ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ
ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΑΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ
ΠΜΣ ΣΤΗΝ ΕΠΙΣΤΗΜΗ ΥΠΟΛΟΓΙΣΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«Διαδίκτυο των Πραγμάτων (Internet of Things IOTs)»

Μπέκος Χρήστος

Α.Μ.: 2022202002016

Επιβλέπων καθηγητής: Κωνσταντίνος Πέππας

Τρίπολη | Νοέμβριος 2021

Περίληψη

Διανύουμε μία εποχή στο πεδίο της τεχνολογίας και ιδιαίτερα στο χώρο των υπολογιστών η οποία αποκαλείται το «Διαδίκτυο των Πραγμάτων(Internet of Things IoT)». Το διαδίκτυο των ευφυών πραγμάτων όπως αλλιώς ονομάζεται, παρέχει δυνατότητες που είναι τεράστιες και αξεπέραστες. Το IoT παρουσιάζεται σαν ένα είδος νευρωνικού δικτύου που αποτελείται από συνδεδεμένα «έξυπνα πράγματα» και τα οποία χρησιμοποιούνται στη καθημερινή ζωή μας. Αποτελείται από έξυπνες συσκευές οι οποίες επιδρούν και επικοινωνούν με άλλες συσκευές με αποτέλεσμα να παράγεται ένας μεγάλος όγκος από δεδομένα τα οποία μπορούν να ελέγξουν αλλά αντικείμενα προκειμένου να διευκολύνουν και να κάνουν ασφαλέστερη τη ζωή μας.

Σκοπός της παρούσας εργασίας, είναι η παρουσίαση μιας όσο το δυνατόν πιο ολοκληρωμένης βιβλιογραφικής ανασκόπησης του βιβλίου **«IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things (Copyright© 2017 Cisco Systems, Inc.)»**, με βάση τις πρόσφατες εξελίξεις σε διάφορούς τομείς της τεχνολογίας. Αποτελείται από 13 κεφάλαια. Στην αρχή κάθε κεφαλαίου δίνεται μια συνοπτική περιγραφή του και μια ανάλυση των τεχνολογιών επικοινωνίας που περιλαμβάνει βασισμένες σε IoT. Καλύπτονται όσο το δυνατόν περισσότεροι κλάδοι στους οποίους μπορούν να υλοποιηθούν. Επίσης, παρουσιάζονται οι τρέχουσες προκλήσεις που πρέπει να αντιμετωπίσει η τεχνολογία για να μπορέσει να ανταπεξέλθει στην υιοθέτησή της σε όλους αυτούς του τομείς.

Λέξεις κλειδιά: Ασφάλεια, εφαρμογές σε διάφορους τομείς, πρωτόκολλα επικοινωνίας, τεχνολογίες πληροφοριών και επικοινωνίας, IoT.

Abstract

We are going through an era in the field of technology and especially in the field of computers which is called the «Internet of Things (IoT)». The internet of intelligent things as it is otherwise called, provides possibilities that are huge and insurmountable. IoT is presented as a kind of neural network consisting of connected "smart things" and which are used in our daily lives. It consists of intelligent devices that interact and communicate with other devices resulting in the production of a large amount of data that can control but objects in order to facilitate and make our lives safer.

The purpose of this paper is to present the most comprehensive bibliographic review of **«IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things (Copyright © 2017 Cisco Systems, Inc.)»**, based on recent developments. in various fields of technology. It consists of 13 chapters. At the beginning of each chapter is a brief description and an analysis of communication technologies that includes IoT based. As many branches as possible can be covered in which they can be implemented. It also presents the current challenges that technology must face in order to be able to cope with its adoption in all these areas.

Keywords: Security, applications in various fields, communication protocols, information and communication technologies, IoT.

ΕΥΧΑΡΙΣΤΙΕΣ

Ευχαριστώ τη σύζυγό μου, τα τρία παιδάκια μας, τους γονείς μου, τους καθηγητές μου και τον επιβλέποντα καθηγητή μου κ. Κωνσταντίνο Πέππα, που ήταν αρωγοί μου, στη προσπάθεια που κατέλαβα για να παρακολουθήσω και να ολοκληρώσω με επιτυχία το μεταπτυχιακό πρόγραμμα στην «Επιστήμη των Υπολογιστών» του Πανεπιστημίου Πελοποννήσου. Επιπρόσθετα θα ήθελα να ευχαριστήσω όλους τους ανωτέρους μου στην εργασία που βρίσκομαι(ΟΛΥΜΠΙΑ ΟΔΟ) οι οποίοι με διευκόλυναν ώστε να μπορέσω να παρακολουθήσω τα μαθήματα του μεταπτυχιακού προγράμματος ανελλιπώς. Τέλος, κάθε συνάδελφό μου με τους οποίους συνεργάστηκα στο μεταπτυχιακό πρόγραμμα.
Πάνω από όλους ευχαριστώ τον Θεό που με αξίωσε να γνωρίσω αξιόλογους ανθρώπους και παιδαγωγούς.

Περιεχόμενα

Ευρετήριο Πινάκων

Ευρετήριο Σχημάτων

Εισαγωγή

Το «Διαδίκτυο των Πραγμάτων(Internet of Things IoT)», είναι ένα δίκτυο συσκευών οι οποίες έχουν πρόσβαση στο διαδίκτυο. Οι συσκευές αυτές χάρη στη τεχνολογία που διαθέτουν μπορούν να αλληλεπιδρούν και να επικοινωνούν με το εξωτερικό περιβάλλον. Πρόκειται για μια σύγχρονη, ασύρματη τεχνολογία που μπορεί να εφαρμοστεί σε πολλούς και διαφορετικούς τομείς του πραγματικού κόσμου και αναφέρεται σε ένα μεγάλο αριθμό συσκευών που έχουν τη δυνατότητα πρόσβασης στο διαδίκτυο, πέραν του προσωπικού υπολογιστή και των κινητών συσκευών. Οι πιο συνηθισμένες εφαρμογές αυτής της τεχνολογίας μέχρι σήμερα, είναι στον τομέα της Ιατρικής(με τη δυνατότητα απομακρυσμένης παρακολούθησης της πορείας της υγείας ενός ασθενή), αλλά και στη γραμμή παραγωγής στο βιομηχανικό τομέα. Καθώς η τεχνολογία και τα ασύρματα δίκτυα εξελίσσονται, η τεχνολογία αυτή συναντάται σε περισσότερες συσκευές και τομείς, τόσο του επιχειρηματικού κόσμου, όσο και της ιδιωτικής ζωής του ανθρώπου. Με άλλα λόγια, είναι η τεχνολογία που καθιστά την επικοινωνία του ανθρώπου, με ένα μεγάλο μέρων της καθημερινότητάς του όπως του σπιτιού, των συσκευών της εργασίας του ακόμα και των ζώων.

Κεφάλαιο 1 Διαδίκτυο των πραγμάτων(Internet of Things IoT)

Αυτό το κεφάλαιο παρέχει μια εισαγωγική ματιά στο Διαδίκτυο των Πραγμάτων και απαντά στην ερώτηση: «Τι είναι το IoT;».
Το IoT αφορά τη σύνδεση των μη συνδεδεμένων, επιτρέποντας στα έξυπνα αντικείμενα να επικοινωνούν με άλλα αντικείμενα, συστήματα και άτομα. Το τελικό αποτέλεσμα είναι ένα ευφυές δίκτυο που επιτρέπει περισσότερο έλεγχο του φυσικού κόσμου και ενεργοποίηση προηγμένων εφαρμογών. Παρέχεται επίσης μια ιστορική ματιά στο IoT, μαζί με μια τρέχουσα άποψη για το IoT ως την επόμενη εξελικτική φάση του Διαδικτύου. Γίνεται αναφορά σε μερικές περιπτώσεις χρήσης υψηλού επιπέδου για να δείξει τον αντίκτυπο του IoT και σε μερικούς τρόπους με τους οποίους θα αλλάξει τον κόσμο μας. Επίσης, συζητούνται οι διαφορές μεταξύ IoT και ψηφιοποίησης, καθώς και η σύγκλιση μεταξύ IT και OT. Τέλος αναφέρονται λεπτομερώς οι προκλήσεις που αντιμετωπίζει το IoT.

Κεφάλαιο 1.1 Τι είναι το Διαδίκτυο των πραγμάτων

Η βασική προϋπόθεση και στόχος του IoT είναι να "συνδέσει τα μη συνδεδεμένα". Αυτό σημαίνει ότι τα αντικείμενα που δεν συνδέονται προς το παρόν σε ένα δίκτυο υπολογιστών(δηλαδή το διαδίκτυο), θα είναι συνδεδεμένα έτσι ώστε να μπορούν να επικοινωνούν και να αλληλεπιδρούν με άτομα και άλλα αντικείμενα. Το IoT είναι μια τεχνολογική μετάβαση στην οποία οι συσκευές θα μας επιτρέψουν να αντιληφθούμε και να ελέγξουμε τον φυσικό κόσμο κάνοντας τα αντικείμενα πιο έξυπνα και συνδέοντάς τα μέσω ενός ευφυούς δικτύου.

Όταν τα αντικείμενα και οι μηχανές μπορούν να ανιχνευθούν και να ελεγχθούν εξ αποστάσεως σε ένα δίκτυο, ενεργοποιείται μια αυστηρότερη ενσωμάτωση μεταξύ του φυσικού κόσμου και των υπολογιστών. Αυτό επιτρέπει βελτιώσεις στους τομείς της αποδοτικότητας, της ακρίβειας, της αυτοματοποίησης και της ενεργοποίησης προηγμένων εφαρμογών.

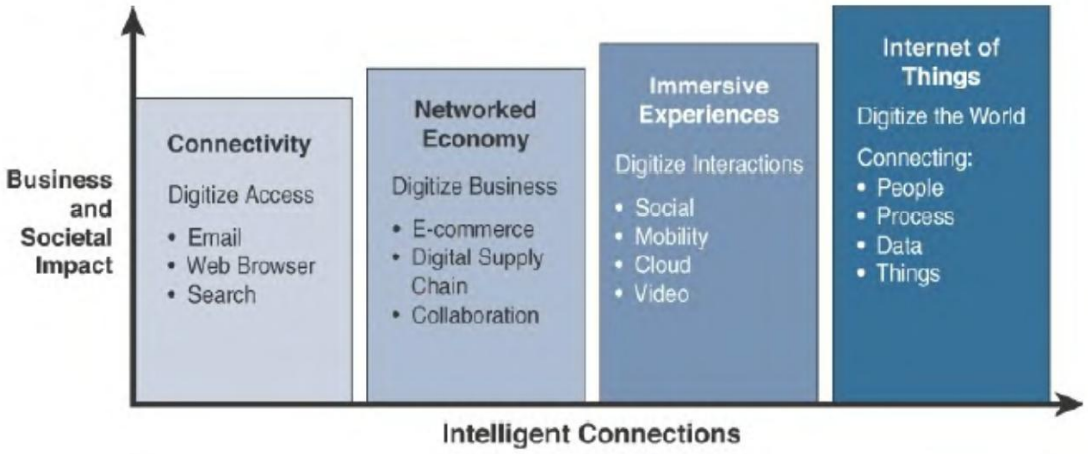
Κεφάλαιο 1.2 Γένεση του IoT

Η ηλικία του IoT λέγεται συχνά ότι ξεκίνησε μεταξύ των ετών 2008 και 2009. Κατά τη διάρκεια αυτής της χρονικής περιόδου, ο αριθμός των συσκευών που ήταν συνδεδεμένες στο Διαδίκτυο επεσκίασε τον παγκόσμιο πληθυσμό. Με περισσότερα «πράγματα» συνδεδεμένα με το Διαδίκτυο από ό, τι οι άνθρωποι στον κόσμο, ήρθε μια νέα εποχή και γεννήθηκε το Διαδίκτυο των Πραγμάτων. Το πρόσωπο που πιστώθηκε για τη δημιουργία του όρου "Internet of Things" είναι ο Kevin Ashton. Ενώ εργαζόταν για την Procter & Gamble το 1999, ο Kevin χρησιμοποίησε αυτή τη φράση για να εξηγήσει μια νέα ιδέα που σχετίζεται με τη σύνδεση της αλυσίδας εφοδιασμού της εταιρείας στο Διαδίκτυο. Ο Kevin εξήγησε στη συνέχεια ότι το IoT περιλαμβάνει τώρα την προσθήκη αισθήσεων στους υπολογιστές. Συγκεκριμένα είπε:

«Τον εικοστό αιώνα, οι υπολογιστές ήταν εγκέφαλοι χωρίς αισθήσεις ήξεραν μόνο αυτά που τους λέγαμε».

Οι υπολογιστές εξαρτώνταν από τον άνθρωπο για να εισάγουν δεδομένα και γνώσεις μέσω πληκτρολόγησης, γραμμικών κωδικών κ.ο.κ. Το IoT αλλάζει αυτό το παράδειγμα. στον εικοστό πρώτο αιώνα, οι υπολογιστές αντιλαμβάνονται τα πράγματα για τον εαυτό τους.
Είναι ευρέως αποδεκτό ότι το IoT είναι μια σημαντική τεχνολογική αλλαγή, αλλά ποια είναι η κλίμακα και η σημασία του; Πού ταιριάζει στην εξέλιξη του Διαδικτύου ;

Όπως φαίνεται στο Σχήμα 1, η εξέλιξη του Διαδικτύου μπορεί να κατηγοριοποιηθεί σε τέσσερις φάσεις. Κάθε μία από αυτές τις φάσεις είχε σημαντικό αντίκτυπο στην κοινωνία και τη ζωή μας. Αυτές οι τέσσερις φάσεις ορίζονται περαιτέρω στον Πίνακα 1.



Σχήμα 1: Εξελικτικές φάσεις του Διαδικτύου.

Κάθε μία από αυτές τις εξελικτικές φάσεις βασίζεται στην προηγούμενη. Με κάθε επόμενη φάση, διατίθεται περισσότερη αξία για τις επιχειρήσεις, τις κυβερνήσεις και την κοινωνία γενικότερα.

Η πρώτη φάση, η συνδεσιμότητα, ξεκίνησε στα μέσα της δεκαετίας του 1990. Στην αρχή, το email και η πρόσβαση στο Διαδίκτυο ήταν πολυτέλεια για πανεπιστήμια και εταιρείες. Η συμμετοχή του μέσου ατόμου στο διαδίκτυο μέσω μόντεμ μέσω τηλεφώνου και ακόμη και η βασική συνδεσιμότητα συχνά φαινόταν σαν ένα μικρό θαύμα. Παρόλο που η συνδεσιμότητα και η ταχύτητά της συνέχισαν να βελτιώνονται, επιτεύχθηκε ένα σημείο

κορεσμού όπου η συνδεσιμότητα δεν ήταν πλέον η κύρια πρόκληση. Το επίκεντρο ήταν τώρα στη μόχλευση της συνδεσιμότητας για αποδοτικότητα και κέρδος.

Αυτό το σημείο καμπής σηματοδότησε την αρχή της δεύτερης φάσης της εξέλιξης του διαδικτύου, που ονομάζεται Δικτυωμένη Οικονομία. Με τη Δικτυωμένη Οικονομία, το ηλεκτρονικό εμπόριο και οι ψηφιακά συνδεδεμένες αλυσίδες εφοδιασμού έγιναν μανία και αυτό προκάλεσε μία από τις μεγαλύτερες διαταραχές των τελευταίων 100 ετών. Οι προμηθευτές και οι πωλητές συνδέθηκαν στενά με τους παραγωγούς και οι διαδικτυακές αγορές γνώρισαν απίστευτη ανάπτυξη. Τα θύματα αυτής της αλλαγής ήταν οι παραδοσιακοί λιανοπωλητές. Η ίδια η οικονομία έγινε πιο ψηφιακά συνυφασμένη καθώς οι προμηθευτές, οι πωλητές και οι καταναλωτές συνδέθηκαν άμεσα.

Η τρίτη φάση(εντυπωσιακές εμπειρίες (Immersive Experiences)), χαρακτηρίζεται από την εμφάνιση κοινωνικών μέσων, τη συνεργασία και την ευρεία κινητικότητα σε μια ποικιλία συσκευών. Η συνδεσιμότητα είναι πλέον διάχυτη, χρησιμοποιώντας πολλαπλές πλατφόρμες από κινητά τηλέφωνα έως tablet έως φορητούς υπολογιστές και επιτραπέζιους υπολογιστές. Αυτή η διάχυτη συνδεσιμότητα με τη σειρά της επιτρέπει την επικοινωνία και τη συνεργασία καθώς και τα κοινωνικά μέσα σε πολλά κανάλια, μέσω email, γραπτών μηνυμάτων, φωνής και βίντεο. Ουσιαστικά, οι αλληλεπιδράσεις από άτομο σε άτομο έχουν ψηφιοποιηθεί.

Η τελευταία φάση είναι το **«Διαδίκτυο των Πραγμάτων».** Οι μηχανές και τα αντικείμενα σε αυτή τη φάση συνδέονται με άλλα μηχανήματα και αντικείμενα, μαζί με τους ανθρώπους. Οι επιχειρήσεις και η κοινωνία έχουν ήδη ξεκινήσει σε αυτόν τον δρόμο και αντιμετωπίζουν τεράστιες αυξήσεις δεδομένων και γνώσεων. Το IoT είναι έτοιμο να αλλάξει τον κόσμο μας με νέους και συναρπαστικούς τρόπους, όπως έχουν κάνει ήδη οι προηγούμενες φάσεις του διαδικτύου.

Internet Phase	Definition
Connectivity (Digitize access)	This phase connected people to email, web services, and search so that information is easily accessed.
Networked Economy (Digitize business)	This phase enabled e-commerce and supply chain enhancements along with collaborative engagement to drive increased efficiency in business processes.
Immersive Experiences (Digitize interactions)	This phase extended the Internet experience to encompass widespread video and social media while always being connected through mobility. More and more applications are moved into the cloud.
Internet of Things (Digitize the world)	This phase is adding connectivity to objects and machines in the world around us to enable new services and experiences. It is connecting the unconnected.

Πίνακας 1: Εξελικτικές φάσεις του διαδικτύου.

Κεφάλαιο 1.3 IoT και ψηφιοποίηση

IoT και η ψηφιοποίηση είναι όροι που χρησιμοποιούνται συχνά εναλλακτικά. Σε υψηλό επίπεδο, το IoT επικεντρώνεται στη σύνδεση «πραγμάτων», όπως αντικειμένων και μηχανών, σε ένα δίκτυο υπολογιστών, όπως το Διαδίκτυο. IoT είναι ένας καλά κατανοητός όρος που χρησιμοποιείται σε ολόκληρο τον κλάδο. Από την άλλη πλευρά, η ψηφιοποίηση μπορεί να σημαίνει διαφορετικά πράγματα για διαφορετικούς ανθρώπους, αλλά γενικά περιλαμβάνει τη σύνδεση των "πραγμάτων" με τα δεδομένα που παράγουν και τις επιχειρηματικές γνώσεις που προκύπτουν. Για παράδειγμα, σε ένα εμπορικό κέντρο όπου έχει αναπτυχθεί η παρακολούθηση τοποθεσίας Wi-Fi, τα «πράγματα» είναι οι συσκευές Wi-Fi. Η παρακολούθηση τοποθεσίας Wi-Fi είναι απλώς η ικανότητα να γνωρίζουμε πού βρίσκεται ένας καταναλωτής σε περιβάλλον λιανικής μέσω της σύνδεσης του έξυπνου τηλεφώνου του με το δίκτυο Wi-Fi του λιανοπωλητή.
Ενώ η αξία της σύνδεσης συσκευών Wi-Fi ή «πραγμάτων» στο διαδίκτυο είναι προφανής και εκτιμάται από τους αγοραστές, η παρακολούθηση της τοποθεσίας σε πραγματικό χρόνο των πελατών Wi-Fi παρέχει ένα συγκεκριμένο επιχειρηματικό όφελος στους ιδιοκτήτες του εμπορικού κέντρου και των καταστημάτων. Σε αυτήν την περίπτωση, βοηθάει την επιχείρηση να καταλάβει πού τείνουν να συγκεντρώνονται οι αγοραστές και πόσο χρόνο περνούν σε διαφορετικά μέρη ενός εμπορικού κέντρου ή καταστήματος. Η ανάλυση αυτών των δεδομένων μπορεί να οδηγήσει σε σημαντικές αλλαγές στις τοποθεσίες εμφάνισης προϊόντων και διαφημίσεων.

Η ψηφιοποίηση, όπως ορίζεται στην απλούστερη μορφή της, είναι η μετατροπή πληροφοριών σε ψηφιακή μορφή. Η ψηφιοποίηση συμβαίνει με τη μία ή την άλλη μορφή εδώ και αρκετές δεκαετίες. Για παράδειγμα, ολόκληρη η βιομηχανία φωτογραφίας έχει ψηφιοποιηθεί. Σχεδόν όλοι έχουν ψηφιακές φωτογραφικές μηχανές αυτές τις μέρες, είτε μεμονωμένες συσκευές είτε ενσωματωμένες στο κινητό τους τηλέφωνο. Σχεδόν κανείς δεν αγοράζει ταινία και τη μεταφέρει σε λιανοπωλητή για να την αναπτύξει. Η ψηφιοποίηση της φωτογραφίας έχει αλλάξει εντελώς την εμπειρία μας όσον αφορά τη λήψη φωτογραφιών.

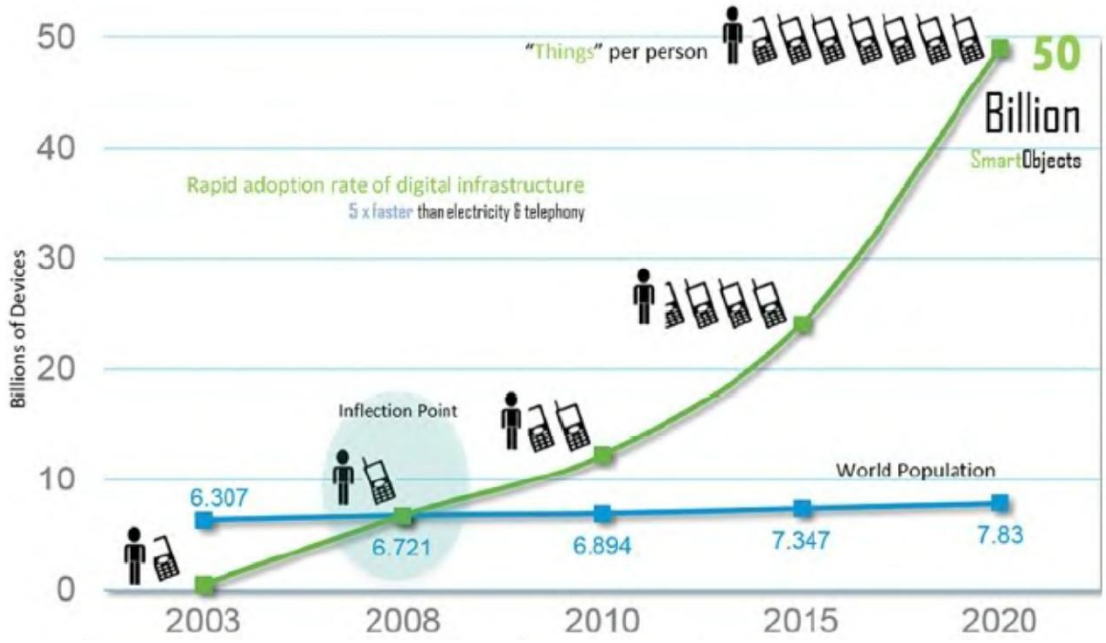
Άλλα παραδείγματα ψηφιοποίησης περιλαμβάνουν τη βιομηχανία ενοικίασης βίντεο και τη μεταφορά. Στο παρελθόν, οι άνθρωποι πήγαιναν σε ένα κατάστημα για να νοικιάσουν ή να αγοράσουν βιντεοκασέτες ή DVD ταινιών. Με την ψηφιοποίηση, σχεδόν όλοι μεταδίδουν περιεχόμενο βίντεο ή αγοράζουν ταινίες ως αρχεία με δυνατότητα λήψης.
Ο κλάδος των μεταφορών βρίσκεται σε φάση ψηφιοποίησης στον τομέα των υπηρεσιών ταξί. Επιχειρήσεις όπως η Uber και η Lyft χρησιμοποιούν ψηφιακές τεχνολογίες για να επιτρέψουν στους ανθρώπους να κάνουν βόλτα χρησιμοποιώντας μια εφαρμογή για κινητά τηλέφωνα. Αυτή η εφαρμογή προσδιορίζει το αυτοκίνητο, τον οδηγό και τα ναύλα. Στη συνέχεια, ο αναβάτης πληρώνει τα ναύλα χρησιμοποιώντας την εφαρμογή. Αυτή η ψηφιοποίηση αποτελεί μια σημαντική διατάραξη για τις εταιρείες που παρέχουν παραδοσιακές υπηρεσίες ταξί.

Στο πλαίσιο του IoT, η ψηφιοποίηση συγκεντρώνει πράγματα, δεδομένα και επιχειρηματική διαδικασία για να καταστήσει τις δικτυακές συνδέσεις πιο συναφείς και πολύτιμες. Ένα καλό παράδειγμα αυτού με το οποίο μπορούν να συσχετιστούν πολλοί είναι στον τομέα της αυτοματοποίησης του σπιτιού με δημοφιλή προϊόντα, όπως το Nest. Με το Nest, οι αισθητήρες καθορίζουν τις επιθυμητές κλιματικές ρυθμίσεις και συνδέονται με άλλα έξυπνα αντικείμενα, όπως συναγερμούς καπνού, βιντεοκάμερες και διάφορες συσκευές τρίτων. Στο παρελθόν, αυτές οι συσκευές και οι λειτουργίες που εκτελούσαν διαχειρίζονταν

και ελέγχονταν ξεχωριστά και δεν μπορούσαν να παρέχουν την ολιστική εμπειρία που είναι πλέον δυνατή.

Κεφάλαιο 1.4 Αντίκτυπος του IoT

Οι προβολές για τον πιθανό αντίκτυπο του IoT είναι εντυπωσιακές. Περίπου 14 δισεκατομμύρια, ή μόλις το 0,06%, των «πραγμάτων» είναι συνδεδεμένα στο Διαδίκτυο σήμερα. Η Cisco Systems προέβλεπε ότι μέχρι το 2020, ο αριθμός αυτός θα έφτανε τα 50 δισεκατομμύρια. Μια βρετανική έκθεση της κυβέρνησης εικάζει ότι αυτός ο αριθμός θα μπορούσε να είναι ακόμη μεγαλύτερος, στην περιοχή των 100 δισεκατομμυρίων αντικειμένων που συνδέονται. Η Cisco εκτιμά περαιτέρω ότι αυτές οι νέες συνδέσεις θα οδηγήσουν σε 19 τρισεκατομμύρια δολάρια σε κέρδη και εξοικονόμηση κόστους.
Το Σχήμα 2 παρέχει μια γραφική ματιά στην αύξηση του αριθμού των συνδεδεμένων συσκευών.



Σχήμα 2: Η ταχεία ανάπτυξη του αριθμού των συσκευών που συνδέονται στο διαδίκτυο.

Αυτό που σημαίνουν αυτοί οι αριθμοί είναι ότι το IoT θα αλλάξει ριζικά τον τρόπο που οι άνθρωποι και οι επιχειρήσεις αλληλεπιδρούν με το περιβάλλον τους. Διαχείριση και παρακολούθηση έξυπνων αντικειμένων χρησιμοποιώντας συνδεσιμότητα σε πραγματικό χρόνο επιτρέπει ένα εντελώς νέο επίπεδο λήψης αποφάσεων με βάση τα δεδομένα. Αυτό με τη σειρά του οδηγεί στη βελτιστοποίηση των συστημάτων και των διαδικασιών και παρέχει νέες υπηρεσίες που εξοικονομούν χρόνο τόσο για τους ανθρώπους όσο και για τις επιχειρήσεις, ενώ βελτιώνουν τη συνολική ποιότητα ζωής.

Τα παρακάτω παραδείγματα απεικονίζουν μερικά από τα οφέλη του IoT και τον αντίκτυπό τους. Αυτά τα παραδείγματα θα σας προσφέρουν μια υψηλού επιπέδου εικόνα των πρακτικών περιπτώσεων χρήσης IoT για να καταδείξουν με σαφήνεια πώς το IoT θα επηρεάσει την καθημερινή ζωή.

Κεφάλαιο 1.5 Συνδεδεμένοι δρόμοι

Το IoT θα επιτρέψει στα αυτόνομα οχήματα να αλληλεπιδρούν καλύτερα με το σύστημα μεταφοράς γύρω τους μέσω αμφίδρομης ανταλλαγής δεδομένων, παρέχοντας παράλληλα σημαντικά δεδομένα στους αναβάτες. Τα αυτόνομα οχήματα χρειάζονται πάντα ενεργοποιημένες, αξιόπιστες επικοινωνίες και δεδομένα από άλλους αισθητήρες που σχετίζονται με τη μεταφορά για να αξιοποιήσουν πλήρως τις δυνατότητές τους.
Συνδεδεμένοι δρόμοι είναι ο όρος που σχετίζει τόσο αυτοκίνητα με οδηγό όσο και με αυτοκίνητα χωρίς οδηγό που ενσωματώνονται πλήρως στη γύρω υποδομή μεταφορών.
Το Σχήμα 3 δείχνει ένα αυτόνομο αυτοκίνητο σχεδιασμένο από την Google.

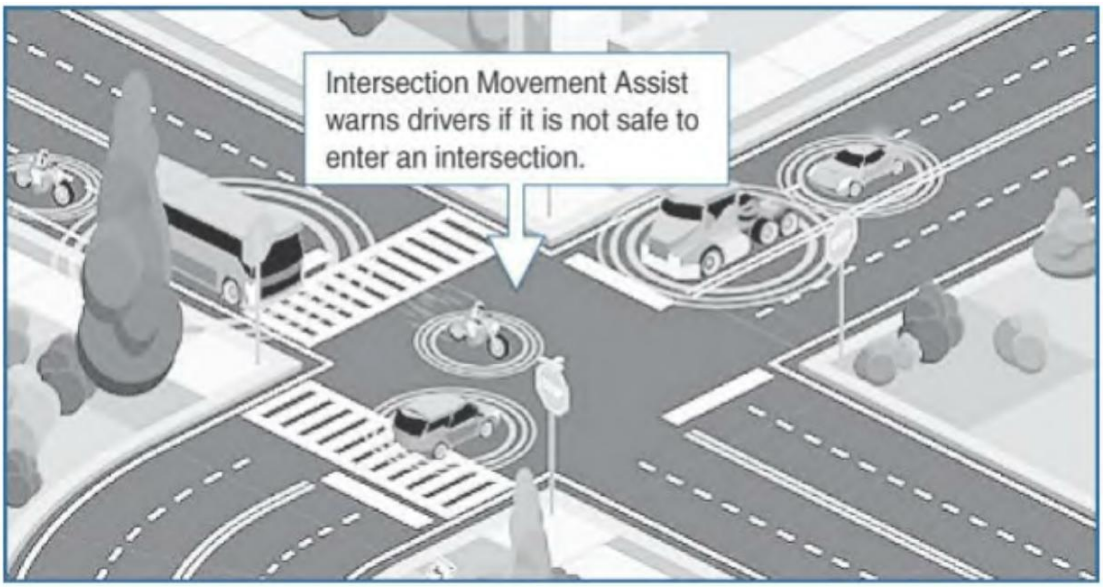
Σχήμα 3: Google's Self-Driving Car.

Οι βασικοί αισθητήρες βρίσκονται ήδη στα αυτοκίνητα. Παρακολουθούν την πίεση λαδιού, την πίεση των ελαστικών, τη θερμοκρασία και άλλες συνθήκες λειτουργίας και παρέχουν δεδομένα σχετικά με τις βασικές λειτουργίες του αυτοκινήτου. Από πίσω από το τιμόνι, ο οδηγός μπορεί να έχει πρόσβαση σε αυτά τα δεδομένα ενώ ελέγχει επίσης το αυτοκίνητο χρησιμοποιώντας εξοπλισμό όπως τιμόνι, πεντάλ κ.ο.κ.

Η ανάγκη για όλες αυτές τις αισθητηριακές πληροφορίες και έλεγχο είναι προφανής. Ο οδηγός πρέπει να είναι σε θέση να κατανοεί, να χειρίζεται και να λαμβάνει κρίσιμες αποφάσεις ενώ συγκεντρώνεται στην ασφαλή οδήγηση. Το Διαδίκτυο των Πραγμάτων επαναλαμβάνει αυτήν την έννοια σε πολύ μεγαλύτερη κλίμακα. Σήμερα, βλέπουμε αυτοκίνητα που παράγονται με χιλιάδες αισθητήρες, για να μετρήσουν τα πάντα, από την κατανάλωση καυσίμου έως την τοποθεσία μέχρι την ψυχαγωγία που παρακολουθεί η οικογένειά σας κατά τη διάρκεια της βόλτας. Καθώς οι κατασκευαστές αυτοκινήτων προσπαθούν να επανεφεύρουν την οδηγική εμπειρία, αυτοί οι αισθητήρες ενεργοποιούνται με IP για να επιτρέπουν την εύκολη επικοινωνία με άλλα συστήματα τόσο μέσα όσο και έξω από το αυτοκίνητο. Επιπλέον, αναπτύσσονται νέοι αισθητήρες και τεχνολογίες επικοινωνίας που επιτρέπουν στα οχήματα να επικοινωνούν με άλλα οχήματα, σήματα κυκλοφορίας, σχολικές ζώνες και άλλα στοιχεία της υποδομής μεταφοράς.

Αρχίζουμε τώρα να συνειδητοποιούμε μια πραγματικά συνδεδεμένη λύση μεταφοράς καθώς, οι συνδεδεμένοι δρόμοι θα αποφέρουν πολλά οφέλη στην κοινωνία. Αυτά τα οφέλη περιλαμβάνουν μειωμένη κυκλοφοριακή συμφόρηση και αστική συμφόρηση, μειωμένα θύματα και θανάτους, αυξημένο χρόνο απόκρισης για οχήματα έκτακτης ανάγκης και μειωμένες εκπομπές οχημάτων.

Για παράδειγμα, για τους δρόμους που συνδέονται με το IoT, είναι δυνατή μια έννοια γνωστή ως Intersection Movement Assist (IMA). Αυτή η εφαρμογή προειδοποιεί έναν οδηγό όταν δεν είναι ασφαλές να εισέλθει σε μια διασταύρωση λόγω μεγάλης πιθανότητας σύγκρουσης. Χάρη στο σύστημα επικοινωνιών μεταξύ των οχημάτων και της υποδομής, αυτό το είδος σεναρίου μπορεί να αντιμετωπιστεί γρήγορα και με ασφάλεια.
Στο Σχήμα 4 φαίνεται μια γραφική αναπαράσταση του IMA.



Σχήμα 4: Εφαρμογή Intersection Movement Assist (IMA).

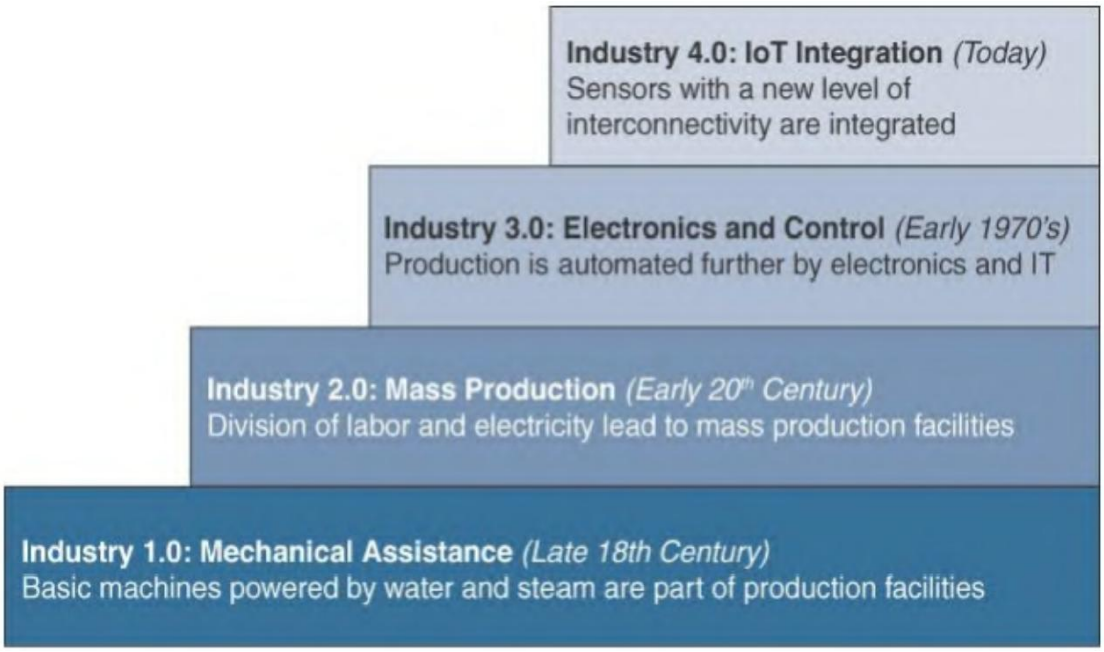
IMA είναι μία από τις πολλές πιθανές οδικές λύσεις που προκύπτουν όταν αρχίζουμε να ενσωματώνουμε το IoT τόσο με τα παραδοσιακά όσο και με τα αυτόνομα οχήματα. Άλλες λύσεις περιλαμβάνουν αυτοματοποιημένη παρακολούθηση οχημάτων, διαχείριση φορτίου και οδικές επικοινωνίες καιρού.

Κεφάλαιο 1.6 Συνδεδεμένο Εργοστάσιο

Οι βιομηχανικές επιχειρήσεις σε όλο τον κόσμο εξοπλίζουν τα εργοστάσιά τους με προηγμένες τεχνολογίες και αρχιτεκτονικές για να επιλύσουν προβλήματα που αντιμετωπίζουν καθώς και να αυξήσουν την ευελιξία και την ταχύτητα της παραγωγής τους. Αυτές οι βελτιώσεις τους βοηθούν να επιτύχουν νέα επίπεδα συνολικής αποτελεσματικότητας εξοπλισμού, απόκρισης εφοδιαστικής αλυσίδας και ικανοποίησης πελατών. Μια σύγκλιση λειτουργικών τεχνολογιών και αρχιτεκτονικών που βασίζονται σε εργοστάσια με παγκόσμια δίκτυα πληροφορικής έχει αρχίσει να εμφανίζεται και αυτό αναφέρεται ως «συνδεδεμένο εργοστάσιο».
Όπως και με τις λύσεις IoT για τους συνδεδεμένους δρόμους που αναφέραμε προηγουμένως, υπάρχει ήδη μεγάλος αριθμός βασικών αισθητήρων στα εργοστασιακά δάπεδα. Ωστόσο, με το IoT, αυτοί οι αισθητήρες όχι μόνο γίνονται πιο προηγμένοι αλλά επιτυγχάνουν ένα νέο επίπεδο συνδεσιμότητας. Είναι πιο έξυπνοι και αποκτούν τη

δυνατότητα επικοινωνίας, κυρίως χρησιμοποιώντας το Πρωτόκολλο Διαδικτύου (IP) μέσω υποδομής Ethernet.
Εκτός από τους αισθητήρες, οι συσκευές στο πάτωμα γίνονται πιο έξυπνες στην ικανότητά τους να μεταδίδουν και να λαμβάνουν μεγάλες ποσότητες πληροφοριών και διαγνωστικών δεδομένων σε πραγματικό χρόνο. Η συνδεσιμότητα Ethernet γίνεται διάχυτη και εξαπλώνεται πέρα από τους κύριους ελεγκτές ενός εργοστασίου σε συσκευές όπως τα ρομπότ στο πάτωμα των εγκαταστάσεων. Επιπλέον, περισσότερες συσκευές με δυνατότητα IP, όπως βιντεοκάμερες, διαγνωστικά έξυπνα αντικείμενα, ακόμη και προσωπικές κινητές συσκευές, προστίθενται στο περιβάλλον κατασκευής.

Ενώ βλέπουμε ότι το IoT προκαλεί την εξέλιξη του διαδικτύου, προκαλεί επίσης εξέλιξη στο τομέα της βιομηχανίας. Το 2016 το Παγκόσμιο Οικονομικό Φόρουμ αναφέρθηκε στην εξέλιξη του διαδικτύου και τον αντίκτυπο του IoT ως «τέταρτη βιομηχανική επανάσταση».
Η πρώτη βιομηχανική επανάσταση, συνέβη στην Ευρώπη στα τέλη του δέκατου όγδοου αιώνα, με την εφαρμογή ατμού και νερού στη μηχανική παραγωγή. Η δεύτερη βιομηχανική επανάσταση, που πραγματοποιήθηκε μεταξύ των αρχών της δεκαετίας του 1870 και των αρχών του εικοστού αιώνα, είδε την εισαγωγή του ηλεκτρικού δικτύου και τη μαζική παραγωγή. Η τρίτη επανάσταση, ήρθε στα τέλη της δεκαετίας του 1960/αρχές της δεκαετίας του 1970, καθώς οι υπολογιστές και τα ηλεκτρονικά άρχισαν να αφήνουν το στίγμα τους στην κατασκευή και σε άλλα βιομηχανικά συστήματα. Η τέταρτη βιομηχανική επανάσταση, συμβαίνει τώρα και το διαδίκτυο των Πραγμάτων την οδηγεί.
Το Σχήμα 5 συνοψίζει αυτές τις τέσσερις βιομηχανικές επαναστάσεις.



Σχήμα 5: Οι τέσσερις βιομηχανικές επαναστάσεις.

Η επανάσταση του IoT στη βιομηχανία μεταφέρει την παραγωγή από ένα αμιγώς αυτοματοποιημένο μοντέλο παραγωγής γραμμών συναρμολόγησης σε ένα μοντέλο όπου οι μηχανές είναι έξυπνες και επικοινωνούν μεταξύ τους. Το IoT στην κατασκευή φέρνει μαζί του την ευκαιρία για την εισαγωγή της νοημοσύνης στα εργοστάσια. Αυτό ξεκινά με τη δημιουργία έξυπνων αντικειμένων, η οποία περιλαμβάνει την ενσωμάτωση αισθητήρων, και ελεγκτών σε σχεδόν οτιδήποτε σχετίζεται με την παραγωγή. Έτσι άνθρωποι και μηχανές συνεργάζονται για την ανάλυση των δεδομένων και τη λήψη έξυπνων αποφάσεων.

Τελικά αυτό οδηγεί σε έναν κόσμο όπου η ανθρώπινη παρακολούθηση και παρέμβαση δεν είναι πλέον απαραίτητες.

Κεφάλαιο 1.7 Έξυπνα συνδεδεμένα κτίρια

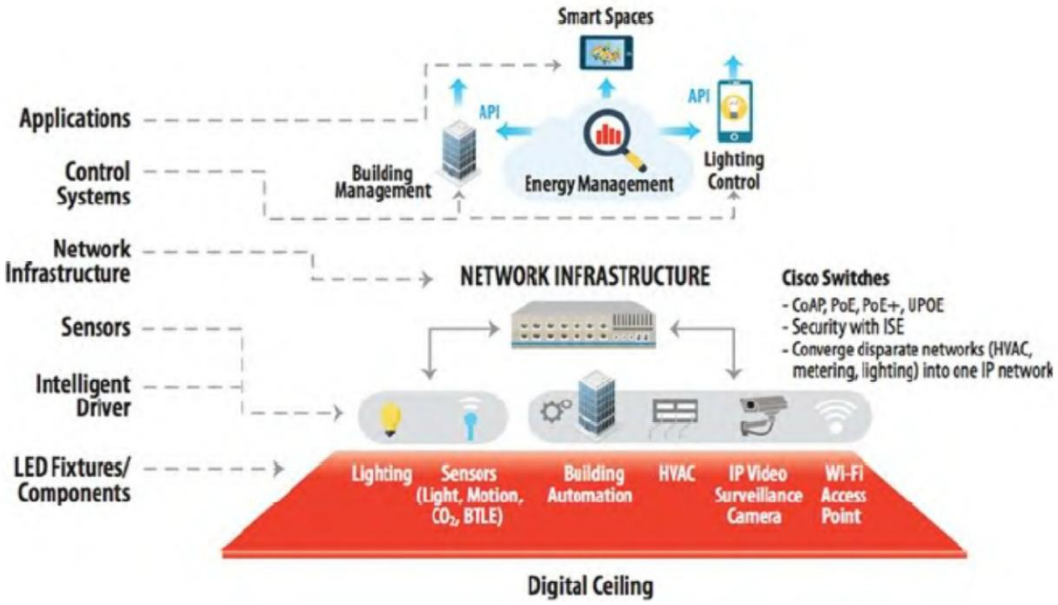
Ένα άλλο μέρος που το IoT προκαλεί αντίκτυπο είναι στο χώρο των έξυπνων συνδεδεμένων κτιρίων. Η λειτουργία ενός κτιρίου είναι να παρέχει ένα εργασιακό περιβάλλον που να διατηρεί τους εργαζόμενους άνετους, αποτελεσματικούς και ασφαλείς. Οι χώροι εργασίας πρέπει να είναι καλά φωτισμένοι και να διατηρούνται σε άνετη θερμοκρασία. Για να διατηρηθεί η ασφάλεια των εργαζομένων, το σύστημα συναγερμού και καταστολής πυρκαγιάς πρέπει να διαχειρίζεται προσεκτικά, όπως και τα συστήματα συναγερμού πόρτας και φυσικής ασφάλειας. Ενώ τα έξυπνα συστήματα για σύγχρονα κτίρια αναπτύσσονται και βελτιώνονται για καθεμία από αυτές τις λειτουργίες, τα περισσότερα από αυτά τα συστήματα λειτουργούν σήμερα ανεξάρτητα το ένα από το άλλο και σπάνια λαμβάνουν υπόψη πού βρίσκονται οι ένοικοι του κτιρίου και πόσα από αυτά υπάρχουν διαφορετικά μέρη του κτιρίου. Ωστόσο, πολλά κτίρια αρχίζουν να αναπτύσσουν αισθητήρες σε όλο το κτίριο για τον εντοπισμό πληρότητας. Αυτά τείνουν να είναι αισθητήρες κίνησης ή αισθητήρες δεμένοι με βιντεοκάμερες.

Οι αισθητήρες πληρότητας ανίχνευσης κίνησης λειτουργούν τέλεια εάν όλοι μετακινούνται σε ένα δωμάτιο με πολύ κόσμο και μπορούν να κλείσουν αυτόματα τα φώτα όταν φύγουν όλοι. Ομοίως, οι αισθητήρες χρησιμοποιούνται συχνά για τον έλεγχο του συστήματος θέρμανσης, εξαερισμού και κλιματισμού (HVAC). Οι αισθητήρες θερμοκρασίας απλώνονται σε όλο το κτίριο και χρησιμοποιούνται για να επηρεάσουν τον έλεγχο του συστήματος διαχείρισης κτιρίου της ροής αέρα σε ένα δωμάτιο. Μια άλλη ενδιαφέρουσα πτυχή του έξυπνου κτιρίου είναι ότι το καθιστά ευκολότερο και φθηνότερο στη διαχείριση. Λαμβάνοντας υπόψη το τεράστιο κόστος που συνεπάγεται η λειτουργία τέτοιων σύνθετων κατασκευών, οι διαχειριστές ενδιαφέρονται ολοένα και περισσότερο για τρόπους που θα κάνουν τα κτίρια πιο αποδοτικά και φθηνότερα στη διαχείριση.

Εναλλακτικά, ο διαχειριστής κτιρίου μπορεί να χρησιμοποιήσει μια παρόμοια προσέγγιση για να δει πού το δάπεδο δεν χρησιμοποιείται αποτελεσματικά και να χρησιμοποιήσει αυτές τις πληροφορίες για τη βελτιστοποίηση του διαθέσιμου χώρου. Αυτό έφερε την εποχή της αυτοματοποίησης κτιρίων, που ενισχύθηκε από το IoT.
Ενώ υπάρχουν πολλές τεχνικές λύσεις για τη φροντίδα της οικοδόμησης συστημάτων, μέχρι πρόσφατα όλα απαιτούσαν ξεχωριστά δίκτυα επικάλυψης, καθένα από τα οποία ήταν υπεύθυνο για το καθήκον του. Σε μια προσπάθεια σύνδεσης αυτών των συστημάτων σε ένα ενιαίο πλαίσιο, το «σύστημα αυτοματισμού κτιρίου (Building Automation System BAS)» αναπτύχθηκε για να παρέχει ένα ενιαίο σύστημα διαχείρισης για τα συστήματα HVAC, φωτισμού, συναγερμού πυρκαγιάς και ανίχνευσης, καθώς και έλεγχο πρόσβασης. Όλα αυτά τα συστήματα ενδέχεται να υποστηρίζουν διαφορετικούς τύπους αισθητήρων και συνδέσεων με το BAS και θα πρέπει να συνδεθούν μεταξύ τους ώστε να μπορεί να διαχειριστεί το κτίριο με συνεκτικό τρόπο; Αυτό τονίζει μια από τις μεγαλύτερες προκλήσεις στο IoT, η οποία συζητείται σε αυτό το βιβλίο: η ετερογένεια των συστημάτων IoT.
Εναλλακτικά, ο διαχειριστής κτιρίου μπορεί να χρησιμοποιήσει μια παρόμοια προσέγγιση για να δει πού το δάπεδο δεν χρησιμοποιείται αποτελεσματικά και να χρησιμοποιήσει αυτές τις πληροφορίες για τη βελτιστοποίηση του διαθέσιμου χώρου. Αυτό έφερε την εποχή της αυτοματοποίησης κτιρίων, που ενισχύθηκε από το IoT.

Μια άλλη πολλά υποσχόμενη τεχνολογία IoT στο έξυπνα συνδεδεμένο κτίριο, και αυτή που βλέπει ευρεία υιοθέτηση, είναι το «ψηφιακό ανώτατο όριο» (digital ceiling).

Το ψηφιακό ανώτατο όριο είναι κάτι περισσότερο από ένα σύστημα ελέγχου φωτισμού. Αυτή η τεχνολογία περιλαμβάνει πολλά από τα διαφορετικά δίκτυα του κτιρίου-συμπεριλαμβανομένου του φωτισμού, του HVAC, των περσίδων, των CCTV (κλειστού κυκλώματος τηλεόρασης) και των συστημάτων ασφαλείας- και τα συνδυάζει σε ένα ενιαίο δίκτυο IP. Το Σχήμα 6 παρέχει ένα πλαίσιο για την ψηφιακή οροφή.



Σχήμα 6: Ένα πλαίσιο για το ψηφιακό ανώτατο όριο.

Κεντρικό στοιχείο της ψηφιακής τεχνολογίας οροφής είναι το σύστημα φωτισμού. Σε ένα ψηφιακό περιβάλλον οροφής, κάθε φωτιστικό συνδέεται απευθείας με το δίκτυο, παρέχοντας έλεγχο και ισχύ στην ίδια υποδομή. Αυτή η μετάβαση στον φωτισμό LED σημαίνει ότι ένα ενιαίο συγκλίνον δίκτυο είναι πλέον σε θέση να περιλαμβάνει φωτιστικά σώματα που αποτελούν μέρος της ενοποιημένης διαχείρισης κτιρίων, καθώς και στοιχεία που διαχειρίζονται από το δίκτυο IT, υποστηρίζοντας φωνή, βίντεο και άλλες εφαρμογές δεδομένων. Αυτή η μακροπρόθεσμη επιχειρηματική περίπτωση που υποστηρίζει μειωμένο κόστος ενέργειας από φωτιστικά LED έναντι παραδοσιακών φώτων φθορισμού ή αλογόνου είναι τόσο σημαντική που η προστιθέμενη αρχική επένδυση στο δίκτυο είναι σχεδόν ασήμαντη.
Ωστόσο, η ύπαρξη μιας συσκευής αισθητήρα με δυνατότητα IP στο ταβάνι σε κάθε σημείο όπου μπορεί να είναι παρόντες άνθρωποι ανοίγει ένα εντελώς νέο σύνολο δυνατοτήτων.
Για παράδειγμα, τα περισσότερα σύγχρονα φωτιστικά οροφής LED υποστηρίζουν αισθητήρες πληρότητας. Αυτοί οι αισθητήρες παρέχουν συλλογή δεδομένων πληρότητας υψηλής ανάλυσης, η οποία μπορεί να χρησιμοποιηθεί για να ανάψει και να σβήσει τα φώτα, και αυτά τα ίδια δεδομένα μπορούν να συνδυαστούν με προηγμένα αναλυτικά στοιχεία για τον έλεγχο άλλων συστημάτων, όπως HVAC και ασφάλεια.

Σε αντίθεση με τους παραδοσιακούς αισθητήρες που χρησιμοποιούν στοιχειώδη ανίχνευση κίνησης, οι σύγχρονοι αισθητήρες φωτισμού ενσωματώνουν μια ποικιλία τεχνολογιών ανίχνευσης πληρότητας, όπως Bluetooth χαμηλής ενέργειας (BLE) και WiFi. Η επιστήμη εδώ είναι απλή: Επειδή σχεδόν κάθε άτομο αυτές τις μέρες φέρει μια έξυπνη συσκευή που υποστηρίζει BLE και Wi-Fi, το μόνο που έχει να κάνει ο αισθητήρας είναι να εντοπίσει αυτά τα συγκεκριμένα BLE ή Wi-Fi από μια κοντινή συσκευή.

Όταν κάποιος περπατά κοντά σε ένα φως, εντοπίζεται η τοποθεσία του ατόμου και το ασύρματο σύστημα μπορεί να στείλει πληροφορίες για τον έλεγχο της ροής του αέρα από το σύστημα HVAC σε αυτήν τη ζώνη σε πραγματικό χρόνο, μεγιστοποιώντας την άνεση του υπαλλήλου γραφείου. Το Σχήμα 7 δείχνει ένα παράδειγμα αισθητήρα πληρότητας σε ψηφιακό φωτιστικό οροφής.

