydogmus, O., & Talu, M. F. (2012). A vision-based measurement installation for programmable logic controllers. *Measurement*, *45*(5), 1098-1104.

Basnight, Z., Butts, J., Lopez Jr, J., & Dube, T. (2013). Firmware modification attacks on programmable logic controllers. *International Journal of Critical Infrastructure Protection*, *6*(2), 76-84.

Biallas, S., Brauer, J., & Kowalewski, S. (2012, September). Arcade. PLC: A verification platform for programmable logic controllers. In *2012 Proceedings of the 27th IEEE/ACM International Conference on Automated Software Engineering* (pp. 338-341). IEEE.

Bolton, W. (2015). *Programmable logic controllers*. Newnes.

Cruz, T., Simoes, P., & Monteiro, E. (2016). Virtualizing programmable logic controllers: Toward a convergent approach. *IEEE Embedded Systems Letters*, *8*(4), 69-72.

Erickson, K. T. (2016). Programmable Logic Controllers: An emphasis on design and application.

Garcia Jr, A. M. (2014). *Firmware modification analysis in programmable logic controllers*. AIR FORCE INSTITUTE OF TECHNOLOGY WRIGHT-PATTERSON AFB OH GRADUATE SCHOOL OF ENGINEERING AND MANAGEMENT.

Huyck, B., Callebaut, L., Logist, F., Ferreau, H. J., Diehl, M., De Brabanter, J., ... & De Moor, B. (2012). Implementation and experimental validation of classic MPC on programmable logic controllers. In *2012 20th Mediterranean Conference on Control & Automation (MED)* (pp. 679-684). IEEE.

Krupa, P., Limon, D., & Alamo, T. (2018). Implementation of model predictive controllers in programmable logic controllers using IEC 61131-3 standard. In *2018 European Control Conference (ECC)* (pp. 1-6). IEEE.

Leverett, É., & Wightman, R. (2013). Vulnerability inheritance programmable logic controllers. In *Proceedings of the Second International Symposium on Research in Grey-Hat Hacking*.

McLaughlin, S. E. (2011). On Dynamic Malware Payloads Aimed at Programmable Logic Controllers. In *HotSec*.

McLaughlin, S., & McDaniel, P. (2012). SABOT: specification-based payload generation for programmable logic controllers. In *Proceedings of the 2012 ACM conference on Computer and communications security* (pp. 439-449).

McMinn, L., & Butts, J. (2012). A firmware verification tool for programmable logic controllers. In *International Conference on Critical Infrastructure Protection* (pp. 59-69). Springer, Berlin, Heidelberg.

Mrosko, M., & Miklovičová, E. (2012). Real-time implementation of predictive control using programmable logic controllers. *International Journal of Systems Applications, Engineering & Development*, *6*(1), 106-113.

Netto, R., & Bagri, A. (2013). Programmable logic controllers. *International Journal of Computer Applications*, *77*(11).

Qasim, S., Ayub, A., Johnson, J., & Ahmed, I. (2021). Attacking the IEC-61131 Logic Engine in Programmable Logic Controllers in Industrial Control Systems. *Cham: Springer International Publishing*.

Schuett, C., Butts, J., & Dunlap, S. (2014). An evaluation of modification attacks on programmable logic controllers. *International Journal of Critical Infrastructure Protection*, *7*(1), 61-68.

Sehr, M. A., Lohstroh, M., Weber, M., Ugalde, I., Witte, M., Neidig, J., ... & Lee, E. A. (2020). Programmable Logic Controllers in the Context of Industry 4.0. *IEEE Transactions on Industrial Informatics*, *17*(5), 3523-3533.

Stone, S., & Temple, M. (2012). Radio-frequency-based anomaly detection for programmable logic controllers in the critical infrastructure. *International Journal of Critical Infrastructure Protection*, *5*(2), 66-73.

Stouffer, K. A., Falco, J. A., & Scarfone, K. A. (2011). Guide to industrial control systems (ICS) security-supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (PLC).

Wang, R., Song, X., Zhu, J., & Gu, M. (2011). Formal modeling and synthesis of programmable logic controllers. *Computers in Industry*, *62*(1), 23-31.

Wang, C. H., & Wu, H. S. (2016). A novel framework to evaluate programmable logic controllers: a fuzzy MCDM perspective. *Journal of Intelligent Manufacturing*, *27*(2), 315-324.

Xiao, Y. J., Xu, W. Y., Jia, Z. H., Ma, Z. R., & Qi, D. L. (2017). NIPAD: a non-invasive power-based anomaly detection scheme for programmable logic controllers. *Frontiers of Information Technology & Electronic Engineering*, *18*(4), 519-534.

Yang, H., Cheng, L., & Chuah, M. C. (2018). Detecting payload attacks on programmable logic controllers (plcs). In *2018 IEEE Conference on communications and network security (CNS)* (pp. 1-9). IEEE.

Zaytoon, J., & Riera, B. (2017). Synthesis and implementation of logic controllers–A review. *Annual reviews in control*, *43*, 152-168.

Zhang, H., Jiang, Y., Hung, W. N., Song, X., Gu, M., & Sun, J. (2013). Symbolic analysis of programmable logic controllers. *IEEE Transactions on Computers*, *63*(10), 2563-2575.