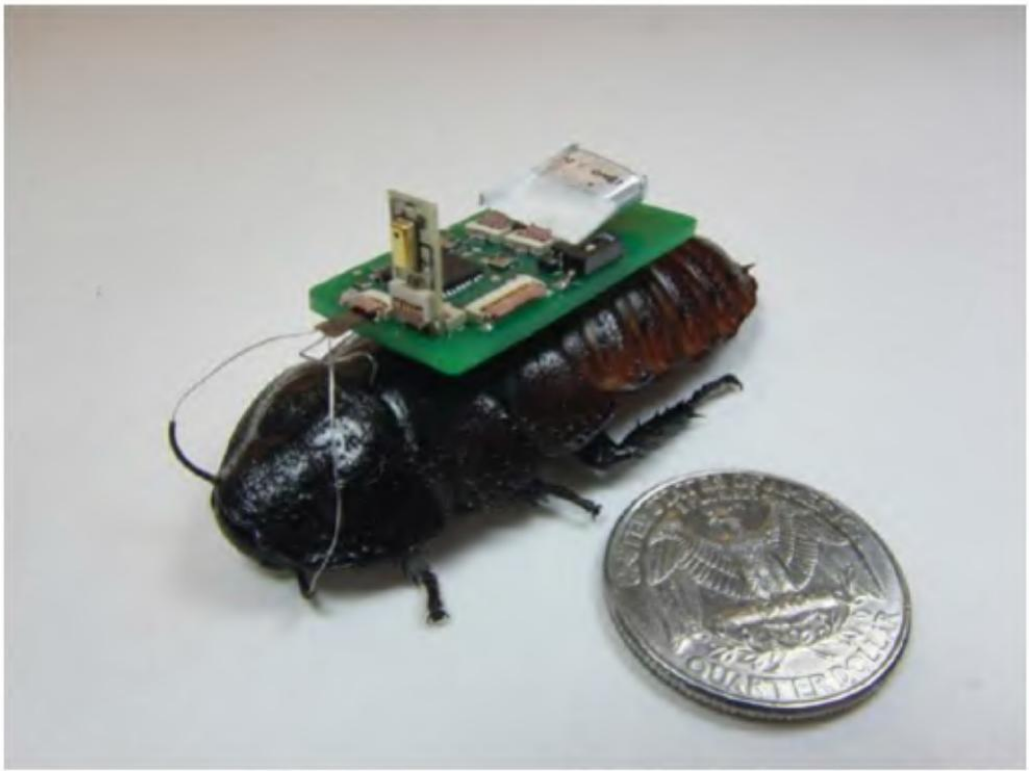
Σχήμα 7: Ένα ψηφιακό φωτιστικό οροφής led με αισθητήρα πληρότητας.

Κεφάλαιο 1.8 Έξυπνα πλάσματα

Το IoT παρέχει επίσης τη δυνατότητα σύνδεσης ζωντανών πραγμάτων στο Διαδίκτυο. Οι αισθητήρες μπορούν να τοποθετηθούν στα ζώα και ακόμη και στα έντομα εξίσου εύκολα με τις μηχανές, και τα οφέλη μπορεί να είναι εξίσου εντυπωσιακά. Μία από τις πιο γνωστές εφαρμογές του IoT σε σχέση με τα ζώα επικεντρώνεται σε αυτό που συχνά αναφέρεται ως «συνδεδεμένη αγελάδα».
Η Sparked, μια ολλανδική εταιρεία, ανέπτυξε έναν αισθητήρα που τοποθετείται στο αυτί μιας αγελάδας. Ο αισθητήρας παρακολουθεί διάφορες πτυχές υγείας της αγελάδας καθώς και τη θέση της και διαβιβάζει τα δεδομένα ασύρματα για ανάλυση από τον αγρότη. Τα δεδομένα από κάθε έναν από αυτούς τους αισθητήρες είναι περίπου 200 MB ετησίως και προφανώς χρειάζεται μια υποδομή δικτύου για να πραγματοποιηθεί η σύνδεση με τους αισθητήρες και να αποθηκευθούν οι πληροφορίες. Επίσης, εξάγονται πληροφορίες πώς οι περιβαλλοντικοί παράγοντες μπορεί να επηρεάζουν το κοπάδι στο σύνολό του και σχετικά με τις αλλαγές στη διατροφή. Αυτό επιτρέπει την έγκαιρη ανίχνευση της νόσου καθώς οι αγελάδες τείνουν να τρώνε λιγότερες ημέρες πριν εμφανίσουν συμπτώματα. Αυτοί οι αισθητήρες επιτρέπουν ακόμη και τον εντοπισμό εγκυμοσύνης στις αγελάδες.

Μια άλλη εφαρμογή του IoT στους οργανισμούς περιλαμβάνει την τοποθέτηση αισθητήρων σε κατσαρίδες. Ενώ το θέμα των κατσαρίδων είναι λίγο ανησυχητικό για πολλούς ανθρώπους, τα πιθανά οφέλη των κατσαρίδων με δυνατότητα IoT θα μπορούσαν να κάνουν τη διαφορά ζωής σε καταστάσεις καταστροφής.

Ερευνητές στο κρατικό πανεπιστήμιο της Βόρειας Καρολίνας ερευνούν πως χρησιμοποιώντας κατσαρίδες μπορούν να βοηθήσουν το προσωπικό έκτακτης ανάγκης να σώσει επιζώντες μετά από μια καταστροφή. Όπως φαίνεται στο σχήμα 8 ένα ηλεκτρονικό σακίδιο συνδέεται με μία κατσαρίδα. Αυτό το σακίδιο επικοινωνεί με τη κατσαρίδα μέσω τμημάτων του σώματός της. Χαμηλού επιπέδου ηλεκτρικοί παλμοί σε μια κεραία από τη μία πλευρά κάνει τη κατσαρίδα να γυρίσει προς την αντίθετη πλευρά επειδή πιστεύει ότι συναντά ένα εμπόδιο. Η κατσαρίδα έχει αισθητήρια όργανα στην κοιλιά που ανιχνεύουν τον κίνδυνο μέσω αλλαγής ρευμάτων αέρα. Όταν το σακίδιο διεγείρει αυτά τα αισθητήρια όργανα, η κατσαρίδα προχωράει μπροστά επειδή πιστεύει ότι πλησιάζει ένα αρπακτικό.



Σχήμα 8: IOT-Ενεργοποιημένη κατσαρίδα, η οποία μπορεί να βοηθήσει στην εύρεση επιζώντων μετά από καταστροφή.

Το ηλεκτρονικό σακίδιο χρησιμοποιεί ασύρματη επικοινωνία με έναν ελεγκτή και μπορεί να "οδηγηθεί" από απόσταση.Η χρήση των κατσαρίδων με αυτόν τον τρόπο επιτρέπει τη χαρτογράφηση χώρων στους οποίους δεν μπορεί να έχει πρόσβαση το προσωπικό διάσωσης, κάτι που βοηθά στην αναζήτηση επιζώντων. Το ηλεκτρονικό σακίδιο πλάτης είναι εξοπλισμένο με κατευθυνόμενα μικρόφωνα που επιτρέπουν την ανίχνευση ορισμένων ήχων και την κατεύθυνση από την οποία προέρχονται. Το λογισμικό μπορεί να αναλύσει τους ήχους για να διασφαλίσει ότι προέρχονται από ένα άτομο και όχι από, για παράδειγμα, έναν σωλήνα που διαρρέει. Οι κατσαρίδες μπορούν στη συνέχεια να κατευθυνθούν προς τους ήχους που μπορεί να υποδεικνύουν άτομα που έχουν παγιδευτεί. Επιπλέον, τα μικρόφωνα παρέχουν τη δυνατότητα στο προσωπικό διάσωσης να ακούει ό, τι ανιχνεύεται.

Αυτά τα παραδείγματα δείχνουν ότι το IoT συχνά υπερβαίνει την απλή προσθήκη αισθητήρων και περισσότερης ευφυΐας σε μη ζωντανά «πράγματα». Τα ζωντανά «πράγματα» μπορούν επίσης να συνδεθούν στο Διαδίκτυο και αυτή η σύνδεση μπορεί να προσφέρει σημαντικά αποτελέσματα.

Κεφάλαιο 1.9 Σύγκλιση IT και OT

Μέχρι πρόσφατα, η τεχνολογία των πληροφοριών (IT) και η λειτουργική τεχνολογία (OT) ζούσαν ως επί το πλείστον σε ξεχωριστούς κόσμους.
Η τεχνολογία των πληροφοριών (information technology IT) υποστηρίζει συνδέσεις στο Διαδίκτυο μαζί με σχετικά δεδομένα και συστήματα τεχνολογίας και επικεντρώνεται στην ασφαλή ροή δεδομένων σε έναν οργανισμό. Η λειτουργική τεχνολογία (operational technology OT) παρακολουθεί και ελέγχει συσκευές και διαδικασίες σε φυσικά λειτουργικά συστήματα. Αυτά τα συστήματα περιλαμβάνουν γραμμές συναρμολόγησης, δίκτυα διανομής κοινής ωφέλειας, εγκαταστάσεις παραγωγής, συστήματα οδοστρωμάτων και πολλά άλλα. Συνήθως, η IT δεν ασχολήθηκε με την παραγωγή και την εφοδιαστική των OT περιβάλλοντων.
Συγκεκριμένα, ο οργανισμός IT είναι υπεύθυνος για τα πληροφοριακά συστήματα μιας επιχείρησης, όπως email, υπηρεσίες αρχείων και εκτυπώσεων, βάσεις δεδομένων κ.ο.κ.
Συγκριτικά, η OT είναι υπεύθυνη για τις συσκευές και τις διαδικασίες που λειτουργούν σε βιομηχανικό εξοπλισμό, όπως εργοστασιακές μηχανές, μετρητές, ενεργοποιητές, συσκευές αυτοματισμού ηλεκτρικής διανομής, συστήματα SCADA (supervisory control and data acquisition -εποπτικός έλεγχος και απόκτηση δεδομένων) κ.ο.κ.
Παραδοσιακά, η OT χρησιμοποιεί αποκλειστικά δίκτυα με εξειδικευμένα πρωτόκολλα επικοινωνίας για τη σύνδεση αυτών των συσκευών και αυτά τα δίκτυα λειτουργούν εντελώς ξεχωριστά από τα δίκτυα IT. Η διαχείριση του OT είναι συνδεδεμένη με τη ζωτική δύναμη μιας εταιρείας. Για παράδειγμα, εάν το δίκτυο που συνδέει τις μηχανές σε ένα εργοστάσιο αποτύχει, τα μηχανήματα δεν μπορούν να λειτουργήσουν και η παραγωγή μπορεί να σταματήσει, επηρεάζοντας αρνητικά τις επιχειρήσεις(της τάξης των εκατομμυρίων δολαρίων). Από την άλλη πλευρά, εάν ο διακομιστής ηλεκτρονικού ταχυδρομείου (που διευθύνεται από το τμήμα IT) αποτύχει για λίγες ώρες, μπορεί να εκνευρίσει τους ανθρώπους, αλλά είναι απίθανο να επηρεάσει τις επιχειρήσεις οπουδήποτε κοντά στο ίδιο επίπεδο.

Ο Πίνακας 2 επισημαίνει μερικές από τις διαφορές μεταξύ των δικτύων IT και OT και τις διάφορες προκλήσεις τους.

Criterion	Industrial OT Network	Enterprise IT Network
Operational focus	Keep the business operating 24x7	Manage the computers, data, and employee communication system in a secure way
Priorities	1. Availability 2. Integrity 3. Security	1. Security 2. Integrity 3. Availability
Types of data	Monitoring, control, and supervisory data	Voice, video, transactional, and bulk data
Security	Controlled physical access to devices	Devices and users authenticated to the network
Implication of failure	OT network disruption directly impacts business	Can be business impacting, depending on industry, but workarounds may be possible
Network upgrades (software or hardware)	Only during operational maintenance windows	Often requires an outage window when workers are not onsite; impact can be mitigated
Security vulnerability	Low: OT networks are isolated and often use proprietary protocols	High: continual patching of hosts is required, and the network is connected to Internet and requires vigilant protection

Πίνακας 2: Σύγκριση Λειτουργικής Τεχνολογίας (OT) και Τεχνολογίας Πληροφοριών (IT).

Με την άνοδο του IoT και των πρωτοκόλλων που βασίζονται σε πρότυπα, όπως το IPv6, οι οργανισμοί IT και OT συγκλίνουν -ή με μεγαλύτερη ακρίβεια-, η OT αρχίζει να υιοθετεί τα πρωτόκολλα δικτύου, την τεχνολογία, τις μεταφορές και τις μεθόδους του οργανισμού IT και ο οργανισμός IT αρχίζει να υποστηρίζει τις λειτουργικές απαιτήσεις που χρησιμοποιεί ο OT. Όταν το IT και το OT αρχίζουν να χρησιμοποιούν τα ίδια δίκτυα, πρωτόκολλα και διαδικασίες, υπάρχουν σαφείς οικονομίες κλίμακας. Όχι μόνο η σύγκλιση μειώνει τον όγκο της κεφαλαιακής υποδομής που απαιτείται, αλλά τα δίκτυα γίνονται ευκολότερα στη λειτουργία και η ευελιξία των ανοικτών προτύπων επιτρέπει ταχύτερη ανάπτυξη και προσαρμοστικότητα στις νέες τεχνολογίες.

Το συνολικό πλεονέκτημα της συνεργασίας IT και OT είναι μια πιο αποδοτική και κερδοφόρα επιχείρηση λόγω του μειωμένου χρόνου διακοπής, του χαμηλότερου κόστους μέσω της οικονομίας κλίμακας, του μειωμένου αποθέματος και του βελτιωμένου χρόνου παράδοσης. Όταν η σύγκλιση IT/OT διαχειρίζεται σωστά, το IoT υποστηρίζεται πλήρως και από τις δύο ομάδες.

Κεφάλαιο 1.10 Προκλήσεις IoT

Πολλά μέρη του IoT έχουν γίνει πραγματικότητα, αλλά ορισμένα εμπόδια πρέπει να ξεπεραστούν για να γίνει το IoT πανταχού παρόν σε ολόκληρη τη βιομηχανία και την καθημερινή μας ζωή.
Παρακάτω επισημαίνονται μερικές από τις σημαντικότερες προκλήσεις και προβλήματα που αντιμετωπίζει σήμερα το IoT.

- Κλίμακα: Ενώ η κλίμακα των δικτύων IT μπορεί να είναι μεγάλη, η κλίμακα του OT μπορεί να είναι αρκετές τάξεις μεγέθους μεγαλύτερη.

- Ασφάλεια: Με περισσότερα «πράγματα» να συνδέονται με άλλα «πράγματα» και ανθρώπους, η ασφάλεια είναι ένα όλο και πιο περίπλοκο ζήτημα για το IoT. Πλέον η ασφάλεια έχει διευρυνθεί πολύ και εάν μια συσκευή χακαριστεί, η συνδεσιμότητά της αποτελεί μείζονα ανησυχία. Μια παραβιασμένη συσκευή μπορεί να χρησιμεύσει ως σημείο εκκίνησης για επίθεση σε άλλες συσκευές και συστήματα. Η ασφάλεια του IoT είναι επίσης διαδεδομένη σχεδόν σε κάθε όψη του IoT.

- Μυστικότητα: Καθώς οι αισθητήρες γίνονται πιο γόνιμοι στην καθημερινή μας ζωή, πολλά από τα δεδομένα που συλλέγουν θα αφορούν συγκεκριμένα άτομα και τις δραστηριότητές τους. Αυτά τα δεδομένα μπορεί να κυμαίνονται από πληροφορίες για την υγεία έως μοντέλα αγορών και συναλλαγές σε καταστήματα λιανικής. Για τις επιχειρήσεις, αυτά τα δεδομένα έχουν νομισματικό χαρακτήρα. Οι οργανισμοί συζητούν τώρα ποιος είναι κάτοχος αυτών των δεδομένων και πώς τα άτομα μπορούν να ελέγξουν εάν μοιράζονται και με ποιον.

- Μεγάλα δεδομένα και αναλύσεις δεδομένων: Το IoT και ο μεγάλος αριθμός αισθητήρων του θα προκαλέσουν έναν κατακλυσμό δεδομένων που πρέπει να αντιμετωπιστούν. Αυτά τα δεδομένα θα παρέχουν κρίσιμες πληροφορίες και πληροφορίες εάν μπορούν να υποβληθούν σε επεξεργασία με αποτελεσματικό τρόπο. Η πρόκληση, ωστόσο, είναι η αξιολόγηση τεράστιων όγκων δεδομένων που προέρχονται από διαφορετικές πηγές σε διάφορες μορφές και το κάνουν έγκαιρα.

- Διαλειτουργικότητα: Όπως και με κάθε άλλη τεχνολογία που γεννιέται, διάφορα πρωτόκολλα και αρχιτεκτονικές κάνουν αναζήτηση για μερίδιο αγοράς και τυποποίηση στο IoT. Ορισμένα από αυτά τα πρωτόκολλα και οι αρχιτεκτονικές βασίζονται σε ιδιόκτητα στοιχεία και άλλα ανοίγουν. Τα πρόσφατα πρότυπα IoT βοηθούν στην ελαχιστοποίηση αυτού του προβλήματος, αλλά συχνά υπάρχουν διάφορα πρωτόκολλα και εφαρμογές διαθέσιμα για δίκτυα IoT. Ενώ η κλίμακα των δικτύων πληροφορικής μπορεί να είναι μεγάλη, η κλίμακα του OT μπορεί να είναι αρκετές τάξεις μεγέθους μεγαλύτερη.

Κεφάλαιο 2 Εισαγωγή στην αρχιτεκτονική και το σχεδιασμό δικτύου IoT

Οι απαιτήσεις των συστημάτων IoT οδηγούν νέες αρχιτεκτονικές που αντιμετωπίζουν την κλίμακα, τους περιορισμούς και τις πτυχές διαχείρισης δεδομένων του IoT. Για την αντιμετώπιση αυτών των αναγκών, προέκυψαν αρκετά μοντέλα αναφοράς για IoT, συμπεριλαμβανομένου του μοντέλου oneM2M IoT και του IoT World Forum's IoT Reference Model.
Τα κοινά σημεία μεταξύ αυτών των μοντέλων είναι η αλληλεπίδραση συσκευών IoT, του δικτύου που τις συνδέει και των εφαρμογών που διαχειρίζονται τα τελικά σημεία. Αυτό το κεφάλαιο παρουσιάζει ένα μοντέλο βασισμένο σε κοινές έννοιες σε αυτές τις αρχιτεκτονικές που διασπά τα στρώματα IoT σε μια απλοποιημένη αρχιτεκτονική που ενσωματώνει δύο παράλληλες στοίβες:

- Core IoT Functional Stack: έχει τρία επίπεδα: τους αισθητήρες και τους ενεργοποιητές IoT, τα στοιχεία δικτύου και τα επίπεδα εφαρμογών και αναλύσεων. Τα στοιχεία δικτύου και τα επίπεδα εφαρμογών περιλαμβάνουν πολλές υποστιβάδες που αντιστοιχούν σε διαφορετικά μέρη του συνολικού συστήματος

- IoT Data Management and Compute Stack: ασχολείται με το πώς και πού φιλτράρονται, συγκεντρώνονται, αποθηκεύονται και αναλύονται τα δεδομένα.

Κεφάλαιο 2.1 Αρχιτεκτονική και σχεδιασμός δικτύου IoT

Ένα δίκτυο υπολογιστών δεν πρέπει ποτέ να δημιουργηθεί χωρίς προσεκτικό σχεδιασμό, εμπεριστατωμένες πολιτικές ασφάλειας και συμμόρφωση με καλά κατανοητές πρακτικές σχεδιασμού. Η αποτυχία στην προσεκτική αρχιτεκτονική ενός δικτύου σύμφωνα με τις αρχές υγιούς σχεδιασμού θα οδηγήσει σε κάτι που είναι δύσκολο να κλιμακωθεί, να διαχειριστεί, να προσαρμοστεί στις οργανωτικές αλλαγές και, το χειρότερο από όλα, να αντιμετωπίσει προβλήματα όταν τα πράγματα πάνε στραβά. Οι περισσότεροι CIOs και CTOs κατανοούν ότι το δίκτυο διευθύνει την επιχείρηση. Εάν το δίκτυο αποτύχει, οι λειτουργίες της εταιρείας μπορεί να επηρεαστούν σοβαρά.
Ακριβώς όπως ένα σπίτι πρέπει να σχεδιάζεται με σκοπό να αντέχει σε πιθανές φυσικές καταστροφές, όπως σεισμικά γεγονότα και τυφώνες, τα συστήματα τεχνολογίας πληροφοριών (IT) πρέπει να σχεδιαστούν ώστε να αντέχουν σε «σεισμούς δικτύου», όπως επιθέσεις διανομής άρνησης υπηρεσίας (DDoS) , μελλοντικές απαιτήσεις ανάπτυξης, διακοπές δικτύου, ακόμη και ανθρώπινο λάθος. Για την αντιμετώπιση αυτών των προκλήσεων, η τέχνη της αρχιτεκτονικής του δικτύου έχει αποκτήσει τεράστια επιρροή σε οργανισμούς πληροφορικής (IT) τις τελευταίες δύο δεκαετίες. Στην πραγματικότητα, για πολλές εταιρείες, η ευθύνη για την επίβλεψη της αρχιτεκτονικής δικτύου θεωρείται συχνά ως μία από τις πιο υψηλές θέσεις σε οργανισμούς πληροφορικής (IT) και επιχειρησιακής τεχνολογίας (OT).

Κεφάλαιο 2.2 Προγράμματα οδήγησης πίσω από νέες αρχιτεκτονικές δικτύων

Αν και οι παραδοσιακές αρχιτεκτονικές δικτύων για την IT μας έχουν εξυπηρετήσει για πολλά χρόνια, δεν είναι κατάλληλες για τις πολύπλοκες απαιτήσεις του IoT. Η βασική διαφορά μεταξύ IT και IoT είναι τα δεδομένα. Ενώ τα συστήματα IT ασχολούνται κυρίως με την αξιόπιστη και συνεχή υποστήριξη επιχειρηματικών εφαρμογών, όπως ηλεκτρονικό ταχυδρομείο, web, βάσεις δεδομένων, συστήματα CRM και ούτω καθεξής, το IoT αφορά όλα τα δεδομένα που παράγονται από αισθητήρες και πώς χρησιμοποιούνται αυτά τα δεδομένα.
Η ουσία των αρχιτεκτονικών του IoT συνεπάγεται τον τρόπο μεταφοράς, συλλογής, ανάλυσης και τελικά δράσης των δεδομένων.
Παρουσάζουμε μερικές από τις διαφορές μεταξύ των δικτύων IT και IoT, με έμφαση στις απαιτήσεις IoT που οδηγούν νέες αρχιτεκτονικές δικτύων και εξετάζει ποιες προσαρμογές χρειάζονται. Συγκεκριμένα:

Κλίμακα:Η κλίμακα ενός τυπικού δικτύου IT είναι της τάξης αρκετών χιλιάδων συσκευών δηλαδή εκτυπωτών, φορητών ασύρματων συσκευών, φορητών υπολογιστών, διακομιστών και ούτω καθεξής. Για ένα παραδοσιακό μοντέλο δικτύωσης τριών επιπέδων της πανεπιστημιούπολης, που υποστηρίζει την πρόσβαση, τη διανομή και τον πυρήνα (με υποαρχιτεκτονικές για WAN, Wi-Fi, κέντρο δεδομένων κ.λπ.), τα πράγματα είναι καλά. Όμως τι συμβαίνει όταν η κλίμακα ενός δικτύου πηγαίνει από μερικές χιλιάδες τελικά σημεία σε μερικά εκατομμύρια; Το IoT εισάγει ένα μοντέλο όπου θα μπορούσε εύκολα να ζητηθεί από ένα μέσο χρησιμότητας, εργοστάσιο, σύστημα μεταφοράς ή πόλη να υποστηρίζει ένα δίκτυο αυτής της κλίμακας. Με βάση τις απαιτήσεις κλίμακας αυτής της σειράς, **το IPv6** είναι το φυσικό θεμέλιο για το επίπεδο δικτύου IoT.

Ασφάλεια: Η συχνότητα και ο αντίκτυπος των κυβερνοεπιθέσεων τα τελευταία χρόνια έχουν αυξηθεί δραματικά. Η προστασία των εταιρικών δεδομένων από εισβολή και κλοπή είναι μία από τις κύριες λειτουργίες του τμήματος πληροφορικής. Τα τμήματα πληροφορικής IT καταβάλλουν μεγάλες προσπάθειες για την προστασία διακομιστών, εφαρμογών και δικτύου, δημιουργώντας μοντέλα σε βάθος άμυνας με επίπεδα ασφάλειας σχεδιασμένα να προστατεύουν τα κοσμήματα στον κυβερνοχώρο της εταιρείας.
Ωστόσο, παρά τις προσπάθειες που συγκεντρώθηκαν για την προστασία δικτύων και δεδομένων, «οι χάκερς», εξακολουθούν να βρίσκουν τρόπους διείσδυσης σε αξιόπιστα δίκτυα. Στα δίκτυα πληροφορικής IT, η πρώτη γραμμή άμυνας είναι συχνά το περιμετρικό τείχος προστασίας. Ωστόσο, τα τελικά σημεία του IoT βρίσκονται συχνά σε ασύρματα δίκτυα αισθητήρων που χρησιμοποιούν φάσμα χωρίς άδεια και δεν είναι ορατά μόνο στον κόσμο μέσω ενός αναλυτή φάσματος, αλλά συχνά φυσικά προσβάσιμα και ευρέως διανεμημένα στο πεδίο.
Τα παραδοσιακά μοντέλα ασφάλειας πληροφορικής IT δεν έχουν σχεδιαστεί για επιθέσεις που εισάγονται από συστήματα IoT με μεγάλη διασπορά. Τα συστήματα IoT απαιτούν συνεπείς μηχανισμούς ελέγχου ταυτότητας, κρυπτογράφησης και πρόληψης εισβολών που κατανοούν τη συμπεριφορά των βιομηχανικών πρωτοκόλλων και μπορούν να ανταποκριθούν σε επιθέσεις σε κρίσιμες υποδομές. Για βέλτιστη ασφάλεια, τα συστήματα IoT πρέπει:

- Να είναι σε θέση να αναγνωρίσουν και να επαληθεύσουν όλες τις οντότητες που εμπλέκονται στην υπηρεσία IoT (δηλαδή πύλες, συσκευές τελικού σημείου, οικιακά δίκτυα, δίκτυα περιαγωγής, πλατφόρμες υπηρεσιών)

- Βεβαίωση ότι όλα τα δεδομένα χρήστη που μοιράζονται μεταξύ της συσκευής τελικού σημείου και των εφαρμογών back-end είναι κρυπτογραφημένα.

- Συμμόρφωση με την τοπική νομοθεσία για την προστασία δεδομένων, έτσι ώστε όλα τα δεδομένα να προστατεύονται και να αποθηκεύονται σωστά.

- Να γίνεται χρήση μιας πλατφόρμας διαχείρισης συνδεσιμότητας IoT και να καθορίζονται πολιτικές ασφάλειας βασισμένες σε κανόνες, ώστε να μπορούν να ληφθούν άμεσα μέτρα εάν εντοπιστεί ανώμαλη συμπεριφορά από συνδεδεμένες συσκευές.

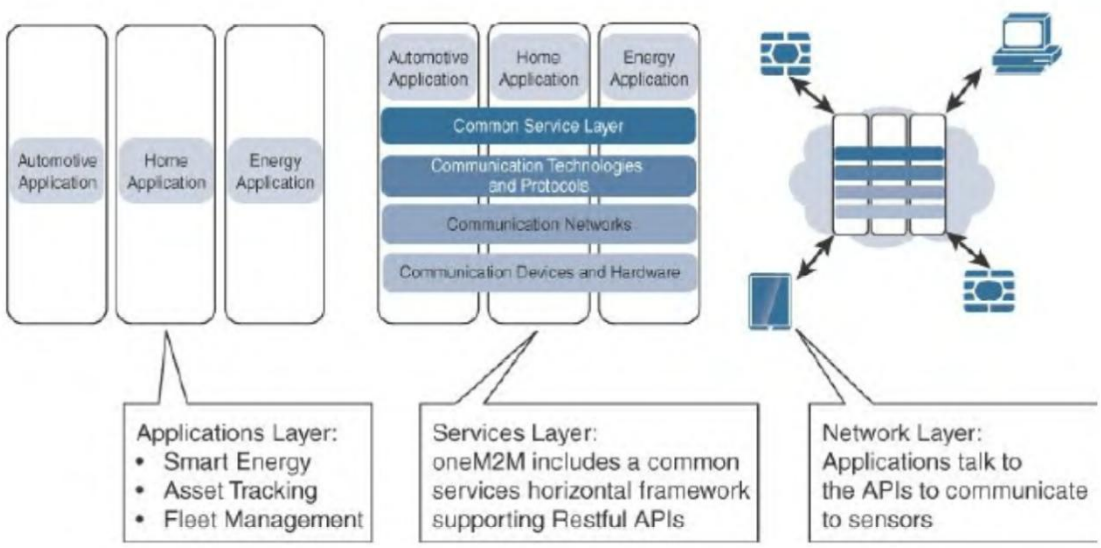
Περιορισμένες συσκευές και δίκτυα: Οι περισσότεροι αισθητήρες IoT έχουν σχεδιαστεί για μία μόνο εργασία και είναι συνήθως μικροί και φθηνοί. Αυτό σημαίνει ότι συχνά έχουν περιορισμένη ισχύ, CPU και μνήμη και μεταδίδουν μόνο όταν υπάρχει κάτι σημαντικό. Λόγω της μεγάλης κλίμακας αυτών των συσκευών και των μεγάλων, ανεξέλεγκτων περιβαλλόντων όπου συνήθως αναπτύσσονται, τα δίκτυα που παρέχουν συνδεσιμότητα τείνουν επίσης να είναι πολύ ζημιογόνα και να υποστηρίζουν πολύ χαμηλούς ρυθμούς δεδομένων. Αυτή είναι μια εντελώς διαφορετική κατάσταση από τα δίκτυα πληροφορικής IT, τα οποία απολαμβάνουν ταχύτητες σύνδεσης πολλών gigabit και τελικές θέσεις με ισχυρούς επεξεργαστές.
Εάν ένα δίκτυο πληροφορικής IT έχει περιορισμούς απόδοσης, η λύση είναι απλή: Αναβάθμιση σε ταχύτερο δίκτυο. Εάν υπάρχουν πάρα πολλές συσκευές σε ένα VLAN και επηρεάζουν την απόδοση, μπορεί να δημιουργηθεί ένα νέο VLAN. Ωστόσο, αυτή η προσέγγιση δεν μπορεί να ανταποκριθεί στον περιορισμένο χαρακτήρα των συστημάτων IoT. Το IoT απαιτεί μια νέα τεχνολογία συνδεσιμότητας που πληροί τόσο την κλίμακα όσο και τους περιορισμούς.

Δεδομένα: Οι συσκευές IoT δημιουργούν ένα βουνό δεδομένων. Σε γενικές γραμμές, τα περισσότερα καταστήματα πληροφορικής IT δεν ενδιαφέρονται ιδιαίτερα για τα μη δομημένα δεδομένα συνομιλίας που δημιουργούνται από συσκευές στο δίκτυο.
Ωστόσο, στο IoT τα δεδομένα είναι πολύ σημαντικά, καθώς είναι αυτό που επιτρέπει στις επιχειρήσεις να παρέχουν νέες υπηρεσίες IoT που βελτιώνουν την εμπειρία των πελατών, μειώνουν το κόστος και παρέχουν νέες ευκαιρίες εσόδων. Αν και τα περισσότερα δεδομένα που δημιουργούνται από το IoT είναι μη δομημένα, οι πληροφορίες που παρέχει μέσω των αναλυτικών στοιχείων μπορούν να φέρουν επανάσταση στις διαδικασίες και να δημιουργήσουν νέα επιχειρηματικά μοντέλα.
Επομένως, σε αντίθεση με τα δίκτυα πληροφορικής IT, τα συστήματα IoT έχουν σχεδιαστεί για να αυξάνουν την κατανάλωση δεδομένων σε όλη την αρχιτεκτονική, τόσο για να φιλτράρουν και να μειώνουν τα περιττά δεδομένα που ανεβαίνουν προς τα πάνω όσο και να παρέχουν την ταχύτερη δυνατή απόκριση σε συσκευές όταν είναι απαραίτητο.

Υποστήριξη παλαιάς συσκευής: Καθώς αναπτύσσονται δίκτυα IoT, πρέπει να υποστηρίζουν τις παλαιότερες συσκευές που υπάρχουν ήδη στο δίκτυο, καθώς και συσκευές με νέες δυνατότητες. Σε πολλές περιπτώσεις, οι παλαιές συσκευές είναι τόσο παλιές που δεν υποστηρίζουν καν IP. Για παράδειγμα, ένα εργοστάσιο μπορεί να αντικαθιστά μηχανές μόνο μία φορά κάθε 20 χρόνια ή ίσως και περισσότερο! Δεν θέλει να αναβαθμίσει μηχανές πολλών εκατομμυρίων δολαρίων μόνο για να μπορεί να τις συνδέσει σε δίκτυο για καλύτερη ορατότητα και έλεγχο. Ωστόσο, πολλά από αυτά τα παλαιά μηχανήματα ενδέχεται να υποστηρίζουν παλαιότερα πρωτόκολλα, όπως σειριακές διεπαφές και να χρησιμοποιούν RS-232. Σε αυτή την περίπτωση, το δίκτυο IoT πρέπει είτε να είναι σε θέση να μεταφράσει κάποιο πρωτόκολλο είτε να χρησιμοποιήσει μια συσκευή πύλης για τη σύνδεση αυτών των τελικών σημείων παλαιού τύπου στο δίκτυο IoT.

Σύγκριση αρχιτεκτονικών IoT: Τα τελευταία χρόνια, έχουν εμφανιστεί αρχιτεκτονικά πρότυπα και πλαίσια για την αντιμετώπιση της πρόκλησης του σχεδιασμού μαζικής κλίμακας δικτύων IoT. Η θεμελιώδης ιδέα σε όλες αυτές τις αρχιτεκτονικές είναι η υποστήριξη δεδομένων, διαδικασίας και των λειτουργιών που εκτελούν οι συσκευές τελικού σημείου. Δύο από τις πιο γνωστές αρχιτεκτονικές είναι αυτές που υποστηρίζονται από το oneM2M και το IoT World Forum (IoTWF).

Η τυποποιημένη αρχιτεκτονική oneM2M IoT: Ο στόχος του oneM2M είναι να δημιουργήσει ένα κοινό επίπεδο υπηρεσιών, το οποίο μπορεί εύκολα να ενσωματωθεί σε συσκευές πεδίου για να επιτρέψει την επικοινωνία με διακομιστές εφαρμογών. Το πλαίσιο του oneM2M επικεντρώνεται σε υπηρεσίες, εφαρμογές και πλατφόρμες IoT. Αυτές περιλαμβάνουν εφαρμογές έξυπνης μέτρησης, έξυπνο δίκτυο, αυτοματοποίηση έξυπνης πόλης, ηλεκτρονική υγεία και συνδεδεμένα οχήματα.
Μία από τις μεγαλύτερες προκλήσεις στο σχεδιασμό μιας αρχιτεκτονικής IoT είναι η αντιμετώπιση της ετερογένειας συσκευών, λογισμικού και μεθόδων πρόσβασης. Με την ανάπτυξη μιας οριζόντιας αρχιτεκτονικής πλατφόρμας, το oneM2M αναπτύσσει πρότυπα που επιτρέπουν τη διαλειτουργικότητα σε όλα τα επίπεδα της στοίβας IoT.
Το Σχήμα 9 απεικονίζει την αρχιτεκτονική oneM2M IoT.



Σχήμα 9: Τα κύρια στοιχεία της αρχιτεκτονικής του OneM2M IoT.

Η αρχιτεκτονική oneM2M χωρίζει τις λειτουργίες IoT σε τρεις κύριους τομείς:

- Επίπεδο εφαρμογών (Applications Layer): Η αρχιτεκτονική oneM2M δίνει μεγάλη προσοχή στη συνδεσιμότητα μεταξύ των συσκευών και των εφαρμογών τους. Αυτός ο τομέας περιλαμβάνει τα πρωτόκολλα επιπέδου εφαρμογής και προσπαθεί να τυποποιήσει ορισμούς API προς βορρά για αλληλεπίδραση με συστήματα επιχειρησιακής νοημοσύνης (BI). Οι εφαρμογές τείνουν να είναι συγκεκριμένες για τη βιομηχανία και έχουν τα δικά τους σύνολα μοντέλων δεδομένων, και έτσι εμφανίζονται ως κάθετες οντότητες.

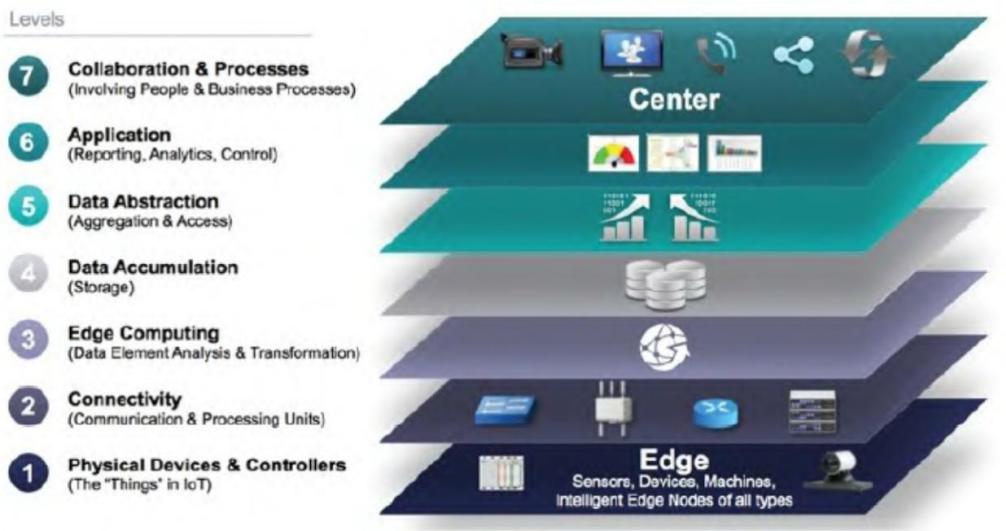
- Επίπεδο υπηρεσιών (Services layer): Αυτό το επίπεδο εμφανίζεται ως οριζόντιο πλαίσιο σε κάθετες εφαρμογές της βιομηχανίας. Σε αυτό το επίπεδο, οι οριζόντιες ενότητες περιλαμβάνουν το φυσικό δίκτυο στο οποίο εκτελούνται οι εφαρμογές

IoT, τα υποκείμενα πρωτόκολλα διαχείρισης και το υλικό. Παραδείγματα περιλαμβάνουν επικοινωνίες backhaul μέσω κινητής τηλεφωνίας, δίκτυα MPLS, VPN και ούτω καθεξής. Η οδήγηση στην κορυφή είναι το κοινό επίπεδο υπηρεσιών.

- Επίπεδο δικτύου (Network layer): Αυτός είναι ο τομέας επικοινωνίας για τις συσκευές και τα τελικά σημεία IoT. Περιλαμβάνει τις ίδιες τις συσκευές και το δίκτυο επικοινωνιών που τις συνδέει.
  Οι ενσωματώσεις αυτής της υποδομής επικοινωνιών περιλαμβάνουν τεχνολογίες ασύρματου πλέγματος, όπως το IEEE 802.15.4 και ασύρματα συστήματα point-to-multipoint, όπως το IEEE 801.11ah. Περιλαμβάνονται επίσης ενσύρματες συνδέσεις συσκευών, όπως οι επικοινωνίες γραμμής ρεύματος IEEE 1901.
  Σε πολλές περιπτώσεις, οι έξυπνες (και μερικές φορές όχι και τόσο έξυπνες) συσκευές επικοινωνούν μεταξύ τους. Σε άλλες περιπτώσεις, η επικοινωνία από μηχανή σε μηχανή δεν είναι απαραίτητη και οι συσκευές επικοινωνούν απλώς μέσω ενός δικτύου περιοχής πεδίου (FAN) για να χρησιμοποιούν εφαρμογές ανά περίπτωση στον τομέα εφαρμογών IoT. Επομένως, ο τομέας της συσκευής περιλαμβάνει επίσης τη συσκευή πύλης, η οποία παρέχει επικοινωνίες στο κεντρικό δίκτυο και λειτουργεί ως σημείο οριοθέτησης μεταξύ των τομέων της συσκευής και του δικτύου.

Κεφάλαιο 2.3 Τυποποιημένη αρχιτεκτονική του IoT World Forum (IoTWF)

Το 2014, η αρχιτεκτονική επιτροπή IoTWF (με επικεφαλής τους Cisco, IBM, Rockwell Automation και άλλους) δημοσίευσε ένα αρχιτεκτονικό μοντέλο αναφοράς IoT επτά επιπέδων. Ενώ υπάρχουν διάφορα μοντέλα αναφοράς IoT, αυτό που παρουσιάστηκε από το IoT World Forum προσφέρει μια καθαρή, απλοποιημένη προοπτική για το IoT και περιλαμβάνει υπολογισμό άκρων, αποθήκευση δεδομένων και πρόσβαση. Παρέχει έναν συνοπτικό τρόπο απεικόνισης του IoT από τεχνική άποψη. Κάθε ένα από τα επτά επίπεδα χωρίζεται σε συγκεκριμένες λειτουργίες και η ασφάλεια περιλαμβάνει ολόκληρο το μοντέλο. Το σχήμα 10 περιγράφει λεπτομερώς το μοντέλο αναφοράς IoT που δημοσιεύτηκε από το IoTWF.

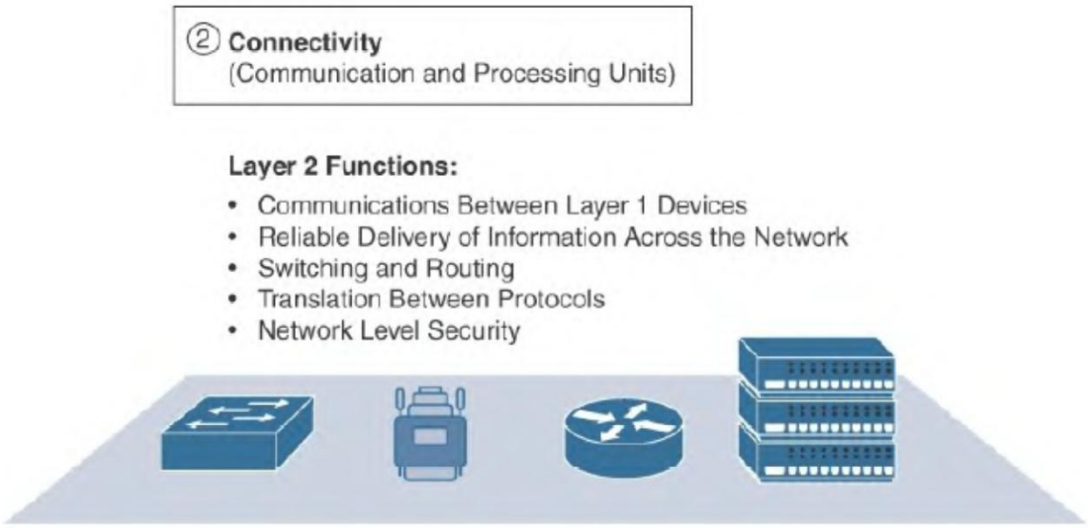


Σχήμα 10: Μοντέλο αναφοράς IoT.

Όπως φαίνεται στο Σχήμα 10 το μοντέλο αναφοράς IoT ορίζει ένα σύνολο επιπέδων με έλεγχο που ρέει από το κέντρο (αυτό μπορεί να είναι είτε μια υπηρεσία cloud είτε ένα ειδικό κέντρο δεδομένων), στην άκρη, η οποία περιλαμβάνει αισθητήρες, συσκευές, μηχανές και άλλους τύπους έξυπνων τελικών κόμβων. Συγκεκριμένα:

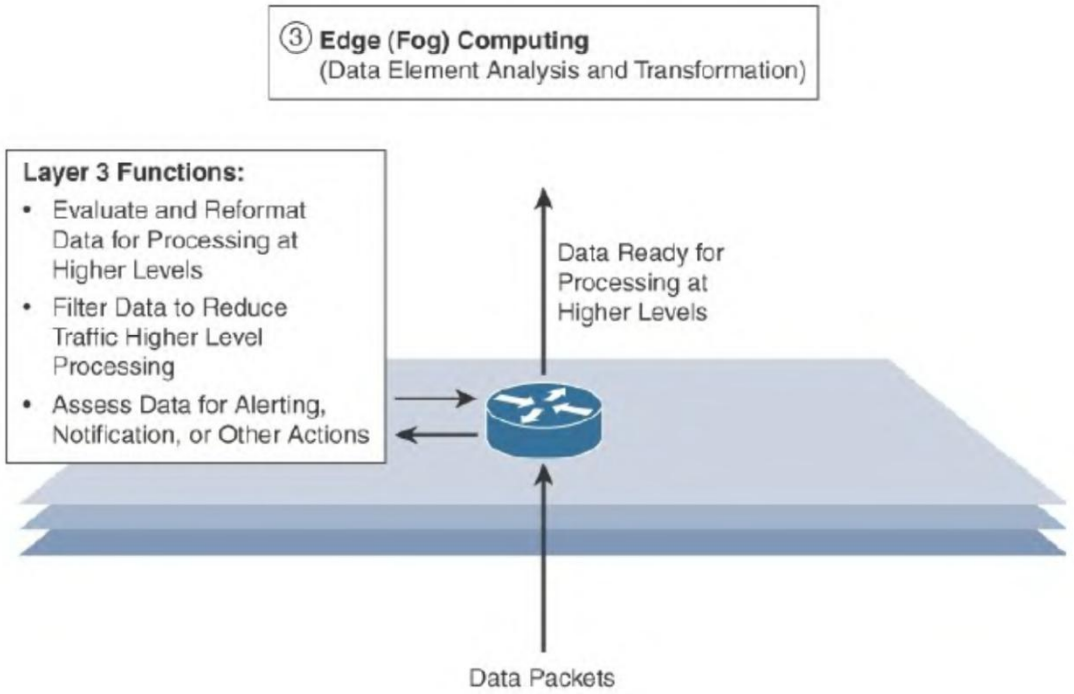
Επίπεδο 1, Φυσικές συσκευές και επίπεδο ελεγκτών: φιλοξενεί τα "πράγματα" στο Διαδίκτυο των Πραγμάτων, συμπεριλαμβανομένων των διαφόρων συσκευών και αισθητήρων τελικού σημείου που στέλνουν και λαμβάνουν πληροφορίες. Το μέγεθος αυτών των "πραγμάτων" μπορεί να κυμαίνεται από σχεδόν μικροσκοπικούς αισθητήρες έως γιγαντιαίες μηχανές σε ένα εργοστάσιο. Η κύρια λειτουργία τους είναι η δημιουργία δεδομένων και η δυνατότητα να ερωτηθούν ή/και να ελεγχθούν μέσω ενός δικτύου.

Επίπεδο 2, Στρώμα συνδεσιμότητας: Η πιο σημαντική λειτουργία αυτού του επιπέδου IoT είναι η αξιόπιστη και έγκαιρη μετάδοση δεδομένων. Πιο συγκεκριμένα, αυτό περιλαμβάνει εκπομπές μεταξύ συσκευών Επιπέδου 1 και του δικτύου και μεταξύ του δικτύου και της επεξεργασίας πληροφοριών που λαμβάνει χώρα στο Επίπεδο 3 (το επίπεδο υπολογιστικού άκρου). Οι λειτουργίες του επιπέδου συνδεσιμότητας περιγράφονται λεπτομερώς στο Σχήμα 11.



Σχήμα 11: Στρώμα λειτουργιών επιπέδου συνδεσιμότητας μοντέλου αναφοράς IoT.

Επίπεδο 3, Υπολογιστικού Άκρου: Σε αυτό το επίπεδο, η έμφαση δίνεται στη μείωση των δεδομένων και τη μετατροπή των ροών δεδομένων δικτύου σε πληροφορίες που είναι έτοιμα για αποθήκευση και επεξεργασία από υψηλότερα επίπεδα. Μία από τις βασικές αρχές αυτού του μοντέλου αναφοράς είναι ότι η επεξεργασία πληροφοριών ξεκινά όσο το δυνατόν νωρίτερα και όσο το δυνατόν πιο κοντά στην άκρη του δικτύου. Το Σχήμα 12, επισημαίνει τις λειτουργίες που χειρίζεται το Επίπεδο 3 του Μοντέλου Αναφοράς IoT.



Σχήμα 12: Λειτουργίες μοντέλου αναφοράς IoT Επιπέδου 3.

Μια άλλη σημαντική λειτουργία που εμφανίζεται στο επίπεδο 3 είναι η αξιολόγηση των δεδομένων για να διαπιστωθεί εάν μπορούν να φιλτραριστούν ή να συγκεντρωθούν πριν σταλούν σε υψηλότερο επίπεδο. Αυτό επιτρέπει επίσης την επαναδιαμόρφωση ή αποκωδικοποίηση δεδομένων, διευκολύνοντας την πρόσθετη επεξεργασία από άλλα συστήματα. Έτσι, μια κρίσιμη συνάρτηση είναι η αξιολόγηση των δεδομένων για να διαπιστωθεί εάν τα προκαθορισμένα όρια ξεπερνούνται και οποιαδήποτε ενέργεια ή ειδοποιήσεις πρέπει να αποσταλούν.

Επίπεδο 4, Στρώμα συσσώρευσης δεδομένων: Καταγράφει δεδομένα και τα αποθηκεύει έτσι ώστε να μπορούν να χρησιμοποιηθούν από εφαρμογές όταν είναι απαραίτητο. Μετατρέπει δεδομένα που βασίζονται σε συμβάντα σε επεξεργασία βάσει ερωτήματος.

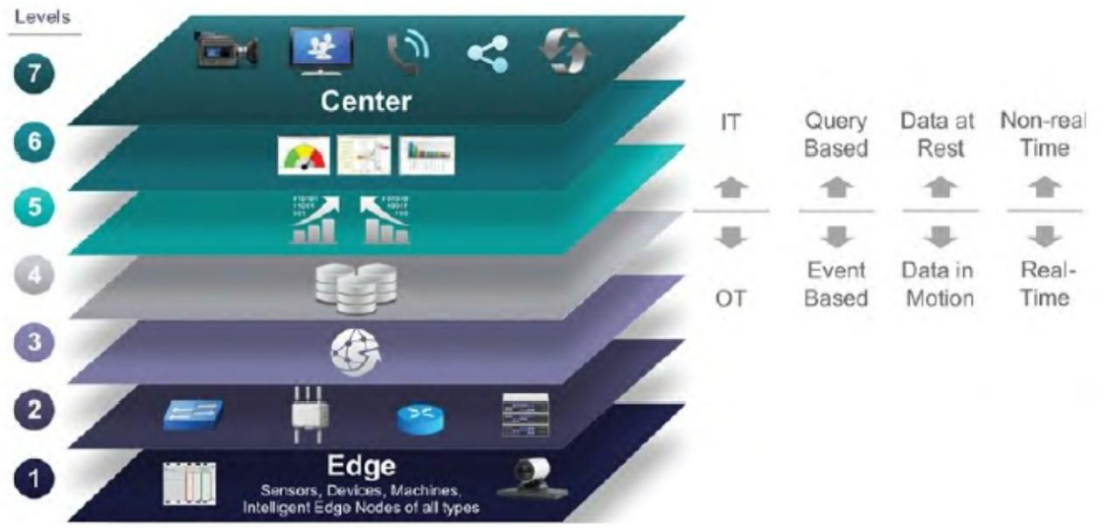
Επίπεδο 5, Αφαίρεσης δεδομένων: Συνδυάζει πολλαπλές μορφές δεδομένων και εξασφαλίζει συνεπή σημασιολογία από διάφορες πηγές. Επιβεβαιώνει ότι το σύνολο δεδομένων είναι πλήρες και ενοποιεί τα δεδομένα σε ένα μέρος ή σε πολλαπλές αποθήκες δεδομένων χρησιμοποιώντας εικονικοποίηση.

Επίπεδο 6, Εφαρμογών: Ερμηνεύει δεδομένα χρησιμοποιώντας εφαρμογές λογισμικού. Οι εφαρμογές μπορούν να παρακολουθούν, να ελέγχουν και να παρέχουν αναφορές με βάση την ανάλυση των δεδομένων.

Επίπεδο 7, Συνεργασίας και διεργασιών: Επεξεργάζεται και μοιράζεται τις πληροφορίες της εφαρμογής. Η συνεργασία και η επικοινωνία πληροφοριών IoT απαιτεί συχνά πολλά βήματα και είναι αυτό που καθιστά το IoT χρήσιμο. Αυτό το επίπεδο μπορεί να αλλάξει τις επιχειρηματικές διαδικασίες και να προσφέρει τα οφέλη του IoT.

Κεφάλαιο 2.4 Ευθύνες IT και OT στο μοντέλο αναφοράς IoT

Τα συστήματα IoT πρέπει να διασχίζουν πολλά όρια πέρα από τα λειτουργικά επίπεδα. Όπως φαίνεται στο Σχήμα 13, το κάτω μέρος της στοίβας είναι γενικά στον τομέα του OT.
Για μια βιομηχανία όπως το πετρέλαιο και το φυσικό αέριο, αυτό περιλαμβάνει αισθητήρες και συσκευές που συνδέονται με αγωγούς, εξέδρες πετρελαίου, μηχανήματα διυλιστηρίου κ.ο.κ. Το επάνω μέρος της στοίβας βρίσκεται στην περιοχή πληροφορικής και περιλαμβάνει πράγματα όπως οι διακομιστές, οι βάσεις δεδομένων και οι εφαρμογές, οι οποίες εκτελούνται σε τμήμα του δικτύου που ελέγχεται από την τεχνολογία πληροφορικής. Στο παρελθόν, το OT και το IT ήταν γενικά πολύ ανεξάρτητα και δεν είχαν μεγάλη ανάγκη καν να μιλήσουν μεταξύ τους.



Σχήμα 13: Μοντέλο αναφοράς IoT - Διαχωρισμός IT και OT.

Στο κάτω μέρος, στα επίπεδα OT, οι συσκευές παράγουν δεδομένα σε πραγματικό χρόνο με τη δική τους ταχύτητα. Όχι μόνο αυτό οδηγεί σε έναν τεράστιο όγκο δεδομένων που μεταφέρονται στο δίκτυο IoT, αλλά ο τεράστιος όγκος δεδομένων υποδηλώνει ότι οι εφαρμογές στο επάνω επίπεδο θα μπορούν να απορροφήσουν τόσα πολλά δεδομένα με τον απαιτούμενο ρυθμό. Για να ικανοποιηθεί αυτή η απαίτηση, τα δεδομένα πρέπει να αποθηκευτούν ή να αποθηκευτούν σε ορισμένα σημεία της στοίβας IoT. Η στρώση της διαχείρισης δεδομένων με αυτόν τον τρόπο σε όλη τη στοίβα βοηθά τα τέσσερα πρώτα επίπεδα να χειρίζονται τα δεδομένα με τη δική τους ταχύτητα.
Ως αποτέλεσμα, τα «δεδομένα σε κίνηση» σε πραγματικό χρόνο πρέπει να οργανωθούν και να αποθηκευτούν έτσι ώστε να καταστούν «δεδομένα σε κατάσταση ηρεμίας» για τις εφαρμογές στα επίπεδα πληροφορικής IT. Οι οργανισμοί IT και OT πρέπει να συνεργαστούν για τη συνολική διαχείριση δεδομένων.

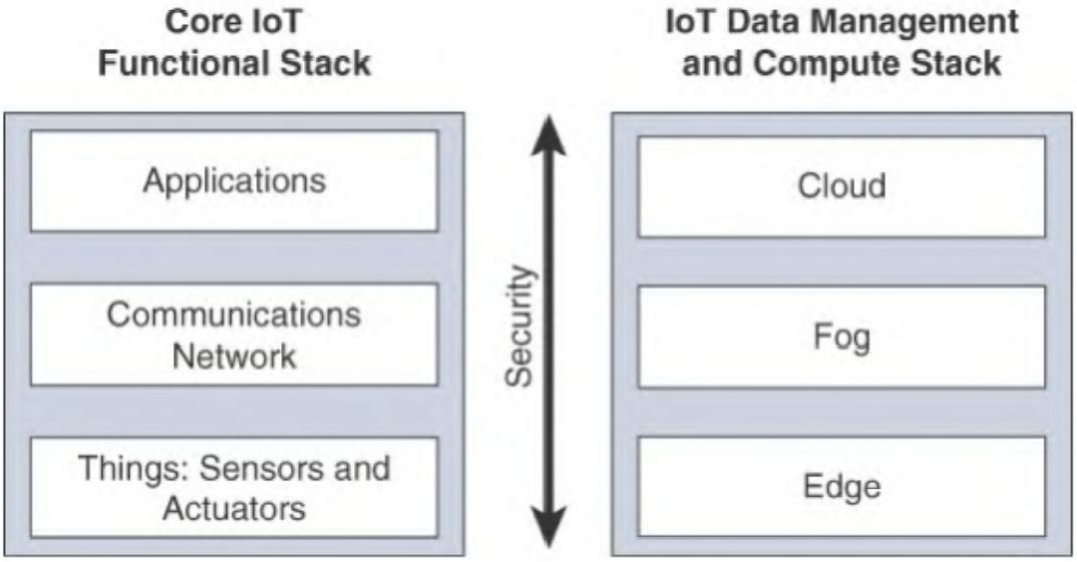
Κεφάλαιο 2.5 Απλοποιημένη αρχιτεκτονική IoT

Αν και υπάρχουν σημαντικές διαφορές μεταξύ των προαναφερθέντων μοντέλων αναφοράς, το καθένα προσεγγίζει το IoT από μια πολυεπίπεδη προοπτική, επιτρέποντας την ανάπτυξη τεχνολογίας και προτύπων κάπως ανεξάρτητα σε κάθε επίπεδο ή τομέα. Το κοινό στοιχείο μεταξύ αυτών των πλαισίων είναι ότι όλοι αναγνωρίζουν τη διασύνδεση των συσκευών τελικού σημείου IoT σε ένα δίκτυο που μεταφέρει τα δεδομένα όπου τελικά χρησιμοποιούνται από εφαρμογές, είτε στο κέντρο δεδομένων,είτε σε διάφορα σημεία

διαχείρισης σε ολόκληρη τη στοίβα . Στην παρούσα εργασία παρουσιάζεται ένα πλαίσιο IoT που αναδεικνύει τα θεμελιώδη δομικά στοιχεία που είναι κοινά στα περισσότερα συστήματα IoT και το οποίο προορίζεται να βοηθήσει στο σχεδιασμό ενός δικτύου IoT.
Αυτό το πλαίσιο παρουσιάζεται ως δύο παράλληλες στοίβες:

- IoT Data Management
- Compute Stack και το Core IoT Functional Stack.

Η μείωση του πλαισίου σε ένα ζεύγος τριών επιπέδων στοίβων σε καμία περίπτωση δεν υποδηλώνει ότι το μοντέλο δεν διαθέτει τις απαραίτητες λεπτομέρειες για την ανάπτυξη μιας εξελιγμένης στρατηγικής IoT. Αντίθετα, η πρόθεση είναι να απλοποιηθεί η αρχιτεκτονική IoT στα πιο βασικά δομικά στοιχεία της και στη συνέχεια να χρησιμοποιηθεί ως θεμέλιο για την κατανόηση βασικών αρχών σχεδιασμού και ανάπτυξης που εφαρμόζονται σε περιπτώσεις χρήσης συγκεκριμένων βιομηχανιών. Όλα τα επίπεδα πιο πολύπλοκων μοντέλων εξακολουθούν να καλύπτονται, αλλά ομαδοποιούνται εδώ σε λειτουργικά μπλοκ που είναι εύκολα κατανοητά. Το Σχήμα 14 απεικονίζει το απλοποιημένο μοντέλο IoT.



Σχήμα 14: Απλοποιημένη αρχιτεκτονική IoT.

Η παρουσίαση της λειτουργικής στοίβας Core IoT (Functional Stack) σε τρία επίπεδα έχει ως στόχο να απλοποιήσει την κατανόηση της αρχιτεκτονικής IoT στα πιο θεμελιώδη δομικά στοιχεία της. Το επίπεδο επικοινωνίας δικτύου της στοίβας IoT περιλαμβάνει ένα σημαντικό ποσό λεπτομερειών και ενσωματώνει μια τεράστια ποικιλία τεχνολογιών. Σε αντίθεση με τα περισσότερα δίκτυα πληροφορικής IT, οι εφαρμογές και το επίπεδο ανάλυσης του IoT δεν υπάρχουν απαραίτητα μόνο στο κέντρο δεδομένων. Λόγω των μοναδικών προκλήσεων και απαιτήσεων του IoT, είναι συχνά απαραίτητο να αναπτυχθούν εφαρμογές και διαχείριση δεδομένων σε όλη την αρχιτεκτονική με κλιμακωτή προσέγγιση, επιτρέποντας τη συλλογή δεδομένων, την ανάλυση και τους ευφυείς ελέγχους σε πολλά σημεία του συστήματος IoT.
Τα τρία επίπεδα διαχείρισης δεδομένων (Data Management) είναι το στρώμα άκρων (διαχείριση δεδομένων στους ίδιους τους αισθητήρες), το επίπεδο ομίχλης (διαχείριση δεδομένων στις πύλες και το δίκτυο διέλευσης) και το επίπεδο cloud (διαχείριση δεδομένων στο σύννεφο ή κεντρικό κέντρο δεδομένων).

Κεφάλαιο 2.6 Η λειτουργική στοίβα Core IoT

Τα δίκτυα IoT χτίζονται γύρω από την έννοια των "πραγμάτων" ή έξυπνων αντικειμένων που εκτελούν λειτουργίες και παρέχουν νέες συνδεδεμένες υπηρεσίες. Αυτά τα αντικείμενα είναι «έξυπνα» επειδή χρησιμοποιούν συνδυασμό πληροφοριών με βάση τα συμφραζόμενα και διαμορφωμένους στόχους για την εκτέλεση ενεργειών. Αυτές οι ενέργειες μπορούν να είναι αυτοδύναμες (δηλαδή, το έξυπνο αντικείμενο δεν βασίζεται σε εξωτερικά συστήματα για τις ενέργειές του).
Ωστόσο, στις περισσότερες περιπτώσεις, το «πράγμα» αλληλεπιδρά με ένα εξωτερικό σύστημα για να αναφέρει πληροφορίες που συλλέγει το έξυπνο αντικείμενο, να ανταλλάξει με άλλα αντικείμενα ή να αλληλεπιδράσει με μια πλατφόρμα διαχείρισης. Σε αυτήν την περίπτωση, η πλατφόρμα διαχείρισης μπορεί να χρησιμοποιηθεί για την επεξεργασία δεδομένων που συλλέγονται από το έξυπνο αντικείμενο και επίσης καθοδηγεί τη συμπεριφορά του έξυπνου αντικειμένου. Από αρχιτεκτονικής άποψης, πολλά στοιχεία πρέπει να συνεργαστούν για να λειτουργήσει ένα δίκτυο IoT:

«Πράγματα»: Επίπεδο αισθητήρων και ενεργοποιητών. Σε αυτό το επίπεδο, οι φυσικές συσκευές πρέπει να ταιριάζουν με τους περιορισμούς του περιβάλλοντος στο οποίο αναπτύσσονται ενώ εξακολουθούν να είναι σε θέση να παρέχουν τις απαραίτητες πληροφορίες.
Τα περισσότερα δίκτυα IoT ξεκινούν από το αντικείμενο ή το "πράγμα" που πρέπει να συνδεθεί. Από αρχιτεκτονική σκοπιά, η ποικιλία τύπων, σχημάτων και αναγκών έξυπνων αντικειμένων οδηγεί την ποικιλία πρωτοκόλλων και αρχιτεκτονικών IoT.
Μια αρχιτεκτονική ταξινόμηση θα μπορούσε να στηρίζεται:

- Στο αν το αντικείμενο μεταφέρει τη δική του ενεργειακή παροχή ή λαμβάνει συνεχή ισχύ από εξωτερική πηγή ενέργειας. Τα πράγματα που λειτουργούν με μπαταρία μπορούν να μετακινηθούν πιο εύκολα από τα αντικείμενα που λειτουργούν με γραμμή. Ωστόσο, οι μπαταρίες περιορίζουν τη διάρκεια ζωής και την ποσότητα ενέργειας που επιτρέπεται να καταναλώσει το αντικείμενο, οδηγώντας έτσι το εύρος και τη συχνότητα μετάδοσης.

- Στο αν το «πράγμα» πρέπει να μετακινηθεί ή να παραμείνει πάντα στην ίδια θέση. Ένας αισθητήρας μπορεί να είναι κινητός επειδή μετακινείται από το ένα αντικείμενο στο άλλο ή επειδή είναι προσαρτημένος σε ένα κινούμενο αντικείμενο.

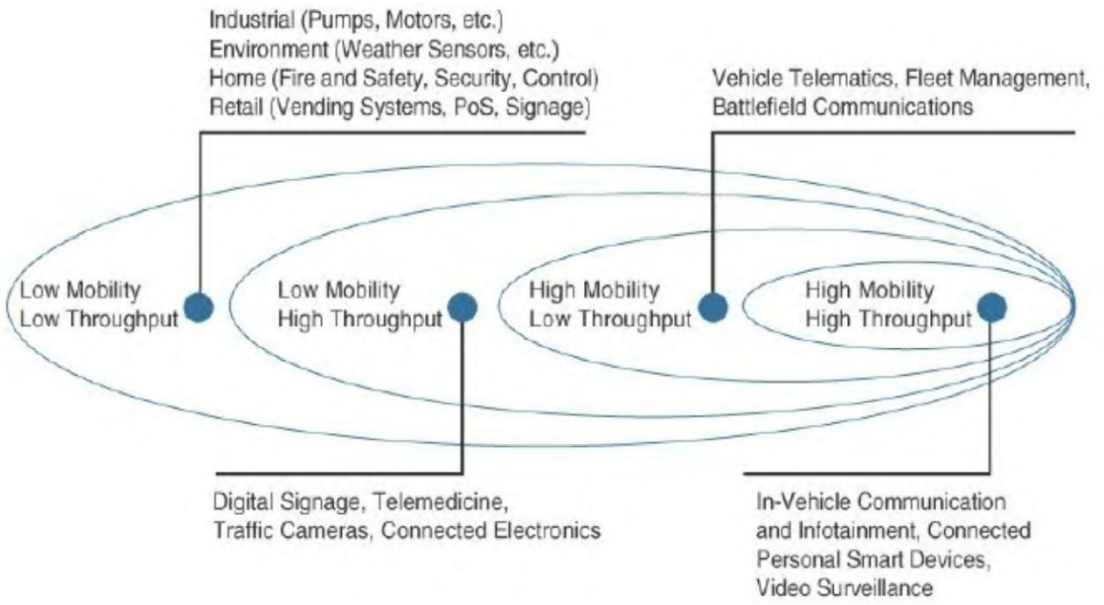
- Στο πόσο συχνά το αντικείμενο πρέπει να αναφέρει τις παραμέτρους που παρακολουθούνται. Ένας αισθητήρας κίνησης μπορεί να αναφέρει επιτάχυνση αρκετές εκατοντάδες ανά δευτερόλεπτο. Οι υψηλότερες συχνότητες οδηγούν σε υψηλότερη κατανάλωση ενέργειας, η οποία μπορεί να δημιουργήσει περιορισμούς στην πιθανή πηγή ενέργειας (και επομένως την κινητικότητα του αντικειμένου) και το εύρος μετάδοσης.

- Σχετικά με την ποσότητα των δεδομένων που ανταλλάσσονται σε κάθε κύκλο αναφοράς. Πλουσιότερα δεδομένα οδηγούν συνήθως σε υψηλότερη κατανάλωση ενέργειας. Αυτή η ταξινόμηση συχνά συνδυάζεται με την προηγούμενη για τον προσδιορισμό της απόδοσης δεδομένων αντικειμένου (χαμηλή απόδοση έως υψηλή απόδοση).

- Στην απόσταση στην οποία βρίσκεται η πύλη.

- Στον αριθμό των έξυπνων αντικειμένων (με παρόμοια ανάγκη επικοινωνίας) σε μια δεδομένη περιοχή, συνδεδεμένα με την ίδια πύλη.

Το Σχήμα 15 παρέχει μερικά παραδείγματα εφαρμογών που ταιριάζουν με το συνδυασμό απαιτήσεων κινητικότητας και απόδοσης.



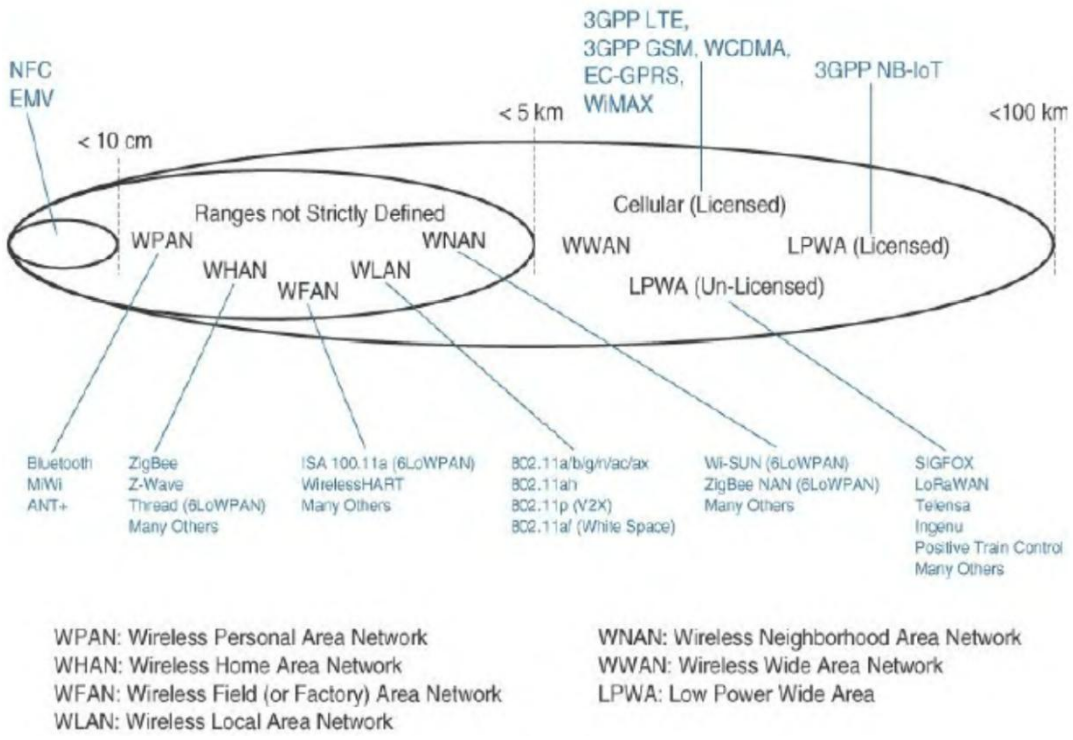
Σχήμα 15: Παράδειγμα εφαρμογών αισθητήρων με βάση την κινητικότητα και την απόδοση.

Οι κατηγορίες που χρησιμοποιούνται για την ταξινόμηση των πραγμάτων μπορούν να επηρεάσουν άλλες παραμέτρους και μπορούν επίσης να επηρεάσουν η μία την άλλη. Για παράδειγμα, ένα πολύ κινητό αντικείμενο που λειτουργεί με μπαταρία (όπως ένα όργανο παρακολούθησης καρδιακών παλμών, για παράδειγμα) έχει πιθανώς έναν μικρό παράγοντα μορφής. Ένας μικρός αισθητήρας είναι ευκολότερο να μετακινηθεί ή να ενσωματωθεί στο περιβάλλον του. Ταυτόχρονα, ένα μικρό και εξαιρετικά κινητό έξυπνο αντικείμενο είναι απίθανο να απαιτεί μεγάλη κεραία και ισχυρή πηγή ενέργειας. Αυτός ο περιορισμός θα περιορίσει το εύρος μετάδοσης και, ως εκ τούτου, τον τύπο του πρωτοκόλλου δικτύου που διατίθεται για τις συνδέσεις του.

«Δίκτυο επικοινωνιών»: Όταν τα έξυπνα αντικείμενα δεν είναι αυτόνομα, πρέπει να επικοινωνούν με ένα εξωτερικό σύστημα. Σε πολλές περιπτώσεις, αυτή η επικοινωνία χρησιμοποιεί ασύρματη τεχνολογία. Αυτό το επίπεδο έχει τέσσερις υποστιβάδες:

1. Πρόσβαση στο δευτερεύον επίπεδο δικτύου: Το τελευταίο μίλι του δικτύου IoT είναι το δίκτυο πρόσβασης. Αυτό αποτελείται συνήθως από ασύρματες τεχνολογίες όπως 802.11ah, 802.15.4g και LoRa. Οι αισθητήρες που είναι συνδεδεμένοι στο δίκτυο πρόσβασης μπορεί επίσης να είναι ενσύρματοι. Μια βασική παράμετρος που καθορίζει την επιλογή της τεχνολογίας πρόσβασης είναι το εύρος μεταξύ του έξυπνου αντικειμένου και του συλλέκτη πληροφοριών.

Το Σχήμα 16 παραθέτει ορισμένες τεχνολογίες πρόσβασης και τις αναμενόμενες αποστάσεις μετάδοσης.



Σχήμα 16: Πρόσβαση σε Τεχνολογίες και Αποστάσεις.

Οι εκτιμήσεις εύρους ομαδοποιούνται με ονόματα κατηγοριών που απεικονίζουν το περιβάλλον ή την κατακόρυφη περιοχή όπου αναμένεται η συλλογή δεδομένων σε αυτό το εύρος. Οι κοινές ομάδες είναι οι εξής:

PAN (προσωπικό δίκτυο περιοχής): Κλίμακα μερικών μέτρων. Αυτός είναι ο προσωπικός χώρος γύρω από ένα άτομο. Μια κοινή ασύρματη τεχνολογία για αυτήν την κλίμακα είναι το Bluetooth.

HAN (δίκτυο οικιακής περιοχής): Κλίμακα μερικών δεκάδων μέτρων. Σε αυτήν την κλίμακα, οι κοινές ασύρματες τεχνολογίες για το IoT περιλαμβάνουν το ZigBee και το Bluetooth Low Energy (BLE).

NAN (δίκτυο περιοχής γειτονιάς): Κλίμακα μερικών εκατοντάδων μέτρων. Ο όρος NAN χρησιμοποιείται συχνά για να αναφερθεί σε μια ομάδα οικιακών μονάδων από τις οποίες συλλέγονται δεδομένα.

FAN (δίκτυο περιοχής πεδίου): Κλίμακα αρκετών δεκάδων μέτρων έως αρκετών εκατοντάδων μέτρων. Το FAN αναφέρεται συνήθως σε έναν υπαίθριο χώρο μεγαλύτερο από μία μόνο ομάδα οικιακών μονάδων. Θεωρείται συχνά ως «ανοιχτός χώρος» (και ως εκ τούτου δεν είναι ασφαλές και δεν ελέγχεται).

LAN (τοπικό δίκτυο): Κλίμακα έως 100 m. Αυτός ο όρος είναι πολύ συνηθισμένος στη δικτύωση και ως εκ τούτου χρησιμοποιείται επίσης συχνά στο χώρο του IoT όταν χρησιμοποιούνται τυπικές τεχνολογίες δικτύωσης (όπως Ethernet ή IEEE 802.11).

Άλλες ταξινομήσεις δικτύων, όπως το MAN (metropolitan area network, με εμβέλεια έως μερικά χιλιόμετρα) και το WAN (δίκτυο ευρείας περιοχής, με εμβέλεια άνω των μερικών χιλιομέτρων), χρησιμοποιούνται επίσης συνήθως.

2 **Gateways και Backhaul SubLayer:** Ένα κοινό σύστημα επικοινωνίας οργανώνει πολλά έξυπνα αντικείμενα σε μια δεδομένη περιοχή γύρω από μια κοινή πύλη. Η πύλη επικοινωνεί απευθείας με τα έξυπνα αντικείμενα. Ο ρόλος της πύλης είναι να προωθήσει τις συλλεγμένες πληροφορίες μέσω ενός μέσου μεγαλύτερης εμβέλειας (που ονομάζεται backhaul) σε έναν κεντρικό σταθμό όπου επεξεργάζονται τις πληροφορίες. Συγκεκριμένα, τα δεδομένα που συλλέγονται από ένα έξυπνο αντικείμενο μπορεί να χρειαστεί να προωθηθούν σε έναν κεντρικό σταθμό όπου επεξεργάζονται τα δεδομένα. Δεδομένου ότι αυτός ο σταθμός βρίσκεται συχνά σε διαφορετική τοποθεσία από το έξυπνο αντικείμενο, τα δεδομένα που λαμβάνονται απευθείας από τον αισθητήρα μέσω μιας τεχνολογίας πρόσβασης πρέπει να προωθούνται σε άλλο μέσο (το backhaul) και να μεταφέρονται στον κεντρικό σταθμό. Η πύλη (Gateway) είναι υπεύθυνη για αυτήν την ενδιάμεση επικοινωνία.

3 **Υποεπίπεδο μεταφοράς δικτύου:** Για να είναι επιτυχής η επικοινωνία, πρέπει να εφαρμοστούν πρωτόκολλα δικτύων και επιπέδων μεταφοράς (όπως IP και UDP), για να υποστηρίζουν την ποικιλία των συσκευών προς σύνδεση και των μέσων χρήσης. Το πρωτόκολλο πρέπει να είναι ανοιχτό και βασισμένο σε πρότυπα για να μπορεί να φιλοξενήσει πολλούς κλάδους και πολλαπλά μέσα. Η επεκτασιμότητα (για τη φιλοξενία χιλιάδων ή εκατομμυρίων αισθητήρων σε ένα μόνο δίκτυο) και η ασφάλεια είναι επίσης κοινές απαιτήσεις. Το IP είναι ένα πρωτόκολλο που πληροί όλες αυτές τις απαιτήσεις.
Η ευελιξία της IP επιτρέπει σε αυτό το πρωτόκολλο να ενσωματωθεί σε αντικείμενα πολύ διαφορετικής φύσης, ανταλλάσσοντας πληροφορίες σε πολύ διαφορετικά μέσα, συμπεριλαμβανομένων δικτύων χαμηλής ισχύος, απώλειας και χαμηλού εύρους ζώνης. Τέλος, τα πρωτόκολλα επιπέδου μεταφοράς που έχουν δημιουργηθεί πάνω από IP (UDP και TCP) μπορούν εύκολα να αξιοποιηθούν για να αποφασίσουν εάν το δίκτυο πρέπει να ελέγχει την παράδοση των πακέτων δεδομένων (με TCP) ή εάν η εργασία ελέγχου πρέπει να αφεθεί στην εφαρμογή (UDP). Το UDP είναι ένα πολύ ελαφρύτερο και γρηγορότερο πρωτόκολλο από το TCP. Ωστόσο, δεν εγγυάται παράδοση πακέτων. Τόσο το TCP όσο και το UDP μπορούν να ασφαλιστούν με TLS/SSL (TCP) ή DTLS (UDP).

4 **Υποεπίπεδο διαχείρισης δικτύου IoT:** Πρέπει να υπάρχουν πρόσθετα πρωτόκολλα που να επιτρέπουν στις εφαρμογές headend να ανταλλάσσουν δεδομένα με τους αισθητήρες. IP, TCP και UDP φέρνουν συνδεσιμότητα σε δίκτυα IoT. Τα πρωτόκολλα ανώτερου επιπέδου πρέπει να φροντίζουν για τη μετάδοση δεδομένων μεταξύ των έξυπνων αντικειμένων και άλλων συστημάτων. Πολλαπλά πρωτόκολλα έχουν αξιοποιηθεί ή έχουν δημιουργηθεί για την επίλυση προβλημάτων επικοινωνίας δεδομένων IoT. Έχουν προταθεί άλλα πρωτόκολλα που προέρχονται από τον ιστό για το χώρο του IoT. Ένα παράδειγμα είναι το WebSocket. Το WebSocket αποτελεί μέρος της προδιαγραφής HTML5 και παρέχει μια απλή αμφίδρομη σύνδεση μέσω μιας μόνο σύνδεσης. Ορισμένες λύσεις IoT χρησιμοποιούν το WebSocket για τη διαχείριση της σύνδεσης μεταξύ του έξυπνου αντικειμένου και μιας εξωτερικής εφαρμογής. Το WebSocket συχνά συνδυάζεται με άλλα πρωτόκολλα, όπως το MQTT για να χειριστεί το τμήμα της επικοινωνίας που σχετίζεται με το IoT.
Με την ίδια λογική επαναχρησιμοποίησης γνωστών μεθόδων, δημιουργήθηκε το πρωτόκολλο επεκτάσιμων μηνυμάτων και παρουσίας (Extensible Messaging and

Presence Protocol XMPP). Το XMPP βασίζεται στα άμεσα μηνύματα και την παρουσία. Επιτρέπει την ανταλλαγή δεδομένων μεταξύ δύο ή περισσότερων συστημάτων και υποστηρίζει την παρουσία και τη συντήρηση λίστας επαφών.
Μπορεί επίσης να χειριστεί τη δημοσίευση/εγγραφή, καθιστώντας την καλή επιλογή για διανομή πληροφοριών σε πολλές συσκευές. Ένας περιορισμός του XMPP είναι η εξάρτησή του από το TCP, το οποίο μπορεί να αναγκάσει τους συνδρομητές να διατηρήσουν ανοικτές συνεδρίες σε άλλα συστήματα και μπορεί να είναι ένας περιορισμός για αντικείμενα με περιορισμένη μνήμη.
Άλλα πρωτόκολλα που μπορούν να χρησιμοποιηθούν είναι το πρωτόκολλο περιορισμένης εφαρμογής (Constrained Application Protocol) CoAP. Το CoAP χρησιμοποιεί ορισμένες μεθόδους παρόμοιες με αυτές του HTTP (όπως λήψη, δημοσίευση, τοποθέτηση και διαγραφή), αλλά υλοποιεί μια πιο σύντομη λίστα, περιορίζοντας έτσι το μέγεθος της κεφαλίδας. Ένα άλλο κοινό πρωτόκολλο IoT που χρησιμοποιείται σε αυτά τα μεσαία έως ανώτερα επίπεδα είναι το Message Queue Telemetry Transport (MQTT).

«Εφαρμογής και ανάλυσης»: Στο επάνω επίπεδο, μια εφαρμογή πρέπει να επεξεργαστεί τα δεδομένα που συλλέγονται, όχι μόνο για τον έλεγχο των έξυπνων αντικειμένων όταν είναι απαραίτητο, αλλά για τη λήψη έξυπνων αποφάσεων με βάση τις πληροφορίες που συλλέγονται και, με τη σειρά του, να καθοδηγήσει τα «πράγματα» ή άλλα συστήματα για να προσαρμοστούν στις αναλυθείσες συνθήκες και να αλλάξουν τη συμπεριφορά ή τις παραμέτρους τους. Πολλαπλές εφαρμογές μπορούν να βοηθήσουν στην αύξηση της αποδοτικότητας ενός δικτύου IoT. Κάθε εφαρμογή συλλέγει δεδομένα και παρέχει μια σειρά από λειτουργίες που βασίζονται στην ανάλυση των δεδομένων που συλλέγονται.

Από αρχιτεκτονικής απόψεως, μια βασική ταξινόμηση μπορεί να είναι η ακόλουθη:

Εφαρμογή ανάλυσης: Αυτός ο τύπος εφαρμογής συλλέγει δεδομένα από πολλά έξυπνα αντικείμενα, επεξεργάζεται τα δεδομένα που συλλέγονται και εμφανίζει πληροφορίες που προκύπτουν από τα δεδομένα που έχουν υποστεί επεξεργασία.

Εφαρμογή ελέγχου: Αυτός ο τύπος εφαρμογής ελέγχει τη συμπεριφορά του έξυπνου αντικειμένου ή τη συμπεριφορά ενός αντικειμένου που σχετίζεται με το έξυπνο αντικείμενο. Ένα παράδειγμα αρχιτεκτονικής συστήματος ελέγχου είναι το **SCADA**.
Το **SCADA** αναπτύχθηκε ως μια καθολική μέθοδος πρόσβασης σε απομακρυσμένα συστήματα και αποστολή οδηγιών. Ένα παράδειγμα όπου χρησιμοποιείται ευρέως το SCADA είναι ο έλεγχος και η παρακολούθηση απομακρυσμένων τερματικών μονάδων (Remote Terminal Units RTU) στο ηλεκτρικό δίκτυο διανομής.

Πολλές προηγμένες εφαρμογές IoT περιλαμβάνουν τόσο μονάδες ανάλυσης όσο και μονάδες ελέγχου. Στις περισσότερες περιπτώσεις, τα δεδομένα συλλέγονται από τα έξυπνα αντικείμενα και υποβάλλονται σε επεξεργασία στην ενότητα ανάλυσης. Το αποτέλεσμα αυτής της επεξεργασίας μπορεί να χρησιμοποιηθεί για την τροποποίηση της συμπεριφοράς έξυπνων αντικειμένων ή συστημάτων που σχετίζονται με τα έξυπνα αντικείμενα. Η μονάδα ελέγχου χρησιμοποιείται για τη μετάδοση των οδηγιών για αλλαγές συμπεριφοράς.

«Έξυπνες Υπηρεσίες (Smart Services)»: Η δυνατότητα χρήσης του IoT για τη βελτίωση των λειτουργιών συχνά ονομάζεται «έξυπνες υπηρεσίες». Βασικά, οι έξυπνες υπηρεσίες χρησιμοποιούν το IoT και στοχεύουν στην αποτελεσματικότητα. Για παράδειγμα, μπορούν να εγκατασταθούν αισθητήρες στον εξοπλισμό για να διασφαλιστεί η συνεχής συμμόρφωση με τους κανονισμούς ή τις απαιτήσεις ασφαλείας.

Αυτή η γωνία αποδοτικότητας μπορεί να λάβει πολλαπλές μορφές, από αισθητήρες παρουσίας σε επικίνδυνες περιοχές έως ανιχνευτές παραβίασης ορίου βάρους σε φορτηγά. Οι «έξυπνες υπηρεσίες» μπορούν επίσης να χρησιμοποιηθούν για τη μέτρηση της αποδοτικότητας των μηχανών ανιχνεύοντας την απόδοση, την ταχύτητα ή άλλες μορφές αξιολόγησης της χρήσης. Ολόκληρες οι λειτουργίες μπορούν να βελτιστοποιηθούν με το IoT.

Για παράδειγμα, στους θαλάμους νοσηλείας στα νοσοκομεία, οι αισθητήρες παρουσίας και κίνησης μπορούν να αξιολογήσουν τον αριθμό των επισκεπτών σε ένα θάλαμο και να ανακατευθύνουν ανάλογα το προσωπικό. Ο ίδιος τύπος λειτουργίας μπορεί να πραγματοποιηθεί σε ένα κατάστημα όπου ένας πελάτης εντοπίζεται ότι μένει περισσότερο από το τυπικό χρονικό διάστημα μπροστά από ένα ράφι. Το προσωπικό μπορεί να πάει για να παράσχει βοήθεια.
Οι «έξυπνες υπηρεσίες» μπορούν να ενσωματωθούν σε ένα σύστημα IoT. Για παράδειγμα, οι αισθητήρες μπορούν να ενσωματωθούν σε μια λάμπα. Ένας αισθητήρας μπορεί να ανάψει ή να σβήσει το φως με βάση την παρουσία ενός ανθρώπου στο δωμάτιο. Ακόμα μπορούν να συνδέουν με άλλα συστήματα στο σπίτι, ώστε να συντονιστεί η αποτελεσματικότητα. Για παράδειγμα, το σύστημα συναγερμού εισόδου στο σπίτι ή το σύστημα θέρμανσης μπορεί να συντονιστεί με τον ανιχνευτή παρουσίας σε μια λάμπα για να προσαρμοστεί στις ανιχνευμένες αλλαγές. Το σύστημα συναγερμού μπορεί να απενεργοποιήσει τους συναγερμούς κίνησης σε ζώνες όπου ανιχνεύεται κάποιο πρόσωπο.
Το σύστημα θέρμανσης μπορεί να προσαρμόσει τη θερμοκρασία στην ανθρώπινη παρουσία ή να εντοπίσει τις προσωπικές προτιμήσεις.

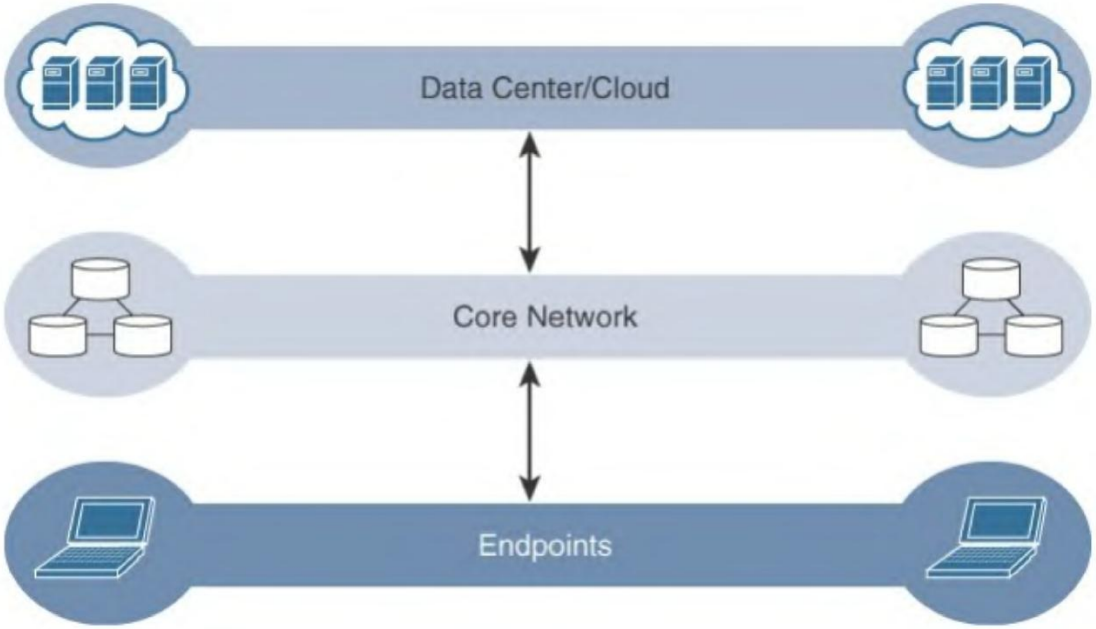
«Διαχείριση δεδομένων IoT και Compute Stack»: τα δεδομένα που παράγονται από αισθητήρες IoT είναι μία από τις μεγαλύτερες προκλήσεις στη δημιουργία ενός συστήματος IoT. Στην περίπτωση των σύγχρονων δικτύων πληροφορικής IT, τα δεδομένα που προέρχονται από υπολογιστή ή διακομιστή δημιουργούνται συνήθως από το μοντέλο επικοινωνίας πελάτη/διακομιστή και εξυπηρετούν τις ανάγκες της εφαρμογής. Στα δίκτυα αισθητήρων, η συντριπτική πλειοψηφία των δεδομένων που δημιουργούνται είναι μη δομημένα και πολύ μικρής χρήσης από μόνα τους. Καθώς ο όγκος των δεδομένων, η ποικιλία των αντικειμένων που συνδέονται στο δίκτυο και η ανάγκη για μεγαλύτερη αποτελεσματικότητα αυξάνονται, εμφανίζονται νέες απαιτήσεις και αυτές οι απαιτήσεις τείνουν να φέρουν την ανάγκη για ανάλυση δεδομένων πιο κοντά στο σύστημα IoT.

Αυτές οι νέες απαιτήσεις περιλαμβάνουν τα ακόλουθα:

1 Ελαχιστοποίηση της καθυστέρησης.
2 Διατήρηση εύρους ζώνης δικτύου.
3 Αύξηση της τοπικής αποδοτικότητας.

Επομένως, μια σημαντική εκτίμηση σχεδιασμού είναι ο τρόπος σχεδιασμού ενός δικτύου IoT για τη διαχείριση αυτού του όγκου δεδομένων με αποτελεσματικό τρόπο, έτσι ώστε τα δεδομένα να μπορούν να αναλυθούν γρήγορα και να οδηγήσουν σε επιχειρηματικά οφέλη.
Ο όγκος των δεδομένων που παράγονται από συσκευές IoT μπορεί να είναι τόσο μεγάλος που μπορεί εύκολα να ξεπεράσει τις δυνατότητες του συστήματος headend στο κέντρο δεδομένων ή στο cloud.
Όπως απεικονίζεται στο Σχήμα 17 η διαχείριση δεδομένων στα παραδοσιακά συστήματα πληροφορικής IT είναι πολύ απλή. Τα τελικά σημεία (φορητοί υπολογιστές, εκτυπωτές, τηλέφωνα IP και ούτω καθεξής) επικοινωνούν μέσω ενός κεντρικού δικτύου IP σε διακομιστές στο κέντρο δεδομένων ή στο cloud.

Τα δεδομένα γενικά αποθηκεύονται στο κέντρο δεδομένων και οι φυσικοί σύνδεσμοι από την πρόσβαση στον πυρήνα είναι συνήθως υψηλό εύρος ζώνης, πράγμα που σημαίνει ότι η πρόσβαση σε δεδομένα πληροφορικής IT είναι γρήγορη.

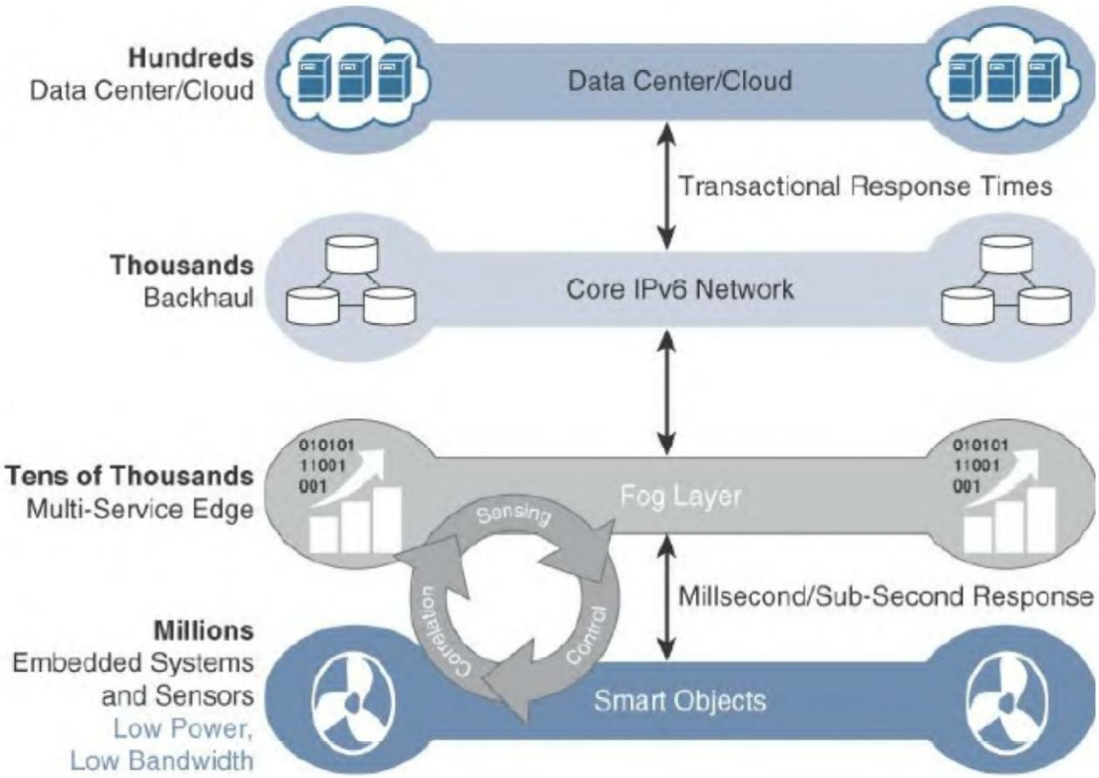


Σχήμα 17: Το Παραδοσιακό Μοντέλο Πληροφορικής IT Cloud Computing.

Τα συστήματα IoT λειτουργούν διαφορετικά. Αρκετά προβλήματα που σχετίζονται με δεδομένα και πρέπει να αντιμετωπιστούν είναι τα εξής:

- Το εύρος ζώνης στα δίκτυα IoT είναι πολύ περιορισμένο.
- Η καθυστέρηση μπορεί να είναι πολύ υψηλή.
- Η αναδιάρθρωση δικτύου από την πύλη μπορεί να είναι αναξιόπιστη και συχνά εξαρτάται από 3G/LTE ή ακόμη και από δορυφορικές συνδέσεις.Ο όγκος των δεδομένων που μεταδίδονται κατά τη διάρκεια της αναδιάρθρωσης μπορεί να είναι μεγάλος και πολλά από τα δεδομένα μπορεί να μην είναι πραγματικά τόσο ενδιαφέροντα (όπως απλά μηνύματα δημοσκοπήσεων).
- Τα μεγάλα δεδομένα γίνονται μεγαλύτερα. Ο τεράστιος όγκος των δεδομένων που δημιουργούνται καθιστά σχεδόν αδύνατη την ανάλυση και την ανταπόκριση σε πραγματικό χρόνο στα δεδομένα.

«Υπολογισμός ομίχλης (Fog Computing)»: Η λύση στις προκλήσεις που αναφέρθηκαν στην προηγούμενη ενότητα είναι η κατανομή της διαχείρισης δεδομένων σε όλο το σύστημα IoT, όσο το δυνατόν πιο κοντά στην άκρη του δικτύου IP. Η πιο γνωστή ενσωμάτωση των υπηρεσιών άκρης στο IoT είναι το «Fog Computing».Οποιαδήποτε συσκευή με υπολογιστικό, αποθηκευτικό χώρο και συνδεσιμότητα δικτύου μπορεί να είναι κόμβος ομίχλης. Η ανάλυση δεδομένων IoT κοντά στο σημείο που συλλέγονται ελαχιστοποιεί την καθυστέρηση, αποφορτίζει gigabytes κίνησης δικτύου από το κεντρικό δίκτυο και διατηρεί ευαίσθητα δεδομένα εντός του τοπικού δικτύου.
Ένα πλεονέκτημα αυτής της δομής είναι ότι το «Fog Computing» επιτρέπει τη συλλογή πληροφοριών (όπως η ανάλυση) και τον έλεγχο από το πλησιέστερο δυνατό σημείο, και με αυτόν τον τρόπο, επιτρέπει καλύτερη απόδοση σε περιορισμένα δίκτυα. Το Σχήμα 18 δείχνει την τοποθέτηση του στρώματος ομίχλης στο IoT Data Management and Compute Stack.



Σχήμα 18: IoT Data Management and Compute Stack with Fog.

Οι εφαρμογές ομίχλης (Fog applications) είναι τόσο διαφορετικές όσο το ίδιο το Διαδίκτυο των Πραγμάτων. Το κοινό τους είναι η μείωση των δεδομένων-η παρακολούθηση ή η ανάλυση δεδομένων σε πραγματικό χρόνο από πράγματα που συνδέονται με το δίκτυο και στη συνέχεια η έναρξη μιας ενέργειας.

Τα καθοριστικά χαρακτηριστικά του υπολογισμού ομίχλης (fog computing) είναι τα εξής:

- Ευαισθητοποίηση σχετικά με την τοποθεσία και χαμηλή καθυστέρηση.Ο κόμβος ομίχλης βρίσκεται όσο το δυνατόν πιο κοντά στο τελικό σημείο του IoT για να παρέχει κατανεμημένους υπολογισμούς.

- Γεωγραφική κατανομή. Οι υπηρεσίες και οι εφαρμογές στοχεύουν στους κόμβους ομίχλης και απαιτούν ευρέως διαδεδομένες αναπτύξεις.

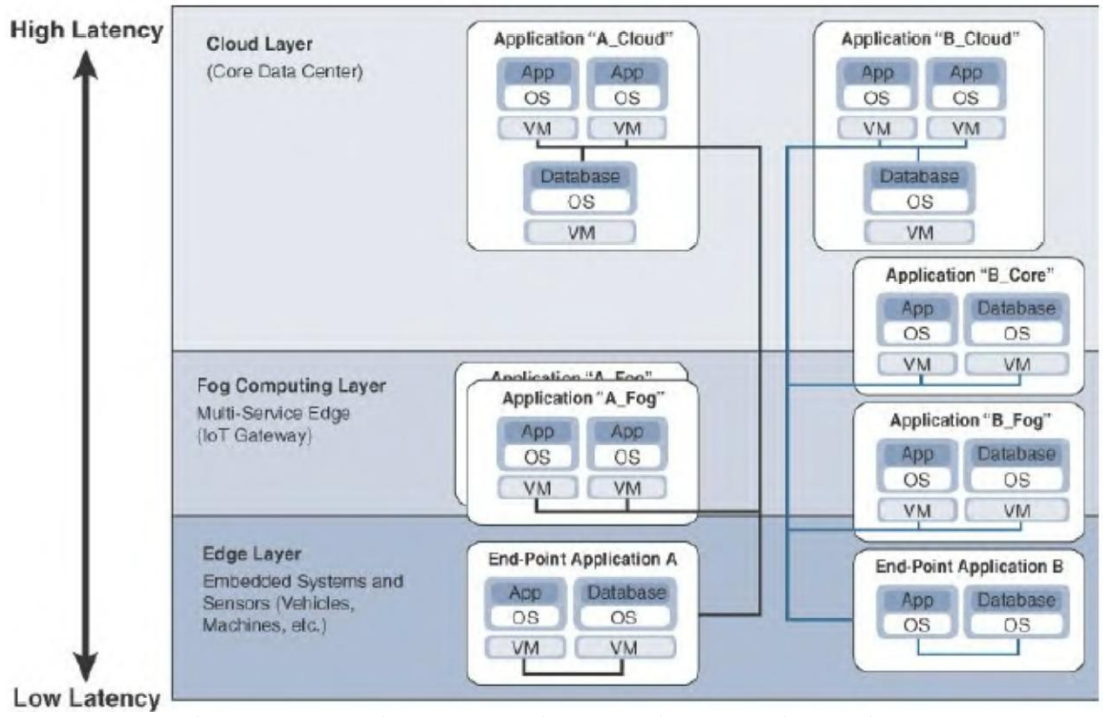
- Ανάπτυξη κοντά στα τελικά σημεία IoT. Οι κόμβοι ομίχλης συνήθως αναπτύσσονται παρουσία μεγάλου αριθμού τελικών σημείων IoT.

- Ασύρματη επικοινωνία μεταξύ του Fog και του τελικού σημείου IoT. Αν και είναι δυνατή η σύνδεση ενσύρματων κόμβων, τα πλεονεκτήματα του Fog είναι μεγαλύτερα όταν έχουμε μεγάλο αριθμό τελικών σημείων και η ασύρματη πρόσβαση είναι ο ευκολότερος τρόπος για να επιτευχθεί τέτοια κλίμακα.

- Χρήση για αλληλεπιδράσεις σε πραγματικό χρόνο. Οι σημαντικές εφαρμογές του Fog περιλαμβάνουν αλληλεπιδράσεις σε πραγματικό χρόνο.Η προ-επεξεργασία

δεδομένων στους κόμβους ομίχλης επιτρέπει στις εφαρμογές ανώτερου επιπέδου να εκτελούν «παρτίδες» επεξεργασίας σε ένα υποσύνολο των δεδομένων.

Το Σχήμα 19 απεικονίζει την ιεραρχική φύση του υπολογισμού άκρων, ομίχλης και νέφους σε ένα σύστημα IoT.



Σχήμα 19: Διανεμημένος υπολογισμός και διαχείριση δεδομένων σε ένα IoT.

Από αρχιτεκτονικής απόψεως, οι πλησιέστεροι κόμβοι ομίχλης στην άκρη του δικτύου λαμβάνουν τα δεδομένα από συσκευές IoT.
Η εφαρμογή ομίχλης (fog application) IoT στη συνέχεια κατευθύνει διαφορετικούς τύπους δεδομένων στο βέλτιστο μέρος και:

- Τα πιο ευαίσθητα στο χρόνο δεδομένα αναλύονται στην άκρη ή στον κόμβο ομίχλης που βρίσκεται πιο κοντά στα πράγματα που δημιουργούν τα δεδομένα.

- Τα δεδομένα που μπορούν να περιμένουν δευτερόλεπτα ή λεπτά για ενέργεια μεταφέρονται σε έναν κόμβο συνάθροισης για ανάλυση και δράση.

- Τα δεδομένα που είναι λιγότερο ευαίσθητα στο χρόνο αποστέλλονται στο cloud για ιστορική ανάλυση, ανάλυση μεγάλων δεδομένων και μακροπρόθεσμη αποθήκευση.

Κεφάλαιο 3 Έξυπνα αντικείμενα: Τα «Πράγματα» στο IoT

Αυτό το κεφάλαιο παρέχει μια λεπτομερή ανάλυση των έξυπνων αντικειμένων και της αρχιτεκτονικής τους. Παρέχει επίσης κατανόηση των περιορισμών και του ρόλου σχεδιασμού τους στα δίκτυα IoT.
Συγκεκριμένα, περιλαμβάνονται οι ακόλουθες ενότητες:

Αισθητήρες, ενεργοποιητές και έξυπνα αντικείμενα (Sensors, Actuators, and Smart Objects): Αυτή η ενότητα ορίζει τους αισθητήρες, τους ενεργοποιητές και τα έξυπνα αντικείμενα και περιγράφει πώς αποτελούν τα θεμελιώδη δομικά στοιχεία των δικτύων IoT.

Δίκτυα αισθητήρων (Sensor Networks): Αυτή η ενότητα καλύπτει το σχεδιασμό, τους οδηγούς για υιοθέτηση και τις προκλήσεις ανάπτυξης δικτύων αισθητήρων.

Κεφάλαιο 3.1 Αισθητήρες, ενεργοποιητές και έξυπνα αντικείμενα (Sensors, Actuators, and Smart Objects)

Τα ασύρματα δίκτυα αισθητήρων και ενεργοποιητών είναι μια μοναδική πλατφόρμα υπολογιστών που μπορεί να διανεμηθεί και να αναπτυχθεί σε μοναδικά περιβάλλοντα όπου τυπικά δεν υπάρχουν παραδοσιακές υπολογιστικές πλατφόρμες. Αυτό προσφέρει μοναδικά πλεονεκτήματα και ευκαιρίες για αλληλεπίδραση και επιρροή σε αυτά τα περιβάλλοντα.

Αυτό το κεφάλαιο αναφέρεταιι στα «πράγματα» που αποτελούν τα δομικά στοιχεία του IoT. Περιλαμβάνει περιγραφές και πρακτικά παραδείγματα αισθητήρων και πώς μπορούν να μετρήσουν το περιβάλλον τους. Παρέχει το ίδιο είδος συζήτησης για τους ενεργοποιητές, οι οποίοι χρησιμοποιούν περιβαλλοντικές πληροφορίες ανίχνευσης με συμπληρωματικό τρόπο για να δράσουν στο περιβάλλον τους.

Επίσης, υπογραμμίζει τις πρόσφατες τάσεις κατασκευής (όπως το MEMS) για την κατασκευή αισθητήρων και ενεργοποιητών όλο και μικρότερων και πιο ενσωματωμένων σε αντικείμενα καθημερινής χρήσης.Τέλος, αναφέρεται σε έξυπνα αντικείμενα, τα οποία είναι τυπικά συσκευές με υψηλούς περιορισμούς με αισθητήρες ή/και ενεργοποιητές, καθώς και πολύ περιορισμένη ισχύ, μετάδοση και υπολογισμό.

Κεφάλαιο 3.1.1 Αισθητήρες

Ένας αισθητήρας κάνει ακριβώς όπως δείχνει το όνομά του: Ανιχνεύει.
Πιο συγκεκριμένα, ένας αισθητήρας μετρά κάποια φυσική ποσότητα και μετατρέπει την ένδειξη μέτρησης σε ψηφιακή αναπαράσταση. Αυτή η ψηφιακή αναπαράσταση τυπικά μεταβιβάζεται σε άλλη συσκευή για μετατροπή σε χρήσιμα δεδομένα που μπορούν να επεξεργασθούν από ευφυείς συσκευές ή ανθρώπους. Οι αισθητήρες δεν περιορίζονται στα αισθητήρια δεδομένα που μοιάζουν με τον άνθρωπο.
Στην πραγματικότητα οι αισθητήρες:

- Είναι σε θέση να παρέχουν ένα εξαιρετικά ευρύ φάσμα πλούσιων και διαφορετικών δεδομένων μέτρησης με πολύ μεγαλύτερη ακρίβεια από τις ανθρώπινες αισθήσεις.

- Παρέχουν υπεράνθρωπες αισθητηριακές δυνατότητες. Αυτή η πρόσθετη διάσταση δεδομένων καθιστά τον φυσικό κόσμο μια απίστευτα πολύτιμη πηγή πληροφοριών.

- Μπορούν να ενσωματωθούν εύκολα σε οποιαδήποτε φυσικά αντικείμενα που συνδέονται εύκολα στο Διαδίκτυο μέσω ενσύρματων ή ασύρματων δικτύων.

Υπάρχουν μυριάδες διαφορετικοί αισθητήρες για να μετρήσουν σχεδόν τα πάντα στον φυσικό κόσμο. Επίσης υπάρχουν διάφοροι τρόποι ομαδοποίησης των αισθητήρων σε διαφορετικές κατηγορίες.
Συγκεκριμένα έχουμε αισθητήρες:

- Ενεργούς ή παθητικούς, με βάση το αν παράγουν ενέργεια και συνήθως απαιτούν εξωτερική τροφοδοσία (ενεργή) ή αν λαμβάνουν απλώς ενέργεια και τυπικά δεν απαιτούν εξωτερική τροφοδοσία (παθητική).

- Επεμβατικούς ή μη επεμβατικούς, με βάση το αν ένας αισθητήρας είναι μέρος του περιβάλλοντος που μετρά (επεμβατικός) ή εξωτερικός σε αυτόν (μη επεμβατικός).

- Επικοινωνίας ή μη επικοινωνίας, με βάση το εάν απαιτούν φυσική επαφή με αυτό που μετρούν (επαφή) ή όχι (μη-επαφή).

- Απόλυτους ή σχετικούς, με βάση το αν μετρούν σε απόλυτη κλίμακα (απόλυτη) ή βάσει διαφοράς με σταθερή ή μεταβλητή τιμή αναφοράς (σχετική).

- Περιοχής εφαρμογής, με βάση τη συγκεκριμένη βιομηχανία όπου χρησιμοποιούνται.

- Μέτρησης, με βάση τον φυσικό μηχανισμό που χρησιμοποιείται για τη μέτρηση της αισθητηριακής εισόδου (για παράδειγμα, θερμοηλεκτρικός, ηλεκτροχημικός, οπτικός, ηλεκτρικός, μηχανικός ρευστών, φωτοελαστικός). Συγκεκριμένα, δείχνουν τι μετρούν, με βάση τις εφαρμογές τους ή τις φυσικές μεταβλητές που μετρούν.

Στους Πίνακες 3 και 4, περιγράφεται μια απλή ταξινόμηση με βάση το φυσικό φαινόμενο που μετρά ένας αισθητήρας.

Sensor Types	Description	Examples
Position	A position sensor measures the position of an object; the position measurement can be either in absolute terms (absolute position sensor) or in relative terms (displacement sensor). Position sensors can be linear, angular, or multi-axis.	Potentiometer, inclinometer, proximity sensor
Occupancy and motion	Occupancy sensors detect the presence of people and animals in a surveillance area, while motion sensors detect movement of people and objects. The difference between the two is that occupancy sensors generate a signal even when a person is stationary, whereas motion sensors do not.	Electric eye, radar
Velocity and acceleration	Velocity (speed of motion) sensors may be linear or angular, indicating how fast an object moves along a straight line or how fast it rotates. Acceleration sensors measure changes in velocity.	Accelerometer, gyroscope
Force	Force sensors detect whether a physical force is applied and whether the magnitude of force is beyond a threshold.	Force gauge, viscometer, tactile sensor (touch sensor)
Pressure	Pressure sensors are related to force sensors, measuring force applied by liquids or gases. Pressure is measured in terms of force per unit area.	Barometer, Bourdon gauge, piezometer
Flow	Flow sensors detect the rate of fluid flow. They measure the volume (mass flow) or rate (flow velocity) of fluid that has passed through a system in a given period of time.	Anemometer, mass flow sensor, water meter

Πίνακας 3: Τύποι αισθητήρων.

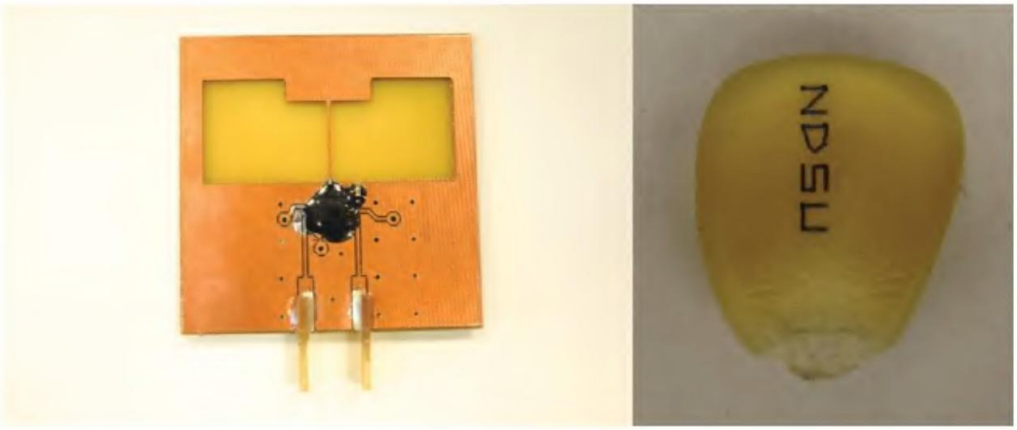
Acoustic	Acoustic sensors measure sound levels and convert that information into digital or analog data signals.	Microphone, geophone, hydrophone
Humidity	Humidity sensors detect humidity (amount of water vapor) in the air or a mass. Humidity levels can be measured in various ways: absolute humidity, relative humidity, mass ratio, and so on.	Hygrometer, humistor, soil moisture sensor
Light	Light sensors detect the presence of light (visible or invisible).	Infrared sensor, photodetector, flame detector
Radiation	Radiation sensors detect radiation in the environment. Radiation can be sensed by scintillating or ionization detection.	Geiger-Müller counter, scintillator, neutron detector
Temperature	Temperature sensors measure the amount of heat or cold that is present in a system. They can be broadly of two types: contact and non-contact. Contact temperature sensors need to be in physical contact with the object being sensed. Non-contact sensors do not need physical contact, as they measure temperature through convection and radiation.	Thermometer, calorimeter, temperature gauge
Chemical	Chemical sensors measure the concentration of chemicals in a system. When subjected to a mix of chemicals, chemical sensors are typically selective for a target type of chemical (for example, a CO_2 sensor senses only carbon dioxide).	Breathalyzer, olfactometer, smoke detector
Biosensors	Biosensors detect various biological elements, such as organisms, tissues, cells, enzymes, antibodies, and nucleic acid.	Blood glucose biosensor, pulse oximetry, electrocardiograph

Πίνακας 4: Τύποι αισθητήρων.

Οι αισθητήρες έρχονται σε όλα τα σχήματα και μεγέθη και, όπως φαίνεται στους Πίνακες 3 και 4 μπορεί να μετρήσει όλους τους τύπους φυσικών συνθηκών.
Μια συναρπαστική περίπτωση χρήσης για την ανάδειξη της ισχύος των αισθητήρων και του IoT είναι στον τομέα της γεωργίας (precision agriculture), η οποία χρησιμοποιεί μια ποικιλία τεχνικών προόδων για τη βελτίωση της αποδοτικότητας, της βιωσιμότητας και της κερδοφορίας των παραδοσιακών γεωργικών πρακτικών.
Αυτό περιλαμβάνει τη χρήση GPS και δορυφορικών αεροφωτογραφιών για τον προσδιορισμό της βιωσιμότητας του πεδίου. ρομπότ για φύτευση υψηλής ακρίβειας, συγκομιδή, άρδευση κ.ο.κ. και ανάλυση σε πραγματικό χρόνο και τεχνητή νοημοσύνη για να προβλέψουν τη βέλτιστη απόδοση των καλλιεργειών, τις καιρικές επιπτώσεις και την ποιότητα του εδάφους. Μεταξύ των σημαντικότερων επιπτώσεων της γεωργίας ακριβείας (precision agriculture), είναι αυτές που ασχολούνται με τη μέτρηση αισθητήρων μιας ποικιλίας χαρακτηριστικών του εδάφους.

Αυτές περιλαμβάνουν τη μέτρηση της ποιότητας του εδάφους σε πραγματικό χρόνο, τα επίπεδα pH, την αλατότητα, τα επίπεδα τοξικότητας, τα επίπεδα υγρασίας για τον προγραμματισμό της άρδευσης, τα επίπεδα θρεπτικών συστατικών για τον προγραμματισμό της λίπανσης κ.ο.κ. Όλα αυτά τα λεπτομερή δεδομένα αισθητήρων μπορούν να αναλυθούν για να παρέχουν πολύτιμη και αποτελεσματική εικόνα για να αυξήσουν την παραγωγικότητα και την απόδοση των καλλιεργειών.

Το Σχήμα 20 δείχνει βίο-αποικοδομήσιμους, παθητικούς μικροαισθητήρες για τη μέτρηση του εδάφους και της καλλιέργειας και των συνθηκών.

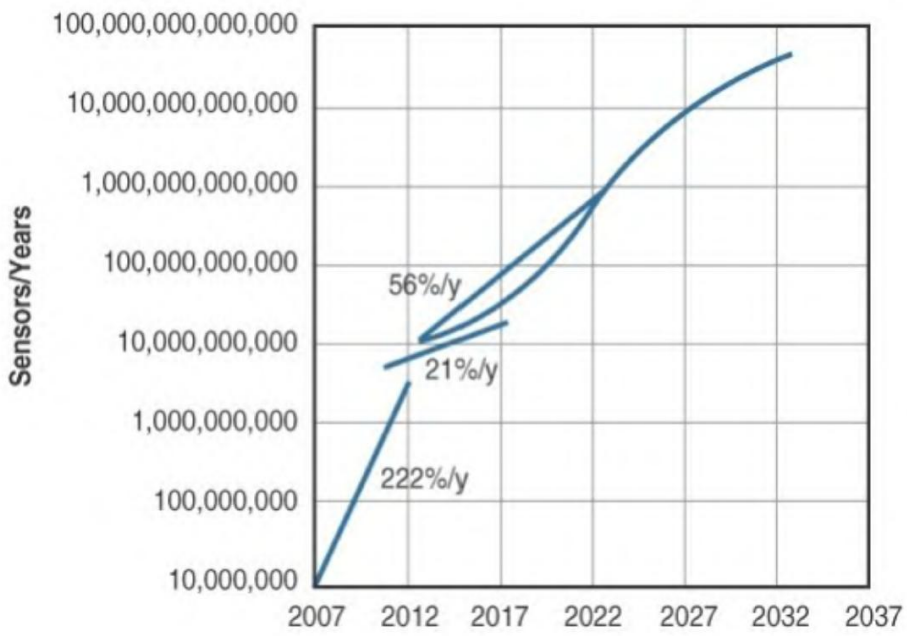


Σχήμα 20: Βίο-διασπώμενοι αισθητήρες που αναπτύχθηκαν από την NDSU για έξυπνη καλλιέργεια.

Ο εκπληκτικός όγκος των αισθητήρων οφείλεται σε μεγάλο βαθμό στο μικρότερο μέγεθος, τον παράγοντα μορφής τους και το μειωμένο κόστος τους. Αυτοί οι παράγοντες καθιστούν δυνατή την οικονομική και τεχνική σκοπιμότητα της ύπαρξης αυξημένης πυκνότητας αισθητήρων σε αντικείμενα όλων των τύπων. Ίσως ο πιο σημαντικός επιταχυντής για την ανάπτυξη αισθητήρων είναι τα κινητά τηλέφωνα. Πάνω από ένα δισεκατομμύριο έξυπνα τηλέφωνα πωλούνται κάθε χρόνο και το καθένα έχει πάνω από δώδεκα αισθητήρες μέσα του (Σχήμα 21) και ο αριθμός αυτός συνεχίζει να αυξάνεται κάθε χρόνο.

Σχήμα 21: Αισθητήρες σε ένα έξυπνο τηλέφωνο.

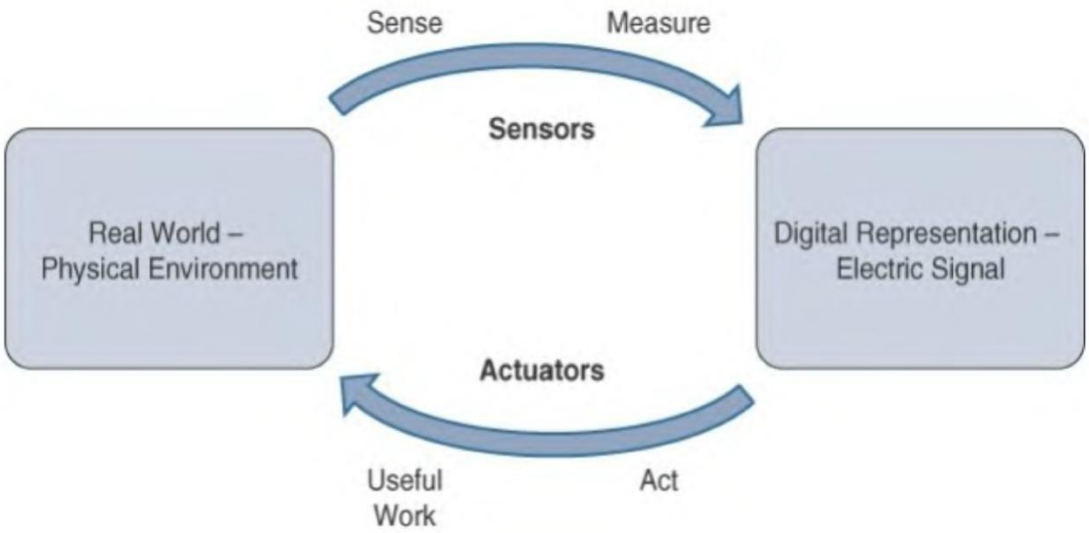
Το Σχήμα 22 δείχνει την εκρηκτική αύξηση από έτος σε έτος τα τελευταία χρόνια και μερικές προβλέψεις για τους αριθμούς αισθητήρων τα επόμενα χρόνια. Υπάρχει ισχυρή πεποίθηση στη βιομηχανία αισθητήρων ότι αυτός ο αριθμός θα εκλείψει ένα τρισεκατομμύριο τα επόμενα χρόνια.



Σχήμα 22: Ανάπτυξη και προβλέψεις στον αριθμό των αισθητήρων.

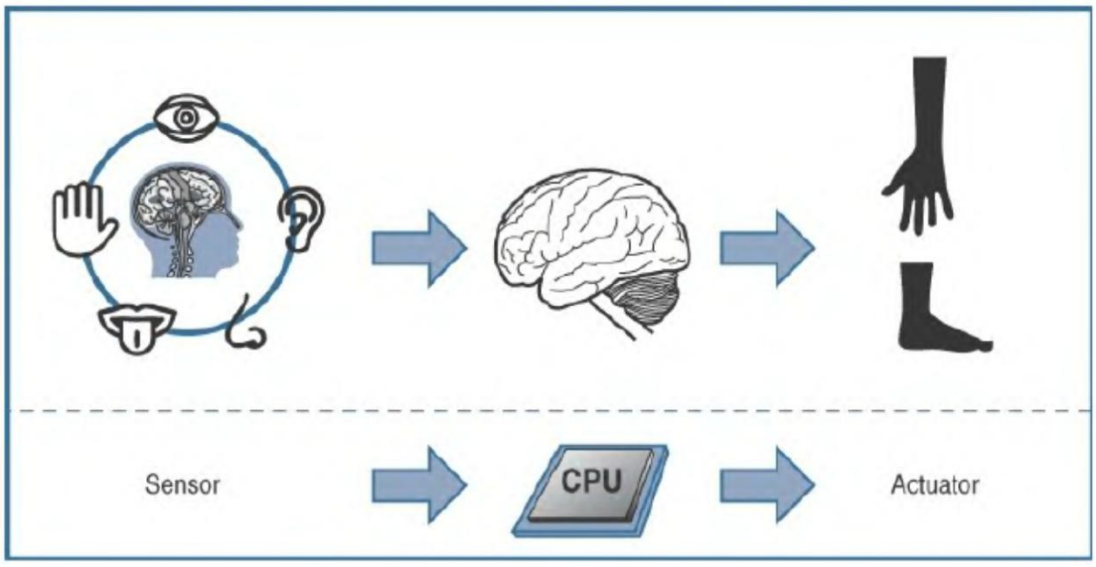
Κεφάλαιο 3.1.2 Ενεργοποιητές (Actuators)

Οι ενεργοποιητές (Sensors),είναι φυσικά συμπληρώματα αισθητήρων. Το Σχήμα 23 καταδεικνύει τη συμμετρία και τη συμπληρωματική φύση αυτών των δύο τύπων συσκευών. Όπως έχουμε αναφέρει, οι αισθητήρες έχουν σχεδιαστεί για να ανιχνεύουν και να μετρούν σχεδόν κάθε μετρήσιμη μεταβλητή στον φυσικό κόσμο. Μετατρέπουν τις μετρήσεις τους (συνήθως αναλογικές) σε ηλεκτρικά σήματα ή ψηφιακές αναπαραστάσεις που μπορούν να καταναλωθούν από έναν ευφυή παράγοντα (μια συσκευή ή έναν άνθρωπο).
Από την άλλη πλευρά, οι ενεργοποιητές, λαμβάνουν κάποιο είδος σήματος ελέγχου (συνήθως ηλεκτρικό σήμα ή ψηφιακή εντολή) που προκαλεί ένα φυσικό αποτέλεσμα, συνήθως κάποιο είδος κίνησης, δύναμης κ.ο.κ.



Σχήμα 23: Αλληλεπίδραση αισθητήρων και ενεργοποιητών με τον φυσικό κόσμο.

Όπως φαίνεται και στο Σχήμα 24, οι άνθρωποι χρησιμοποιούν τις πέντε αισθήσεις τους για να αντιληφθούν και να μετρήσουν το περιβάλλον τους. Τα αισθητήρια όργανα μετατρέπουν αυτές τις αισθητηριακές πληροφορίες σε «ηλεκτρικές παρορμήσεις» που το νευρικό σύστημα στέλνει στον εγκέφαλο για επεξεργασία.
Ομοίως, οι αισθητήρες IoT είναι συσκευές που ανιχνεύουν και μετρούν τον φυσικό κόσμο και (τυπικά) σηματοδοτούν τις μετρήσεις τους ως ηλεκτρικά σήματα που αποστέλλονται σε κάποιον τύπο μικροεπεξεργαστή ή μικροελεγκτή για πρόσθετη επεξεργασία.
Ο ανθρώπινος εγκέφαλος σηματοδοτεί τη λειτουργία και την κίνηση του κινητήρα και το νευρικό σύστημα μεταφέρει αυτές τις πληροφορίες στο κατάλληλο τμήμα του μυϊκού συστήματος.



Σχήμα 24: Σύγκριση λειτουργικότητας αισθητήρα και ενεργοποιητή με ανθρώπους.

Αντίστοιχα, ένας επεξεργαστής μπορεί να στείλει ένα ηλεκτρικό σήμα σε έναν ενεργοποιητή που μεταφράζει το σήμα σε κάποιο είδος κίνησης (γραμμική, περιστροφική κ.λπ.)

Αυτή η αλληλεπίδραση μεταξύ αισθητήρων, ενεργοποιητών και επεξεργαστών και η παρόμοια λειτουργικότητα στα βιολογικά συστήματα αποτελεί τη βάση για διάφορα τεχνικά πεδία, συμπεριλαμβανομένης της ρομποτικής και της βιομετρίας.

Οι ενεργοποιητές διαφέρουν πολύ στη λειτουργία, το μέγεθος, το σχέδιο κ.λπ. Μερικοί συνηθισμένοι τρόποι ταξινόμησης των ενεργοποιητών γίνεται με βάση:

- Τον τύπο κίνησης, που παράγουν για παράδειγμα, γραμμικοί, περιστροφικοί, ένας/δύο/τρεις άξονες.
- Την ισχύ εξόδου τους, για παράδειγμα, υψηλή ισχύς, χαμηλή ισχύς, μικρή ισχύς.
- Τον αριθμό των εξόδων - δυαδικό ή συνεχές - σταθερής κατάστασης.
- Την περιοχή εφαρμογής**,** όπου χρησιμοποιούνται.
- Το είδος-τύπο της ενέργειας τους.

Ο Πίνακας 5, δείχνει τους ενεργοποιητές που ταξινομούνται ανά τύπο ενέργειας και μερικά παραδείγματα για κάθε τύπο.

Type	Examples
Mechanical actuators	Lever, screw jack, hand crank
Electrical actuators	Thyristor, biopolar transistor, diode
Electromechanical actuators	AC motor, DC motor, step motor
Electromagnetic actuators	Electromagnet, linear solenoid
Hydraulic and pneumatic actuators	Hydraulic cylinder, pneumatic cylinder, piston, pressure control valves, air motors
Smart material actuators (includes thermal and magnetic actuators)	Shape memory alloy (SMA), ion exchange fluid, magnetorestrictive material, bimetallic strip, piezoelectric bimorph
Micro- and nanoactuators	Electrostatic motor, microvalve, comb drive

Πίνακας 5: Ταξινόμηση ενεργοποιητή κατά τον τύπο ενέργειας.

Οι πιο ενδιαφέρουσες περιπτώσεις χρήσης για το IoT είναι εκείνες όπου οι αισθητήρες και οι ενεργοποιητές συνεργάζονται με έξυπνο και συμπληρωματικό τρόπο. Αυτός ο ισχυρός συνδυασμός μπορεί να χρησιμοποιηθεί για την επίλυση καθημερινών προβλημάτων.
Με βάση το προηγούμενο παράδειγμα στο τομέα της γεωργίας (precision agriculture) από τη προηγούμενη ενότητα μπορούμε να δείξουμε πώς οι ενεργοποιητές μπορούν να συμπληρώσουν και να ενισχύσουν μια λύση μόνο για αισθητήρες.
Συγκεκριμένα, οι έξυπνοι αισθητήρες που χρησιμοποιούνται για την αξιολόγηση της ποιότητας του εδάφους (μετρώντας μια ποικιλία εδαφών, θερμοκρασίας και χαρακτηριστικών των φυτών) μπορούν να συνδεθούν με ηλεκτρικά ελεγχόμενους ενεργοποιητές βαλβίδων που ελέγχουν νερό, φυτοφάρμακα, λιπάσματα, ζιζανιοκτόνα κ.ο.κ.
Η έξυπνη ενεργοποίηση ενός ενεργοποιητή υψηλής ακρίβειας που βασίζεται σε καλά καθορισμένες ενδείξεις αισθητήρων για τη θερμοκρασία, το pH, την υγρασία του εδάφους/αέρα, τα επίπεδα θρεπτικών συστατικών κ.λπ., για την παροχή μιας εξαιρετικά

βελτιστοποιημένης και προσαρμοσμένης στο περιβάλλον λύσης είναι μια πραγματικά έξυπνη καλλιέργεια (precision agriculture).

Κεφάλαιο 3.1.3 Μικροηλεκτρομηχανικά συστήματα (Micro-Electro-Mechanical Systems MEMS)

Τα μικροηλεκτρομηχανικά συστήματα (MEMS) ή μικρομηχανές, μπορούν να ενσωματώσουν και να συνδυάσουν ηλεκτρικά και μηχανικά στοιχεία, όπως αισθητήρες και ενεργοποιητές, σε πολύ μικρή κλίμακα (χιλιοστών ή λιγότερο). Ένα από τα κλειδιά αυτής της τεχνολογίας είναι μια τεχνική μικροκατασκευής που είναι παρόμοια με αυτήν που χρησιμοποιείται για μικροηλεκτρονικά ολοκληρωμένα κυκλώματα. Αυτή η προσέγγιση επιτρέπει τη μαζική παραγωγή με πολύ χαμηλό κόστος. Οι συσκευές MEMS έχουν ήδη χρησιμοποιηθεί ευρέως σε μια ποικιλία διαφορετικών εφαρμογών και μπορούν να βρεθούν σε πολύ οικείες καθημερινές συσκευές. Για παράδειγμα, τα έξυπνα τηλέφωνα χρησιμοποιούν τεχνολογίες MEMS για πράγματα όπως επιταχυνσιόμετρα και γυροσκόπια.

Κεφάλαιο 3.1.4 Έξυπνα Αντικείμενα (Smart Objects)

Έξυπνα αντικείμενα, είναι αυτά που μετατρέπουν τα καθημερινά αντικείμενα σε ένα δίκτυο ευφυών αντικειμένων που είναι σε θέση να μάθουν και να αλληλεπιδράσουν με το περιβάλλον τους με ουσιαστικό τρόπο.
Ένα έξυπνο αντικείμενο, είναι μια συσκευή που έχει, τουλάχιστον, τα ακόλουθα τέσσερα καθοριστικά χαρακτηριστικά (Σχήμα 25).

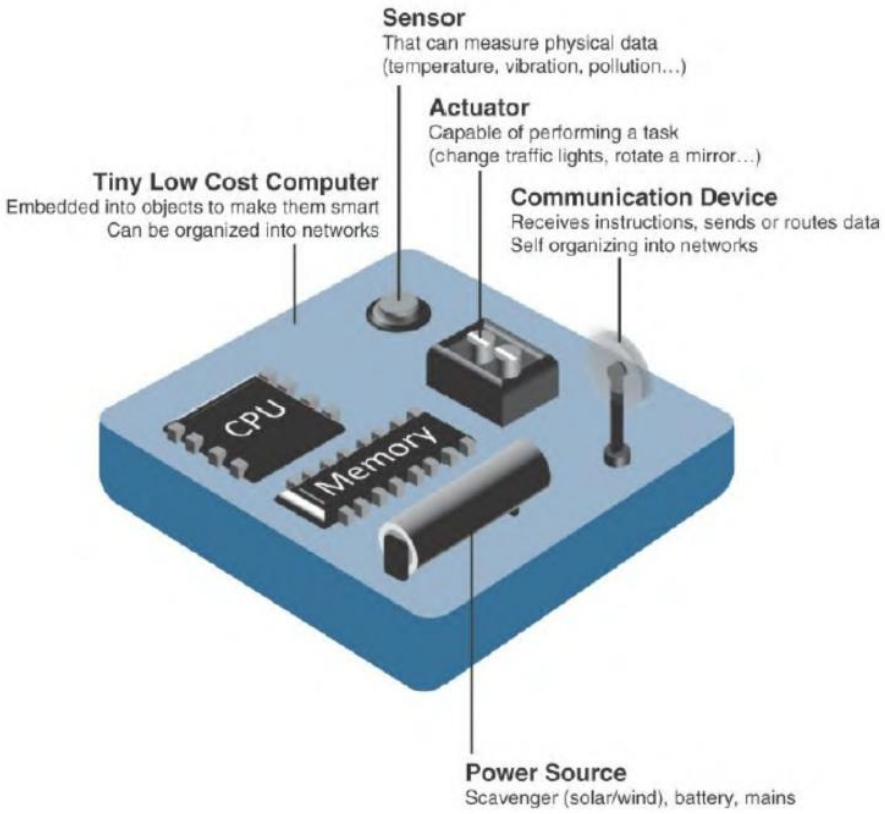
1. Μονάδα επεξεργασίας: Ένα έξυπνο αντικείμενο έχει κάποιο τύπο μονάδας επεξεργασίας για την απόκτηση δεδομένων, την επεξεργασία και την ανάλυση πληροφοριών ανίχνευσης που λαμβάνει ο αισθητήρας, τον συντονισμό των σημάτων ελέγχου σε οποιονδήποτε ενεργοποιητή και τον έλεγχο μιας ποικιλίας λειτουργιών στο έξυπνο αντικείμενο, συμπεριλαμβανομένων των συστημάτων επικοινωνίας και ισχύος. Ο πιο συνηθισμένος είναι ένας μικροελεγκτής λόγω του μικρού συντελεστή μορφής του, της ευελιξίας, της απλότητας προγραμματισμού, της πανταχού παρουσίας, της χαμηλής κατανάλωσης ενέργειας και του χαμηλού κόστους.

2. Αισθητήρας ή/και ενεργοποιητής: Ένα έξυπνο αντικείμενο είναι ικανό να αλληλεπιδρά με τον φυσικό κόσμο μέσω αισθητήρων και ενεργοποιητών. Στην πραγματικότητα, ένα έξυπνο αντικείμενο μπορεί να περιέχει έναν ή πολλούς αισθητήρες και/ή ενεργοποιητές, ανάλογα με την εφαρμογή.

3. Συσκευή επικοινωνίας: Η μονάδα επικοινωνίας είναι υπεύθυνη για τη σύνδεση ενός έξυπνου αντικειμένου με άλλα έξυπνα αντικείμενα και τον έξω κόσμο (μέσω του δικτύου). Οι συσκευές επικοινωνίας για έξυπνα αντικείμενα μπορούν να είναι είτε ενσύρματες είτε ασύρματες. Συντριπτικά, στα δίκτυα IoT, τα έξυπνα αντικείμενα συνδέονται ασύρματα για διάφορους λόγους, συμπεριλαμβανομένου του κόστους, της περιορισμένης διαθεσιμότητας υποδομής και της ευκολίας ανάπτυξης.

4. Πηγή ενέργειας: Τα έξυπνα αντικείμενα έχουν στοιχεία που πρέπει να τροφοδοτούνται. Συνήθως, τα έξυπνα αντικείμενα είναι περιορισμένης ισχύος, αναπτύσσονται για πολύ μεγάλο χρονικό διάστημα και δεν είναι εύκολα

προσβάσιμα. Αυτός ο συνδυασμός, ειδικά όταν το έξυπνο αντικείμενο βασίζεται στην ισχύ της μπαταρίας, υποδηλώνει ότι η αποδοτικότητα ισχύος, η συνετή διαχείριση ισχύος, οι λειτουργίες ύπνου, το υλικό εξαιρετικά χαμηλής κατανάλωσης ενέργειας και ούτω καθεξής είναι κρίσιμα στοιχεία σχεδιασμού.



Σχήμα 25: Χαρακτηριστικά ενός έξυπνου αντικειμένου.

Κεφάλαιο 3.2 Δίκτυα αισθητήρων (Sensor Networks)

Ένα δίκτυο αισθητήρων/ενεργοποιητών (Sensor Networks SANET), όπως υποδηλώνει το όνομα, είναι ένα δίκτυο αισθητήρων που ανιχνεύουν και μετρούν το περιβάλλον τους και/ή ενεργοποιητές που δρουν στο περιβάλλον τους. Τα SANET προσφέρουν εξαιρετικά συντονισμένες δυνατότητες ανίχνευσης και ενεργοποίησης. Τα έξυπνα σπίτια είναι ένας τύπος SANET που εμφανίζουν αυτόν τον συντονισμό μεταξύ κατανεμημένων αισθητήρων και ενεργοποιητών. Για παράδειγμα, τα έξυπνα σπίτια μπορούν να έχουν αισθητήρες θερμοκρασίας που είναι δικτυωμένοι με ενεργοποιητές θέρμανσης, εξαερισμού και κλιματισμού (HVAC). Όταν ένας αισθητήρας ανιχνεύσει μια καθορισμένη θερμοκρασία, αυτό μπορεί να ενεργοποιήσει έναν ενεργοποιητή να αναλάβει δράση και να θερμάνει ή να δροσίσει το σπίτι όπως απαιτείται. Τέτοια δίκτυα μπορούν θεωρητικά να συνδεθούν με ενσύρματο ή ασύρματο τρόπο.

Πλεονεκτήματα και μειονεκτήματα που προσφέρει μια ασύρματη λύση:

Πλεονεκτήματα:

- Μεγαλύτερη ευελιξία ανάπτυξης (ειδικά σε ακραία περιβάλλοντα ή δυσπρόσιτα μέρη).
- Απλούστερη κλιμάκωση σε μεγάλο αριθμό κόμβων.
- Χαμηλότερο κόστος υλοποίησης.
- Ευκολότερη μακροχρόνια συντήρηση.
- Αβίαστη εισαγωγή νέων κόμβων αισθητήρα/ενεργοποιητή.
- Καλύτερα εξοπλισμένος για να χειρίζεται δυναμικές/γρήγορες αλλαγές τοπολογίας

Μειονεκτήματα:

- Δυνητικά λιγότερο ασφαλής (για παράδειγμα, παραβιασμένα σημεία πρόσβασης).
- Χαμηλότερες ταχύτητες μετάδοσης.
- Μεγαλύτερο επίπεδο επιπτώσεων/επιρροής από το περιβάλλον.

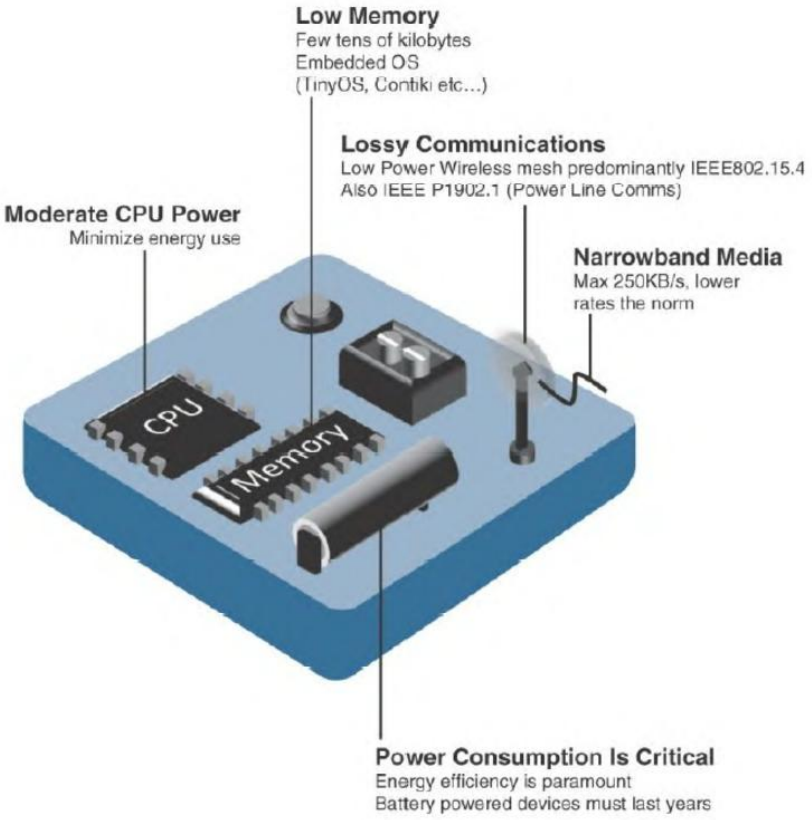
Όχι μόνο το ασύρματο επιτρέπει πολύ μεγαλύτερη ευελιξία, αλλά είναι επίσης μια ολοένα και πιο φθηνή και αξιόπιστη τεχνολογία σε ένα ευρύ φάσμα συνθηκών - ακόμη και εξαιρετικά σκληρών.Αυτά τα χαρακτηριστικά είναι ο βασικός λόγος που τα ασύρματα SANET είναι η πανταχού παρούσα τεχνολογία δικτύωσης για το IoT.

Κεφάλαιο 3.2.1 Ασύρματα δίκτυα αισθητήρων (Wireless Sensor Networks WSNs)

Τα ασύρματα δίκτυα αισθητήρων αποτελούνται από ασύρματα συνδεδεμένα έξυπνα αντικείμενα, τα οποία μερικές φορές αναφέρονται ως **motes**. Το Σχήμα 26 απεικονίζει ορισμένες από αυτές τις υποθέσεις και τους περιορισμούς που συνήθως εμπλέκονται σε WSNs.
Οι παρακάτω είναι μερικοί από τους πιο σημαντικούς περιορισμούς των έξυπνων αντικειμένων στα WSNs:

- Περιορισμένη ισχύ επεξεργασίας.
- Περιορισμένη μνήμη.
- Χαμένη επικοινωνία.
- Περιορισμένες ταχύτητες μετάδοσης.
- Περιορισμένη ισχύς.

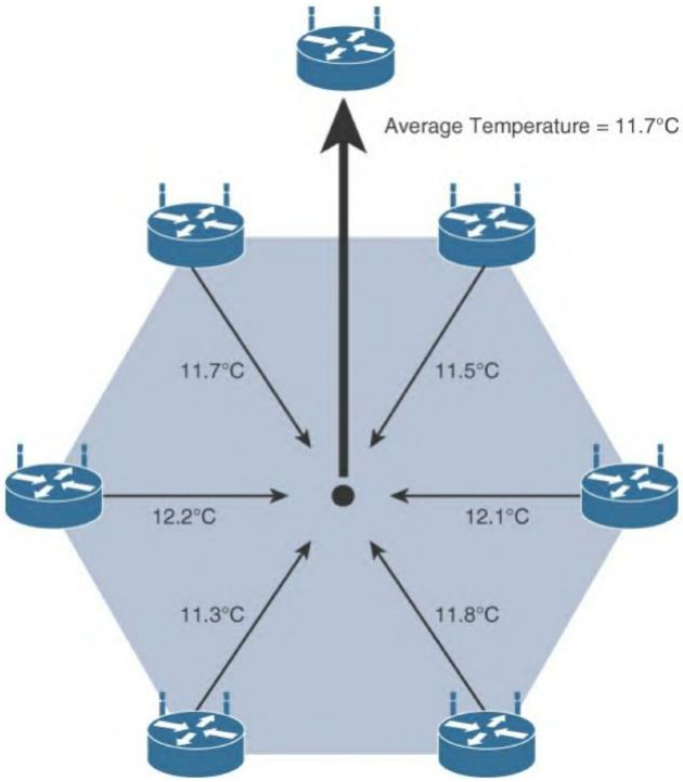
Αυτοί οι περιορισμοί επηρεάζουν σημαντικά τον τρόπο σχεδιασμού, ανάπτυξης και χρήσης των WSNs.



Σχήμα 26: Περιορισμοί σχεδιασμού για ασύρματα έξυπνα αντικείμενα.

Το γεγονός ότι οι μεμονωμένοι κόμβοι αισθητήρων είναι συνήθως τόσο περιορισμένοι είναι ένας λόγος που συχνά αναπτύσσονται σε πολύ μεγάλους αριθμούς. Καθώς το κόστος των κόμβων αισθητήρων συνεχίζει να μειώνεται, η δυνατότητα ανάπτυξης πολύ περιττών αισθητήρων καθίσταται ολοένα και πιο εφικτή. Επειδή πολλοί αισθητήρες είναι πολύ φθηνοί και αντιστοίχως ανακριβείς, η δυνατότητα ανάπτυξης έξυπνων αντικειμένων σε πλεονασμό επιτρέπει αυξημένη ακρίβεια.
Τέτοιος μεγάλος αριθμός αισθητήρων επιτρέπει την εισαγωγή ιεραρχιών έξυπνων αντικειμένων. Μια τέτοια ιεραρχία παρέχει, μεταξύ άλλων οργανωτικών πλεονεκτημάτων, τη δυνατότητα συγκέντρωσης παρόμοιων μετρήσεων αισθητήρων από κόμβους αισθητήρων που βρίσκονται σε κοντινή απόσταση μεταξύ τους.

Το Σχήμα 27 δείχνει ένα παράδειγμα μιας τέτοιας συνάρτησης συγκέντρωσης δεδομένων σε ένα WSNs όπου οι ενδείξεις θερμοκρασίας από μια λογική ομάδα αισθητήρων θερμοκρασίας συγκεντρώνονται ως μέση ένδειξη θερμοκρασίας.



Σχήμα 27: Συγκέντρωση δεδομένων σε ασύρματα δίκτυα αισθητήρων.

Κεφάλαιο 3.2.2 Πρωτόκολλα επικοινωνίας για ασύρματα δίκτυα αισθητήρων

Υπάρχουν χιλιάδες διαφορετικοί τύποι αισθητήρων και ενεργοποιητών. Τα WSNs εξελίσσονται επίσης από δίκτυα μίας χρήσης σε πιο ευέλικτα δίκτυα πολλαπλών χρήσεων που μπορούν να χρησιμοποιούν συγκεκριμένους τύπους αισθητήρων για πολλές διαφορετικές εφαρμογές ανά πάσα στιγμή.

Τα πρωτόκολλα που διέπουν την επικοινωνία για WSNs πρέπει να ασχολούνται με τα εγγενή καθοριστικά χαρακτηριστικά των WSNs και τις περιορισμένες συσκευές μέσα σε αυτά. Το γεγονός ότι τα WSNs αναπτύσσονται συχνά σε εξωτερικούς χώρους σε απρόβλεπτα περιβάλλοντα προσθέτει ακόμη μια μεταβλητή που πρέπει να ληφθεί υπόψη, επειδή προφανώς δεν έχουν σχεδιαστεί όλα τα πρωτόκολλα επικοινωνίας για να είναι εξίσου αποτελεσματικά.

Τα ασύρματα δίκτυα αισθητήρων αλληλεπιδρούν με το περιβάλλον τους. Οι αισθητήρες συχνά παράγουν μεγάλες ποσότητες δεδομένων ανίχνευσης και μέτρησης που πρέπει να υποβληθούν σε επεξεργασία. Αυτά τα δεδομένα μπορούν να επεξεργαστούν τοπικά από τους κόμβους ενός WSNs ή σε μηδενικά ή περισσότερα ιεραρχικά επίπεδα σε δίκτυα IoT.

Τελικά, χρησιμοποιούνται για να παρέχουν μια πλατφόρμα για μια ποικιλία έξυπνων υπηρεσιών IoT. Όπως συμβαίνει με οποιαδήποτε άλλη εφαρμογή δικτύωσης, έτσι ώστε να λειτουργούν σε περιβάλλοντα πολλαπλών τύπων, αυτά τα πρωτόκολλα επικοινωνίας πρέπει να είναι τυποποιημένα. Αυτή είναι μια κρίσιμη εξάρτηση για το IoT και ένας από τους σημαντικότερους παράγοντες επιτυχίας.

Το IoT είναι μια από αυτές τις σπάνιες τεχνολογίες που επηρεάζει όλες τις κάθετες και βιομηχανίες, πράγμα που σημαίνει ότι η τυποποίηση των πρωτοκόλλων επικοινωνίας είναι μια περίπλοκη εργασία, που απαιτεί ορισμό πρωτοκόλλου σε πολλά επίπεδα της στοίβας, καθώς και μεγάλο συντονισμό μεταξύ πολλών οργανισμών ανάπτυξης προτύπων.

Κεφάλαιο 4 Σύνδεση έξυπνων αντικειμένων

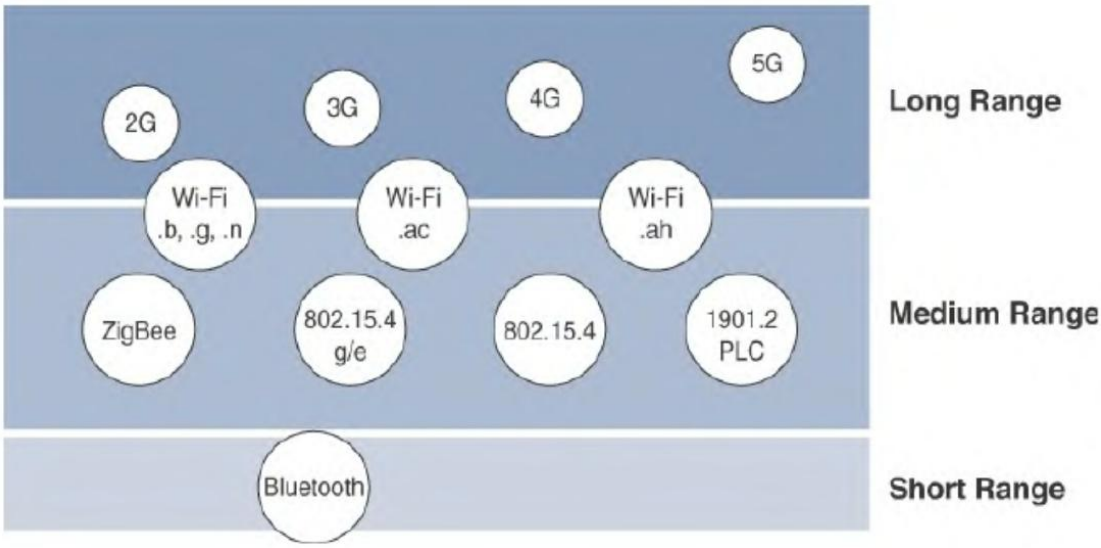
Η ασύρματη επικοινωνία επικρατεί στον κόσμο της σύνδεσης έξυπνων αντικειμένων, κυρίως επειδή διευκολύνει την ανάπτυξη και επιτρέπει στα έξυπνα αντικείμενα να είναι κινητά, αλλάζοντας τοποθεσία χωρίς να χάνεται η συνδεσιμότητα. Οι συσκευές και οι αισθητήρες IoT πρέπει να είναι συνδεδεμένοι στο δίκτυο για να χρησιμοποιηθούν τα δεδομένα τους. Εκτός από το ευρύ φάσμα αισθητήρων, ενεργοποιητών και έξυπνων αντικειμένων που αποτελούν το IoT, υπάρχουν επίσης πολλά διαφορετικά πρωτόκολλα που χρησιμοποιούνται για τη σύνδεσή τους. Οι διάφορες τεχνολογίες που χρησιμοποιούνται για τη σύνδεση αισθητήρων μπορεί να διαφέρουν σημαντικά ανάλογα με τα κριτήρια που χρησιμοποιούνται για την ανάλυσή τους.

Αυτό το κεφάλαιο ρίχνει μια ματιά στα χαρακτηριστικά και τα κριτήρια επικοινωνίας που είναι σημαντικά για τις τεχνολογίες που χρησιμοποιούν τα έξυπνα αντικείμενα για τη συνδεσιμότητά τους, καθώς και μια βαθύτερη εμβάθυνση σε μερικές από τις σημαντικότερες τεχνολογίες που αναπτύσσονται σήμερα. Τέλος γίνεται αναφορά στα πρωτόκολλα εφαρμογής για IoT.

Κεφάλαιο 4.1 Χαρακτηριστικά και Κριτήρια Επικοινωνίας

1.Εύρος(Range)

Η κατηγοριοποίηση τεχνολογιών ενσύρματης και ασύρματης πρόσβασης φαίνεται στο Σχήμα 28.



Σχήμα 28: Τοπίο ασύρματης πρόσβασης.

Μικρή εμβέλεια (Short range): Οι ασύρματες τεχνολογίες μικρής εμβέλειας θεωρούνται συχνά ως εναλλακτική λύση σε σειριακό καλώδιο, υποστηρίζοντας δεκάδες μέτρα μέγιστης απόστασης μεταξύ δύο συσκευών. Αυτές οι μέθοδοι επικοινωνίας μικρής εμβέλειας βρίσκονται μόνο σε μια μειοψηφία εγκαταστάσεων IoT.

Μεσαίο εύρος (Medium range): Αυτό το εύρος είναι η κύρια κατηγορία τεχνολογιών πρόσβασης IoT. Στην περιοχή των δεκάδων έως εκατοντάδων μέτρων, είναι διαθέσιμες πολλές προδιαγραφές και εφαρμογές. Η μέγιστη απόσταση είναι γενικά μικρότερη από 1

μίλι μεταξύ δύο συσκευών, αν και οι τεχνολογίες ραδιοσυχνοτήτων δεν έχουν καθορισμένες πραγματικές μέγιστες αποστάσεις, εφόσον το ραδιοφωνικό σήμα μεταδίδεται και λαμβάνεται στο πλαίσιο της ισχύουσας προδιαγραφής.

Μεγάλη εμβέλεια (Long range): Οι αποστάσεις μεγαλύτερες από 1 μίλι μεταξύ δύο συσκευών απαιτούν τεχνολογίες μεγάλης εμβέλειας. Ασύρματα παραδείγματα είναι τα 2G, 3G, 4G και ορισμένες εφαρμογές υπαίθριων τεχνολογιών IEEE 802.11 Wi-Fi και Low-Power Wide-Area (LPWA).

2. Ζώνες συχνοτήτων (Frequency Bands)

Το ραδιοφάσμα ρυθμίζεται από χώρες ή/και οργανισμούς, όπως η Διεθνής Ένωση Τηλεπικοινωνιών (International Telecommunication Union ITU) και η Ομοσπονδιακή Επιτροπή Επικοινωνιών (Federal Communications Commission FCC). Αυτές οι ομάδες καθορίζουν τους κανονισμούς και τις απαιτήσεις μετάδοσης για διάφορες ζώνες συχνοτήτων. Εστιάζοντας στις τεχνολογίες πρόσβασης IoT, οι ζώνες συχνοτήτων που αξιοποιούνται από ασύρματες επικοινωνίες κατανέμονται μεταξύ αδειοδοτημένων και μη αδειοδοτημένων ζωνών.

Το φάσμα αδειών ισχύει γενικά για τεχνολογίες **μεγάλης εμβέλειας** IoT και κατανέμεται σε υποδομές επικοινωνιών που αναπτύσσονται από παρόχους υπηρεσιών, δημόσιες υπηρεσίες (για παράδειγμα, πρώτοι ανταποκριτές, στρατιωτικοί), ραδιοτηλεοπτικοί φορείς και υπηρεσίες κοινής ωφέλειας. Ένα σημαντικό στοιχείο για τις υποδομές πρόσβασης IoT που επιθυμούν να χρησιμοποιήσουν άδεια φάσματος είναι ότι οι χρήστες πρέπει να εγγραφούν σε υπηρεσίες όταν συνδέουν τις συσκευές τους IoT. Αυτό προσθέτει περισσότερη πολυπλοκότητα σε μια ανάπτυξη που περιλαμβάνει μεγάλο αριθμό αισθητήρων και άλλων συσκευών IoT, αλλά σε αντάλλαγμα για το τέλος συνδρομής, ο διαχειριστής δικτύου μπορεί να εγγυηθεί την αποκλειστικότητα της χρήσης συχνότητας στην περιοχή -στόχο και ως εκ τούτου μπορεί να πουλήσει μια καλύτερη εγγύηση υπηρεσίας.
Η ITU έχει επίσης ορίσει φάσμα χωρίς άδεια για τα βιομηχανικά, επιστημονικά και ιατρικά (ISM) τμήματα των ραδιοσυχνοτήτων.Αυτές οι συχνότητες χρησιμοποιούνται σε πολλές τεχνολογίες επικοινωνιών για συσκευές **μικρής εμβέλειας** (Short-Range Devices SRDs).

3. Κατανάλωση ενέργειας (Power Consumption)

Ενώ ο ορισμός της συσκευής IoT είναι πολύ ευρύς, υπάρχει μια σαφής οριοθέτηση μεταξύ τροφοδοτούμενων κόμβων και κόμβων με μπαταρία. Ένας τροφοδοτούμενος κόμβος έχει άμεση σύνδεση με μια πηγή ενέργειας και οι επικοινωνίες συνήθως δεν περιορίζονται από κριτήρια κατανάλωσης ενέργειας. Ωστόσο, η ευκολία ανάπτυξης των τροφοδοτούμενων κόμβων περιορίζεται από τη διαθεσιμότητα μιας πηγής ενέργειας, γεγονός που καθιστά την κινητικότητα πιο περίπλοκη.
Οι κόμβοι που λειτουργούν με μπαταρία προσφέρουν πολύ μεγαλύτερη ευελιξία στις συσκευές IoT. Αυτοί οι κόμβοι συχνά ταξινομούνται με την απαιτούμενη διάρκεια ζωής των μπαταριών τους. Οι τεχνολογίες ασύρματης πρόσβασης IoT πρέπει να καλύπτουν τις ανάγκες χαμηλής κατανάλωσης ενέργειας και συνδεσιμότητας για κόμβους με μπαταρία.
Αυτό οδήγησε στην εξέλιξη ενός νέου ασύρματου περιβάλλοντος γνωστού ως **Low-Power Wide-Area (LPWA).**

4. Τοπολογία (Topology)

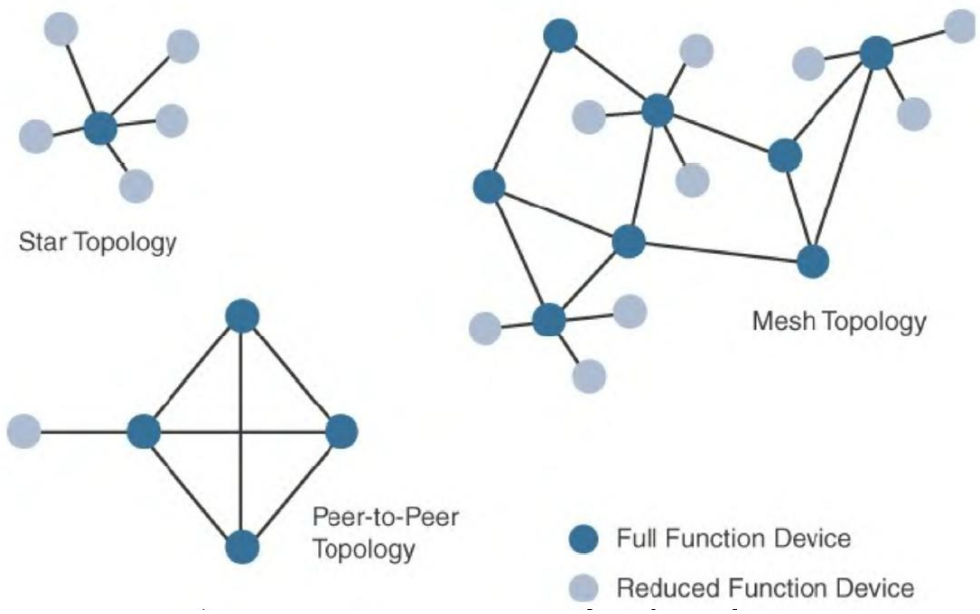
Μεταξύ των διαθέσιμων τεχνολογιών πρόσβασης για τη σύνδεση συσκευών IoT, κυριαρχούν τρία κύρια σχέδια τοπολογίας:

- star: Επικρατεί σε τεχνολογίες μικρής και μεγάλης εμβέλειας, όπως φαίνεται στα δίκτυα κινητής τηλεφωνίας, LPWA και Bluetooth. Αυτές οι τοπολογίες χρησιμοποιούν έναν μόνο κεντρικό σταθμό βάσης ή έναν ελεγκτή για να επιτρέπουν επικοινωνίες με καταληκτικά σημεία.

- peer-to-peer: Αυτές οι τοπολογίες επιτρέπουν σε οποιαδήποτε συσκευή να επικοινωνεί με οποιαδήποτε άλλη συσκευή, εφόσον βρίσκονται μεταξύ τους. Βασίζονται σε πολλές συσκευές πλήρους λειτουργίας και επιτρέπουν πιο πολύπλοκους σχηματισμούς, όπως η τοπολογία δικτύωσης πλέγματος.

- mesh

Για τεχνολογίες μεσαίας εμβέλειας, είναι συνηθισμένη και οι τρείς τοπολογίες star, mesh, και peer-to-peer, όπως φαίνεται στο Σχήμα 29.



Σχήμα 29: Τοπολογίες Star, Peer-to-Peer και Mesh.

5. Περιορισμένες συσκευές (Constrained Devices)

Internet Engineering Task Force (IETF) αναγνωρίζει στο RFC 7228 ότι αναπτύσσονται διαφορετικές κατηγορίες συσκευών IoT. Το RFC 7228 δίνει ορισμένους ορισμούς περιορισμένων κόμβων. Αυτοί οι ορισμοί βοηθούν στη διαφοροποίηση των περιορισμένων κόμβων από απεριόριστους κόμβους, όπως διακομιστές, επιτραπέζιους ή φορητούς υπολογιστές και ισχυρές κινητές συσκευές όπως έξυπνα τηλέφωνα. Οι περιορισμένοι κόμβοι έχουν περιορισμένους πόρους που επηρεάζουν το σύνολο και τις δυνατότητες δικτύωσης.

6. Δίκτυα περιορισμένων κόμβων (Constrained-Node Networks)

Ενώ αρκετές από τις τεχνολογίες πρόσβασης IoT, (όπως το Wi-Fi), ισχύουν για φορητούς υπολογιστές, έξυπνα τηλέφωνα και ορισμένες συσκευές IoT, ωστόσο, μόνο ορισμένες τεχνολογίες πρόσβασης IoT είναι οι πιο κατάλληλες για τη συγκεκριμένη σύνδεση περιορισμένων κόμβων. Χαρακτηριστικά παραδείγματα είναι οι τεχνολογίες πρόσβασης IEEE 802.15.4 και 802.15.4g RF, IEEE 1901.2a PLC, LPWA και IEEE 802.11ah.
Τα δίκτυα περιορισμένων κόμβων συχνά αναφέρονται ως δίκτυα χαμηλής ισχύος και απώλειας (low-power and lossy networks LLNs).
Η χαμηλή ισχύς στο πλαίσιο των LLN αναφέρεται στο γεγονός ότι οι κόμβοι πρέπει να ανταποκρίνονται στις απαιτήσεις από τροφοδοτούμενους με μπαταρίες περιορισμένους κόμβους.

7. Ποσοστό δεδομένων και απόδοση (Data Rate and Throughput)

Οι ρυθμοί δεδομένων που διατίθενται από τεχνολογίες πρόσβασης IoT κυμαίνονται από 100 bps με πρωτόκολλα όπως το Sigfox έως δεκάδες megabit ανά δευτερόλεπτο με τεχνολογίες όπως LTE και IEEE 802.11ac. Ωστόσο, η πραγματική απόδοση είναι μικρότερη από το ρυθμό δεδομένων. Τεχνολογίες που δεν έχουν σχεδιαστεί ειδικά για IoT, (όπως το Wi-Fi), ταιριάζουν καλά με εφαρμογές IoT με υψηλές απαιτήσεις εύρους ζώνης. Οι τεχνολογίες μικρής εμβέλειας μπορούν επίσης να παρέχουν μεσαία έως υψηλά ποσοστά δεδομένων που έχουν αρκετή απόδοση για να συνδέσουν μερικά τελικά σημεία.
Οι τεχνολογίες πρόσβασης IoT που αναπτύχθηκαν για περιορισμένους κόμβους βελτιστοποιούνται για χαμηλή κατανάλωση ενέργειας, αλλά είναι επίσης περιορισμένες ως προς τον ρυθμό δεδομένων, ο οποίος εξαρτάται από την επιλεγμένη ζώνη συχνοτήτων και την απόδοση.

8. Καθυστέρηση (Latency and Determinism)

Σε περιορισμένα δίκτυα, η καθυστέρηση μπορεί να κυμαίνεται από μερικά χιλιοστά του δευτερολέπτου έως δευτερόλεπτα και οι εφαρμογές και οι στοίβες πρωτοκόλλων πρέπει να αντιμετωπίζουν αυτές τις ευρείες τιμές.

9. Ωφέλιμο φορτίο (Overhead and Payload)

Κατά την εξέταση τεχνολογιών περιορισμένης πρόσβασης δικτύου, είναι σημαντικό να αναθεωρηθούν τα χαρακτηριστικά μεγέθους ωφέλιμου φορτίου MAC που απαιτούν οι εφαρμογές. Επιπλέον, θα πρέπει να γνωρίζετε τυχόν απαιτήσεις για IP.

Κεφάλαιο 4.2 Τεχνολογίες Πρόσβασης IoT (IoT Access Technologies)

Τα ασύρματα επίπεδα IEEE 802.15.4 PHY και MAC είναι ώριμες προδιαγραφές που αποτελούν τη βάση για διάφορα πρότυπα και προϊόντα της βιομηχανίας (Πίνακας 6). Το επίπεδο PHY προσφέρει μέγιστη ταχύτητα έως 250 kbps, αλλά αυτό ποικίλλει με βάση τη διαμόρφωση και τη συχνότητα. Το στρώμα MAC για το 802.15.4 είναι ισχυρό και χειρίζεται τον τρόπο μετάδοσης και λήψης δεδομένων μέσω του επιπέδου PHY. Συγκεκριμένα, το στρώμα MAC χειρίζεται τη συσχέτιση και την αποσύνδεση συσκευών προς/από ένα PAN, αξιόπιστες επικοινωνίες μεταξύ συσκευών, ασφάλεια και το σχηματισμό διαφόρων τοπολογιών.
Κάθε τεχνολογία πρόσβασης στο IoT βασίζεται στα ακόλουθα πρότυπα. Συνοπτικά αναφέρονται τα εξής:

1.Τυποποίηση (Standardization and Alliances)

Αναφέρεται σε φορείς τυποποίησης που διατηρούν τα πρωτόκολλα για μια τεχνολογία. Το IEEE 802.15.4 (τεχνολογία ασύρματης πρόσβασης για συσκευές χαμηλού κόστους και χαμηλού ρυθμού δεδομένων που τροφοδοτούνται ή λειτουργούν με μπαταρίες.) ορίζει προδιαγραφές χαμηλού ρυθμού δεδομένων PHY και MAC για ασύρματα προσωπικά δίκτυα περιοχής (wireless personal area networks WPAN). Αυτό το πρότυπο έχει εξελιχθεί με την πάροδο των ετών και είναι μια γνωστή λύση για ασύρματες συσκευές χαμηλής πολυπλοκότητας με χαμηλούς ρυθμούς δεδομένων που χρειάζονται πολλούς μήνες ή και χρόνια ζωής μπαταρίας. Τα επίπεδα IEEE 802.15.4 PHY και MAC είναι τα θεμέλια για αρκετές στοίβες πρωτοκόλλων δικτύωσης.
Αυτές οι στοίβες πρωτοκόλλων χρησιμοποιούν το 802.15.4 σε φυσικό επίπεδο και επίπεδο επιπέδου σύνδεσης, αλλά τα ανώτερα επίπεδα είναι διαφορετικά. Αυτές οι στοίβες πρωτοκόλλου προωθούνται ξεχωριστά μέσω διαφόρων οργανισμών και συχνά εμπορεύονται. Μερικές από τις πιο γνωστές στοίβες πρωτοκόλλων που βασίζονται στο 802.15.4 επισημαίνονται στον Πίνακα 6.

Protocol	Description
ZigBee	Promoted through the ZigBee Alliance, ZigBee defines upper-layer components (network through application) as well as application profiles Common profiles include building automation, home automation, and healthcare. ZigBee also defines device object functions, such as device role, device discovery, network join, and security. For more information on ZigBee, see the ZigBee Alliance webpage, at www.zigbee.org. ZigBee is also discussed in more detail later in the next Section.
6LoWPAN	6LoWPAN is an IPv6 adaptation layer defined by the IETF 6LoWPAN working group that describes how to transport IPv6 packets over IEEE 802.15.4 layers. RFCs document header compression and IPv6 enhancements to cope with the specific details of IEEE 802.15.4. (For more information on 6LoWPAN, see Chapter 5.)
ZigBee IP	An evolution of the ZigBee protocol stack, ZigBee IP adopts the 6LoWPAN adaptation layer, IPv6 network layer, and RPL routing protocol. In addition, it offers improvements to IP security. ZigBee IP is discussed in more detail later in this chapter.
ISA100.11a	ISA100.11a is developed by the International Society of Automation (ISA) as "Wireless Systems for Industrial Automation: Process Control and Related Applications." It is based on IEEE 802.15.4-2006, and specifications were published in 2010 and then as IEC 62734. The network and transport layers are based on IETF 6LoWPAN, IPv6, and UDP standards.
WirelessHART	WirelessHART, promoted by the HART Communication Foundation, is a protocol stack that offers a time-synchronized, self-organizing, and self-healing mesh architecture, leveraging IEEE 802.15.4-2006 over the 2.4 GHz frequency band. A good white paper on WirelessHART can be found at http://www.emerson.com/resource/blob/system-engineering-guidelines-iec-62591-wirelesshart--data-79900.pdf
Thread	Constructed on top of IETF 6LoWPAN/IPv6, Thread is a protocol stack for a secure and reliable mesh network to connect and control products in the home. Specifications are defined and published by the Thread Group at www.threadgroup.org.

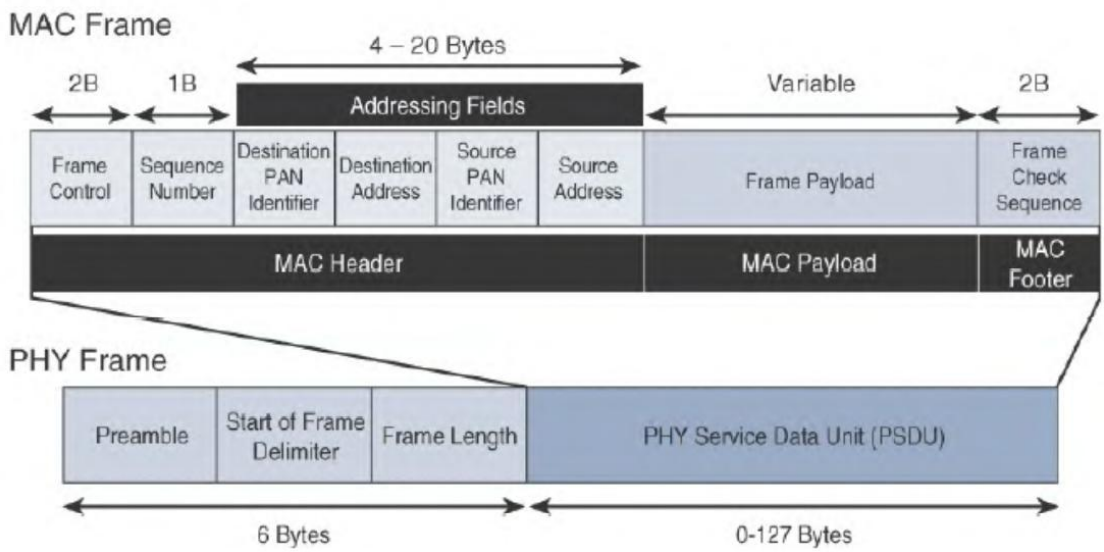
Πίνακας 6: Στοίβες πρωτοκόλλων που χρησιμοποιούν IEEE 802.15.4.

2. Φυσικό επίπεδο(Physical layer): Αναφέρονται σε ενσύρματες ή ασύρματες μεθόδους και στις σχετικές συχνότητες. Το πρότυπο 802.15.4 υποστηρίζει έναν εκτεταμένο αριθμό επιλογών PHY που κυμαίνονται από 2,4 GHz έως συχνότητες υπο GHz σε ζώνες ISM. Το αρχικό πρότυπο IEEE 802.15.4-2003 καθόρισε μόνο τρεις επιλογές PHY που βασίζονται στη διαμόρφωση άμεσου φάσματος διασποράς αλληλουχίας (direct sequence spread spectrumDSSS). Το DSSS είναι μια τεχνική διαμόρφωσης κατά την οποία ένα σήμα σκοπίμως σκορπίζεται στον τομέα συχνοτήτων, με αποτέλεσμα μεγαλύτερο εύρος ζώνης.

3.Επίπεδο MAC (MAC layer): Επίπεδο Media Access Control (MAC), το οποίο γεφυρώνει το φυσικό επίπεδο με τον έλεγχο σύνδεσης δεδομένων. Το επίπεδο MAC IEEE 802.15.4 διαχειρίζεται την πρόσβαση στο κανάλι PHY καθορίζοντας πώς οι συσκευές στην ίδια περιοχή θα μοιράζονται τις εκχωρημένες συχνότητες. Σε αυτό το επίπεδο, ο προγραμματισμός και η δρομολόγηση των πλαισίων δεδομένων είναι επίσης συντονισμένος.
Τέσσερις τύποι πλαισίων MAC καθορίζονται στο 802.15.4:

- Πλαίσιο δεδομένων(Data frame): Διαχειρίζεται όλες τις μεταφορές δεδομένων.
- Πλαίσιο φάρου(Beacon frame): Χρησιμοποιείται στη μετάδοση φάρων από έναν συντονιστή PAN.
- Πλαίσιο αναγνώρισης(Acknowledgement frame): Επιβεβαιώνει την επιτυχή λήψη ενός πλαισίου.
- Πλαίσιο εντολών MAC(MAC command Frame):Υπεύθυνο για τον έλεγχο της επικοινωνίας μεταξύ συσκευών.

Κάθε ένας από αυτούς τους τέσσερις τύπους πλαισίων MAC 802.15.4 ακολουθεί τη μορφή πλαισίου που φαίνεται στο Σχήμα 30.Όπως βλέπουμε το πλαίσιο MAC μεταφέρεται ως φορτίο PHY.



Σχήμα 30: Μορφή MAC IEEE 802.15.4.

4. Τοπολογία (Topology): Οι τοπολογίες που υποστηρίζονται από την τεχνολογία. Τα δίκτυα που βασίζονται στο IEEE 802.15.4 μπορούν να δημιουργηθούν ως τοπολογίες star, peer-to-peer,ή mesh. Τα δίκτυα mesh συνδέουν πολλούς κόμβους. Αυτό επιτρέπει στους κόμβους που θα ήταν εκτός εμβέλειας εάν προσπαθούσαν να επικοινωνήσουν απευθείας σε ενδιάμεσους κόμβους για τη μεταφορά επικοινωνιών.

5. **Ασφάλεια (Security):** Πτυχές ασφάλειας της τεχνολογίας. Η προδιαγραφή IEEE 802.15.4 χρησιμοποιεί το Advanced Encryption Standard (AES) με μήκος κλειδιού 128-bit ως βασικό αλγόριθμο κρυπτογράφησης για την ασφάλεια των δεδομένων του. Εκτός από την κρυπτογράφηση των δεδομένων, το AES στο 802.15.4 επικυρώνει επίσης τα δεδομένα που αποστέλλονται. Αυτό επιτυγχάνεται με έναν κωδικό ακεραιότητας μηνύματος (message integrity code MIC), ο οποίος υπολογίζεται για ολόκληρο το πλαίσιο χρησιμοποιώντας το ίδιο κλειδί AES που χρησιμοποιείται για κρυπτογράφηση.

6. Ανταγωνιστικές τεχνολογίες (Competitive technologies): Άλλες τεχνολογίες που είναι παρόμοιες και μπορεί να είναι κατάλληλες εναλλακτικές λύσεις στη δεδομένη τεχνολογία. Όπως περιγράφεται αναλυτικά στον Πίνακα 6 τα επίπεδα IEEE 802.15.4 PHY και MAC είναι τα θεμέλια για πολλά προφίλ δικτύωσης που ανταγωνίζονται μεταξύ τους σε διάφορα περιβάλλοντα πρόσβασης IoT. Αυτοί οι διάφοροι προμηθευτές και οργανισμοί δημιουργούν στοίβες πρωτοκόλλου ανώτερου επιπέδου πάνω από έναν πυρήνα 802.15.4.
Ανταγωνίζονται και διακρίνονται βάσει χαρακτηριστικών και δυνατοτήτων σε αυτά τα ανώτερα στρώματα.

Κεφάλαιο 4.3 Πρωτόκολλα εφαρμογής για IoT

Δύο πρωτόκολλα το TCP και το UDP έχουν τη θέση τους στα δίκτυα IoT, ανάλογα με την εφαρμογή. Ειδικά πρωτόκολλα, όπως το CoAP και το MQTT, χειρίζονται τις απαιτήσεις δεδομένων εφαρμογών IoT και είναι αρκετά αποτελεσματικά για έξυπνα αντικείμενα που πρέπει να επικοινωνούν μέσω δικτύου χαμηλού εύρους ζώνης.
Συγκεκριμένα με το πρωτόκολλο TCP/IP, δύο κύρια πρωτόκολλα καθορίζονται για το επίπεδο μεταφοράς (Transport Layer):

1.Πρωτόκολλο ελέγχου μετάδοσης (Transmission Control Protocol TCP): Αυτό το πρωτόκολλο προσανατολισμένο στη σύνδεση απαιτεί μια περίοδο σύνδεσης για να καθοριστεί μεταξύ της πηγής και του προορισμού πριν από την ανταλλαγή δεδομένων
Για παράδειγμα, μπορούμε αυτό να το δούμε ως ισοδύναμο με μια παραδοσιακή τηλεφωνική συνομιλία, στην οποία πρέπει να είναι συνδεδεμένα δύο τηλέφωνα και να δημιουργηθεί ο σύνδεσμος επικοινωνίας για να μπορέσουν να μιλήσουν τα μέρη.

2.Πρωτόκολλο δεδομένων χρήστη (User Datagram Protocol UDP): Με αυτό το πρωτόκολλο χωρίς σύνδεση, τα δεδομένα μπορούν να αποσταλούν γρήγορα μεταξύ πηγής και προορισμού - αλλά χωρίς εγγύηση παράδοσης. Για παράδειγμα, μπορούμε αυτό να το δούμε στο παραδοσιακό σύστημα παράδοσης αλληλογραφίας, στο οποίο ένα γράμμα αποστέλλεται ταχυδρομικά σε έναν προορισμό. Η επιβεβαίωση της παραλαβής αυτής της επιστολής δεν γίνεται μέχρι να σταλεί άλλη επιστολή σε απάντηση.

Με την υπεροχή των ανθρώπινων αλληλεπιδράσεων στο Διαδίκτυο, το TCP είναι το κύριο πρωτόκολλο που χρησιμοποιείται στο επίπεδο μεταφοράς. Αυτό οφείλεται σε μεγάλο βαθμό στα εγγενή χαρακτηριστικά του, όπως η ικανότητά του να μεταφέρει μεγάλο όγκο δεδομένων σε μικρότερα σύνολα πακέτων. Επιπλέον, εξασφαλίζει επανασυναρμολόγηση με σωστή ακολουθία, έλεγχο ροής και αναμετάδοση χαμένων πακέτων.
Αντίθετα, το UDP χρησιμοποιείται συχνότερα είτε στο πλαίσιο υπηρεσιών δικτύου, όπως το Domain Name System (DNS), το Network Time Protocol (NTP), το Simple Network Management Protocol (SNMP) και το Dynamic Host Control Protocol (DHCP), είτε για κίνηση δεδομένων σε πραγματικό χρόνο, συμπεριλαμβανομένης της φωνής και του βίντεο μέσω IP.

Υπάρχουν διάφορες μέθοδοι για τη μεταφορά δεδομένων εφαρμογών IoT (Application Transport Methods). Συγκεκριμένα:

- Μέθοδος Application layer protocol not present: σε αυτή τη μέθοδο, το ωφέλιμο φορτίο δεδομένων μεταφέρεται απευθείας πάνω από τα κατώτερα στρώματα. Χρειάζεται ένας μεσολαβητής δεδομένων IoT για την κλιμάκωση αυτής της μεθόδου μεταφοράς δεδομένων εφαρμογής.

- Μέθοδος όπου το επίπεδο εφαρμογής είναι προσαρμοσμένο σε IP. Αυτή η τεχνική χρησιμοποιεί ένα επίπεδο προσαρμογής IP για τη μεταφορά δεδομένων εφαρμογής που προέρχονται από μια στοίβα χωρίς IP.

- Μέθοδος όπου τα γενικά πρωτόκολλα βασίζονται στον ιστό (όπως το HTTP), τα οποία μπορούν να χρησιμοποιηθούν με μη περιορισμένα δίκτυα, όπως Ethernet και Wi-Fi.

- Μέθοδος, που αναφέρεται στο χειρισμό δεδομένων εφαρμογών IoT στα ανώτερα στρώματα. Αυτή η μέθοδος χειρίζεται περιορισμένους κόμβους και δίκτυα και συνιστάται για τα περισσότερα δίκτυα IoT.

Κεφάλαιο 5 Δεδομένα και αναλυτικά στοιχεία για το IoT (Data and Analytics for IoT)

Τα συστήματα IoT παράγουν τεράστιο όγκο δεδομένων. Η επιχειρηματική αξία του IoT δεν έγκειται μόνο στη δυνατότητα σύνδεσης συσκευών, αλλά προέρχεται από την κατανόηση των δεδομένων που δημιουργούν αυτές οι συσκευές. Επομένως, εμφανίστηκε μια νέα μορφή διαχείρισης δεδομένων: **Αναλύσεις δεδομένων IoT**.

Αυτό το κεφάλαιο παρέχει μια επισκόπηση του πεδίου ανάλυσης δεδομένων για IoT, συμπεριλαμβανομένων των ακόλουθων τμημάτων:

Ανάλυση δεδομένων για το IoT.
Μηχανική εκμάθηση (Machine Learning).
Εργαλεία και τεχνολογία Big Data Analytics.
Edge Streaming Analytics.
Network Analytics

Παραδοσιακά η διαχείριση δεδομένων πραγματοποιήθηκε από σχεσιακές βάσεις δεδομένων, οι οποίες φρόντιζαν για καλά δομημένα δεδομένα σε πίνακες όπου οι σχέσεις μεταξύ πινάκων και δομών δεδομένων ήταν καλά κατανοητές και ήταν εύκολα προσβάσιμες μέσω SQL. Ωστόσο, η πλειοψηφία των δεδομένων που παράγονται από συσκευές IoT δεν είναι δομημένα. Καθώς τα δεδομένα IoT συλλέγονται με την πάροδο του χρόνου, γίνονται μεγάλα δεδομένα και απαιτούν ειδικό χειρισμό προκειμένου να αποκαλυφθούν τα πρότυπα μέσα από αυτό το μεγάλο όγκο δεδομένων. Για αυτό, απαιτούνται ειδικοί αλγόριθμοι που εκτελούν μηχανική εκμάθηση για την επεξεργασία των δεδομένων και την εύρεση μοτίβων.
Διαφορετικοί τύποι μηχανικής εκμάθησης μπορούν να χρησιμοποιηθούν για συγκεκριμένους σκοπούς, συμπεριλαμβανομένων εποπτευόμενων, μη εποπτευόμενων και νευρωνικών δικτύων (supervised, unsupervised, and neural networks).

Η επεξεργασία των συνολικών δεδομένων IoT γίνεται στο cloud ή στο κέντρο δεδομένων και πραγματοποιείται από συστήματα ανάλυσης μεγάλων δεδομένων, όπως NoSQL, Hadoop και MPP. Αυτά τα συστήματα έχουν σχεδιαστεί ειδικά για να αντιμετωπίζουν τον τεράστιο όγκο δεδομένων, ταχύτητα και ποικιλία δεδομένων που παράγονται από συστήματα IoT.

Με την πάροδο του χρόνου, έχουν αναπτυχθεί συστήματα ανάλυσης ροής όχι μόνο για να φιλτράρουν και να μειώνουν τα δεδομένα που παράγονται από συσκευές IoT, αλλά και να επιτρέπουν την απόκριση σχεδόν σε πραγματικό χρόνο στις συσκευές IoT όσο το δυνατόν πιο κοντά στην άκρη του δικτύου.

Τέλος, σε αυτό το κεφάλαιο εξετάζεται μια διαφορετική μορφή ανάλυσης δεδομένων , η ανάλυση δικτύου (**Network Analytic).** Η ανάλυση δικτύου δεν εξετάζει το περιεχόμενο των δεδομένων, αλλά χρησιμοποιείται για να ανακαλύψει μοτίβα στην επικοινωνιακή συμπεριφορά του δικτύου, βοηθώντας στον εντοπισμό και την πρόληψη των τρωτών σημείων ασφαλείας, τον προγραμματισμό της εξέλιξης του δικτύου και την καλύτερη κατανόηση της συμπεριφοράς των διαφόρων στοιχείων του δικτύου.

Κεφάλαιο 5.1 Ανάλυση δεδομένων για IoT

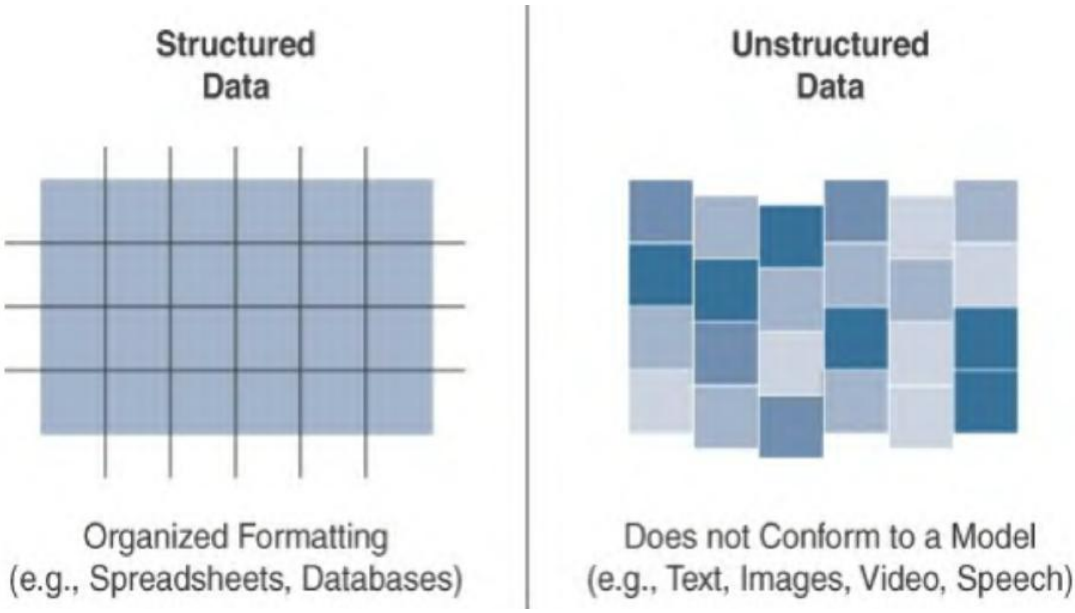
Στον κόσμο του IoT, η δημιουργία τεράστιων όγκων δεδομένων από αισθητήρες είναι κοινή και μια από τις μεγαλύτερες προκλήσεις (όχι μόνο από την άποψη της μεταφοράς αλλά και από τη σκοπιά της διαχείρισης δεδομένων). Ένα εξαιρετικό παράδειγμα του μεγάλου όγκου δεδομένων που μπορούν να παραχθούν από το IoT βρίσκεται στη βιομηχανία εμπορικής αεροπορίας και στους αισθητήρες που αναπτύσσονται σε ένα αεροσκάφος.
Οι σύγχρονοι κινητήρες τζετ είναι εξοπλισμένοι με χιλιάδες αισθητήρες που παράγουν εντυπωσιακά 10 GB δεδομένων ανά δευτερόλεπτο. Για παράδειγμα, οι σύγχρονοι κινητήρες τζετ, παρόμοιοι με αυτόν που φαίνεται στο Σχήμα 31, μπορεί να είναι εξοπλισμένοι με περίπου 5000 αισθητήρες.

Σχήμα 31: Εμπορικός κινητήρας jet.

Ως εκ τούτου, ένα δίκλινο εμπορικό αεροσκάφος με αυτούς τους κινητήρες που λειτουργούν κατά μέσο όρο 8 ώρες την ημέρα θα παράγει πάνω από 500 TB δεδομένων, και αυτά είναι μόνο τα δεδομένα από τους κινητήρες.
Τα αεροσκάφη σήμερα έχουν χιλιάδες άλλους αισθητήρες συνδεδεμένους με το πλαίσιο και άλλα συστήματα. Στην πραγματικότητα, μια πτέρυγα ενός σύγχρονου jumbo jet είναι εξοπλισμένη με 10.000 αισθητήρες. Αυτό το παράδειγμα δεν είναι παρά ένα από τα πολλά που αναδεικνύουν το πρόβλημα των μεγάλων δεδομένων που επιδεινώνεται από το IoT.
Η ανάλυση αυτού του όγκου δεδομένων με τον πιο αποτελεσματικό δυνατό τρόπο εμπίπτει «στην ομπρέλα» της ανάλυσης δεδομένων.
Η ανάλυση δεδομένων πρέπει να είναι σε θέση να προσφέρει εύχρηστες γνώσεις από τα δεδομένα, ανεξάρτητα από την ποσότητα ή το ύφος, ή αν τα πλήρη οφέλη του IoT δεν μπορούν να πραγματοποιηθούν. Ανάλογα με τον τρόπο κατηγοριοποίησης των δεδομένων, μπορούν να εφαρμοστούν διάφορα εργαλεία ανάλυσης δεδομένων και μέθοδοι επεξεργασίας.

Δύο σημαντικές κατηγοριοποιήσεις από άποψη IoT είναι αν τα δεδομένα είναι δομημένα ή μη δομημένα (structured or unstructured) και αν είναι σε κίνηση ή σε ηρεμία (Data in Motion Versus Data at Rest).
Αναφέρουμε συνοπτικά αυτές τις δύο κατηγορίες. Συγκεκριμένα:

Δομημένα και μη δομημένα δεδομένα. Τα δομημένα δεδομένα και τα μη δομημένα δεδομένα είναι σημαντικές ταξινομήσεις καθώς συνήθως απαιτούν διαφορετικά σύνολα εργαλείων από την άποψη της ανάλυσης δεδομένων. Το Σχήμα 32 παρέχει μια σύγκριση υψηλού επιπέδου δομημένων δεδομένων και μη δομημένων δεδομένων.



Σχήμα 32: Σύγκριση μεταξύ δομημένων και μη δομημένων δεδομένων.

Τα δομημένα δεδομένα σημαίνουν ότι:

- Ακολουθούν ένα μοντέλο ή ένα σχήμα που καθορίζει τον τρόπο με τον οποίο τα δεδομένα αναπαριστώνται ή οργανώνονται, πράγμα που σημαίνει ότι ταιριάζει καλά με ένα παραδοσιακό σύστημα διαχείρισης σχεσιακής βάσης δεδομένων (relational database management system RDBMS).

- Βρίσκονται σε απλή μορφή πίνακα όπως για παράδειγμα, ένα υπολογιστικό φύλλο όπου τα δεδομένα καταλαμβάνουν ένα συγκεκριμένο κελί και μπορούν να οριστούν και να αναφερθούν ρητά.
- Μπορούν να βρεθούν στα περισσότερα υπολογιστικά συστήματα και περιλαμβάνουν τα πάντα, από τραπεζικές συναλλαγές και τιμολόγια έως αρχεία καταγραφής υπολογιστή και διαμορφώσεις δρομολογητή. Τα δεδομένα IoT χρησιμοποιούν συχνά δομημένες τιμές, όπως θερμοκρασία, πίεση, υγρασία και ούτω καθεξής, οι οποίες αποστέλλονται σε γνωστή μορφή.
- Διαμορφώνονται εύκολα, αποθηκεύονται, αναζητούνται και επεξεργάζονται.
- Διαχειρίζονται και επεξεργάζονται πιο εύκολα λόγω της καλά καθορισμένης οργάνωσής τους.

Τα μη δομημένα δεδομένα:

- Στερούνται λογικού σχήματος για την κατανόηση και την αποκωδικοποίηση των δεδομένων μέσω παραδοσιακών μέσων προγραμματισμού. Παραδείγματα αυτού του τύπου δεδομένων περιλαμβάνουν κείμενο, ομιλία, εικόνες και βίντεο. Κατά γενικό κανόνα, όλα τα δεδομένα που δεν ταιριάζουν σε ένα προκαθορισμένο μοντέλο δεδομένων ταξινομούνται ως μη δομημένα δεδομένα.
- Μπορεί να είναι πιο δύσκολο να αντιμετωπιστούν και συνήθως απαιτούν πολύ διαφορετικά εργαλεία ανάλυσης για την επεξεργασία των δεδομένων.

Σύμφωνα με ορισμένες εκτιμήσεις, περίπου το 80% των δεδομένων μιας επιχείρησης είναι μη δομημένα. Εξαιτίας αυτού του γεγονότος, οι μέθοδοι ανάλυσης δεδομένων που μπορούν να εφαρμοστούν σε μη δομημένα δεδομένα, όπως η γνωστική υπολογιστική και η μηχανική εκμάθηση, συγκεντρώνουν επάξια μεγάλη προσοχή. Με εφαρμογές μηχανικής εκμάθησης, όπως η επεξεργασία φυσικής γλώσσας (NLP), μπορούμε να αποκωδικοποιήσουμε την ομιλία. Με εφαρμογές αναγνώρισης εικόνας/προσώπου, μπορούμε να εξάγουμε κρίσιμες πληροφορίες από ακίνητες εικόνες και βίντεο.

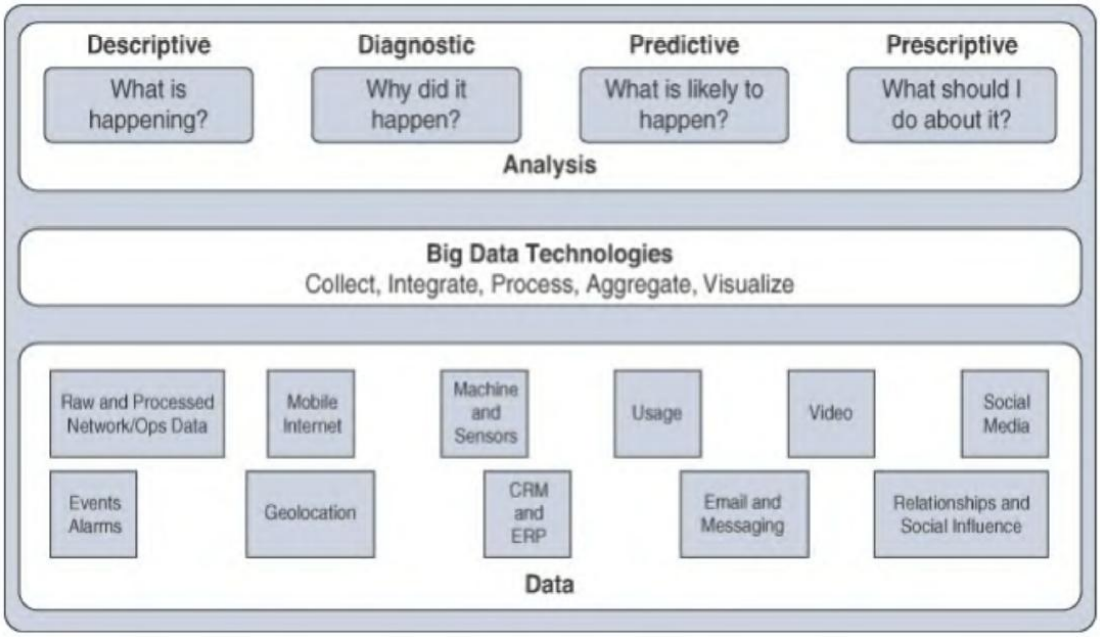
Δεδομένα σε κίνηση -Δεδομένα σε ηρεμία ((Data in Motion Versus Data at Rest). Όπως και στα περισσότερα δίκτυα, τα δεδομένα στα δίκτυα IoT είτε βρίσκονται σε μεταφορά («δεδομένα σε κίνηση») είτε διατηρούνται ή αποθηκεύονται («δεδομένα σε ηρεμία»). Παραδείγματα δεδομένων σε κίνηση περιλαμβάνουν παραδοσιακές ανταλλαγές πελάτη/διακομιστή, όπως περιήγηση στον ιστό και μεταφορές αρχείων, και email. Τα δεδομένα που αποθηκεύονται σε σκληρό δίσκο, πίνακα αποθήκευσης ή μονάδα USB είναι δεδομένα σε κατάσταση ηρεμίας.

Από την άποψη του IoT, τα δεδομένα από έξυπνα αντικείμενα θεωρούνται δεδομένα σε κίνηση καθώς περνούν από το δίκτυο καθ 'οδόν προς τον τελικό του προορισμό. Αυτό συχνά επεξεργάζεται στην άκρη, χρησιμοποιώντας υπολογισμούς Fog. Όταν τα δεδομένα υποβάλλονται σε επεξεργασία στην άκρη, μπορεί να φιλτραριστούν και να διαγραφούν ή να προωθηθούν για περαιτέρω επεξεργασία και πιθανή αποθήκευση σε έναν κόμβο fog(ομίχλης) ή στο κέντρο δεδομένων. Όταν τα δεδομένα φτάνουν στο κέντρο δεδομένων, είναι δυνατή η επεξεργασία τους σε πραγματικό χρόνο, ακριβώς όπως στην άκρη, ενώ είναι ακόμα σε κίνηση.

Τα δεδομένα σε κατάσταση ηρεμίας στα δίκτυα IoT μπορούν συνήθως να βρεθούν σε μεσίτες (brokers) IoT ή σε κάποιο είδος συστοιχίας αποθήκευσης στο κέντρο δεδομένων.

Αμέτρητα εργαλεία, ειδικά εργαλεία για δομημένα δεδομένα σε σχετικές βάσεις δεδομένων, είναι διαθέσιμα από την άποψη της ανάλυσης δεδομένων. Το πιο γνωστό από αυτά τα εργαλεία είναι το Hadoop.

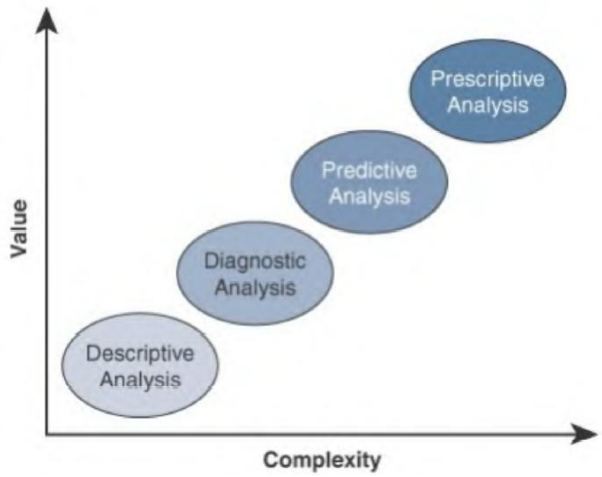
Η ανάλυση δεδομένων αναλύεται συνήθως από τους τύπους των αποτελεσμάτων που παράγονται. Όπως φαίνεται στο Σχήμα 33, υπάρχουν τέσσερις τύποι αποτελεσμάτων ανάλυσης δεδομένων.



Σχήμα 33: Τύποι αποτελεσμάτων ανάλυσης δεδομένων.

Περιγραφική(Diagnostic): μας ενημερώνει τι συμβαίνει, είτε τώρα είτε στο παρελθόν. Για παράδειγμα, ένα θερμόμετρο σε έναν κινητήρα φορτηγού αναφέρει τιμές θερμοκρασίας κάθε δευτερόλεπτο.
Διαγνωστική(Descriptive): όταν μας απασχολεί ο λόγος που κάτι συνέβη(το «γιατί»), η ανάλυση διαγνωστικών δεδομένων μπορεί να δώσει την απάντηση.
Προγνωστική(Predictive): στοχεύει στην πρόβλεψη προβλημάτων ή ζητημάτων πριν εμφανιστούν.
Προστατευτική(Prescriptive): προτείνει λύσεις για επερχόμενα προβλήματα.

Το Σχήμα 34 απεικονίζει τους τέσσερις τύπους ανάλυσης δεδομένων και πώς κατατάσσονται ως αύξηση της πολυπλοκότητας και της αξίας.



Σχήμα 34: Εφαρμογή παραγόντων αξίας και πολυπλοκότητας στους τύπους ανάλυσης δεδομένων.

Όπως μπορούμε να δούμε η περιγραφική ανάλυση είναι το λιγότερο περίπλοκη και ταυτόχρονα προσφέρει τη μικρότερη αξία. Από την άλλη πλευρά, η συντακτική ανάλυση παρέχει τη μεγαλύτερη αξία, αλλά είναι η πιο περίπλοκη στην εφαρμογή.
Η πλειονότητα της ανάλυσης δεδομένων στον χώρο του IoT βασίζεται σε περιγραφική και διαγνωστική ανάλυση, αλλά μια στροφή προς την προβλεπτική και προληπτική ανάλυση συμβαίνει ευλόγως για τις περισσότερες επιχειρήσεις και οργανισμούς.

Κεφάλαιο 5.2 Μηχανική εκμάθηση (Machine Learning)

Ένα από τα βασικά θέματα στο IoT είναι να κατανοήσουμε τα δεδομένα που δημιουργούνται. Επειδή πολλά από αυτά τα δεδομένα μπορεί να φαίνονται ακατανόητα με γυμνό μάτι, απαιτούνται εξειδικευμένα εργαλεία και αλγόριθμοι για να βρεθούν οι σχέσεις δεδομένων που θα οδηγήσουν σε νέες επιχειρηματικές γνώσεις. Αυτό μας φέρνει στο θέμα της μηχανικής εκμάθησης (Machine Learning ML).

Τα δεδομένα που συλλέγονται από έξυπνα αντικείμενα πρέπει να αναλυθούν και πρέπει να γίνουν έξυπνες ενέργειες με βάση αυτές τις αναλύσεις. Η χειροκίνητη εκτέλεση αυτού του είδους λειτουργίας είναι σχεδόν αδύνατη (ή πολύ, πολύ αργή και αναποτελεσματική). Απαιτούνται μηχανές για την γρήγορη επεξεργασία πληροφοριών και την άμεση αντίδραση όταν πληρούνται τα όρια. Η μηχανική εκμάθηση είναι, στην πραγματικότητα, μέρος ενός ευρύτερου συνόλου τεχνολογιών που συνήθως ομαδοποιούνται με τον όρο τεχνητή νοημοσύνη (artificial intelligence AI). Στην πραγματικότητα, η τεχνητή νοημοσύνη περιλαμβάνει οποιαδήποτε τεχνολογία που επιτρέπει σε ένα υπολογιστικό σύστημα να μιμείται την ανθρώπινη νοημοσύνη χρησιμοποιώντας οποιαδήποτε τεχνική, από πολύ προηγμένη λογική έως βασικούς βρόχους αποφάσεων «αν-τότε- αλλιώς».

Οποιοσδήποτε υπολογιστής χρησιμοποιεί κανόνες για τη λήψη αποφάσεων ανήκει σε αυτόν τον τομέα. Ένα απλό παράδειγμα είναι μια εφαρμογή που μπορεί να μας βοηθήσει να βρούμε το σταθμευμένο αυτοκίνητό μας. Μια ανάγνωση GPS της θέσης μας ανά τακτά χρονικά διαστήματα υπολογίζει την ταχύτητά μας. Ένα βασικό σύστημα κατωφλίου καθορίζει εάν οδηγούμε (για παράδειγμα, "εάν η ταχύτητα είναι μεγαλύτερη από 20 μίλια / ώρα ή 30 χλμ. / Ώρα, τότε ξεκινά τον υπολογισμό της ταχύτητας"). Όταν σταθμεύουμε και αποσυνδεόμαστε από το σύστημα Bluetooth του αυτοκινήτου, η εφαρμογή καταγράφει απλώς τη θέση όταν συμβαίνει η αποσύνδεση.

Πέρα από την εμφάνιση της τεχνητής νοημοσύνης (ο υπολογιστής γνωρίζει ότι είμαστε σταθμευμένοι και όπου συνέβη αυτό), το σύνολο κανόνων είναι πολύ απλό. Σε πιο πολύπλοκες περιπτώσεις, οι στατικοί κανόνες δεν μπορούν απλώς να εισαχθούν στο πρόγραμμα, επειδή απαιτούν παραμέτρους που μπορούν να αλλάξουν ή που δεν είναι κατανοητές. Αυτή η διαδικασία ονομάζεται **μηχανική εκμάθηση (Machine Learning ML)**.

Το ML ασχολείται με οποιαδήποτε διαδικασία όπου ο υπολογιστής χρειάζεται να λάβει ένα σύνολο δεδομένων (που υποβάλλονται σε επεξεργασία) για να βοηθήσει στην εκτέλεση μιας εργασίας με μεγαλύτερη αποτελεσματικότητα.
Το ML είναι ένα τεράστιο πεδίο, αλλά μπορεί απλά να χωριστεί σε δύο κύριες κατηγορίες:

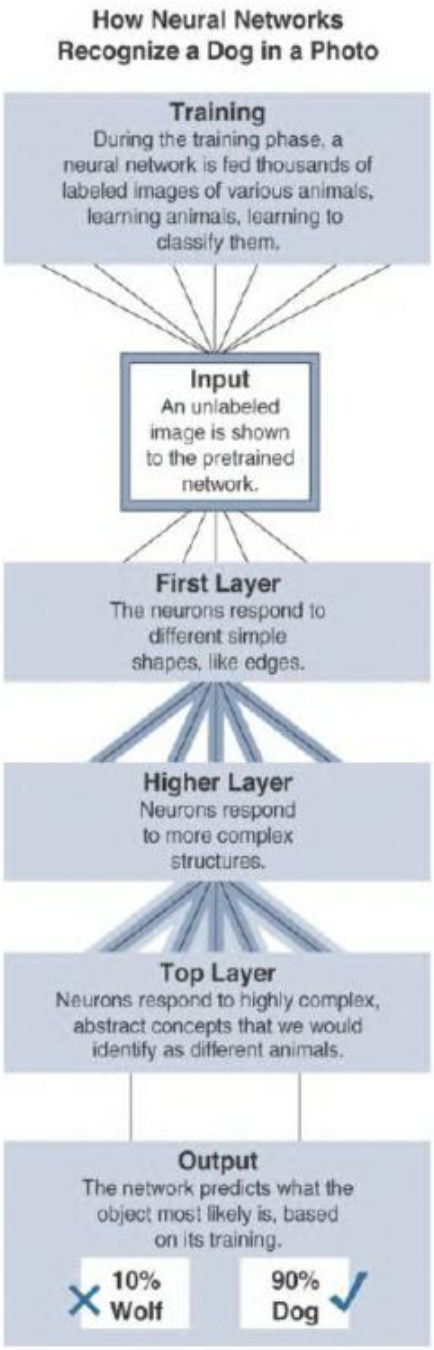
1.Εποπτευόμενη Μάθηση (Supervised Learning): το μηχάνημα εκπαιδεύεται με στοιχεία για τα οποία υπάρχει γνωστή σωστή απάντηση. Με τεχνικές εποπτείας μάθησης, εκατοντάδες ή χιλιάδες εικόνες εισάγονται στο μηχάνημα και κάθε εικόνα επισημαίνεται (ανθρώπινη ή μη ανθρώπινη σε αυτή την περίπτωση).

Αυτό ονομάζεται εκπαιδευτικό σετ. Ένας αλγόριθμος χρησιμοποιείται για τον προσδιορισμό κοινών παραμέτρων και κοινών διαφορών μεταξύ των εικόνων. και την χωρίς επίβλεψη μάθηση.

2.Μάθηση χωρίς επίβλεψη (Unsupervised Learning): σε ορισμένες περιπτώσεις, η εποπτευόμενη μάθηση δεν είναι η καλύτερη μέθοδος ώστε ένα μηχάνημα να βοηθήσει σε μια ανθρώπινη απόφαση. Αυτός ο τύπος μάθησης δεν παρακολουθείται επειδή δεν υπάρχει γνωστή εκ των προτέρων μια «καλή» ή «κακή» απάντηση. Είναι η παραλλαγή από μια συμπεριφορά ομάδας που επιτρέπει στον υπολογιστή να μάθει ότι κάτι είναι διαφορετικό.

Κεφάλαιο 5.3 Νευρωνικά δίκτυα(Neural Networks)

Τα νευρωνικά δίκτυα(Neural Networks), είναι μέθοδοι ML που μιμούνται τον τρόπο λειτουργίας του ανθρώπινου εγκεφάλου. Οι πληροφορίες περνούν από διαφορετικούς αλγόριθμους (που ονομάζονται μονάδες), καθένας από τους οποίους είναι υπεύθυνος για την επεξεργασία μιας πτυχής της πληροφορίας. Η προκύπτουσα τιμή μιας μονάδας υπολογισμού μπορεί να χρησιμοποιηθεί απευθείας ή να τροφοδοτηθεί σε άλλη μονάδα για να συμβεί περαιτέρω επεξεργασία. Σε αυτή την περίπτωση, το νευρωνικό δίκτυο λέγεται ότι έχει πολλά επίπεδα. Η μεγάλη αποτελεσματικότητα των νευρωνικών δικτύων είναι ότι κάθε μονάδα επεξεργάζεται ένα απλό τεστ και συνεπώς ο υπολογισμός είναι αρκετά γρήγορος. Αυτό το μοντέλο παρουσιάζεται στο Σχήμα 35.



Σχήμα 35: Παράδειγμα νευρωνικού δικτύου.

Κατά μια έννοια, τα νευρωνικά δίκτυα βασίζονται στην ιδέα ότι οι πληροφορίες διαιρούνται σε βασικά στοιχεία και κάθε στοιχείο έχει ένα βάρος. Τα βάρη που συγκρίνονται μαζί αποφασίζουν την ταξινόμηση αυτών των πληροφοριών . Όταν το αποτέλεσμα ενός στρώματος τροφοδοτείται σε ένα άλλο στρώμα, η διαδικασία ονομάζεται «βαθιά μάθηση»(deep learning). Βαθιά επειδή η διαδικασία εκμάθησης έχει περισσότερα από ένα στρώματα).

Ένα πλεονέκτημα της «βαθιάς μάθησης», είναι ότι η ύπαρξη περισσότερων επιπέδων επιτρέπει την πλουσιότερη ενδιάμεση επεξεργασία και αναπαράσταση των δεδομένων.

Σε κάθε στρώμα, τα δεδομένα μπορούν να μορφοποιηθούν ώστε να χρησιμοποιούνται καλύτερα από το επόμενο επίπεδο.

Αυτή η διαδικασία αυξάνει την αποτελεσματικότητα του συνολικού αποτελέσματος.) είναι μέθοδοι ML που μιμούνται τον τρόπο λειτουργίας του ανθρώπινου εγκεφάλου. Οι πληροφορίες περνούν από διαφορετικούς αλγόριθμους (που ονομάζονται μονάδες), καθένας από τους οποίους είναι υπεύθυνος για την επεξεργασία μιας πτυχής της πληροφορίας. Η προκύπτουσα τιμή μιας μονάδας υπολογισμού μπορεί να χρησιμοποιηθεί απευθείας ή να τροφοδοτηθεί σε άλλη μονάδα για να συμβεί περαιτέρω επεξεργασία. Σε αυτή την περίπτωση, το νευρωνικό δίκτυο λέγεται ότι έχει πολλά επίπεδα.

Κεφάλαιο 5.4 Εργαλεία και τεχνολογία - Big Data Analytics

Η ανάλυση μεγάλων δεδομένων μπορεί να αποτελείται από πολλά διαφορετικά κομμάτια λογισμικού που συλλέγουν, αποθηκεύουν, χειρίζονται και αναλύουν όλους τους διαφορετικούς τύπους δεδομένων. Το Hadoop βρίσκεται στον πυρήνα πολλών από τις σημερινές εφαρμογές μεγάλων δεδομένων ωστόσο δεν είναι το μοναδικό. Η ανάλυση μεγάλων δεδομένων μπορεί να αποτελείται από πολλά διαφορετικά κομμάτια λογισμικού που συλλέγουν, αποθηκεύουν, χειρίζονται και αναλύουν όλους τους διαφορετικούς τύπους δεδομένων. Βοηθά στην καλύτερη κατανόηση του τοπίου καθορίζοντας τι είναι τα μεγάλα δεδομένα και τι δεν είναι.

Γενικά, ο κλάδος κοιτάζει τα «τρία V» για να κατηγοριοποιήσει τα μεγάλα δεδομένα:

1. Ταχύτητα(Velocity): αναφέρεται στο πόσο γρήγορα συλλέγονται και αναλύονται τα δεδομένα. Το σύστημα διανομής αρχείων Hadoop έχει σχεδιαστεί για να απορροφά και να επεξεργάζεται δεδομένα πολύ γρήγορα. Τα έξυπνα αντικείμενα μπορούν να παράγουν δεδομένα μηχανών και αισθητήρων με πολύ γρήγορο ρυθμό και απαιτούν βάση δεδομένων ή συστήματα αρχείων ικανά για εξίσου γρήγορες λειτουργίες απορρόφησης.
2. Ποικιλία (Variety): αναφέρεται σε διαφορετικούς τύπους δεδομένων. Συχνά τα δεδομένα κατηγοριοποιούνται ως δομημένα, ήμι-δομημένα ή μη δομημένα. Διαφορετικές τεχνολογίες βάσεων δεδομένων μπορεί να μπορούν να δεχτούν μόνο έναν από αυτούς τους τύπους. Το Hadoop είναι σε θέση να συλλέξει και να αποθηκεύσει και τους τρεις τύπους.
3.Όγκος(Volume): αναφέρεται στην κλίμακα των δεδομένων. Τυπικά, αυτό μετριέται από gigabytes στο πολύ χαμηλό άκρο έως petabytes ή ακόμη και exabytes δεδομένων στο άλλο άκρο.

Τα χαρακτηριστικά των μεγάλων δεδομένων μπορούν να καθοριστούν από τις πηγές και τους τύπους δεδομένων. Συγκεκριμένα:
Πρώτο, είναι τα δεδομένα μηχανήματος, τα οποία δημιουργούνται από συσκευές IoT και είναι συνήθως μη δομημένα δεδομένα.
Δεύτερο, είναι τα δεδομένα συναλλαγών, τα οποία προέρχονται από πηγές που παράγουν δεδομένα από συναλλαγές σε αυτά τα συστήματα και έχουν υψηλό όγκο και δομημένα.
Τρίτο, είναι οι πηγές δεδομένων κοινωνικής δικτύωσης, οι οποίες είναι συνήθως υψηλού όγκου και δομημένες.
Τέταρτο, είναι τα επιχειρηματικά δεδομένα, τα οποία είναι δομημένα δεδομένα και χαμηλότερα σε όγκο.
Ως εκ τούτου, τα μεγάλα δεδομένα αποτελούνται από δεδομένα από όλες αυτές τις ξεχωριστές πηγές. Οι επιχειρήσεις έχουν χρησιμοποιήσει σχεσιακές βάσεις δεδομένων για την αποθήκευση δομημένων πληροφοριών. Νέες τεχνολογίες και τεχνικές στην αγορά διαχείρισης δεδομένων άνοιξαν νέες δυνατότητες για δεδομένα αισθητήρων και μηχανών.
Αυτές οι τεχνολογίες βάσεων δεδομένων εντάσσονται σε κατηγορίες που η καθεμία έχει πλεονεκτήματα και πιθανά μειονεκτήματα όταν χρησιμοποιούνται σε περιβάλλον IoT.

Οι τρεις πιο δημοφιλείς από αυτές τις κατηγορίες είναι τα μαζικά παράλληλα συστήματα επεξεργασίας, NoSQL και Hadoop

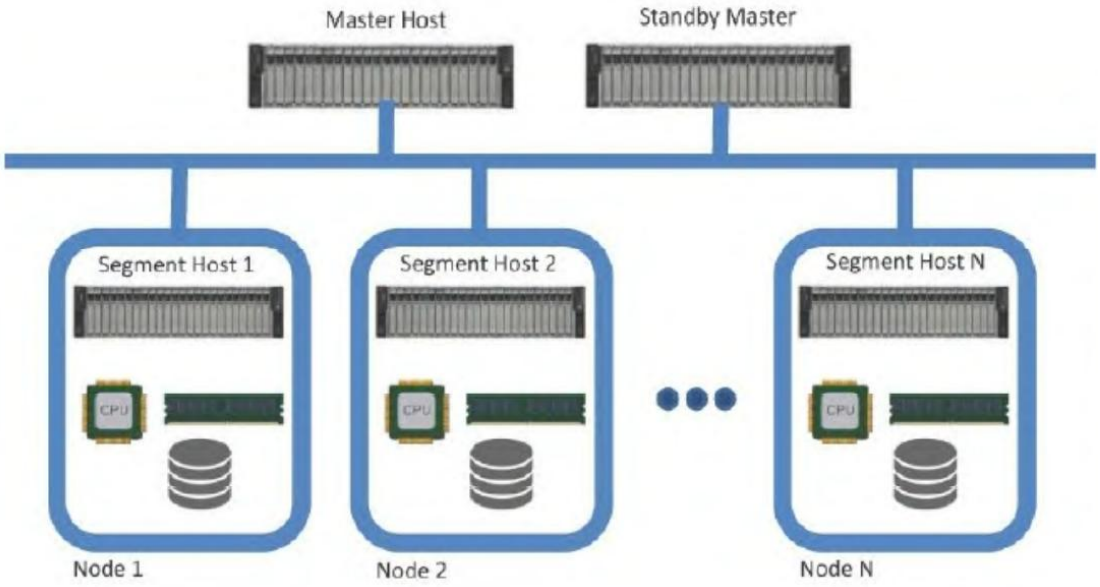
Οι τρεις πιο δημοφιλείς από αυτές τις κατηγορίες είναι

- Μαζικής παράλληλης επεξεργασίας (Massively parallel processing MPP).
- NoSQL.
- Hadoop.

Κεφάλαιο 5.4.1 Μαζικής παράλληλης επεξεργασίας (Massively parallel processing MPP)

Οι σχεσιακές βάσεις δεδομένων, συχνά ομαδοποιούνται σε μια ευρεία κατηγορία αποθήκευσης δεδομένων που ονομάζεται αποθήκες δεδομένων. Αν και αποτελούν το επίκεντρο των περισσότερων αρχιτεκτονικών δεδομένων, χρησιμοποιούνται συχνά για μακροπρόθεσμη αρχειοθέτηση και ερωτήματα δεδομένων που μπορεί συχνά να διαρκέσουν λεπτά ή ώρες. Οι βάσεις δεδομένων μαζικής παράλληλης επεξεργασίας (Massively parallel processing MPP) βασίστηκαν στην ιδέα των αποθηκών σχεσιακών δεδομένων, αλλά έχουν σχεδιαστεί για να είναι πολύ πιο γρήγορες, αποδοτικές και να υποστηρίζουν μειωμένους χρόνους ερωτήσεων. Για να επιτευχθεί αυτό, οι βάσεις δεδομένων MPP εκμεταλλεύονται πολλαπλούς κόμβους (υπολογιστές) σχεδιασμένους σε αρχιτεκτονική κλίμακας, έτσι ώστε τόσο τα δεδομένα όσο και η επεξεργασία να κατανέμονται σε πολλά συστήματα.

Μια αρχιτεκτονική MPP (Σχήμα 36) περιέχει συνήθως έναν μόνο κύριο κόμβο που είναι υπεύθυνος για το συντονισμό όλης της αποθήκευσης και επεξεργασίας δεδομένων σε ολόκληρο το σύμπλεγμα.



Σχήμα 36: MPP Shared-Nothing Architecture.

Κεφάλαιο 5.4.2 Βάσεις δεδομένων NoSQL

Το NoSQL είναι μια κατηγορία βάσεων δεδομένων που υποστηρίζουν ημί-δομημένα και μη δομημένα δεδομένα, επιπλέον των δομημένων δεδομένων που διαχειρίζονται οι αποθήκες δεδομένων και τα MPPs. Αναπτύχθηκε για να υποστηρίξει τις υψηλές ταχύτητες και επείγουσες απαιτήσεις δεδομένων των σύγχρονων εφαρμογών ιστού που συνήθως δεν απαιτούν πολύ επαναλαμβανόμενη χρήση.

Παρόμοια με άλλα καταστήματα δεδομένων, όπως MPP και Hadoop, το NoSQL είναι κατασκευασμένο ώστε να επιτρέπει στη βάση δεδομένων να εκτείνεται σε πολλούς κεντρικούς υπολογιστές και να μπορεί ακόμη και να διανεμηθεί γεωγραφικά. Η επέκταση των βάσεων δεδομένων NoSQL σε άλλους κόμβους είναι παρόμοια με την επέκταση σε άλλα κατανεμημένα συστήματα δεδομένων, όπου η διαχείριση πρόσθετων κεντρικών υπολογιστών γίνεται από έναν κύριο κόμβο ή διεργασία.
Αυτή η επέκταση μπορεί να αυτοματοποιηθεί με ορισμένες εφαρμογές NoSQL ή να παρέχεται με μη αυτόματο τρόπο. Αυτό το επίπεδο ευελιξίας καθιστά το NoSQL έναν καλό υποψήφιο για τη συγκράτηση δεδομένων μηχανών και αισθητήρων που σχετίζονται με έξυπνα αντικείμενα.
Πολλές βάσεις δεδομένων NoSQL παρέχουν πρόσθετες δυνατότητες, όπως η δυνατότητα αναζήτησης και ανάλυσης δεδομένων εντός της ίδιας της βάσης δεδομένων, εξαλείφοντας την ανάγκη μετακίνησης και επεξεργασίας τους αλλού.

Το NoSQL περιλαμβάνει πολλούς διαφορετικούς τύπους βάσεων δεδομένων, συμπεριλαμβανομένων των ακόλουθων:

Αποθήκευση εγγράφων(Document stores): βάση δεδομένων που αποθηκεύει ημί-δομημένα δεδομένα, όπως XML ή JSON. Έχουν μηχανές ερωτήματος και δυνατότητες ευρετηρίου που επιτρέπουν πολλά βελτιστοποιημένα ερωτήματα.

Αποθήκες κλειδιών-τιμών(Key-value stores): βάση δεδομένων που αποθηκεύει πίνακες όπου ένα κλειδί συνδυάζεται με μια σχετική τιμή. Αυτές οι βάσεις δεδομένων είναι εύκολο να δημιουργηθούν και εύκολο να κλιμακωθούν.

Αποθήκες ευρείας στήλης(Wide-column stores): βάση δεδομένων που αποθηκεύει παρόμοια με μια αποθήκη κλειδιών-τιμών, αλλά η μορφοποίηση των τιμών μπορεί να διαφέρει από σειρά σε σειρά, ακόμη και στον ίδιο πίνακα.

Αποθήκες γραφημάτων (Graph stores): βάση δεδομένων που οργανώνεται με βάση τις σχέσεις μεταξύ στοιχείων. Τα καταστήματα γραφημάτων χρησιμοποιούνται συνήθως για κοινωνικά μέσα ή επεξεργασία φυσικής γλώσσας, όπου οι συνδέσεις μεταξύ δεδομένων είναι πολύ σχετικές.

Κεφάλαιο 5.4.3 Hadoop

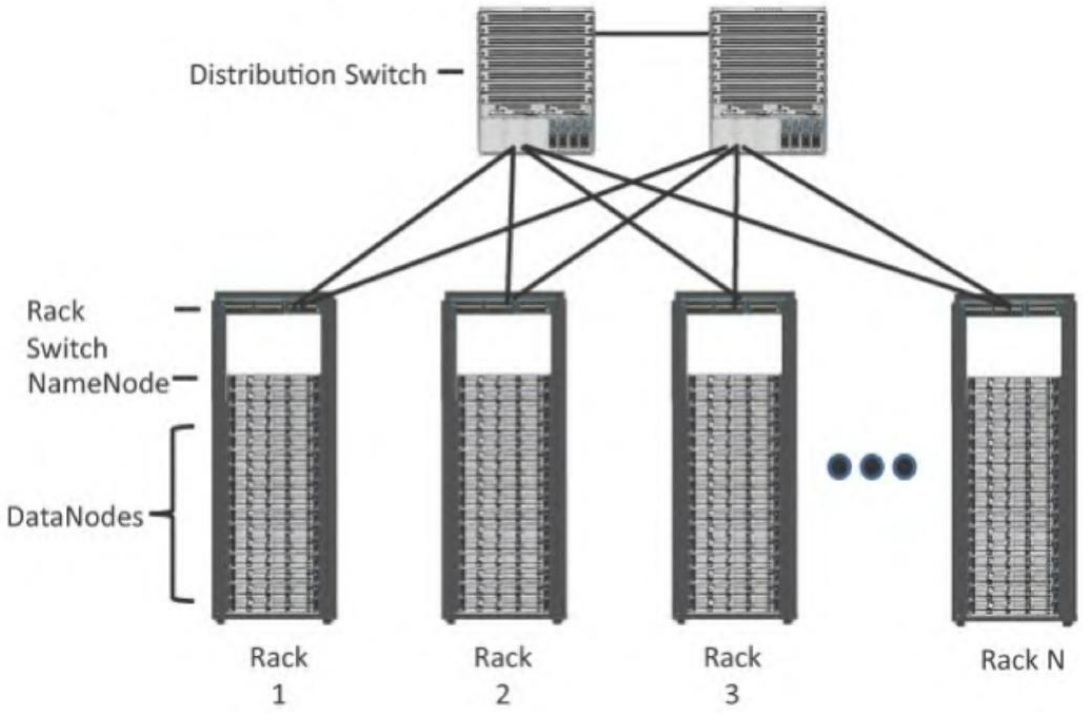
Το Hadoop είναι αναμφισβήτητα η πιο δημοφιλής επιλογή ως αποθήκη δεδομένων και μηχανή επεξεργασίας. Αναπτύχθηκε αρχικά ως αποτέλεσμα έργων στη Google και το Yahoo και η αρχική πρόθεση ήταν να κάνει «αναζήτηση»(index) σε εκατομμύρια ιστότοπους και να επιστρέψει γρήγορα αποτελέσματα αναζήτησης για μηχανές αναζήτησης ανοιχτού κώδικα.

Αρχικά, αυτό το έργο είχε δύο βασικά στοιχεία:

- Hadoop Distributed File System (HDFS): Ένα σύστημα αποθήκευσης δεδομένων σε πολλούς κόμβους.

- MapReduce: Μια κατανεμημένη μηχανή επεξεργασίας που χωρίζει μια μεγάλη εργασία σε μικρότερες που μπορούν να εκτελεστούν παράλληλα.

Όπως και τα συστήματα MPP και NoSQL, το Hadoop βασίζεται σε μια αρχιτεκτονική κλιμάκωσης που αξιοποιεί την τοπική επεξεργασία, τη μνήμη και την αποθήκευση για τη διανομή εργασιών και την παροχή ενός κλιμακούμενου συστήματος αποθήκευσης δεδομένων. Τόσο το MapReduce όσο και το HDFS εκμεταλλεύονται αυτήν την κατανεμημένη αρχιτεκτονική για να αποθηκεύουν και να επεξεργάζονται τεράστιες ποσότητες δεδομένων και έτσι μπορούν να αξιοποιήσουν πόρους από όλους τους κόμβους του συμπλέγματος.
Για το HDFS, αυτή η δυνατότητα χειρίζεται από εξειδικευμένους κόμβους στο σύμπλεγμα, συμπεριλαμβανομένων των NameNodes και DataNodes (Σχήμα 37).



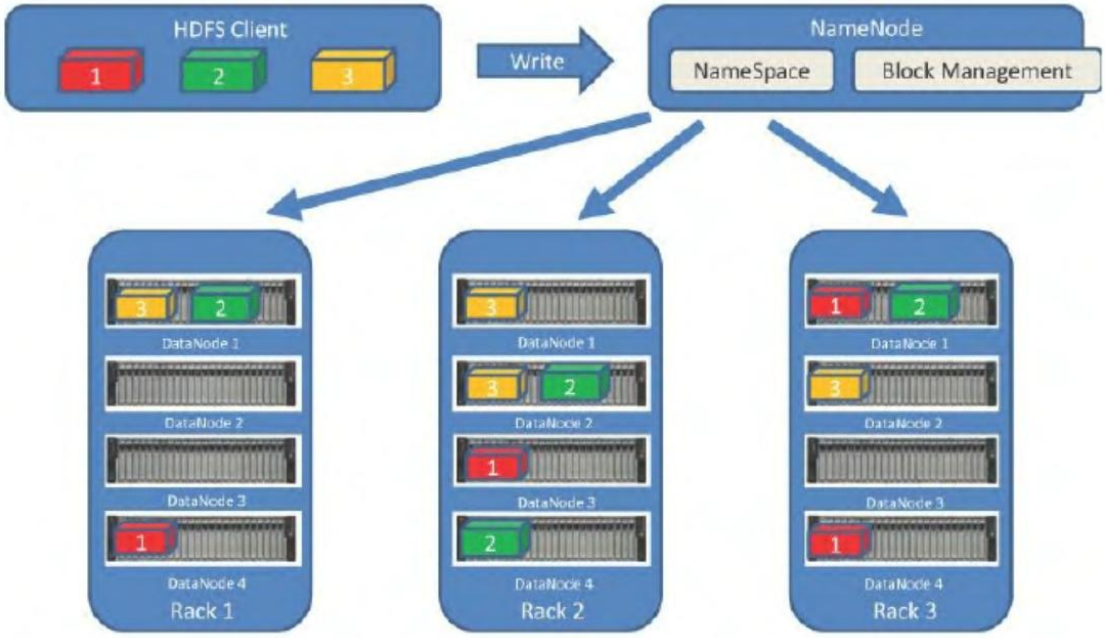
Σχήμα 37: Διανεμημένο σύμπλεγμα Hadoop.

Συγκεκριμένα:

NameNodes: Αυτό είναι ένα κρίσιμο κομμάτι στα δεδομένα που προσθέτει, μετακινεί, διαγράφει και διαβάζει σε HDFS. Συντονίζουν πού αποθηκεύονται τα δεδομένα και διατηρούν έναν χάρτη για το πού αποθηκεύεται και πού αναπαράγεται κάθε μπλοκ δεδομένων.Το NameNode είναι επίσης υπεύθυνο για την καθοδήγηση των DataNodes όπου πρέπει να γίνει η αντιγραφή.

DataNodes: Αυτοί είναι οι διακομιστές όπου τα δεδομένα αποθηκεύονται προς την κατεύθυνση του NameNode. Είναι σύνηθες να υπάρχουν πολλά DataNodes σε ένα σύμπλεγμα Hadoop για την αποθήκευση των δεδομένων. Τα μπλοκ δεδομένων κατανέμονται σε πολλούς κόμβους και συχνά αναπαράγονται τρεις, τέσσερις ή περισσότερες φορές σε κόμβους για πλεονασμό.

Το Σχήμα 38 δείχνει τη σχέση μεταξύ NameNodes και DataNodes και τον τρόπο κατανομής των μπλοκ δεδομένων σε ολόκληρο το σύμπλεγμα.



Σχήμα 38: Σύνταξη αρχείου σε HDFS.

Κεφάλαιο 5.5 Edge Streaming Analytics

Στον κόσμο του IoT, τεράστιες ποσότητες δεδομένων δημιουργούνται εν κινήσει και συχνά πρέπει να αναλυθούν και να απαντηθούν άμεσα. Όχι μόνο ο όγκος των δεδομένων που παράγονται είναι τεράστιος, αλλά τα δεδομένα μπορεί να είναι τόσο ευαίσθητα στο χρόνο που χρειάζονται άμεση προσοχή. Στο πλαίσιο του IoT, με αναλύσεις ροής που εκτελούνται στην άκρη (είτε στους ίδιους τους αισθητήρες είτε πολύ κοντά τους), είναι δυνατό να επεξεργαστούμε δεδομένα σε πραγματικό χρόνο χωρίς να περιμένουμε τα αποτελέσματα από μια μελλοντική εργασία επεξεργασίας παρτίδας στο cloud. Αυτό δεν σημαίνει ότι η ανάλυση ροής αντικαθιστά την ανάλυση μεγάλων δεδομένων στο cloud. Και οι δύο έχουν ρόλους να συμβάλουν στη βελτίωση των επιχειρηματικών ιδεών και διαδικασιών.

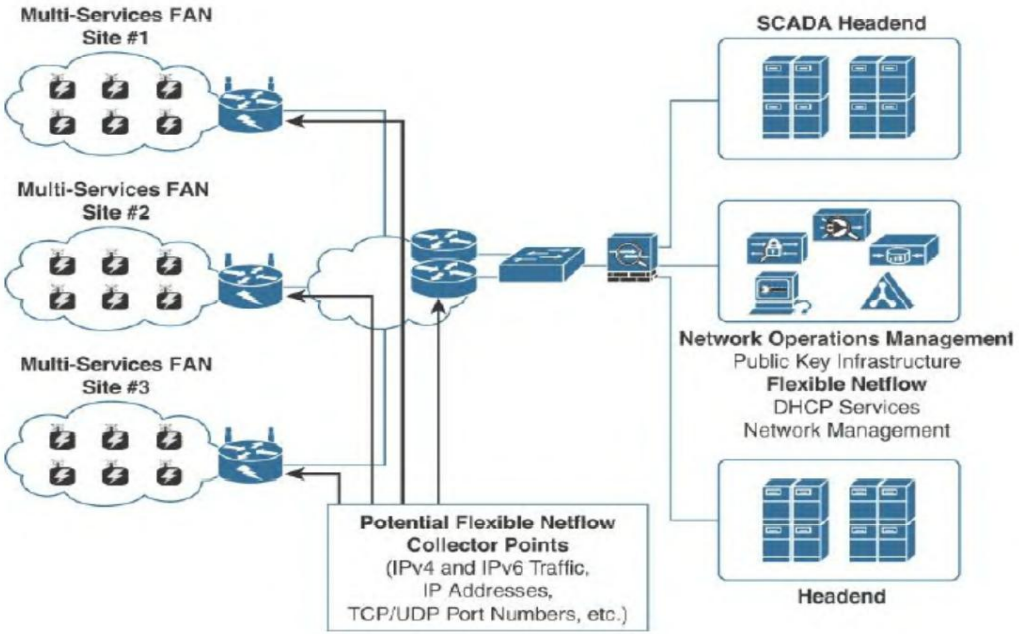
Από μια άποψη, εάν δημιουργούνται μη επεξεργάσιμα δεδομένα στο κέντρο δεδομένων, είναι λογικό να τα αναλύσουμε εκεί. Εάν όμως η πλειοψηφία των δεδομένων δημιουργούνται σε απομακρυσμένες τοποθεσίες από αισθητήρες που είναι διασκορπισμένοι σε μια ευρεία περιοχή, τότε για να είναι πραγματικά αποτελεσματικά, τα δεδομένα πρέπει να αναλυθούν και να απαντηθούν όσο το δυνατόν πιο κοντά.
Από την άποψη της ασφάλειας, η άμεση πρόσβαση σε αναλυμένα και προ-επεξεργασμένα δεδομένα στο άκρο επιτρέπει επίσης σε έναν οργανισμό να εντοπίσει ανωμαλίες στο δίκτυό του, ώστε αυτές οι ανωμαλίες να μπορούν να περιοριστούν γρήγορα πριν εξαπλωθούν στο υπόλοιπο δίκτυο.

Οι βασικές τιμές των αναλυτικών στοιχείων ροής άκρων(edge streaming analytics) περιλαμβάνουν τα ακόλουθα:

Μείωση δεδομένων στην άκρη(Reducing data at the edge): Τα συγκεντρωτικά δεδομένα που δημιουργούνται από συσκευές IoT είναι γενικά ανάλογα με τον αριθμό των συσκευών. Η κλίμακα αυτών των συσκευών είναι πιθανό να είναι τεράστια, καθώς και η ποσότητα δεδομένων που παράγουν. Η μετάδοση όλων αυτών των δεδομένων στο cloud είναι αναποτελεσματική και δαπανηρή όσον αφορά το εύρος ζώνης και την υποδομή του δικτύου.
Ανάλυση και απόκριση στην άκρη(Analysis and response at the edge): Ορισμένα δεδομένα είναι χρήσιμα μόνο στην άκρη (όπως ένα σύστημα ανατροφοδότησης εργοστασιακού ελέγχου). Σε τέτοιες περιπτώσεις, τα δεδομένα αναλύονται καλύτερα και ενεργούνται εκεί όπου δημιουργούνται.
Ευαισθησία στο χρόνο(Time sensitivity): Όταν απαιτείται έγκαιρη ανταπόκριση στα δεδομένα, η μετάδοση δεδομένων στο cloud για μελλοντική επεξεργασία οδηγεί σε μεγάλη καθυστέρηση.

Κεφάλαιο 5.6 Ανάλυση δικτύου(Network Analytics)

Μια άλλη μορφή ανάλυσης που είναι εξαιρετικά σημαντική στη διαχείριση συστημάτων IoT είναι η ανάλυση δικτύου(Network Analytics).
Σε αντίθεση με τα συστήματα ανάλυσης δεδομένων που συζητήθηκαν προηγουμένως και αφορούν την εύρεση μοτίβων στα δεδομένα που παράγονται από τα τελικά σημεία, η ανάλυση δικτύου ασχολείται με την ανακάλυψη προτύπων στις ροές επικοινωνίας από την άποψη της κίνησης δικτύου. Η ανάλυση δικτύου έχει τη δύναμη να αναλύει λεπτομέρειες των προτύπων επικοινωνίας που γίνονται από πρωτόκολλα και να το συσχετίζει σε όλο το δίκτυο. Επιτρέπει να κατανοούμε τι πρέπει να θεωρείται φυσιολογική συμπεριφορά σε ένα δίκτυο και να εντοπίζουμε γρήγορα σφάλματα που υποδηλώνουν προβλήματα δικτύου λόγω μη βέλτιστων διαδρομών, ή παρεμβατικών κακόβουλων προγραμμάτων. Το Σχήμα 38 δείχνει την ανάλυση επισκεψιμότητας δικτύου περιοχής πεδίου (FAN) που εκτελείται στο δρομολογητή συγκέντρωσης σε ένα έξυπνο δίκτυο.



Σχήμα 39: Παράδειγμα Smart Grid FAN Analytics with NetFlow.

Κεφάλαιο 6 Ασφάλιση IoT

Καθώς οι βιομηχανίες εκσυγχρονίζονται επιδιώκοντας επιχειρησιακή αποτελεσματικότητα, βελτιωμένη ασφάλεια και ανταγωνιστικές ικανότητες, πρέπει να το κάνουν με ασφάλεια.
Οι διαδικασίες εκσυγχρονισμού συχνά προκαλούν μεγαλύτερη συνδεσιμότητα στο πλαίσιο παλαιότερων και ιδιαίτερα ευάλωτων περιουσιακών στοιχείων και διαδικασιών OT.

Η ασφάλεια είναι μια διαδικασία που πρέπει να εφαρμόζεται συνέχεια. Για να επιτευχθεί η ασφάλεια, ένας οργανισμός πρέπει να είναι σε θέση να καθορίσει τους κινδύνους και να κάνει τεκμηριωμένες επιλογές σχετικά με τον καλύτερο τρόπο αντιμετώπισής τους.
Η συνδεσιμότητα δικτύου μπορεί να εξασφαλιστεί με τον κατάλληλο εξοπλισμό και πολιτικές. Οι απειλές από μη ασφαλείς πρακτικές, επιθέσεις και ανάγκες απομακρυσμένης πρόσβασης μπορούν να εντοπιστούν και να ελεγχθούν με ειδικές βιομηχανικές συσκευές και πρακτικές ασφάλειας.
Τα περιβάλλοντα τεχνολογίας πληροφοριών (Information technology IT) έχουν αντιμετωπίσει ενεργές επιθέσεις και απειλές για την ασφάλεια των πληροφοριών για πολλές δεκαετίες, σε αντίθεση με τα περιβάλλοντα λειτουργικής τεχνολογίας (operational technologyOT) που είχαν περιορισμένη σύνδεση με άλλα δίκτυα. Έτσι, η ιστορία των κυβερνοεπιθέσεων σε συστήματα OT είναι πολύ μικρότερη.
Η ασφάλεια στον κόσμο του OT αντιμετωπίζει επίσης ένα ευρύτερο φάσμα από ό, τι στον κόσμο της πληροφορικής IT.

Αυτό το κεφάλαιο επικεντρώνεται:

- Στις βασικές αρχές της ασφάλειας περιβαλλόντων OT.
- Περιγράφει τα χαρακτηριστικά δικτύου OT που επηρεάζουν την ασφάλεια.
- Αναφέρεται στις προτεραιότητες ασφάλειας: Ακεραιότητα Διαθεσιμότητα Εμπιστευτικότητα.
- Αναφέρεται στην εστίαση της ασφαλείας.

Κεφάλαιο 6.1 Βασικές αρχές της ασφάλειας περιβαλλόντων OT

Δύο από τις σημαντικότερες προκλήσεις για τη διασφάλιση βιομηχανικού περιβάλλοντος ήταν ο αρχικός σχεδιασμός και η συνεχής συντήρηση. Οι αρχικές προκλήσεις σχεδιασμού προέκυψαν από την ιδέα ότι τα δίκτυα ήταν ασφαλή λόγω φυσικού διαχωρισμού από την επιχείρηση με ελάχιστη ή καθόλου συνδεσιμότητα με τον έξω κόσμο και από την υπόθεση ότι οι επιτιθέμενοι δεν είχαν επαρκή γνώση για να πραγματοποιήσουν επιθέσεις ασφαλείας. Σε πολλές περιπτώσεις, ο αρχικός σχεδιασμός του δικτύου είναι σωστός και ακολουθεί ακόμη καλά καθορισμένες βιομηχανικές βέλτιστες πρακτικές και πρότυπα, όπως το μοντέλο Purdue για την ιεραρχία ελέγχου.

Τα βιομηχανικά πρωτόκολλα, όπως ο εποπτικός έλεγχος και η απόκτηση δεδομένων (supervisory control and data acquisition SCADA) αντιμετωπίζουν κοινά ζητήματα ασφάλειας. Παρουσιάζονται περιληπτικά ορισμένα κοινά βιομηχανικά πρωτόκολλα και οι αντίστοιχες ανησυχίες τους για την ασφάλεια.

Modbus: βρίσκεται συνήθως σε πολλούς κλάδους, όπως βοηθητικά προγράμματα και περιβάλλοντα κατασκευής, και έχει πολλές παραλλαγές (για παράδειγμα, σειριακό, TCP / IP). Είναι ένα από τα πιο ευρέως χρησιμοποιούμενα πρωτόκολλα σε βιομηχανικές εγκαταστάσεις και η ανάπτυξή του διέπεται από τον οργανισμό Modbus. Οι προκλήσεις ασφάλειας που υπήρχαν με το Modbus δεν είναι ασυνήθιστες.

Ο έλεγχος ταυτότητας των τελικών σημείων επικοινωνίας δεν ήταν μια προεπιλεγμένη λειτουργία, διότι θα επέτρεπε σε μια ακατάλληλη πηγή να στείλει ακατάλληλες εντολές στον παραλήπτη.

Πρωτόκολλο διανεμημένου δικτύου(Distributed Network Protocol DNP3):βρίσκεται σε πολλά σενάρια ανάπτυξης και βιομηχανίες. Είναι συνηθισμένο σε βοηθητικά προγράμματα και βρίσκεται επίσης σε διακριτά και συνεχή συστήματα διαδικασίας. Όπως και με πολλά άλλα πρωτόκολλα(ICS/SCADA), προοριζόταν για σειριακή επικοινωνία μεταξύ ελεγκτών και απλών IEDs. Το DNP3 έχει δώσει μεγάλη έμφαση στην αξιόπιστη παράδοση μηνυμάτων. Αυτή η έμφαση, αν και είναι συνήθως πολύ επιθυμητή, έχει μια συγκεκριμένη αδυναμία από την άποψη της ασφάλειας. Στην περίπτωση του DNP3, οι συμμετέχοντες επιτρέπουν ανεπιθύμητες απαντήσεις, οι οποίες θα μπορούσαν να προκαλέσουν μια ανεπιθύμητη απάντηση. Το στοιχείο ασφάλειας που λείπει εδώ είναι η ικανότητα να δημιουργηθεί εμπιστοσύνη στην κατάσταση του συστήματος και συνεπώς η ικανότητα εμπιστοσύνης στην αλήθεια των πληροφοριών που παρουσιάζονται.

Πρωτόκολλο επικοινωνιών (Inter-Control Center Communications Protocol) ICCP: είναι ένα κοινό πρωτόκολλο ελέγχου σε βοηθητικά προγράμματα που χρησιμοποιείται συχνά για επικοινωνία μεταξύ βοηθητικών υπηρεσιών. Δεδομένου ότι πρέπει να διασχίσει τα όρια μεταξύ διαφορετικών δικτύων, διατηρεί ένα επιπλέον επίπεδο έκθεσης και κινδύνου που θα μπορούσε να εκθέσει ένα βοηθητικό πρόγραμμα σε κυβερνοεπιθέσεις. Σε αντίθεση με άλλα πρωτόκολλα ελέγχου, το ICCP σχεδιάστηκε από την αρχή για να λειτουργεί μέσω WAN. Οι αρχικές εκδόσεις του ICCP είχαν αρκετά σημαντικά κενά στον τομέα της ασφάλειας. Μια βασική ευπάθεια είναι ότι το σύστημα δεν απαιτούσε έλεγχο ταυτότητας για επικοινωνία. Επίσης, η κρυπτογράφηση στο πρωτόκολλο δεν ενεργοποιήθηκε ως προεπιλεγμένη συνθήκη, εκθέτοντας έτσι συνδέσεις σε επιθέσεις man-in-the-middle (MITM) και replay.

Έλεγχος διαδικασίας OPC(OLE for Process Control): βασίζεται στη μεθοδολογία διαλειτουργικότητας της Microsoft (Object Linking and Embedding OLE). Στα βιομηχανικά δίκτυα ελέγχου, το OPC περιορίζεται στη λειτουργία στα υψηλότερα επίπεδα του χώρου ελέγχου, με εξάρτηση από πλατφόρμες που βασίζονται σε Windows. Οι ανησυχίες γύρω από το OPC ξεκινούν από το λειτουργικό σύστημα στο οποίο λειτουργεί. Πολλές από τις συσκευές Windows στον λειτουργικό χώρο είναι παλιές, δεν έχουν διορθωθεί πλήρως και κινδυνεύουν λόγω πληθώρα γνωστών τρωτών σημείων.

Πρωτόκολλα Διεθνούς Ηλεκτροτεχνικής Επιτροπής (International Electrotechnical Commission Protocols IECs): Το IEC 61850 δημιουργήθηκε για να επιτρέψει στον κατασκευαστή τη μηχανική συστημάτων παροχής ηλεκτρικού ρεύματος, η οποία, με τη σειρά της, θα επέτρεπε τη διαλειτουργικότητα μεταξύ προμηθευτών και τυποποιημένα πρωτόκολλα επικοινωνίας.

Τρεις τύποι μηνυμάτων ορίστηκαν αρχικά:

- MMS (Manufacturing Message Specification): είναι ένα πρωτόκολλο πελάτη/διακομιστή που αξιοποιεί το TCP/IP. Παρέχει την ίδια λειτουργικότητα με άλλα πρωτόκολλα SCADA, όπως το IEC 60870 και το Modbus.
- GOOSE (Generic Object Oriented Substation Event): είναι ένα πρωτόκολλο που λειτουργεί μέσω multicast και Ethernet. Επιτρέπει στα IEDs να ανταλλάσσουν δεδομένα «οριζόντια», μεταξύ θυρίδων και μεταξύ υποσταθμών, ειδικά για σήματα αλληλοσύνδεσης, μέτρησης και ενεργοποίησης.

- SV (Sampled Values): είναι ένα πρωτόκολλο που λειτουργεί μέσω multicast και Ethernet. Μεταφέρει δείγματα τάσης και ρεύματος, συνήθως στο δίαυλο διεργασίας, αλλά μπορεί επίσης να ρέει πάνω από το δίαυλο σταθμού.

Το IECs 61850 έχει αρκετές γνωστές ελλείψεις ασφαλείας που θα μπορούσαν να αξιοποιηθούν από εξειδικευμένους επιτιθέμενους για να θέσουν σε κίνδυνο ένα σύστημα ελέγχου. Ο έλεγχος ταυτότητας είναι ενσωματωμένος στο MMS, αλλά βασίζεται σε κωδικούς πρόσβασης αγαπημένου κειμένου και ο έλεγχος ταυτότητας δεν είναι διαθέσιμος στο GOOSE ή στο SV. Το υλικό-λογισμικό συνήθως δεν είναι υπογεγραμμένο, πράγμα που σημαίνει ότι δεν υπάρχει τρόπος επαλήθευσης της γνησιότητας ή της ακεραιότητάς του. Το GOOSE και το SV έχουν περιορισμένη ακεραιότητα μηνυμάτων, γεγονός που καθιστά σχετικά εύκολη την παραποίηση ενός εκδότη.

Κεφάλαιο 6.2 Χαρακτηριστικά δικτύου OT που επηρεάζουν την ασφάλεια

Ενώ τα δίκτυα IT και OT αρχίζουν να συγκλίνουν, εξακολουθούν να διατηρούν πολλά διαφορετικά χαρακτηριστικά όσον αφορά τον τρόπο λειτουργίας και την κίνηση που χειρίζονται. Αυτές οι διαφορές επηρεάζουν τον τρόπο με τον οποίο αντιμετωπίζονται στο πλαίσιο μιας στρατηγικής ασφάλειας.
Συγκεκριμένα, όταν, συγκρίνουμε τον τρόπο με τον οποίο ρέει η κίνηση στα δίκτυα IT και OT παρατηρούμε ότι στα:

- Δίκτυα IT, υπάρχουν πολλές διαφορετικές ροές δεδομένων. Οι ροές δεδομένων επικοινωνίας που προέρχονται από ένα τυπικό τελικό σημείο IT κινούνται σχετικά μακριά. Συχνά διασχίζουν το δίκτυο μέσω επιπέδων διακοπτών και τελικά φτάνουν σε ένα σύνολο τοπικών ή απομακρυσμένων διακομιστών, στους οποίους μπορούν να συνδεθούν απευθείας. Τα δεδομένα με τη μορφή ηλεκτρονικού ταχυδρομείου, μεταφοράς αρχείων ή υπηρεσιών εκτύπωσης πιθανότατα θα φτάσουν στο κεντρικό κέντρο δεδομένων, όπου ανταποκρίνονται ή θα ενεργοποιήσουν ενέργειες σε περισσότερες τοπικές υπηρεσίες, όπως έναν εκτυπωτή. Σε περίπτωση ηλεκτρονικού ταχυδρομείου ή περιήγησης στο διαδίκτυο, το τελικό σημείο ξεκινά ενέργειες που αφήνουν τα όρια του εταιρικού δικτύου και πιθανώς ταξιδεύουν στη γη.

- Δίκτυα OT: υπάρχουν δύο τύποι λειτουργικής κίνησης.
  Ο πρώτος τύπος είναι η τοπική επισκεψιμότητα, που μπορεί να περιέχεται σε ένα συγκεκριμένο πακέτο ή περιοχή για να παρέχει τοπική παρακολούθηση και έλεγχο κλειστού βρόχου. Αυτή είναι η επισκεψιμότητα χρησιμοποιείται για διαδικασίες σε πραγματικό χρόνο (ή σχεδόν σε πραγματικό χρόνο) και δεν χρειάζεται να εγκαταλείψει τα επίπεδα ελέγχου της διαδικασίας.
  Ο δεύτερος τύπος κίνησης, χρησιμοποιείται για την παρακολούθηση και τον έλεγχο περιοχών ή ζωνών ή του συνολικού συστήματος. Το SCADA είναι ένα καλό παράδειγμα αυτού, όπου πληροφορίες σχετικά με απομακρυσμένες συσκευές ή συνοπτικές πληροφορίες από μια λειτουργία μοιράζονται σε επίπεδο συστήματος, έτσι ώστε οι χειριστές να μπορούν να κατανοήσουν πώς λειτουργεί το συνολικό σύστημα ή τμήματα αυτού.Στη συνέχεια μπορούν να εφαρμόσουν τις κατάλληλες εντολές ελέγχου με βάση αυτές τις πληροφορίες.

Τα δίκτυα IT, είναι συνήθως πιο ενημερωμένα και χρησιμοποιούν σύγχρονες τεχνολογίες. Αυτές οι σύγχρονες πρακτικές δικτύωσης είναι ζωτικής σημασίας για την ικανοποίηση του υψηλού βαθμού ευελιξίας που απαιτείται στο περιβάλλον της IT. Η εικονική δικτύωση, οι εικονικοί χώροι εργασίας και οι εικονικοί διακομιστές είναι συνηθισμένοι. Είναι πιθανό ότι υπάρχει μεγάλη ποικιλία τύπων συσκευών που συμμετέχουν ενεργά σε οποιοδήποτε δίκτυο κάθε φορά.

Τα βιομηχανικά δίκτυα συχνά εξακολουθούν να βασίζονται σε σειριακές τεχνολογίες επικοινωνίας ή έχουν μικτές σειριακές και Ethernet. Αυτό σημαίνει ότι όχι μόνο πολλές συσκευές δεν διαθέτουν δυνατότητες IP, αλλά δεν είναι καν δυνατό να παρακολουθούν και να εξασφαλίζουν τη σειριακή κίνηση με τον ίδιο τρόπο που κάνετε για IP ή Ethernet. Σε ορισμένα περιβάλλοντα, το δίκτυο παραμένει πολύ στατικό, πράγμα που σημαίνει ότι μπορεί να δημιουργηθεί μια βασική βάση μοτίβων κίνησης και να παρακολουθείται για αλλαγές. Σε στατικά περιβάλλοντα, η ορατότητα συσκευών, πρωτοκόλλων και ροών κίνησης μπορεί να διαχειριστεί και να εξασφαλιστεί ευκολότερα. Ωστόσο, υπάρχει συνεχής αύξηση των κινητών συσκευών και της σύνδεσης ad hoc, ειδικά σε βιομηχανίες όπως οι μεταφορές και οι έξυπνες πόλεις, καθώς και αύξηση των περιουσιακών στοιχείων του κινητού στόλου σε πληθώρα άλλων βιομηχανιών.

Κεφάλαιο 6.3 Προτεραιότητες ασφάλειας: Ακεραιότητα Διαθεσιμότητα Εμπιστευτικότητα

Σε ένα πεδίο IT, το πιο κρίσιμο στοιχείο και ο στόχος των επιθέσεων ήταν η πληροφορία. Σε ένα πεδίο OT, τα κρίσιμα στοιχεία είναι οι συμμετέχοντες στη διαδικασία: εργαζομένων και εξοπλισμού.
Οι προτεραιότητες ασφαλείας αποκλίνουν με βάση αυτές τις διαφορές. Στον κόσμο των επιχειρήσεων IT, υπάρχουν νομικές, κανονιστικές και εμπορικές υποχρεώσεις για την προστασία των δεδομένων, ιδίως δεδομένων ατόμων που μπορεί ή όχι να απασχολούνται στον οργανισμό. Αυτή η έμφαση στην προστασία της ιδιωτικής ζωής επικεντρώνεται στην εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα(confidentiality, integrity, and availability) των δεδομένων.
Ο αντίκτυπος της απώλειας μιας υπολογιστικής συσκευής θεωρείται ελάχιστος σε σύγκριση με τις πληροφορίες που θα μπορούσε να περιέχει ή να παρέχει πρόσβαση. Συγκριτικά, στον κόσμο των OT, η απώλεια μιας συσκευής λόγω ευπάθειας ασφαλείας σημαίνει ότι η παραγωγή σταματά και η εταιρεία δεν μπορεί να εκτελέσει τη βασική της λειτουργία. Η απώλεια πληροφοριών που είναι αποθηκευμένες σε αυτές τις συσκευές είναι μικρότερη ανησυχία, αλλά σίγουρα υπάρχουν εμπιστευτικά σύνολα δεδομένων στο περιβάλλον λειτουργίας που ενδέχεται να έχουν οικονομικές επιπτώσεις, όπως διατυπώσεις και διαδικασίες. Σε έναν επιχειρησιακό χώρο, η ασφάλεια και η συνέχεια των συμμετεχόντων στη διαδικασία θεωρείται το πιο κρίσιμο μέλημα. Έτσι, ο στόχος είναι η συνεχής λειτουργία των συσκευών και η ασφάλεια των ανθρώπων που τις χειρίζονται. Το αποτέλεσμα είναι να τονιστεί η διαθεσιμότητα, η ακεραιότητα και το απόρρητο. Ο αντίκτυπος της απώλειας εδώ επεκτείνεται ακόμη και στην απώλεια ζωής.

Κεφάλαιο 6.4 Εστίαση ασφαλείας

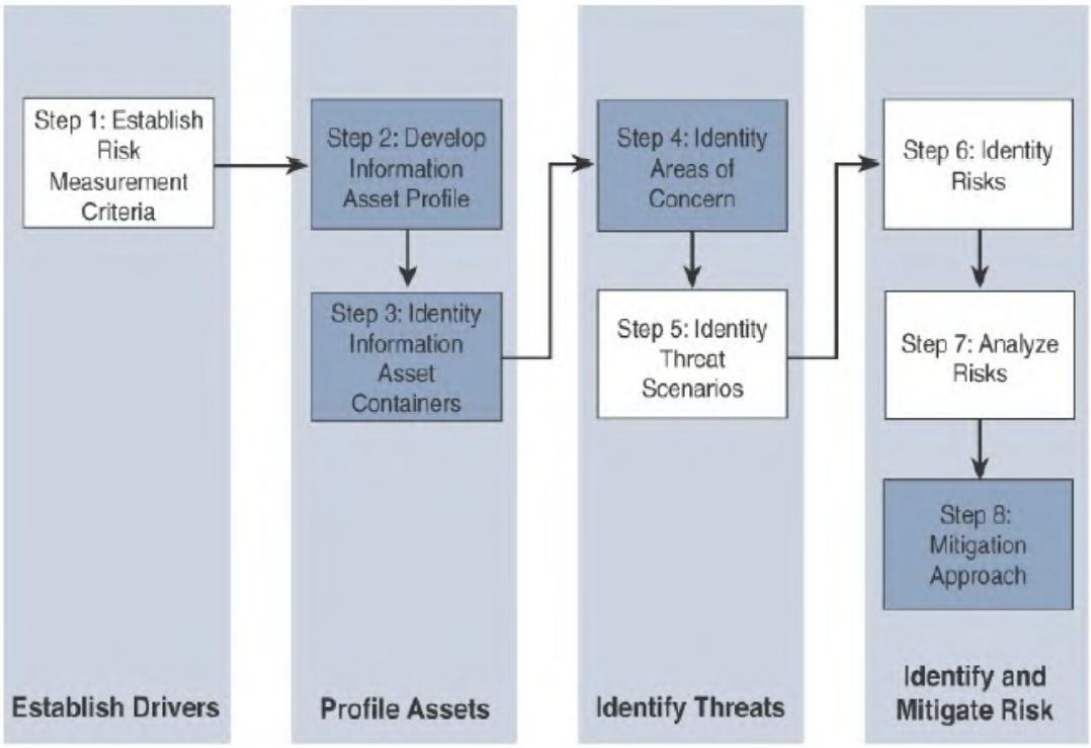
Η εστίαση στην ασφάλεια καθοδηγείται συχνά από το ιστορικό των επιπτώσεων στην ασφάλεια που έχει βιώσει ένας οργανισμός. Σε ένα περιβάλλον IT, οι πιο οδυνηρές εμπειρίες ήταν συνήθως καμπάνιες εισβολής στις οποίες εξάγονται ή αλλοιώνονται κρίσιμα δεδομένα. Το αποτέλεσμα ήταν μια σημαντική επένδυση σε αγαθά και ανθρώπινο δυναμικό για τη μείωση αυτών των εξωτερικών απειλών και την ελαχιστοποίηση των πιθανών εσωτερικών κακόβουλων παραγόντων. Στον χώρο του OT, το ιστορικό απώλειας που οφείλεται σε εξωτερικούς παράγοντες δεν ήταν τόσο μεγάλο, παρόλο που η πιθανότητα βλάβης σε ανθρώπινη κλίμακα είναι σαφώς σημαντικά υψηλότερη. Το αποτέλεσμα είναι ότι τα γεγονότα ασφαλείας που έχουν αντιμετωπιστεί προέρχονται περισσότερο από ανθρώπινο λάθος παρά από εξωτερικές επιθέσεις.
Το ενδιαφέρον και οι επενδύσεις στη βιομηχανική ασφάλεια αφορούσαν κυρίως τα τυπικά επίπεδα ελέγχου πρόσβασης.

Στο βιομηχανικό περιβάλλον, υπάρχουν πολλά πρότυπα και βέλτιστες πρακτικές που διατίθενται για να βοηθήσουν στην κατανόηση του κινδύνου και τον τρόπο μετριασμού του. Το IEC 62443 είναι το πιο συχνά χρησιμοποιούμενο πρότυπο παγκοσμίως σε βιομηχανικό περιβάλλον. Αποτελείται από πολλά μέρη, συμπεριλαμβανομένου του 62443-3-2 για την εκτίμηση κινδύνου και του 62443-3-3 για τις θεμελιώδεις απαιτήσεις που χρησιμοποιούνται για τη διασφάλιση του βιομηχανικού περιβάλλοντος από την άποψη της δικτύωσης και των επικοινωνιών. Επίσης, το ISO 27001 χρησιμοποιείται ευρέως για διαχείριση διαδικασιών και ασφάλειας πληροφοριών.

Το κλειδί για κάθε βιομηχανικό περιβάλλον είναι ότι πρέπει να αντιμετωπίσει την ασφάλεια ολιστικά και όχι μόνο να εστιάσει στην τεχνολογία. Πρέπει να περιλαμβάνει άτομα, διαδικασίες καθώς και όλα τα συστατικά του οικοσυστήματος των προμηθευτών που αποτελούν ένα σύστημα ελέγχου. Δύο συστήματα τα οποία χρησιμοποιούνται για τη δημιουργία ενός πιο ασφαλούς περιβάλλοντος, αλλά με διαφορετικές προσεγγίσεις και σύνολα προτεραιοτήτων, είναι τα εξής:

OCTAVE Allegro (Operationally Critical Threat, Asset and Vulnerability Evaluation): υποθέτει ότι μια ισχυρή ομάδα ασφαλείας δεν είναι σε κατάσταση αναμονής ή είναι έτοιμη να ξεκινήσει μια ολοκληρωμένη ανασκόπηση της ασφάλειας. Αυτή η προσέγγιση και οι υποθέσεις που κάνει είναι απολύτως κατάλληλες, δεδομένου ότι σε πολλούς τομείς επιχειρησιακής τεχνολογίας λείπουν παρόμοια ανθρώπινα στοιχεία που εστιάζουν στην ασφάλεια.

Το Σχήμα 40 απεικονίζει τα βήματα και τις φάσεις του OCTAVE Allegro.



Σχήμα 40: OCTAVE Allegro - Βήματα και φάσεις.

Το πρώτο βήμα της μεθοδολογίας OCTAVE Allegro, είναι να καθοριστεί ένα κριτήριο μέτρησης κινδύνου. Το κριτήριο της μέτρησης του κινδύνου είναι ότι σε οποιοδήποτε σημείο των μεταγενέστερων σταδίων, η ιεράρχηση μπορεί να πραγματοποιηθεί έναντι του μοντέλου αναφοράς.

Το δεύτερο βήμα, είναι η ανάπτυξη ενός προφίλ στοιχείων το οποίο συμπληρώνεται με χαρακτηριστικά που σχετίζονται με κάθε στοιχείο, συμπεριλαμβανομένων ιδιοκτητών, θεματοφυλάκων, ατόμων, ρητών απαιτήσεων ασφάλειας και τεχνολογικών στοιχείων, εύρος(containers) περιουσιακών στοιχείων

Το τρίτο βήμα, είναι να προσδιορίσουμε το εύρος(containers) στοιχείων δηλαδή το εύρος των μεταφορών και πιθανών τοποθεσιών όπου ενδέχεται να βρίσκονται οι πληροφορίες. Αυτό αναφέρεται στα υπολογιστικά στοιχεία και στα δίκτυα με τα οποία επικοινωνούν. Ωστόσο, μπορεί επίσης να σημαίνει φυσικές εκδηλώσεις όπως έντυπα έγγραφα ή ακόμη και άτομα που γνωρίζουν τις πληροφορίες.

Το τέταρτο βήμα, είναι να εντοπιστούν οι τομείς που μας απασχολούν. Σε αυτό το σημείο, απομακρυνόμαστε από τη ροή δεδομένων και την εστίαση χαρακτηριστικών σε ένα σημείο όπου οι κρίσεις γίνονται μέσω μιας αντιστοίχισης χαρακτηριστικών που σχετίζονται με την ασφάλεια σε πιο χρήσιμες περιπτώσεις χρήσης. Σε αυτό το στάδιο, ο αναλυτής αναζητά προφίλ κινδύνου και εμβαθύνει στην ανάλυση κινδύνου που αναφέρθηκε προηγουμένως.

Στο πέμπτο βήμα, εντοπίζονται τα σενάρια απειλών. Οι απειλές αναγνωρίζονται ως πιθανά ανεπιθύμητα γεγονότα. Αυτός ο ορισμός σημαίνει ότι τα αποτελέσματα τόσο από κακόβουλα όσο και από τυχαία αίτια αποτελούν βιώσιμες απειλές. Στο πλαίσιο της επιχειρησιακής εστίασης, αυτό είναι ένα πολύτιμο ζήτημα.

Στο έκτο βήμα, εντοπίζονται κίνδυνοι. Μέσα στο OCTAVE, κίνδυνος είναι η πιθανότητα ενός ανεπιθύμητου αποτελέσματος.

Το έβδομο βήμα, είναι η ανάλυση κινδύνου, με την προσπάθεια να καταβληθεί στην ποιοτική αξιολόγηση των επιπτώσεων του κινδύνου. Εδώ τα κριτήρια μέτρησης κινδύνου που ορίζονται στο πρώτο βήμα εισάγονται ρητά στη διαδικασία.

Στο όγδοο βήμα εφαρμόζεται ο μετριασμός(ή μείωση). Τρεις αποφάσεις υπάρχουν που πρέπει να ληφθούν σε αυτό το στάδιο.
α) Κάποιος μπορεί να είναι να αποδεχτεί έναν κίνδυνο και να μην κάνει τίποτα, εκτός από την τεκμηρίωση της κατάστασης, τα πιθανά αποτελέσματα και τους λόγους αποδοχής του κινδύνου.
β) Να μετριαστεί ο κίνδυνος με όποια προσπάθεια ελέγχου απαιτείται. Περνώντας στα σενάρια απειλών για προφίλ περιουσιακών στοιχείων, θα πρέπει να εντοπιστεί και στη συνέχεια να εφαρμοστεί ένα ζεύγος αντισταθμιστικών ελέγχων για τον μετριασμό αυτών των ζευγαριών κινδύνου / κινδύνου.
γ) Η τελική πιθανή ενέργεια είναι η αναβολή μιας απόφασης, που σημαίνει ότι ο κίνδυνος ούτε γίνεται αποδεκτός ούτε μετριάζεται. Αυτό μπορεί να συνεπάγεται περαιτέρω έρευνα ή δραστηριότητα, αλλά δεν απαιτείται από τη διαδικασία.

FAIR (Factor Analysis of Information Risk): είναι ένα τεχνικό πρότυπο που δίνει έμφαση τόσο στους σαφείς ορισμούς όσο και στην ιδέα ότι ο κίνδυνος και τα σχετικά χαρακτηριστικά είναι μετρήσιμα. Οι μετρήσεις είναι ένας βασικός τομέας έμφασης, ο οποίος θα πρέπει να προσφέρεται για έναν επιχειρησιακό κόσμο με πλούσιο επιχειρησιακά δεδομένα.

Κεφάλαιο 7 IoT στη βιομηχανία

Ο κόσμος της βιομηχανίας, κινείται γρήγορα προς τον ψηφιακό μετασχηματισμό. Ο έλεγχος του κόστους και η βελτίωση της αποδοτικότητας ήταν πάντα σημαντικοί για τους κατασκευαστές, αλλά καθώς τα μοντέλα της βιομηχανίας αλλάζουν και ο ανταγωνισμός αυξάνει, η πρωταρχική εστίαση στρέφεται τώρα προς την καινοτομία και τα βελτιωμένα επιχειρηματικά μοντέλα. Οι οικονομικές αλλαγές πυροδοτούν μια μαζική διαταραχή στη μεταποιητική βιομηχανία, με οδηγό την πρόοδο στην ψηφιοποίηση και το IoT.

Αυτό το κεφάλαιο εξετάζει αρχιτεκτονικές που χρησιμοποιούνται για την ψηφιοποίηση των εργοστασίων και τη σύνδεση μηχανών. Επίσης, περιλαμβάνει:

- Την εισαγωγή στη συνδεδεμένη βιομηχανία, εξετάζοντας τις τεχνολογίες που δημιουργούν την ψηφιακή πρόοδο στην κατασκευή.
- Τεχνολογίες δικτύωσης βιομηχανικών αυτοματισμών και συστημάτων ελέγχου.
- Πρωτόκολλα βιομηχανικού ελέγχου αυτοματισμού.
- Βασικά ζητήματα ασφάλειας στο εργοστάσιο
- Τρόπους για την εφαρμογή υπολογισμών άκρων στο συνδεδεμένο εργοστάσιο για τη βελτίωση της διαχείρισης δεδομένων και της προβολής.

Κεφάλαιο 7.1 Αρχιτεκτονική για συνδεδεμένη βιομηχανία (An Architecture for the Connected Factory)

Η προσπάθεια για ευελιξία και μαζική προσαρμογή απαιτεί δραστικές βελτιώσεις στην τεχνολογία σε εργοστάσια που παλαιώνουν λόγω περιορισμού του κόστους. Ο ψηφιακός μετασχηματισμός απαιτεί την υιοθέτηση βασικών προόδων της τεχνολογίας των πληροφοριών, πολλές από τις οποίες έχουν ήδη αποδειχθεί και υιοθετηθεί ευρέως σε άλλους κλάδους. Η πιο σημαντική τάση στην κατασκευή βρίσκεται στο λογισμικό.

Πολλά πράγματα που προηγουμένως απαιτούσαν υλικό στην καθημερινή μας ζωή μπορούν τώρα να επιτευχθούν με το λογισμικό. Ένα παράδειγμα είναι οι τηλεφωνητές.Τα μικρά κουτιά εγγραφής με μικροσκοπικές κασέτες που χρησιμοποιούνται από τους αυτόματους τηλεφωνητές βρίσκονται τώρα ως λογισμικό στο έξυπνο τηλέφωνό ή στους διακομιστές που φιλοξενούνται από τον πάροχο υπηρεσιών μας.
Το ίδιο συμβαίνει στις βιομηχανικές ρυθμίσεις και ένας αυξανόμενος αριθμός φυσικών ελέγχων διατίθεται πλέον ως λογισμικό διαθέσιμο μέσω της διεπαφής ανθρώπου-μηχανής (human- machine interface HMI). Το πλεονέκτημα του λογισμικού έναντι του υλικού είναι ότι οι νέες λειτουργίες και οι ενημερώσεις κώδικα λογισμικού διαχειρίζονται πιο απλά και οικονομικά.

Μπαίνουμε τώρα σε έναν κόσμο όπου οι κατασκευαστές μηχανών από απόσταση μπορούν να επιδιορθώνουν ένα μηχάνημα που προκαλεί σφάλματα, στέλνοντας απλώς μια ενημέρωση λογισμικού στο μηχάνημα. Επιπλέον, μέσω της τεχνητής νοημοσύνης (artificial intelligence AI), οι μηχανές είναι πλέον σε θέση να αυτοδιαγνώσουν προβλήματα. Τα ζητήματα αποκαλύπτονται αρκετές ημέρες πριν συμβεί διακοπή και το μηχάνημα επιδιορθώνεται μέσω μιας ενημέρωσης λογισμικού κατά τη διάρκεια ενός προγραμματισμένου παραθύρου συντήρησης. Η ανάλυση λογισμικού διαδραματίζει επίσης ουσιαστικό ρόλο στη βελτίωση της ευελιξίας και της αποδοτικότητας της κατασκευής. Οι κατασκευαστές πρέπει να έχουν πλήρη προβολή στους βασικούς δείκτες απόδοσης (key performance indicators KPIs) που ενοποιούν τις δραστηριότητες στο εργοστάσιο, στην επιχείρηση και σε όλη την αλυσίδα εφοδιασμού. Αυτή η συλλογή και ανάλυση δεδομένων σε πραγματικό χρόνο αποτελεί κύριο επίκεντρο πρωτοβουλιών IoT για κορυφαίους κατασκευαστές.

Κεφάλαιο 7.1.1 Μοντέλα αναφοράς βιομηχανικών αυτοματισμών και συστημάτων ελέγχου(industrial automation and control systems IACS)

Οι εταιρείες έχουν αρχίσει να συνδέουν τα βιομηχανικά τους συστήματα αυτοματισμού και ελέγχου (industrial automation and control systems IACS) με εφαρμογές IT και εργαλεία ανάλυσης για να παρέχουν δυνατότητες ελέγχου και ανάλυσης που οδηγούν σε λειτουργικά και επιχειρηματικά οφέλη. Το CPwE(αναφέρεται παρακάτω) είναι ένα αρχιτεκτονικό πλαίσιο που παρέχει υπηρεσίες δικτύου σε συσκευές και εξοπλισμό IACS και προωθεί την ασφαλή ενσωμάτωση στο εταιρικό δίκτυο.
Τα περιβάλλοντα παραγωγής βασίστηκαν σε πολλούς διαφορετικούς τύπους τεχνολογιών για να επιτρέψουν την επικοινωνία στο εργοστάσιο. Αυτές συχνά εξαρτώνται από ειδικά πρωτόκολλα επικοινωνίας για προμηθευτές, τα οποία με τη σειρά τους απαιτούν δίκτυα ειδικά σχεδιασμένα και ειδικά για προμηθευτές.
Σήμερα, το Ethernet και η IP έχουν γίνει το πρότυπο για τα συστήματα επικοινωνίας IACS. Το μοντέλο αναφοράς IACS χρησιμοποιεί ένα λογικό πλαίσιο για να περιγράψει τις λειτουργίες δικτύου και ασφάλειας του κατασκευαστικού συστήματος. Το λογικό πλαίσιο του IACS προσδιορίζει λειτουργικές ζώνες και επίπεδα του εργοστασίου παραγωγής και καθορίζει τις λειτουργίες σε κάθε επίπεδο.
Αυτές οι ζώνες ορίζονται ως εξής:

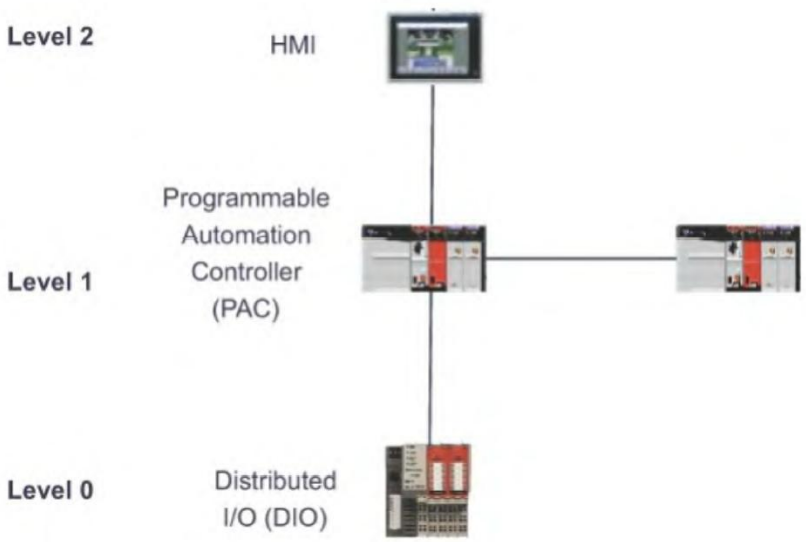
- Ζώνη ασφαλείας: Τα συστήματα στη ζώνη ασφαλείας είναι συνήθως ενσύρματα Η λειτουργία του συστήματος ασφαλείας σε αυτήν τη ζώνη είναι να παρέχει απενεργοποίηση IACS (κουμπί «διακοπής») σε περίπτωση έκτακτης ανάγκης.

- Ζώνη παραγωγής: αποτελείται από ζώνες κυψέλης/περιοχής(Επίπεδα 0-2) και δραστηριότητες κατασκευής σε επίπεδο τόπου (Επίπεδο 3).Η ζώνη παραγωγής είναι σημαντική επειδή όλες οι εφαρμογές, οι συσκευές και οι ελεγκτές IACS που είναι κρίσιμοι για την παρακολούθηση και τον έλεγχο των λειτουργιών IACS των εγκαταστάσεων είναι εδώ. Για να υποστηριχθούν οι ασφαλείς λειτουργίες των εγκαταστάσεων και η λειτουργία των εφαρμογών IACS, υπάρχει ένας ασφαλής διαχωρισμός της ζώνης παραγωγής και της επιχειρησιακής ζώνης (Επίπεδα 4 και 5).

- Ζώνη κυψέλης/περιοχής: είναι η περιοχή της μηχανής μέσα σε ένα εργοστάσιο. Υπάρχουν συνήθως πολλαπλές ζώνες κυττάρων / περιοχών μέσα σε ένα φυτό. Για παράδειγμα, σε ένα εργοστάσιο ηλεκτρονικών ειδών, ένα κελί/περιοχή μπορεί να είναι η περιοχή της διαδικασίας συναρμολόγησης. Η ζώνη κελιού/περιοχής μπορεί να αποτελείται από έναν μόνο ελεγκτή και σχετικές συσκευές ή μπορεί να είναι πολλοί ελεγκτές σε μια μεγάλη γραμμή συναρμολόγησης.

Για τον έλεγχο της λειτουργικής διαδικασίας, οι συσκευές IACS πρέπει να επικοινωνούν σε πραγματικό χρόνο με άλλες συσκευές IACS, πράγμα που σημαίνει ότι το δίκτυο που τις συνδέει πρέπει να είναι γρήγορο και αξιόπιστο. Αυτή η ζώνη έχει ουσιαστικά τρία επίπεδα δραστηριότητας:

Επίπεδο 0, Διαδικασία: είναι το επίπεδο «πραγμάτων» στην κατασκευή IoT και αποτελείται από αισθητήρες και ενεργοποιητές που εμπλέκονται στη διαδικασία κατασκευής. Αυτές οι συσκευές IoT εκτελούν λειτουργίες IACS, όπως μετακίνηση ρομπότ κατασκευής, ψεκασμό, οδήγηση κινητήρα και συγκόλληση. Αυτές οι συσκευές επικοινωνούν με τις βασικές συσκευές ελέγχου στο Επίπεδο 1.
Επίπεδο 1, Βασικός έλεγχος: είναι το σημείο όπου βρίσκονται οι ελεγκτές που κατευθύνουν τη διαδικασία παραγωγής. Αυτοί οι ελεγκτές αλληλεπιδρούν με συσκευές IoT επιπέδου 0. Στη διακριτή κατασκευή, ένας ελεγκτής είναι συνήθως ένα PLC και στην κατασκευή διεργασιών, είναι γνωστό ως σύστημα κατανεμημένου ελέγχου (DCS).
Επίπεδο 2, Εποπτικός έλεγχος περιοχής: περιλαμβάνει λειτουργίες εντός της ζώνης κελιού/περιοχής που απαιτούν εποπτεία και λειτουργία χρόνου εκτέλεσης. Ορισμένα παραδείγματα περιλαμβάνουν HMIs, συναγερμούς και σταθμούς εργασίας ελέγχου.
Το Σχήμα 41 απεικονίζει τους τύπους συσκευής και τις αντίστοιχες διεπαφές στα επίπεδα 0-2.



Σχήμα 41: IACS Controller Traffic Flow.

Επίπεδο 3,Επίπεδο ιστότοπου: Οι εφαρμογές και οι λειτουργίες στο Επίπεδο 3 περιλαμβάνουν συστήματα SCADA, διακομιστές αρχείων, σταθμούς εργασίας δωματίου ελέγχου, συστήματα προγραμματισμού και συστήματα αναφοράς.

Αποστρατιωτικοποιημένη ζώνη (Demilitarized zone DMZ): είναι η οριοθέτηση CPwE μεταξύ του λειτουργικού δικτύου της μονάδας και του παραδοσιακού δικτύου. Η ασφάλεια του DMZ είναι ζωτικής σημασίας για τις λειτουργίες των εγκαταστάσεων καθώς προστατεύει τα μηχανήματα σε χαμηλότερο επίπεδο από κακόβουλες δραστηριότητες που ενδέχεται να εμφανιστούν στο παραδοσιακό επιχειρηματικό δίκτυο.

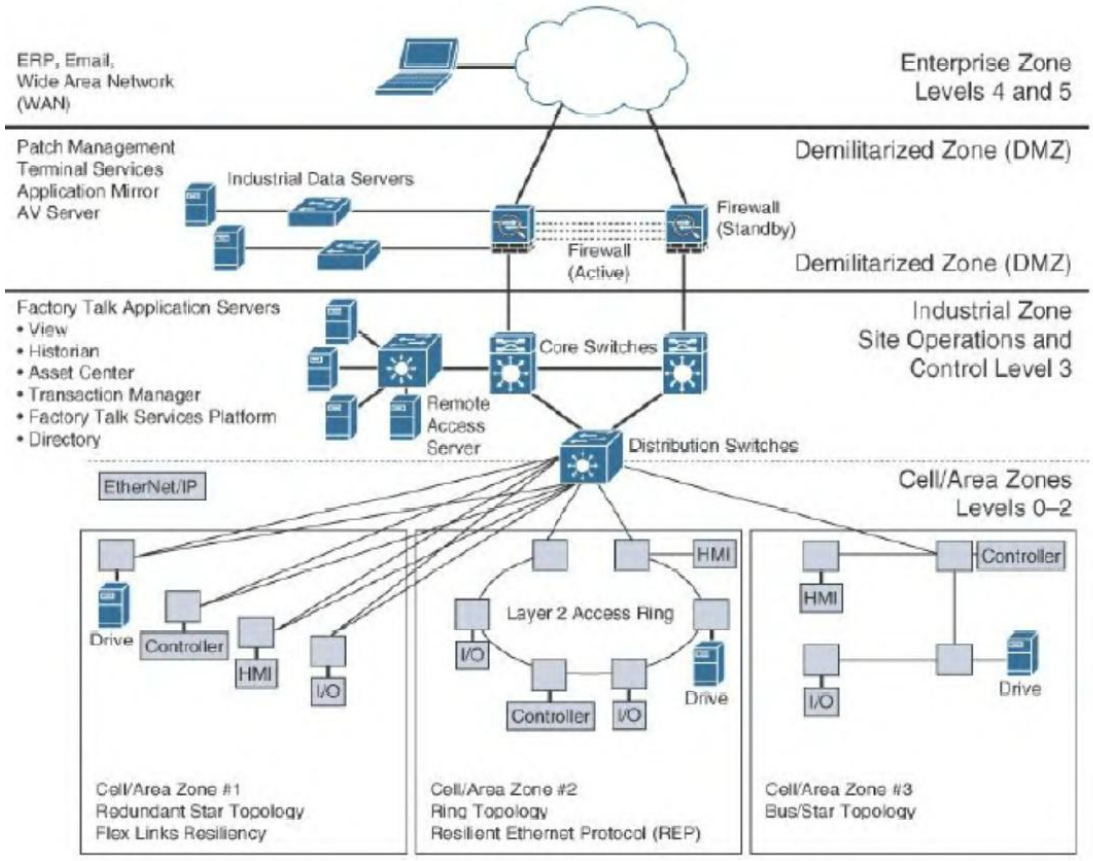
Επιχειρηματική ζώνη: Τα επίπεδα 4 και 5 στην επιχειρησιακή ζώνη σχετίζονται με παραδοσιακές λειτουργίες δικτύωσης IT/επιχειρήσεων, συμπεριλαμβανομένων υπηρεσιών αρχείων, συνδεσιμότητας Διαδικτύου και συστημάτων ηλεκτρονικού ταχυδρομείου.

Κεφάλαιο 7.1.2 Μοντέλο αναφοράς CPwE

Με την αποδοχή του Ethernet για βιομηχανικές εφαρμογές, εμφανίστηκαν πολλά νέα πρωτόκολλα επικοινωνιών που εκμεταλλεύονται τόσο το Ethernet όσο και το TCP / IP.
Η Cisco και η Rockwell Automation ξεκίνησαν από κοινού την ανάπτυξη του μοντέλου αναφοράς Converged Plantwide Ethernet (CPwE), το οποίο επικεντρώνεται κυρίως στη μεταφορά EtherNet / IP.
Το Σχήμα 42 απεικονίζει τη συνολική αρχιτεκτονική δικτύου CPwE. Σε αυτό το πλαίσιο, η ζώνη κελιού / περιοχής περιέχει τις συσκευές IACS από τα επίπεδα 0 έως 2. Οι συσκευές που βρίσκονται εδώ, όπως τα HMIs και οι ελεγκτές, ανήκουν σε ένα δίκτυο κυψέλης / περιοχής. Ένα HMIσ είναι απλώς η διεπαφή μεταξύ του μηχανήματος και του ανθρώπινου χειριστή.
Στην αρχιτεκτονική CPwE, οι συσκευές IACS επικοινωνούν με EtherNet / IP και ελέγχουν την κίνηση σε πραγματικό χρόνο σε όλο το κελί / περιοχή χρησιμοποιώντας Ethernet. Όπως φαίνεται στο Σχήμα 42, οι διακόπτες διανομής(distribution switches) μεταξύ της κυψέλης / περιοχής και βιομηχανικών ζωνών αποτελούν σημείο οριοθέτησης. Επειδή αυτοί οι διακόπτες διανομής αγγίζουν το ίδιο τμήμα Ethernet με τους διακόπτες πρόσβασης στο κελί / περιοχή, θεωρούνται επίσης συσκευές υποδομής κυψέλης / περιοχής και συνήθως απαιτούνται ανθεκτικές συσκευές. Ο διακόπτης διανομής είναι επίσης το σημείο οριοθέτησης μεταξύ του επιπέδου 2 και του επιπέδου 3.

Η βιομηχανική ζώνη(industrial zone), είναι ανάλογη με το επίπεδο 3 του μοντέλου αναφοράς IACS και είναι επίσης πολύ παρόμοια με ένα παραδοσιακό δίκτυο πανεπιστημιούπολης. Τα περισσότερα εργοστάσια έχουν μόνο μία βιομηχανική ζώνη. Όπως και με τα περισσότερα δίκτυα της πανεπιστημιούπολης, η βιομηχανική ζώνη ενσωματώνει διακόπτες πρόσβασης για λειτουργίες IT και βασικές λειτουργίες δικτύου. Επίσης, παρέχει συνδεσιμότητα δικτύου μέσω δρομολογημένων διακοπτών διανομής σε πολλαπλές ζώνες κυψέλης / περιοχής, όπως απαιτείται. Τέλος, υποστηρίζει δυνατότητες δρομολόγησης IP για συσκευές IACS που απαιτούν υποστήριξη εφαρμογών επιπέδου 3.

Η αποστρατικοποιημένη ζώνη (demilitarized zone DMZ), είναι η ζώνη που βρίσκεται μεταξύ των βιομηχανικών και επιχειρησιακών ζωνών και χρησιμοποιείται για την ασφαλή διαχείριση των ροών κίνησης μεταξύ δικτύων στις γειτονικές ζώνες. Αυτό είναι επίσης το σημείο όπου τυπικά εφαρμόζεται ένα τείχος προστασίας εγκαταστάσεων για τον έλεγχο της ροής κίνησης προς και έξω από το δίκτυο των εγκαταστάσεων.



Σχήμα 42: Αρχιτεκτονική CPwE με τρεις διαφορετικές ζώνες Ethernet κυψελών/περιοχών.

Κεφάλαιο 7.2 Πρωτόκολλα ελέγχου βιομηχανικού αυτοματισμού (Industrial Automation Control Protocols)

Τα συστήματα εφαρμογών βιομηχανικού αυτοματισμού χρησιμοποιούν ένα μοναδικό σύνολο πρωτοκόλλων για έλεγχο, κίνηση, συγχρονισμό και ασφάλεια. Η ανάπτυξη αυτών των βιομηχανικών πρωτοκόλλων ξεκίνησε πολύ πριν από την εποχή του Ethernet και της IP, αλλά τα τελευταία χρόνια έχουν γίνει προσπάθειες να προσαρμοστούν αυτά τα πρωτόκολλα αυτοματισμού για να επωφεληθούν από τα οφέλη των σύγχρονων μηχανισμών μεταφοράς. Ο κατάλογος των διαθέσιμων πρωτοκόλλων ελέγχου αυτοματισμού είναι πολύ μεγάλος, αλλά τα τρία με τη μεγαλύτερη υιοθέτηση είναι τα εξής:

- EtherNet / IP.
- PROFINET.
- Modbus / TCP.

Στις επόμενες δύο ενότητες αναφέρουμε περιληπτικά τα δύο πρωτόκολλα EtherNet / IP και PROFINET.

Κεφάλαιο 7.2.1 Πρωτόκολλο EtherNet / IP και CIP

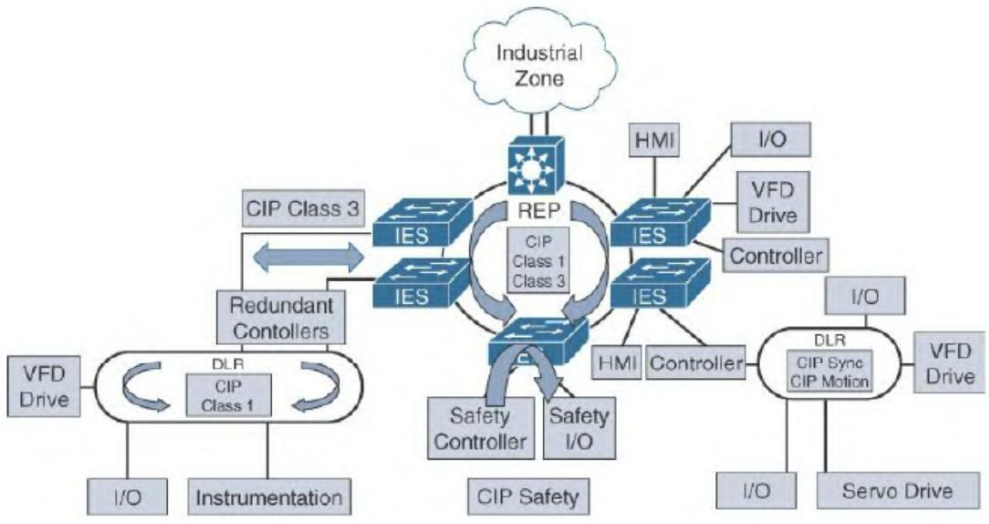
Το EtherNet / IP είναι ένα ανοιχτό πρότυπο για συστήματα βιομηχανικών αυτοματισμών που αναπτύχθηκε από τη Rockwell Automation και τώρα διαχειρίζεται η Open DeviceNet Vendors Association (ODVA). **Να σημειώσουμε**, ότι στην περίπτωση του EtherNet / IP, το «IP» σημαίνει «βιομηχανικό πρωτόκολλο» και όχι «πρωτόκολλο διαδικτύου».
Τα Βιομηχανικά Πρωτόκολλα χρησιμοποιούνται ειδικά για τον χειρισμό εφαρμογών βιομηχανικού αυτοματισμού, όπως αυτές για έλεγχο, ασφάλεια, κίνηση και διαμόρφωση.

Το EtherNet / IP προσαρμόζει το Κοινό Βιομηχανικό Πρωτόκολλο (Common Industrial Protocol CIP) σε τυπική τεχνολογία Ethernet και TCP / IP.
Το CIP είναι ένα πρωτόκολλο επικοινωνίας που χρησιμοποιείται για έλεγχο εισόδου / εξόδου, διαμόρφωση συσκευής και συλλογή δεδομένων σε συστήματα αυτοματισμού και ελέγχου. Περιλαμβάνει δυνατότητες για τους ακόλουθους τύπους επικοινωνιών:

Σιωπηρή ανταλλαγή μηνυμάτων(Implicit messaging): Αυτός ο τύπος μηνυμάτων περιλαμβάνει δεδομένα εισόδου / εξόδου σε πραγματικό χρόνο, λειτουργικά δεδομένα ασφάλειας, δεδομένα ελέγχου κίνησης και συχνά πολλαπλή εκπομπή UDP.

Ρητή ανταλλαγή μηνυμάτων(Explicit messaging): Αυτός ο τύπος μηνυμάτων περιλαμβάνει διαμόρφωση, διάγνωση και συλλογή δεδομένων και βασίζεται σε μηνύματα unicast TCP.

Το Σχήμα 43 απεικονίζει ένα δίκτυο παραγωγής βασισμένο στο EtherNet / IP. Το πρωτόκολλο REP χρησιμοποιείται ως μηχανισμός ανθεκτικότητας μεταξύ των βιομηχανικών διακοπτών Ethernet (IES) για τη μετάδοση μηνυμάτων CIP Class 1 (Ethernet πραγματικού χρόνου) και Class 3 (TCP).



Σχήμα 43: Ένα δίκτυο εργοστασίου βασισμένο στο EtherNet/IP.

Το EtherNet / IP καθορίζει επίσης ένα πρωτόκολλο πλεονασμού γνωστό ως Devel Level Ring (DLR), το οποίο χρησιμοποιείται όταν το σύστημα απαιτεί συνεχή λειτουργία και είναι σε θέση να επιτύχει επανασύγκλιση υψηλής ταχύτητας σε περίπτωση διακοπής δακτυλίου(ring break). Το DLR αναπτύσσεται βέλτιστα όταν οι συσκευές διαθέτουν ενσωματωμένο διακόπτη δύο θυρών και δεν απαιτούν ξεχωριστούς βιομηχανικούς διακόπτες Ethernet.

Κεφάλαιο 7.2.2 Πρωτόκολλο PROFINET

Το PROFINET (Process Field Net) είναι μια ευρέως χρησιμοποιούμενη βιομηχανική τεχνολογία για την ανταλλαγή δεδομένων μεταξύ ελεγκτών και συσκευών. Το PROFINET (σε αντίθεση με το Modbus TCP, το οποίο χρησιμοποιεί TCP για επικοινωνία μεταξύ συσκευών -απαιτώντας έτσι οι συσκευές να δημιουργούν και να διατηρούν μια σύνδεση υποδοχής TCP- ή το EtherNet / IP που χρησιμοποιεί UDP) είναι σε θέση να στέλνει και να λαμβάνει δεδομένα απευθείας στο επίπεδο εφαρμογής, χωρίς να περιμένουμε για επεξεργασία στη στοίβα TCP / IP, η οποία έχει τη δυνατότητα εισαγωγής μεταβλητής καθυστέρησης. Είναι πλήρως συμβατό με το τυπικό IEEE 802.3 Ethernet, πράγμα που σημαίνει ότι οι κανονικές συσκευές Ethernet μπορούν να συνυπάρχουν με συσκευές εισόδου / εξόδου PROFINET και ελεγκτές στο ίδιο τμήμα.

Οι αρχιτεκτονικές PROFINET αποτελούνται από τα ακόλουθα:

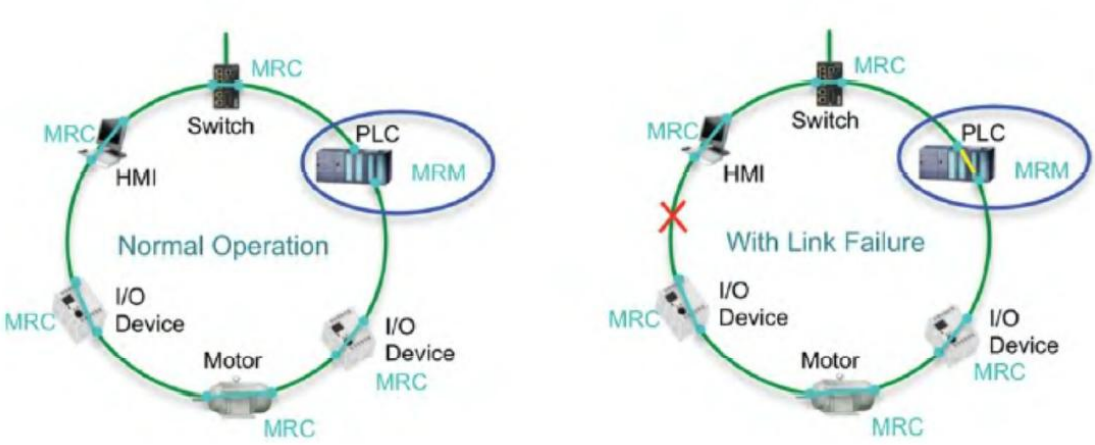
- Βιομηχανικές συσκευές αυτοματισμού(Industrial automation devices): περιλαμβάνουν ρομπότ, αισθητήρες, ενεργοποιητές και μονάδες δίσκου.

- HMIs: παρέχουν οπτικές αναφορές κατάστασης και έλεγχο των βιομηχανικών συσκευών αυτοματισμού.

- Ελεγκτές (Controllers): περιλαμβάνουν PLCs και κατανεμημένες συσκευές εισόδου/εξόδου.

Η αρχιτεκτονική PROFINET είναι παρόμοια από πολλές απόψεις με την αρχιτεκτονική CPwE. Συγκεκριμένα, παρόμοια με το CPwE, το PROFINET, αξιοποιεί το μοντέλο Purdue για ιεραρχία ελέγχου. Η ζώνη κελιού / περιοχής (Επίπεδα 0-2) είναι εκεί όπου η περισσότερη κίνηση PROFINET σε πραγματικό χρόνο κινείται μεταξύ συσκευών συστημάτων βιομηχανικού αυτοματισμού. Η άνω ζώνη παραγωγής λειτουργεί ως σημείο συνάθροισης για μία ή περισσότερες ζώνες κυψέλης / περιοχής. Επίσης, η αρχιτεκτονική PROFINET χρησιμοποιεί αυστηρές μεθόδους διαχωρισμού της κίνησης για την προστασία εφαρμογών βιομηχανικού αυτοματισμού από εξωτερικές και εσωτερικές διακοπές. Διαταραχές στο δίκτυο ελέγχου - ακόμη και σύντομες διάρκειας μόλις χιλιοστών του δευτερολέπτου - μπορούν να δημιουργήσουν σημαντικές επιπτώσεις στη λειτουργία μιας εγκατάστασης παραγωγής.

Όπως φαίνεται και στο Σχήμα 44, η ανθεκτικότητα του δικτύου(Network resiliency) είναι το κύριο ζητούμενο στην αρχιτεκτονική PROFINET. Όπως και με το CPwE, η ζώνη κελιού / περιοχής είναι η κύρια ζώνη όπου εκτελούνται οι περισσότερες από τις δραστηριότητες βιομηχανικού αυτοματισμού. Αυτή η ζώνη πρέπει να θεωρηθεί ως μια απομονωμένη οντότητα του περιβάλλοντος παραγωγής, όπου η διαθεσιμότητα και οι επιδόσεις είναι οι πιο σημαντικοί παράγοντες.



Σχήμα 44: Λειτουργία PROFINET MRP.

Κεφάλαιο 7.3 Υπηρεσίες ταυτότητας εργοστασιακής ασφάλειας

Καθώς οι μέθοδοι πρόσβασης στο βιομηχανικό δίκτυο επεκτείνονται, η πολυπλοκότητα της διαχείρισης της ασφάλειας πρόσβασης στο δίκτυο και του ελέγχου άγνωστων κινδύνων συνεχίζει να αυξάνεται. Τα δίκτυα IACS πρέπει να προστατεύονται από μη αξιόπιστους υπολογιστές, όπως αυτοί που χρησιμοποιούνται από εργολάβους ή συνεργάτες προμηθευτές.
Με τον πολλαπλασιασμό των συσκευών σε εργοστάσια παραγωγής και περιορισμένους επιχειρησιακούς πόρους, ο αντίκτυπος της αποτυχίας εντοπισμού και αποκατάστασης των απειλών για την ασφάλεια εισάγει σημαντικό κίνδυνο για τις εγκαταστάσεις σε ολόκληρο το εργοστάσιο. Οι υπηρεσίες ταυτότητας δικτύου παρέχουν ένα επιπλέον επίπεδο πρόσβασης και ελέγχου δικτύου προσδιορίζοντας τον τύπο του υπολογιστή, του λειτουργικού συστήματος και του χρήστη που έχει πρόσβαση στο δίκτυο. Με βάση την ταυτότητα και την εφαρμογή μιας αντίστοιχης πολιτικής, οι υπηρεσίες ταυτότητας είναι σε θέση να προωθήσουν τις πολιτικές ασφαλείας στην υποδομή δικτύου στην οποία έχει πρόσβαση ο υπολογιστής. Δεδομένου ότι οι υπηρεσίες ταυτότητας συνδέονται συνήθως με υπηρεσίες καταλόγου (όπως LDAP ή Microsoft Active Directory), η συνήθης πρακτική είναι η χρήση ενός κεντρικά διαχειριζόμενου μοντέλου υπηρεσιών ταυτότητας, με το τμήμα IT να διατηρεί τη διαχείριση του συστήματος ταυτότητας που λειτουργεί από τη βιομηχανική ζώνη.

Η αρχιτεκτονική ασφαλείας, πρέπει να υποστηρίζει τόσο τις ενσύρματες όσο και τις ασύρματες μεθόδους πρόσβασης από το προσωπικό της μονάδας και τους εργολάβους. Αυτό επιτυγχάνεται με την ανάπτυξη ενός κεντρικού συστήματος υπηρεσιών ταυτότητας που είναι ικανό να καθορίσει ένα όριο εμπιστοσύνης σε όλα τα σημεία πρόσβασης δικτύου. Αυτή η προσέγγιση παρέχει τα ακόλουθα οφέλη:

- Ολοκληρωμένη συγκεντρωτική πολιτική για πρόσβαση στο δίκτυο τόσο στις ζώνες παραγωγής όσο και στις επιχειρήσεις.
- Κανόνες και πολιτικές ελέγχου πρόσβασης.
- Υπηρεσίες πύλης επισκεπτών για εργολάβους και επισκέπτες.

Μέσω της ενσωμάτωσης ενός κεντρικού συστήματος ταυτότητας, οι πολιτικές μπορούν να εφαρμοστούν σε όλο το δίκτυο σε πραγματικό χρόνο, ώστε οι χρήστες να έχουν συνεπή πρόσβαση στις υπηρεσίες τους τόσο από ενσύρματες όσο και από ασύρματες συνδέσεις.

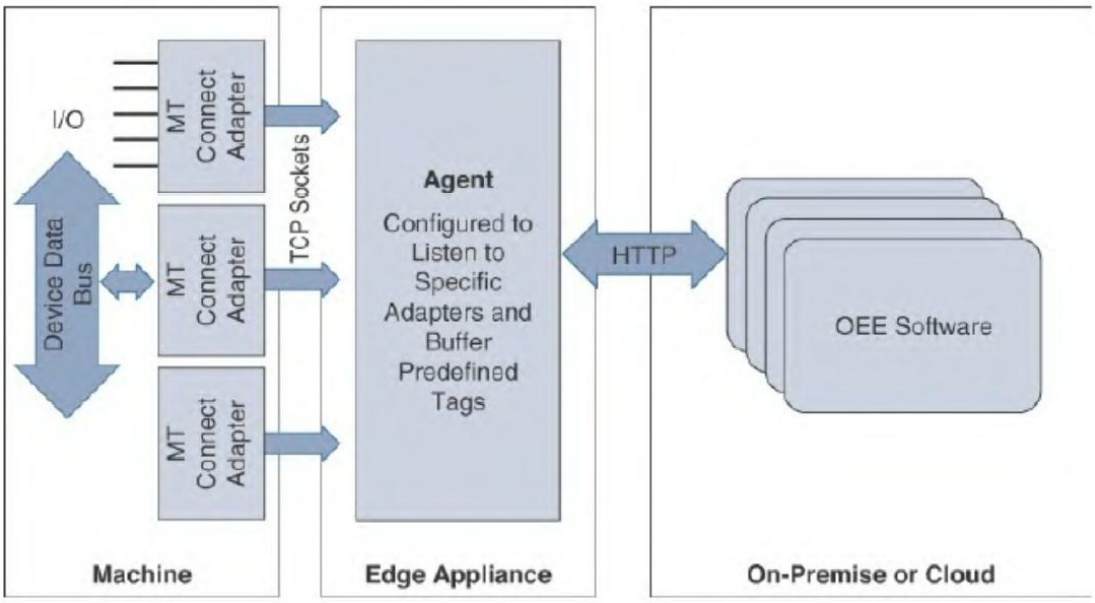
Επιπλέον, άγνωστες συσκευές κατευθύνονται σε έναν διοικητικά καθορισμένο ασφαλή προορισμό, χωρίς πρόσβαση σε τοπικούς πόρους στις εγκαταστάσεις ολόκληρης της εγκατάστασης, ενώ οι αξιόπιστες συσκευές έχουν πρόσβαση σε βασικές πλατφόρμες στη βιομηχανική ζώνη. Τα εργαλεία εξυπηρέτησης ταυτότητας επιτρέπουν επίσης κεντρικές υπηρεσίες πύλης επισκεπτών, καθώς και πολιτικές για την εγγραφή αυτοεξυπηρέτησης προσωπικού, πωλητών, συνεργατών και επισκεπτών.

Κεφάλαιο 7.4 Υπολογισμός άκρων στο Συνδεδεμένο Εργοστάσιο(Edge Computing in the Connected Factory)

Οι μηχανές που είναι εγκατεστημένες στο πάτωμα του εργοστασίου είναι ικανές να παράγουν τεράστιο όγκο δεδομένων. Ένας τρόπος με τον οποίο πολλά εργοστάσια αντιμετώπισαν αυτήν την πρόκληση είναι η ανάπτυξη υπολογιστών για τη συλλογή αυτών των δεδομένων. Η συλλογή δεδομένων από υπολογιστές στο πάτωμα του εργοστασίου έχει οδηγήσει σε προκλήσεις συντήρησης και ασφάλειας, καθώς κάθε υπολογιστής απαιτεί επιδιορθώσεις και αναβαθμίσεις λειτουργικού συστήματος. Οι αστοχίες υλικού είναι επίσης συχνές επειδή οι συσκευές συχνά δεν είναι ανθεκτικές για εργοστασιακές συνθήκες. Σαφώς, αυτή η προσέγγιση καθιστά πολύ δύσκολο για τις επιχειρήσεις να συγκεντρώσουν, να αφομοιώσουν και να ανταποκριθούν αποτελεσματικά στα δεδομένα. Μια τέτοια προσέγγιση είναι ένα σημαντικό εμπόδιο για την προβολή και τα κακώς επιχειρηματικά οφέλη που θα μπορούσαν να προκύψουν από την ανάλυση εργοστασιακών δεδομένων.

Η εξέλιξη της πληροφορικής όπως είναι λεγόμενο συνδεδεμένα μηχανήματα και υπολογισμός άκρων(Connected Machines and Edge Computing) βοηθά στην επίλυση αυτών των προβλημάτων. Η σύνδεση μηχανών(εγκατεστημένες στο πάτωμα του εργοστασίου) σε εφαρμογές απαιτεί μοντέλο επικοινωνίας και σχήμα δεδομένων που είναι επεκτάσιμο, ασφαλές και εύκολο στην εφαρμογή.
Έχουν αναπτυχθεί αρκετά πρωτόκολλα επικοινωνιών ανοικτής κατασκευής που παρέχουν διαλειτουργικότητα μεταξύ συσκευών και λογισμικού, επιτρέποντας να παρακολουθούμε και να συλλέγουμε δεδομένα από μηχανές εγκατεστημένες στο πάτωμα του εργοστασίου. Αυτά τα πρωτόκολλα βασίζονται γενικά σε XML ή HTTP.

Οι νέες εξελίξεις στις πλατφόρμες υπολογιστικών άκρων συνδυάζουν τη δυνατότητα αλλαγής, NAT, δρομολόγησης και ασφάλειας σε μία μόνο ανθεκτική συσκευή άκρης(single ruggedized edge appliance). Αυτή η προσέγγιση υπηρεσιών μειώνει το κόστος για ασφαλή συλλογή δεδομένων μηχανών και βελτιστοποιεί τους διαθέσιμους πόρους δικτύου και το εύρος ζώνης αναλύοντας δεδομένα πριν από τη διαβίβασή τους στο κέντρο δεδομένων ή στο cloud για περαιτέρω ανάλυση.
Η συσκευή άκρης περιλαμβάνει συνήθως ένα ανοιχτού κώδικα και αποτελεσματικό λειτουργικό σύστημα όπως το Linux, το οποίο εκτελεί μια εφαρμογή ροής ανάλυσης και τους απαιτούμενους τυπικούς παράγοντες δεδομένων που απαιτούνται για τους αντίστοιχους τύπους μηχανών.
Το Σχήμα 45 απεικονίζει τον προσαρμογέα υλικού(hardware adapter), του μηχανήματος που χρησιμοποιείται για τη διαβίβαση δεδομένων σε έναν παράγοντα στον κόμβο άκρης / άκρη της συσκευής για ανάλυση. Στη συνέχεια αποστέλλονται στο cloud για περαιτέρω ανάλυση μόνο επεξεργασμένα δεδομένα



Σχήμα 45: Μοντέλο συνδεδεμένου μηχανήματος βασισμένο στο MTConnect.

Κεφάλαιο 8 Πετρέλαιο και φυσικό αέριο

Καθώς η τεχνολογία έχει προχωρήσει, η βιομηχανία πετρελαίου και φυσικού αερίου έχει αρχίσει να καινοτομεί μέσω της σύνδεσης με τα περιουσιακά στοιχεία και τις γνώσεις που αποκτήθηκαν μέσω των παραγόμενων δεδομένων. Το πετρέλαιο και το φυσικό αέριο είναι από τους πιο κρίσιμους πόρους που χρησιμοποιούνται στη σύγχρονη κοινωνία. Σήμερα, η κύρια εστίαση των εταιρειών πετρελαίου και φυσικού αερίου είναι στους τρόπους μείωσης του κόστους, βελτίωσης της αποδοτικότητας και της ταχύτητας από τις υπάρχουσες επενδύσεις.
Μεταξύ των σημαντικότερων βασικών δεικτών απόδοσης (key performance indicators KPIs) της βιομηχανίας περιλαμβάνεται ο έλεγχος του κόστους παραγωγής και η βελτίωση της συνολικής υγείας και ασφάλειας επικίνδυνων περιβαλλόντων. Πρόκειται για μια βιομηχανία όπου ένας αυξανόμενος αριθμός κυβερνοεπιθέσεων θέτει σε κίνδυνο την ασφάλεια και δημιουργεί απώλειες. Αυτό συμβαίνει σε ένα πλαίσιο όπου οι βαθιές τεχνολογικές εξελίξεις διαταράσσουν τους παραδοσιακούς τρόπους εργασίας και οδηγούν τις γρήγορες αλλαγές στην παραγωγικότητα. Η αύξηση των δεδομένων, η προηγμένη ανάλυση, η αυξημένη αυτοματοποίηση και η συνδεσιμότητα φέρνουν μια αλλαγή στο πώς και πού επιτυγχάνεται η εργασία.

Όπως και με άλλες βιομηχανίες, οι εταιρείες πετρελαίου και φυσικού αερίου χρησιμοποιούν το IoT για μεγάλη ποικιλία εφαρμογών. Οι λύσεις IoT συμβάλλουν στην καλύτερη πρόσβαση στις υπάρχουσες πηγές δεδομένων, καθώς και στην εκπλήρωση των απαιτήσεων συμμόρφωσης και στην αύξηση της ασφάλειας των εργαζομένων. Η βιομηχανία πετρελαίου και φυσικού αερίου κατασκευάζει νέες λύσεις IoT για το συνδεδεμένο διυλιστήριο, το κέντρο ελέγχου, και τον αγωγό πετρελαίου. Αυτές οι λύσεις ακολουθούν το μοντέλο Purdue για τον έλεγχο της ιεραρχίας, το οποίο βοηθά στον προσδιορισμό των αρχιτεκτονικών επιπέδων και των ζωνών ασφαλείας. Λόγω της φύσης των εγκαταστάσεων πετρελαίου και φυσικού αερίου και των χώρων εργασίας, η ασύρματη τεχνολογία χρησιμοποιείται ευρέως για τη σύνδεση αισθητήρων και βιομηχανικών συστημάτων ελέγχου.

Το Wi-Fi και τα ασύρματα συστήματα όπως το ISA100.11 και το WirelessHART είναι δημοφιλή σε αυτόν τον κλάδο και επιλύουν πολύ συγκεκριμένες προκλήσεις.

Οι εφαρμογές IoT στους κλάδους πετρελαίου και φυσικού αερίου αναφέρονται:

- Στη παρακολούθηση της κατάστασης ή της συμπεριφοράς των βιομηχανικών συσκευών προκειμένου να παρέχεται ορατότητα και έλεγχος.
- Στη βελτιστοποίηση διαδικασιών και χρήσης πόρων.
- Στη βελτίωση της λήψης επιχειρηματικών αποφάσεων.

Αυτό το κεφάλαιο διερευνά το IoT στο πετρέλαιο και το φυσικό αέριο και πώς η ψηφιοποίηση είναι μια εξέλιξη σε αυτόν τον κλάδο. Εξετάζει περιπτώσεις χρήσης και καινοτόμες αρχιτεκτονικές που χρησιμοποιούνται για την ψηφιοποίηση αυτής της βιομηχανίας.

Επίσης γίνεται αναφορά:

- Στην εισαγωγή στη βιομηχανία πετρελαίου και φυσικού αερίου και περιγράφει τους βασικούς παράγοντες της αγοράς σε αυτόν τον κλάδο.
- Στις βασικές προκλήσεις που αντιμετωπίζει η βιομηχανία πετρελαίου και φυσικού αερίου, μερικές από τις οποίες επηρεάζονται από τις παγκόσμιες οικονομικές συνθήκες, καθώς και πώς οι νέες τεχνολογίες διαταράσσουν παλαιότερους τρόπους πρακτικής.
- Στη βελτίωση της λειτουργικής απόδοσης, και τις τεχνολογίες που χρησιμοποιούνται σε συστήματα IoT πετρελαίου και φυσικού αερίου.
- Στα βασικά ζητήματα ασφάλειας στη βιομηχανία πετρελαίου και φυσικού αερίου, καθώς και πώς μπορούν να αντιμετωπιστούν με τη σωστή μεθοδολογία σχεδιασμού.

Κεφάλαιο 8.1 Εισαγωγή στη βιομηχανία πετρελαίου και φυσικού αερίου

Ένας από τους σημαντικότερους παράγοντες που επηρεάζουν τη βιομηχανία πετρελαίου και φυσικού αερίου είναι η αστάθεια των τιμών. Στο επίκεντρο αυτής της αστάθειας βρίσκεται η ανισορροπία προσφοράς και ζήτησης. Οι κλιματικές πολιτικές χαμηλών εκπομπών άνθρακα δημιουργούν έναν κόσμο πλούσιο σε πόρους. Οι τεχνολογίες ανανεώσιμων πηγών ενέργειας(ένα κρίσιμο στοιχείο του πυλώνα χαμηλού άνθρακα του παγκόσμιου ενεργειακού εφοδιασμού), κερδίζουν γρήγορα έδαφος, βοηθούμενες από τις παγκόσμιες επιδοτήσεις και πολιτικές για το κλίμα. Σε πολλά μέρη του κόσμου, αυτή η τάση είχε ως αποτέλεσμα τη μείωση της ζήτησης για συμβατικές πρωτογενείς πηγές ενέργειας, συμπεριλαμβανομένου του πετρελαίου, του φυσικού αερίου και του άνθρακα.

Οι αγορές ενέργειας είναι ιδιαίτερα ευμετάβλητες, συχνά λόγω της ανισορροπίας μεταξύ προσφοράς και ζήτησης ενέργειας. Πολλές από τις χώρες παραγωγής πετρελαίου αντλούν πετρέλαιο σε επίπεδα ρεκόρ, οδηγώντας σε χαμηλές παγκόσμιες τιμές ενέργειας. Αυτή η κατάσταση έχει οδηγήσει σε σημαντική εστίαση στο κόστος, την αποδοτικότητα και την ταχύτητα, με τις εταιρείες πετρελαίου και φυσικού αερίου να προσπαθούν να επωφεληθούν περισσότερο από τις υπάρχουσες επενδύσεις τους και να αντισταθούν σε νέες. Η βιομηχανία πετρελαίου και φυσικού αερίου αντιμετωπίζει προκλήσεις, πολλές από τις οποίες επηρεάζονται από τις παγκόσμιες οικονομικές συνθήκες.

Επιπλέον, οι νέες τεχνολογίες φέρνουν νέες προκλήσεις και ευκαιρίες. Το IoT και η ψηφιοποίηση ανοίγουν το δρόμο σε νέες βελτιώσεις στην αποδοτικότητα και νέα επιχειρηματικά μοντέλα.

Στην έκθεσή της για το 2014 η Gartner εντόπισε τις ακόλουθες βασικές τάσεις ψηφιοποίησης:

- Με Προηγμένη ανάλυση και μοντελοποίηση (σχεδιασμός και βελτιστοποίηση επιχειρηματικών περιουσιακών στοιχείων).
- Σε μεγάλα δεδομένα (σχεδιασμός και βελτιστοποίηση επιχειρηματικών περιουσιακών στοιχείων).
- Στη σύγκλιση IT / OT (ψηφιακά κοιτάσματα πετρελαίου).
- Σε έξυπνα μηχανήματα (ψηφιακά πεδία πετρελαίου).
- Στην εκτεταμένη υποδομή (ψηφιακά κοιτάσματα πετρελαίου).
- Στη κινητικότητα (διαισθητική ροή εργασίας).
- Σε ανώτερες σουίτες μοντελοποίησης (διαισθητική ροή εργασίας).
- Στη συνεργασία (διαισθητική ροή εργασίας).
- Στο Cloud (επιχειρησιακά συστήματα πετρελαίου και φυσικού αερίου).
- Στη διαχείριση απόδοσης περιουσιακών στοιχείων (επιχειρησιακά συστήματα πετρελαίου και φυσικού αερίου)

Οι κύριες προκλήσεις της βιομηχανίας πετρελαίου και φυσικού αερίου μπορούν να χωριστούν σε τρεις κύριες κατηγορίες και οι οποίες αναφέρονται στη:
Α.) Λειτουργική αποδοτικότητα και μείωση κόστους.
Β.) Ασφάλεια.
Γ.) Γρηγορότερη και καλύτερη λήψη αποφάσεων.

Αυτές οι προκλήσεις παρουσιάζονται στον Πίνακα 7 και ανάγκασαν τη βιομηχανία να υιοθετήσει νέες τεχνολογίες που επέφεραν βελτιώσεις στους τομείς της ασφάλειας, του χρόνου διακοπής, της αποδοτικότητας, της προστασίας του περιβάλλοντος και της ακεραιότητας των περιουσιακών στοιχείων.

Security in a context of sophisticated attacks	
■ Secure operations	■ Patch management ■ Compliance monitoring ■ Secure remote access
■ Network reliability	■ Availability ■ Scalability ■ Data management ■ Bandwidth ■ QoS ■ Cybersecurity
■ Asset safety and security	■ Physical safety and security ■ Protection against overpressures ■ Shutdown management
■ People safety and security	■ People monitoring and worker down tracking ■ Physical safety and security
■ Business continuity	■ Operations dashboard and remediation ■ Process automation
■ Cybersecurity risk and vulnerabilities	■ Intrusion prevention and detection ■ Proactive incident monitoring
Improved decision making in a context of data storm	
■ Faster and better decision making	■ Data analytics ■ Decentralized computing and data storage
■ Knowledge management and skills shortage	■ People training ■ Knowledge management

Πίνακας 7: Προκλήσεις και απαιτήσεις της βιομηχανίας πετρελαίου και φυσικού αερίου.

Κεφάλαιο 8.2 IoT και η βιομηχανία πετρελαίου και φυσικού αερίου

Η βιομηχανία πετρελαίου και φυσικού αερίου ήταν ένας από τους πρώτους βιομηχανικούς τομείς που άρχισαν να αξιοποιούν τη δύναμη της τεχνολογίας. Η φύση των δραστηριοτήτων, των διαδικασιών και της εξάρτησής της από τα δεδομένα έχει αναγκάσει την ευρεία χρήση της ανάλυσης δεδομένων, από τεχνικές εξερεύνησης έως βιομηχανική προληπτική συντήρηση και όχι μόνο. Σε γενικές γραμμές, τα κοιτάσματα πετρελαίου και φυσικού αερίου είναι επικίνδυνες ζώνες για τον άνθρωπο, επομένως η ύψιστη σημασία δίνεται στην υγεία, την ασφάλεια και το περιβάλλον.

Σε αυτό το πλαίσιο, η κατοχή δυνατοτήτων ψηφιακής νοημοσύνης με επικοινωνία από μηχανή σε μηχανή μπορεί να βοηθήσει στην επίτευξη λειτουργιών χωρίς την ανάγκη

φυσικής ανθρώπινης παρουσίας, καθιστώντας έτσι το περιβάλλον ασφαλέστερο.Συνεπώς, το IoT είναι απαραίτητο για αυτόν τον κλάδο.

Το IoT και η ψηφιοποίηση επιφέρουν σημαντικές βελτιώσεις στη βιομηχανία πετρελαίου και φυσικού αερίου. Συγκεκριμένα συμβάλουν:

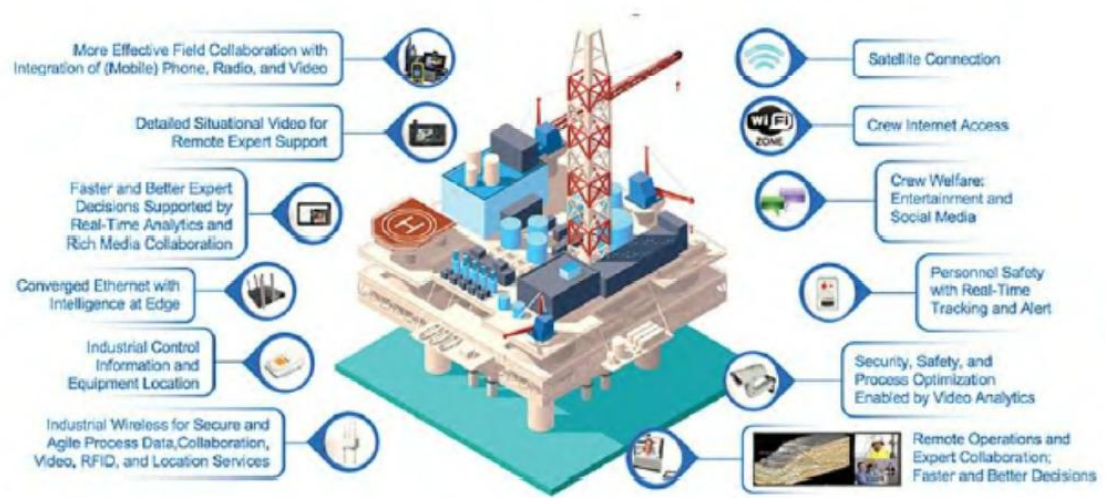
- Στη δυνατότητα απόκτησης εφικτών δεδομένων. Οι οικονομικά αποδοτικές τεχνολογίες επικοινωνίας, όπως το βιομηχανικό Wi-Fi, το LTE και το LoRa, δίνουν τη δυνατότητα στη βιομηχανία να αποκτήσει δεδομένα από ορισμένα περιουσιακά στοιχεία είτε για πρώτη φορά είτε σε πραγματικό χρόνο.
- Στο περιορισμό των κινδύνων. Οι αναλύσεις, μπορούν να χρησιμοποιηθούν για τη μετατροπή δεδομένων σε πραγματικό χρόνο που δημιουργούνται από την υποδομή IoT σε προβλέψιμες και λειτουργικές γνώσεις που διευκολύνουν ταχύτερες και καλύτερες αποφάσεις, αυξημένη ασφάλεια των εργαζομένων και βελτιωμένη ασφάλεια στον κυβερνοχώρο.
- Στη βελτίωση της παραγωγικότητας. Αξιοποιώντας τόσο το IoT όσο και τα συστήματα συνεργασίας για την επέκταση της σπάνιας εμπειρογνωμοσύνης σε απομακρυσμένες τοποθεσίες, την παροχή πληροφοριών σε πραγματικό χρόνο στις σωστές ομάδες τη σωστή στιγμή και την παροχή ενός αποτελεσματικού μηχανισμού για την προσέλκυση και εκπαίδευση της επόμενης γενιάς εργαζομένων.
- Στη κερδοφόρα ανάπτυξη. Η ανάπτυξη μπορεί να επιτευχθεί με τον μετασχηματισμό των επιχειρηματικών διαδικασιών μέσω του IoT.

Στις παρακάτω υποενότητες, αναφέρονται μερικές περιπτώσεις χρήσεως του IoT σε τομεις του πετρελαίου και φυσικού αερίου

Κεφάλαιο 8.2.1 Πεδίο πετρελαίου(connected oil field)

Η βελτίωση της λειτουργικής αποδοτικότητας αποτελεί βασικό στοιχείο για πολλά στελέχη της βιομηχανίας, ειδικά λαμβάνοντας υπόψη το κόστος που συνεπάγεται η εξερεύνηση και η εξόρυξη υδρογονανθράκων, από την επεξεργασία έως τη διανομή του τελικού προϊόντος στον τελικό καταναλωτή.
Σε μια προσπάθεια μείωσης του κόστους και αύξησης της αποδοτικότητας, οι αρχιτεκτονικές του IoT πρέπει να προσαρμοστούν σε διαφορετικές περιπτώσεις χρήσης σε βασικούς τομείς πετρελαίου και φυσικού αερίου, συμπεριλαμβανομένου του συνδεδεμένου διυλιστηρίου, του συνδεδεμένου πετρελαίου και του συνδεδεμένου αγωγού. Αυτές οι περιπτώσεις χρήσης απεικονίζουν τον τρόπο με τον οποίο η τεχνολογία μπορεί να υιοθετηθεί στη λειτουργική ροή της βιομηχανίας πετρελαίου και φυσικού αερίου, προκειμένου να βελτιστοποιηθεί η παραγωγικότητα, να μειωθεί το κόστος και να γίνει πιο γρήγορη η διαδικασία της επιχειρησιακής απόφασης.

Χαρακτηριστικό παράδειγμα αρχιτεκτονικής IoT που δημιουργήθηκε για να υποστηρίξει τη βιομηχανία πετρελαίου και φυσικού αερίου είναι το συνδεδεμένο πεδίο πετρελαίου(connected oil field) , όπως φαίνεται στο Σχήμα 46.



Σχήμα 46: IoT και η χρήση του σε περιπτώσεις πετρελαίου και φυσικού αερίου .

Ως πεδίο πετρελαίου ορίζεται μια περιοχή, είτε χερσαία είτε υπεράκτια, όπου ορισμένα πηγάδια εξάγουν αργό πετρέλαιο κάτω από το έδαφος ή από τον βυθό. Συνήθως, τα υπεράκτια κοιτάσματα πετρελαίου βρίσκονται σε απομακρυσμένες περιοχές ή στη μέση της θάλασσας, καθιστώντας δύσκολη την πρόσβαση και την επικοινωνία με αυτά.
Ως αποτέλεσμα, η ανάγκη για μια ισχυρή αλλά αυτόνομη υποδομή επικοινωνιών είναι σημαντική. Η υποδομή της υπεράκτιας εξέδρας πετρελαίου πρέπει να υποστηρίζει την επίγνωση της κατάστασης για τη λειτουργία του συστήματος γεώτρησης, την επικοινωνία με τα κεντρικά γραφεία και τα συστήματα παρακολούθησης της υγείας, της ασφάλειας και του περιβάλλοντος. Επίσης, επειδή το προσωπικό που εργάζεται στον πετρελαϊκό χώρο ζει στις εγκαταστάσεις για μεγάλο χρονικό διάστημα, απαιτούνται επίσης επικοινωνίες για ψυχαγωγικούς σκοπούς και κοινωνικούς σκοπούς. Λόγω της απομακρυσμένης και απομονωμένης φύσης των κοιτασμάτων πετρελαίου, μεγάλο μέρος της υποδομής επικοινωνίας τους βασίζεται στην ασύρματη τεχνολογία.

Κεφάλαιο 8.2.2 Πεδίο Διυλιστηρίου (Refinery)

Τα διυλιστήρια και οι μονάδες επεξεργασίας είναι συνήθως μεγάλα συγκροτήματα με πολλαπλά κτίρια, δεξαμενές αποθήκευσης και διασυνδεδεμένα υπόγεια και υπέργεια συστήματα σωληνώσεων. Λειτουργούν σε καθημερινή βάση ασταμάτητα(24x7), με σύνθετα συστήματα να παρακολουθούν συνεχώς παραμέτρους λειτουργίας, όπως είναι η ροή, το επίπεδο δεξαμενής, η θερμοκρασία, κραδασμοί, πίεση, ακόμη και την παρουσία επικίνδυνων ή εκρηκτικών αερίων που παράγονται κατά τη διαδικασία διύλισης αργού λαδιού. Το Σχήμα 47 επισημαίνει μερικές από τις κοινές περιπτώσεις χρήσης IoT σε ένα σύγχρονο διυλιστήριο πετρελαίου ή φυσικού αερίου.

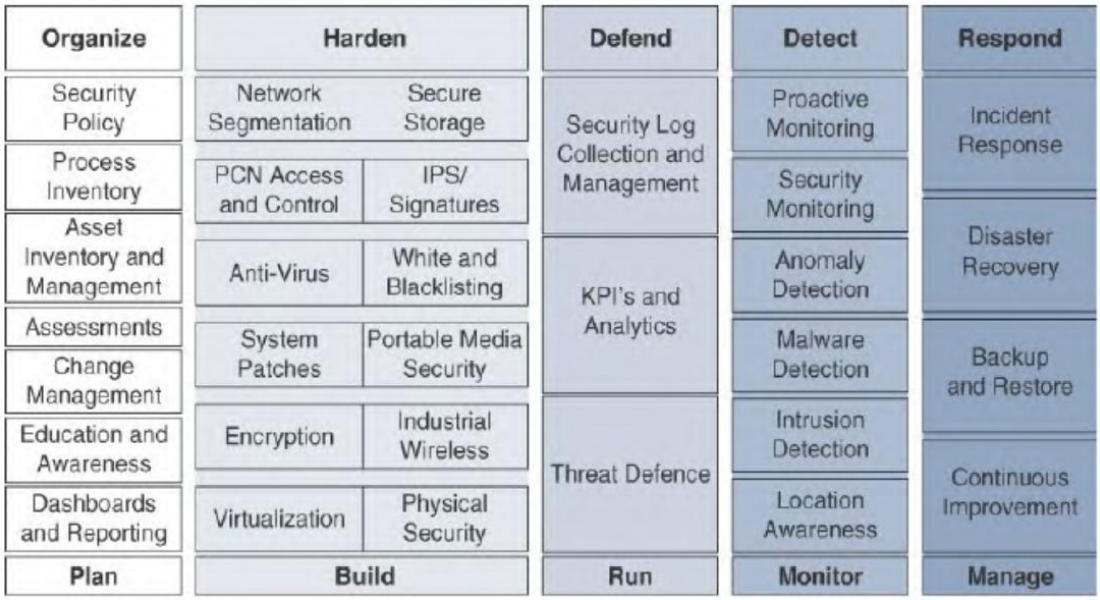
Σχήμα 47: IoT και η χρήση του σε περιπτώσεις σύγχρονου Δυιλιστηρίου πετρελαίου και φυσικού αερίου.

Τα διυλιστήρια είναι χώροι εργασίας για μόνιμο προσωπικό, εξωτερικές εταιρείες και εργολάβους που εργάζονται μέσα στο χώρο αυτό. Οι φορείς ελέγχου διασφαλίζουν ότι το διυλιστήριο λειτουργεί όπως πρέπει. Τα διυλιστήρια περιλαμβάνουν επίσης προσωπικό συντήρησης που διατηρεί τον εξοπλισμό του διυλιστηρίου σε καλή κατάσταση λειτουργίας και πραγματοποιεί επισκευές όταν χρειάζεται. Όλα αυτά τα συστήματα και οι άνθρωποι συνεχίζουν να εργάζονται με αποτελεσματικό, αποδοτικό και ασφαλή τρόπο μέσω της εφαρμογής συστημάτων ελέγχου, ασφάλειας και διαχείρισης. Αυτά τα συστήματα απαιτούν συστήματα επικοινωνιών που είναι γρήγορα και αξιόπιστα.

Κεφάλαιο 8.3 Πλαίσιο ελέγχου κινδύνων για την ασφάλεια στον κυβερνοχώρο στο IoT

Καθώς οι εταιρείες πετρελαίου και φυσικού αερίου συνεχίζουν να υιοθετούν νέες τεχνολογίες, καινούριες και διαφορετικές συσκευές συνδέονται σε δίκτυα. Αυτό οδηγεί στην πιθανή πρόκληση επιθέσεων ασφαλείας (σκόπιμες, ακούσιες, εξωτερικές και εσωτερικές) και οι εταιρείες πρέπει να αντιμετωπίσουν τους πιθανόν κινδύνους που προκύπτουν. Επιπλέον, η ανάγκη για καλύτερη ροή πληροφοριών και λήψη αποφάσεων απαιτεί τη διασύνδεση βιομηχανικών δικτύων με συστήματα και εφαρμογές δεδομένων.
Η αναφορά, η παρακολούθηση της συμμόρφωσης και ο έλεγχος της κατάστασης των συστημάτων που αναπτύσσονται στο περιβάλλον PCN(Process Control Network) μπορούν να παρέχουν τις απαραίτητες πληροφορίες για το επίπεδο κινδύνου και έκθεσης του περιβάλλοντος OT ανά πάσα στιγμή.
Η εξοικονόμηση κόστους είναι εξίσου σημαντική κινητήρια δύναμη, μαζί με τη βελτιωμένη παρακολούθηση και τη δυνατότητα διευκόλυνσης της επιχειρηματικής ευελιξίας μέσω ασφαλών, ευέλικτων και τυποποιημένων πλατφορμών. Η δυνατότητα ενημέρωσης με ασφάλεια των λειτουργικών συστημάτων μπορεί να μειώσει σημαντικά τα λειτουργικά έξοδα. Όλες αυτές οι εξελίξεις ανέδειξαν τη σημασία της κυβερνοασφάλειας, καθιστώντας την μία από τις κορυφαίες προτεραιότητες στη βιομηχανία πετρελαίου και φυσικού αερίου.

Ένα πλαίσιο ελέγχου κινδύνων(Risk Control Framework) χρησιμοποιείται για τα PCNs για την καλύτερη ασφάλεια των συστημάτων OT. Αυτό το πλαίσιο χαρτογραφεί ένα σύνολο πρακτικών και ελέγχων για την καταπολέμηση των πιο σημαντικών φορέων επίθεσης στο PCN. Αυτοί οι έλεγχοι και οι πρακτικές απεικονίζονται στο Σχήμα 48



Σχήμα 48: Πλαίσιο ελέγχου PCN Risk Control.

Χρησιμοποιώντας το πλαίσιο ελέγχου του κινδύνου, είναι δυνατό ένα πιο ισχυρό επίπεδο ασφάλειας. Αυτό το πρότυπο επιδιώκει να ενεργοποιήσει τη συνδεσιμότητα συστημάτων, διασφαλίζοντας παράλληλα ότι η συνδεσιμότητα χειρίζεται με ασφάλεια και περιορίζει την ικανότητα ενός εισβολέα να εκμεταλλεύεται συστήματα.

Οι κύριοι τομείς στους οποίους απευθύνεται το πλαίσιο ελέγχου του κινδύνου κατηγοριοποιούνται ως πέντε κύριοι πυλώνες:

1 Οργάνωση(Organize): Στο πλαίσιο της φάσης προγραμματισμού, οι πολιτικές και οι διαδικασίες πρέπει να καθιερωθούν και να ακολουθηθούν καθ 'όλη τη διάρκεια του κύκλου ζωής ενός δικτύου ή συστήματος, με τα απαραίτητα επίπεδα πίνακα εργαλείων και αναφορές να τα συμπληρώνουν. Η απογραφή των εξαρτημάτων που περιλαμβάνουν διάφορα συστήματα πρέπει να είναι ακριβής και λεπτομερής.
2 Harden: Αυτός ο πυλώνας περιλαμβάνει την εφαρμογή της τμηματοποίησης του δικτύου, η οποία διαχωρίζει περιβάλλοντα IT και OT και ελέγχει τη ροή επικοινωνίας μεταξύ τους. Η επιδιόρθωση συστήματος, η προστασία AV και η φορητή ασφάλεια μέσων διασφαλίζουν προστασία από γνωστές απειλές, ενώ η φυσική ασφάλεια εμποδίζει την πρόσβαση σε εξοπλισμό από μη εξουσιοδοτημένα άτομα.
3 Ανίχνευση(Detect): Αυτό είναι μέρος της φάσης παρακολούθησης, κατά την οποία γίνεται αναζήτηση οποιασδήποτε ανώμαλης συμπεριφοράς εντός του PCN. Προσδιορίζονται στοιχεία ελέγχου για τον εντοπισμό κακόβουλου λογισμικού ή άλλων απειλών ασφαλείας.
4 Προστασία(Defend): Οι περιοχές που περιλαμβάνονται σε αυτόν τον πυλώνα διασφαλίζουν ότι υπάρχει επαρκής συλλογή δεδομένων, τα οποία μπορούν να αναλυθούν για τον προσδιορισμό των απειλών και των απαντήσεων σε αυτές.
5 Απάντηση(Respond): Ο τελευταίος πυλώνας είναι υπεύθυνος για τη διασφάλιση της απαραίτητης υγιεινής, με την εφαρμογή των σωστών πολιτικών δημιουργίας αντιγράφων ασφαλείας και αποκατάστασης και αποκατάστασης καταστροφών.

Το πλαίσιο ελέγχου των κινδύνων για τα PCNs παρέχει μέτρα άμυνας για την οργάνωση, τον αποκλεισμό, τη συλλογή, την υπεράσπιση, τον εντοπισμό και την απάντηση σε απειλές για την ασφάλεια στον κυβερνοχώρο.

Κεφάλαιο 9 Utilities

Τα utilities αποτελούν βασικό στήριγμα του σύγχρονου κόσμου. Είτε πρόκειται για ηλεκτρική ενέργεια, είτε για φυσικό αέριο είτε για το νερό, τα utilities παρέχουν υπηρεσίες που διαχειρίζονται τις πόλεις, τις επιχειρήσεις και, μάλιστα, ολόκληρη την οικονομία. Ενώ τα βοηθητικά προγράμματα(utilities) σε όλο τον κόσμο βασίζονται σε μεγάλο βαθμό σε παλαιά τεχνολογία και πρωτόκολλα, επαναστατικές τεχνολογίες(disruptive technologies) και νέες απαιτήσεις στο ηλεκτρικό δίκτυο τα καθιστούν ως από τους πρώτους υιοθετητές του IoT. Η αξιόπιστη ηλεκτρική ενέργεια είναι απαραίτητη για τον σύγχρονο πολιτισμό.

Σε αυτό το κεφάλαιο γίνεται μια αναφορά:

- Στά διάφορα στοιχεία της αρχιτεκτονικής του GridBlocks. Το GridBlocks χωρίζει διάφορες λειτουργίες του ηλεκτρικού δικτύου σε 11 επίπεδα, επιτρέποντας στα ψηφιακά προγράμματα να ψηφιοποιηθούν με συστηματικό και μεθοδικό τρόπο, συμπεριλαμβανομένου του πρωτογενούς υποσταθμού GridBlock.
- Στη χρήση του SCADA και στην κατεύθυνση της τυποποίησης μέσω του προτύπου IEC 61850.
- Στο δίκτυο περιοχής GridBlock, συμπεριλαμβανομένου του τρόπου με τον οποίο οι ανεμιστήρες πολλαπλών χρήσεων οδηγούν ένα δίκτυο διανομής πολλαπλών υπηρεσιών.
- Στην ασφάλεια Έξυπνου Πλέγματος(Smart Grid Security). Διερευνά έννοιες όπως ασφάλεια SCADA, NERC CIP και πρακτικές ασφάλειας για το δίκτυο διανομής.

Κεφάλαιο 9.1 Βιομηχανία κοινής ωφελείας(Power Utility Industry) - Διαίρεση IT / OT στα Utilities

Καθώς οι φθηνές και αξιόπιστες σειριακές επικοινωνίες έγιναν ευρέως διαθέσιμες, προέκυψαν περισσότερες δυνατότητες, σε χαμηλότερες τιμές, επιτρέποντας ευρεία ανάπτυξη. Δεδομένης της μακροζωίας των συστημάτων ηλεκτρικού ελέγχου και παρακολούθησης, καθώς και της τεράστιας κλίμακας δικτύων κοινής ωφέλειας(utility networks), δεν είναι απλά οικονομικό να αντικατασταθούν όλα τα παλαιά συστήματα κοινής ωφέλειας όταν διατίθενται νέες τεχνολογίες. Εγκατάσταση νέων συστημάτων με νέες δυνατότητες και χαμηλότερες τιμές εξοπλισμού, επιφέρουν μεγαλύτερη αξιοπιστία και οφέλη κόστους στις επιχειρήσεις κοινής ωφέλειας.

Ενώ τα δίκτυα OT δεν είναι τόσο ευέλικτα όσο τα αντίστοιχα IT, τα τμήματα μηχανικής OT προσαρμόζονται συνεχώς για να επωφελούνται από νεότερες τεχνολογίες που υποστηρίζουν το ηλεκτρικό δίκτυο. Αυτό περιλαμβάνει την ανάπτυξη τρόπων υποστήριξης πολλών παλαιών συστημάτων σε νέα δίκτυα. Οι μηχανικοί OT αναζητούν καλύτερους και πιο οικονομικούς τρόπους για να κάνουν πράγματα. Αυτό συχνά περιλαμβάνει τη χρήση τεχνολογίας IT όποτε είναι δυνατόν. Η τεχνολογία IT έχει το πλεονέκτημα της ευρείας υιοθέτησης στον κλάδο, πράγμα που σημαίνει ότι είναι εύκολο να βρεθούν εξειδικευμένα άτομα για να σχεδιάσουν και να υποστηρίξουν δίκτυα και διακομιστές εφαρμογών. Η πρόκληση ήταν(και συνεχίζει να είναι), η κατανόηση των φυσικών συστημάτων OT και η διασφάλιση ότι είναι δυνατή η διασύνδεση με την τεχνολογία IT, η οποία βασίζεται κυρίως στην τεχνολογία δικτύωσης IP.

Καθώς τα δίκτυα κοινής ωφέλειας OT αρχίζουν να μετακινούνται σε επικοινωνίες IP και χρησιμοποιούν αρχιτεκτονικές IoT, τα μεγέθη των δικτύων OT γίνονται τάξεις μεγέθους μεγαλύτερα από αυτά των αντίστοιχων IT.

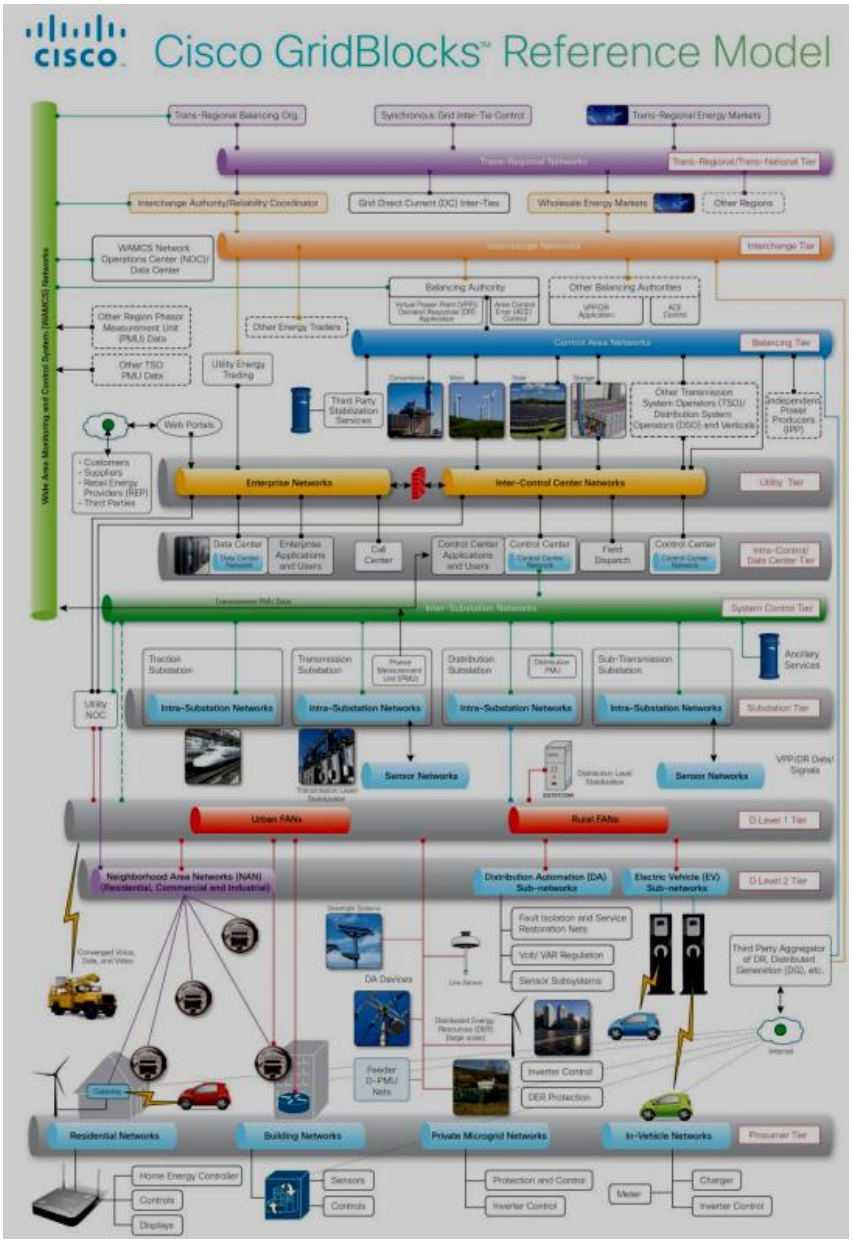
Στο παρελθόν, το IT και το OT ήταν εντελώς ξεχωριστές ομάδες. Σήμερα, καθώς τα δίκτυα συγκλίνουν, το OT και το IT πρέπει να συνεργάζονται στενά. Ορισμένοι μηχανικοί OT μαθαίνουν τις δεξιότητες IP που απαιτούνται για τη δημιουργία και την υποστήριξη πολύπλοκων συστημάτων OT και οι μηχανικοί IT μαθαίνουν σημαντικές πτυχές του βασικού συστήματος OT.
Αυτές οι προκλήσεις έχουν ξεκινήσει την εποχή του έξυπνου δικτύου που είναι συνδυασμός ηλεκτρικού δικτύου και της τεχνολογίας πληροφοριών και επικοινωνιών (information and communications technology ICT), με στόχο την αποτελεσματική παροχή βιώσιμων, οικονομικών και ασφαλών προμηθειών ηλεκτρικής ενέργειας.

Η βιομηχανία κοινής ωφελείας αντιμετωπίζει τώρα την πρόκληση της ανάπτυξης νέων βιομηχανικών προτύπων που επιτρέπουν την ασφαλή διασύνδεση εκατομμυρίων συσκευών υποσταθμών και διανομής OT στο επιχειρησιακό δίκτυο IT. Για να επιτευχθεί αυτό με επιτυχία, πρέπει να ακολουθηθεί μια αρχιτεκτονική προσέγγιση. Το μοντέλο αναφοράς GridBlocks παρέχει μια τέτοια αρχιτεκτονική για βοηθητικά προγράμματα.

Κεφάλαιο 9.2 Μοντέλο αναφοράς GridBlocks

Η Cisco ήταν μία από τις πρώτες εταιρείες που αναγνώρισαν ότι ήταν απαραίτητη μια συστηματική αρχιτεκτονική για την ενσωμάτωση συστημάτων σε όλα τα στάδια της αλυσίδας εφοδιασμού ηλεκτρικού ρεύματος σε σύγχρονα συστήματα επικοινωνιών. Η αρχιτεκτονική πρέπει να λάβει υπόψη τον γρήγορο εκσυγχρονισμό των τεχνολογιών έξυπνου δικτύου, ενώ ταυτόχρονα υποστηρίζει μια σειρά από παλιές τεχνολογίες που είναι πιθανό να υπάρχουν για πολλά χρόνια στο μέλλον. Το μοντέλο αναφοράς που ανέπτυξε ήταν το GridBlocks.

Παρόλο που υπάρχουν και άλλα μοντέλα αναφοράς, το GridBlocks είναι εύκολο τόσο για αρχάριους όσο και για προχωρημένους χρήστες. Το μοντέλο αναφοράς GridBlocks, που φαίνεται στο Σχήμα 49, απεικονίζει ολόκληρη την αλυσίδα εφοδιασμού ηλεκτρικής ενέργειας από ευρείας περιοχής παραγωγής ενέργειας, κέντρα ελέγχου, δίκτυα μεταφοράς, υποσταθμούς και δίκτυα διανομής.



Σχήμα 49: Αρχιτεκτονική αναφοράς GridBlocks.

Η αρχιτεκτονική αναφοράς GridBlocks παρέχει τα ακόλουθα οφέλη στους φορείς(χειριστές) βοηθητικών προγραμμάτων(κοινής ωφέλειας):

- Λεπτομέρειες για ένα ευέλικτο μοντέλο βασισμένο σε επίπεδα που υποστηρίζει σταδιακές βελτιώσεις σε λογικά τμήματα (επίπεδα) του πλέγματος.
- Βοηθά στην ασφαλή ενσωμάτωση τόσο νέων όσο και παλαιότερων τεχνολογιών, βελτιώνοντας τη συνολική διαχείριση και την ορατότητα των στοιχείων του δικτύου.
- Βασίζεται σε ανοικτά πρότυπα, κυρίως IP και υποστηρίζει τη διαλειτουργικότητα προωθώντας έτσι χαμηλότερο κόστος.
- Επιτρέπει την ενοποίηση και τη σύγκλιση δικτύων κοινής ωφέλειας, η οποία έχει ως αποτέλεσμα τον εξορθολογισμό των λειτουργιών και τη μείωση των λειτουργικών δαπανών ενώ παράλληλα δημιουργεί νέα αξία μέσω αυξημένης λειτουργικότητας.
- Παρέχει έναν ψηφιακό χάρτη πορείας για τις επιχειρήσεις κοινής ωφέλειας, επιτρέποντάς τους να εκσυγχρονίσουν σταδιακά διάφορα μέρη του δικτύου.

Όπως απεικονίζεται στο Σχήμα 49, η αρχιτεκτονική αναφοράς Cisco GridBlocks είναι οργανωμένη σε 11 μέρη (ή επίπεδα), τα οποία δικτυώνουν όλες τις πτυχές της αλυσίδας τροφοδοσίας παροχής ενέργειας. Η βασική στρατηγική αυτού του μοντέλου είναι να ενώσει τις παλαιότερα αποσυνδεδεμένες λειτουργίες του δικτύου μέσω επικοινωνιών δικτύου σε μια συγκλίνουσα αρχιτεκτονική δικτύου. Κάθε βαθμίδα του δικτύου μπορεί να λειτουργεί από διαφορετικά τμήματα της ίδιας εταιρείας ενέργειας ή ακόμη και από διαφορετικές εταιρείες κατά μήκος της αλυσίδας εφοδιασμού ισχύος, ενώ ταυτόχρονα υποστηρίζει ασφαλείς διασυνδέσεις μεταξύ κάθε βαθμίδας. Ενώ το μοντέλο που βασίζεται στη βαθμίδα GridBlocks υποστηρίζει επίσης την ενοποίηση στοιχείων δικτύου σε μια ενιαία συγκλίνουσα αρχιτεκτονική. Οι βαθμίδες, ξεκινώντας από την κάτω βαθμίδα που φαίνεται στο Σχήμα 49 είναι οι εξής:

Επίπεδο καταναλωτή: περιλαμβάνει κατανεμημένους ενεργειακούς πόρους (distributed energy resources DER) που παράγουν τοπική ενέργεια από τον ήλιο ή από άλλα μέσα. Θα μπορούσε επίσης να περιλαμβάνει συστήματα αποθήκευσης ενέργειας και φορτία απόκρισης σε ηλεκτρικά οχήματα ή βιομηχανικές εγκαταστάσεις.

Επίπεδα διανομής: αυτό το τμήμα του δικτύου βρίσκεται μεταξύ του υποσταθμού διανομής και του τελικού χρήστη. Χωρίζεται σε δύο δευτερεύοντα στοιχεία, ως εξής: Βαθμός διανομής επιπέδου 2 και Βαθμός διανομής επιπέδου 1.

Επίπεδο υποσταθμού: περιλαμβάνει όλα τα δίκτυα υποσταθμών τόσο στους υποσταθμούς μετάδοσης όσο και στους υποσταθμούς διανομής. Οι υποσταθμοί μετάδοσης συνδέουν πολλαπλές γραμμές μεταφοράς και συνήθως περιλαμβάνουν υψηλότερες τάσεις (115 kV και άνω) και τροφοδοτούν ενέργεια προς τους σταθμούς διανομής. Τα δίκτυα αυτής της βαθμίδας έχουν μεγάλη ποικιλία απαιτήσεων, από βασικούς δευτερεύοντες υποσταθμούς έως πολύπλοκους πρωτογενείς υποσταθμούς που παρέχουν κρίσιμες λειτουργίες παροχής ενέργειας, όπως η τηλεπροστασία Μέσα στον υποσταθμό, υπάρχουν συχνά αυστηρές απαιτήσεις δικτύου, όπως ανθεκτικότητα, απόδοση, συγχρονισμός χρόνου και ασφάλεια.

Βαθμός ελέγχου συστήματος: περιλαμβάνει δίκτυα ευρείας περιοχής (wide area networks WANs) που συνδέουν υποσταθμούς μεταξύ τους και με κέντρα ελέγχου. Οι συνδέσεις WANs σε αυτήν τη βαθμίδα απαιτούν μερικές από τις πιο αυστηρές μετρήσεις απόδοσης καθυστέρησης και ανθεκτικότητας σε κάθε κλάδο. Τα δίκτυα υποσταθμού WANs απαιτούν ευελιξία και επεκτασιμότητα και μπορεί να περιλαμβάνουν διαφορετικούς τύπους μέσων, συμπεριλαμβανομένων ινών ή μικροκυμάτων.

Βαθμίδα κέντρου ενδοελέγχου / κέντρου ενδοδεδομένων: πρόκειται για τη βαθμίδα μέσα στα κέντρα δεδομένων χρησιμότητας και τα κέντρα ελέγχου. Τόσο τα κέντρα δεδομένων όσο και τα κέντρα ελέγχου βρίσκονται στο ίδιο λογικό επίπεδο, αλλά έχουν πολύ διαφορετικές απαιτήσεις. Ένα κέντρο δεδομένων είναι πολύ οικείο στους μηχανικούς IT, καθώς περιέχει εφαρμογές και υπηρεσίες σε επίπεδο επιχείρησης. Ένα κέντρο ελέγχου περιέχει συστήματα πραγματικού χρόνου που λειτουργούν και ελέγχουν το ίδιο το δίκτυο, συμπεριλαμβανομένων συστημάτων διανομής και μετάδοσης ισχύος και παρακολούθησης.

Βαθμός χρησιμότητας: πρόκειται για τη βαθμίδα που φιλοξενεί τα δίκτυα επιχειρήσεων πανεπιστημιούπολης. Η βαθμίδα χρησιμότητας είναι το σημείο σύνδεσης μεταξύ του κέντρου ελέγχου και του εταιρικού δικτύου και χρησιμοποιεί τείχη προστασίας με τις κατάλληλες πολιτικές ασφαλείας για να διασφαλίσει ότι μόνο η αξιόπιστη κίνηση από το εταιρικό δίκτυο εισέρχεται στο κέντρο ελέγχου. Τα περισσότερα βοηθητικά προγράμματα λειτουργούν με πολλαπλά κέντρα ελέγχου και έχουν πολύ διεσπαρμένα επιχειρησιακά

δίκτυα, πράγμα που σημαίνει ότι αυτά τα δίκτυα πρέπει να συνδέονται με ασφάλεια είτε μέσω δικτύων μετρό είτε μέσω WANs.

Βαθμίδα εξισορρόπησης: πρόκειται για τη βαθμίδα που υποστηρίζει συνδέσεις μεταξύ τρίτων φορέων παραγωγής ενέργειας και αρχών εξισορρόπησης. Οι περισσότερες επιχειρήσεις κοινής ωφέλειας συνδέονται με άλλες επιχειρήσεις κοινής ωφέλειας και μπορούν να αγοράζουν και να πωλούν ηλεκτρική ενέργεια το ένα από το άλλο όταν είναι απαραίτητο. Κατά καιρούς, μπορεί να υπάρχει περίσσεια ισχύος σε ένα βοηθητικό πρόγραμμα και έλλειψη ηλεκτρικής ενέργειας σε ένα άλλο. Η αρχή εξισορρόπησης έχει την ευθύνη της διαχείρισης της ζήτησης ηλεκτρικής ενέργειας έναντι της προσφοράς στο δίκτυο.

Βαθμίδα ανταλλαγής: Το δίκτυο αυτής της βαθμίδας επιτρέπει την αγορά και πώληση ηλεκτρικής ενέργειας μεταξύ φορέων κοινής ωφέλειας. Στον κόσμο της χρησιμότητας, η ηλεκτρική ενέργεια πραγματοποιείται με τον ίδιο τρόπο όπως και άλλα προϊόντα, όπως το πετρέλαιο και το φυσικό αέριο. Η πώληση ή η αγορά ηλεκτρικής ενέργειας πρέπει να πραγματοποιηθεί σε πραγματικό χρόνο. Τα δίκτυα αυτής της βαθμίδας επιτρέπουν στην εταιρεία να αγοράζει όχι μόνο ηλεκτρική ενέργεια όταν χρειάζεται, αλλά και να κερδίζει πωλώντας ενέργεια σε άλλες επιχειρήσεις κοινής ωφέλειας, όταν υπάρχει η ευκαιρία.

Διαπεριφερειακή / διακρατική βαθμίδα: Σε αυτό το επίπεδο βρίσκονται οι συνδέσεις δικτύου μεταξύ σύγχρονων δικτύων για την εναλλαγή ισχύος, καθώς και η παρακολούθηση του δικτύου και η διαχείριση της ροής ισχύος.

Βαθμίδα συστήματος μέτρησης και ελέγχου ευρείας περιοχής (Wide area measurement and control system WAMCS): αυτή η βαθμίδα περιλαμβάνει συνδέσεις με ένα κρίσιμο στοιχείο του δικτύου ηλεκτρικής ενέργειας, μονάδες διαχείρισης ενέργειας (power management units PMUs), οι οποίες είναι υπεύθυνες για μετρήσεις ισχύος ευρείας περιοχής στο δίκτυο. Λόγω του εύρους αυτής της βαθμίδας, πρέπει να συνδεθεί με αρκετές από τις άλλες βαθμίδες και έτσι απεικονίζεται ως κάθετη βαθμίδα στο Σχήμα 49.

Το μοντέλο αναφοράς GridBlocks είναι ένα χρήσιμο εργαλείο και σχέδιο που μπορεί να χρησιμοποιηθεί ως θεμέλιο για τη δημιουργία στοιχείων δικτύου εντός των επιπέδων και τη σύνδεσή τους με άλλες βαθμίδες. Επίσης, παρέχει, μια θεμελιώδη ομαδοποίηση των δυνατοτήτων του δικτύου σε «μπλοκ πλέγματος» που μπορεί να επεκταθεί με πολύ μεγαλύτερη λεπτομέρεια.

Κεφάλαιο 9.2.1 SCADA

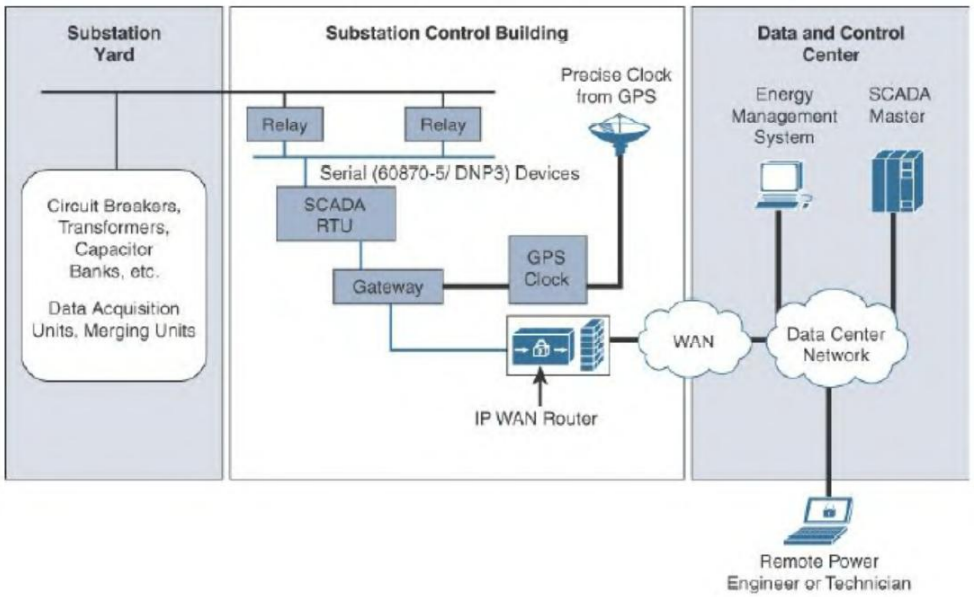
Ένα από τα μεγαλύτερα προοδευτικά άλματα τις τελευταίες δεκαετίες στη βιομηχανία ηλεκτρικής ενέργειας ήταν η δυνατότητα σύνδεσης συσκευών και ελέγχου αυτών μέσω τηλεπικοινωνιακών δικτύων και το IoT τώρα κάνει αυτό το άλμα σε ένα εντελώς νέο επίπεδο.

Το SCADA είναι ένα σύστημα με το οποίο οι απομακρυσμένες συσκευές μπορούν να παρακολουθούνται και να ελέγχονται από έναν κεντρικό διακομιστή. Παίζει έναν κρίσιμο ρόλο στον υποσταθμό, επιτρέποντας (όπως υποδηλώνει το όνομα) ελέγχους και απόκτηση δεδομένων από απομακρυσμένες συσκευές, γνωστές ως απομακρυσμένες τερματικές μονάδες (remote terminal units RTUs) και έξυπνες ηλεκτρονικές συσκευές (intelligent electronic devices IEDs).

Οι RTUs και οι IEDs είναι συσκευές ελεγχόμενες από μικροεπεξεργαστές συνδεδεμένες στο υλικό του δικτύου ηλεκτρικής ενέργειας, όπως ηλεκτρικά ρελέ, ελεγκτές φορτίου, ελεγκτές διακόπτη κυκλώματος, ελεγκτές πυκνωτών κ.ο.κ. Στον κόσμο του SCADA, η απομακρυσμένη συσκευή ονομάζεται SCADA slave και ο διακομιστής ονομάζεται SCADA master.
Το SCADA ξεκίνησε τη δεκαετία του 1950, πολύ πριν υπάρξουν δίκτυα υπολογιστών. Προοριζόταν να είναι ένα σύστημα στο οποίο ένας χειριστής θα μπορούσε να διαχειριστεί απομακρυσμένες βιομηχανικές συσκευές από ένα κεντρικό σημείο (συχνά ένα κεντρικό σύστημα υπολογιστή). Στην αρχή, τα συστήματα SCADA ήταν ανεξάρτητα, χωρίς σύνδεση με άλλα συστήματα και βασίζονταν σχεδόν εξ ολοκλήρου σε ιδιόκτητα πρωτόκολλα. Με την πάροδο του χρόνου, τα απομακρυσμένα δίκτυα WAN επέτρεψαν τη σύνδεση SCADA να επεκταθεί σε RTUs, αλλά αυτές οι συνδέσεις ήταν τυπικά σειριακές συνδέσεις από σημείο σε σημείο που χρησιμοποιούσαν διεπαφές RS-232 ή RS-485 και μεταφέρονταν μέσω κυκλωμάτων TDM.

Με την πάροδο του χρόνου, το SCADA άρχισε να υιοθετεί πρωτόκολλα βασισμένα σε πρότυπα και στην αρχιτεκτονική ανοιχτού δικτύου. Αντί να βασίζεται σε αποκλειστικούς σειριακούς συνδέσμους, το LAN υποσταθμού άρχισε να χρησιμοποιείται για μεταφορά, με έναν τοπικό SCADA να βρίσκεται σε κάθε υποσταθμό. Καθώς τα δίκτυα IP WAN υψηλής ταχύτητας, ανθεκτικότητας και ευελιξίας έγιναν διαθέσιμα, οι υπηρεσίες SCADA άρχισαν να διασκορπίζονται σε όλο το δίκτυο και μπορούσαν να χρησιμοποιήσουν ένα κεντρικό SCADA master στο κέντρο ελέγχου. Τα πιο ευρέως διαδεδομένα πρωτόκολλα επικοινωνίας SCADA είναι τα Modbus, IEC 60870-5 και Distributed Network Protocol (DNP3).

Το Σχήμα 50 απεικονίζει έναν υποσταθμό παλαιού τύπου όπου τα ηλεκτρικά ρελέ συνδέονται μέσω σειριακών (RS-232 ή RS-485) συνδέσεων σε RTUs, οι οποίες με τη σειρά τους συνδέονται με μια συσκευή πύλης SCADA που είναι συνδεδεμένη στο δίκτυο υποσταθμών Ethernet.
Μια συσκευή πύλης SCADA λειτουργεί συνήθως με έναν από τους δύο τρόπους. Ο πρώτος τρόπος είναι η μετάφραση πρωτοκόλλου. Παραδείγματα αυτού περιλαμβάνουν DNP3 έως DNP3 / IP ή IEC 60870-5-101 (σειριακό) έως 60870-5-104 (TCP / IP). Ο δεύτερος τρόπος με τον οποίο μπορεί να λειτουργήσει μια συσκευή πύλης είναι η σήραγγα της σειριακής κίνησης μέσω του δικτύου IP.



Σχήμα 50: Παραδοσιακό δίκτυο υποσταθμών SCADA με σειριακό RTUs.

Κεφάλαιο 9.3 Δίκτυο Πεδίου (Field Area Network FAN) GridBlock

Η βιομηχανία ηλεκτρικών βοηθητικών υπηρεσιών βρίσκεται στην κορυφή του IoT. Πουθενά αλλού αυτό δεν έχει αποδειχθεί περισσότερο από ό, τι στο δίκτυο περιοχής πεδίου (FAN). Το FAN GridBlock έχει σχεδιαστεί για να είναι πολλαπλών υπηρεσιών, πράγμα που σημαίνει ότι δεν βασίζεται σε συγκεκριμένες προμηθευτές, ιδιόκτητες τεχνολογίες που θα μπορούσαν να περιορίσουν τη χρήση του σε έναν και μόνο σκοπό, όπως πολλά παλαιά συστήματα OT. Στο παρελθόν, τα πρότυπα διαδικτύου απλώς δεν υπήρχαν για τη δημιουργία δικτύων μέτρησης ή αυτοματοποίησης διανομής (distribution automation DA) με βάση ανοικτά πρότυπα. Για αυτό ήταν απαραίτητο να δημιουργηθεί ένα αποκλειστικό και ανεξάρτητο δίκτυο για κάθε εφαρμογή.

Τα βασικά πλεονεκτήματα του σύγχρονου FAN που το καθιστούν ελκυστικό για τα Utilities είναι ότι:

- Βασίζεται στα ανοιχτά πρότυπα. Τα βασικά στοιχεία του δικτύου, της μεταφοράς και των επιπέδων εφαρμογής έχουν τυποποιηθεί από οργανισμούς όπως το IETF και το IEEE και είναι διαλειτουργικά με άλλες συμβατές συσκευές.

- Λόγω ευελιξίας υποστηρίζει το τελικό σημείο. Τα τελικά σημεία IoT που βασίζονται σε IPv6 είναι ευέλικτα και μπορούν να χρησιμοποιηθούν σε μια μεγάλη ποικιλία τοποθεσιών, όπως AMI (μετρητές), μονάδες φωτισμού δρόμου, συσκευές απόκρισης ζήτησης και σημεία αυτοματοποίησης διανομής, όπως SCADA RTUs.

- Παρουσιάζει ευέλικτες επιλογές ανάπτυξης headend. Επειδή το FAN χρησιμοποιεί μεταφορά IPv6, τα σημεία συγκέντρωσης headend και το σύστημα ασφαλείας μπορούν είτε να αναπτυχθούν εντός του χώρου είτε να φιλοξενηθούν στο cloud.

- Έχει ευέλικτες επιλογές backhaul. Το FAN συνήθως απαιτεί δρομολογητή περιοχής πεδίου (field area router FAR) που είναι τοποθετημένος στη περιοχή βοηθητικών υπηρεσιών ή σε κάποια άλλη τοποθεσία Το FAR είναι το σημείο τερματισμού του δικτύου πλέγματος. Είναι συνήθως διαθέσιμη μια μεγάλη ποικιλία επιλογών backhaul, όπως LTE, 3G, WiMAX, οπτικές ίνες, ακόμη και δορυφορική backhaul σε πολύ απομακρυσμένες κοινότητες.

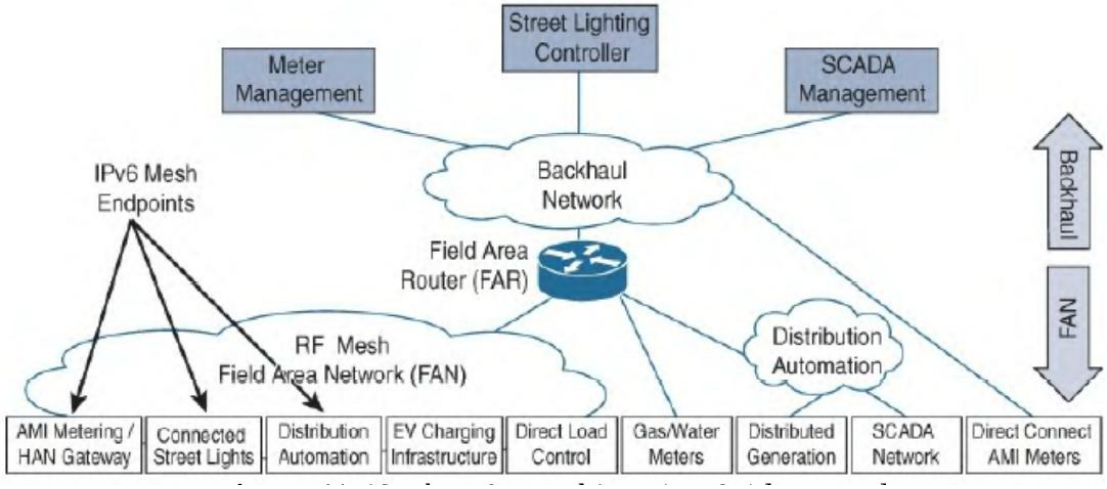
- Υποστηρίζει παλαιότερες εφαρμογές. Μέσω της χρήσης μιας πύλης, συσκευές παλαιού τύπου (όπως σειριακές RTUs) μπορούν να συνδεθούν με τον IPv6 FAN σε κλίμακα.

- Παρέχει δυνατότητα κλιμάκωσης. Το IPv6 είναι ικανό να κλιμακωθεί σε δεκάδες εκατομμύρια τελικά σημεία, που διαχειρίζονται εύκολα τους μετρητές και τα φώτα του δρόμου σε ένα μεγάλο δίκτυο κοινής ωφέλειας.

- Παρέχει υψηλή ασφάλεια. Το FAN GridBlock ενσωματώνει πολλαπλά επίπεδα ασφάλειας, συμπεριλαμβανομένης της κρυπτογράφησης εφαρμογών και επιπέδου δικτύου, καθώς και έλεγχο ταυτότητας τελικού σημείου.

- Είναι σταθερό και ανθεκτικό. Χάρη στην ευελιξία του IPv6, ένας καλά σχεδιασμένος FAN είναι σε θέση να προσφέρει ισχυρή διαθεσιμότητα και ανθεκτικότητα στο δίκτυο.

Όπως αναφέραμε το FAN GridBlock αξιοποιεί πολλά πρότυπα, συμπεριλαμβανομένων των IPv6, IEEE 802.15.4 mesh, CoAP και LTE. Αυτή η ευέλικτη και ανοικτή προσέγγιση προτύπων προωθεί δυνατότητες πολλαπλών λειτουργιών plug-and-play με ένα καλά κατανοητό πλαίσιο για την ασφάλεια, την ποιότητα των υπηρεσιών, την ανθεκτικότητα και τις υπηρεσίες διαχείρισης δικτύου. Το αποτέλεσμα είναι ένα ευρύ φάσμα δυνατοτήτων που υπερβαίνουν κατά πολύ τις περιπτώσεις χρήσης μετρήσεων. Το Σχήμα 51 παρουσιάζει ένα δίκτυο πολλαπλών υπηρεσιών FAN που υποστηρίζει εφαρμογές όπως σταθμούς επαναφόρτισης EV, συνδεδεμένα φώτα του δρόμου, τελικά σημεία απόκρισης ζήτησης, έξυπνους μετρητές και συνδέσεις με απομακρυσμένα SCADA RTUs στο δίκτυο διανομής.



Σχήμα 51: Δίκτυο πλέγματος πολλαπλών υπηρεσιών FAN.

Τέλος, να αναφέρουμε ότι το FAN έχει ορισμένους βασικούς περιορισμούς συμπεριλαμβανομένου του περιορισμένου εύρους ζώνης και της μεγάλης καθυστέρησης μεταξύ των κόμβων, πράγμα που σημαίνει ότι δεν είναι κατάλληλες για εφαρμογές πλούσιες σε μέσα όπως η παρακολούθηση βίντεο. Ωστόσο, υπάρχουν πολλές εφαρμογές χαμηλότερου εύρους ζώνης που καθιστούν τα FANs ιδανικά για utilities και άλλες βιομηχανίες, συμπεριλαμβανομένων των έξυπνων συνδεδεμένων πόλεων.

Κεφάλαιο 9.4 Ασφάλεια Έξυπνου Πλέγματος(Smart Grid Security)

Το IoT αποτελεί κινητήρια δύναμη για μια νέα γενιά ασφάλειας σε βοηθητικά προγράμματα(utilities). Σε απάντηση της απειλής για εγκλήματα στον κυβερνοχώρο κατά των υπηρεσιών κοινής ωφελείας, η Ομοσπονδιακή Ρυθμιστική Επιτροπή Ενέργειας (Federal Energy Regulatory Commission FERC) της αμερικανικής κυβέρνησης έδωσε εντολή σε όλες τις εταιρείες ενέργειας να συμμορφώνονται με το πρότυπο NERC's CIP v6 από την 1η Ιουλίου 2016.
Συγκεκριμένα, το NERC CIP:

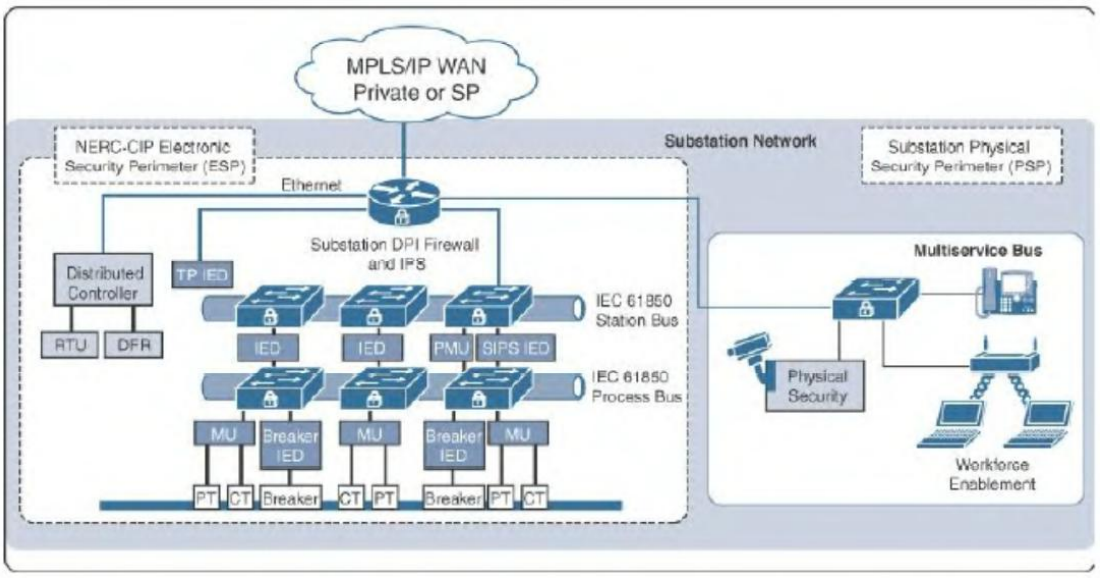
- Χρησιμοποιεί μια προσέγγιση ασφάλειας εκτίμησης κινδύνου.

- Βοηθά τα βοηθητικά προγράμματα(utilities), να επικεντρωθούν σε αυτό που είναι πραγματικά σημαντικό: την προστασία των δικτύων τους από επιθέσεις, τόσο από μέσα όσο και από έξω. Για παράδειγμα, αντί για την επιβολή συγκεκριμένου τύπου και επιπέδου προστασίας από ιούς, το NERC CIP v6 βασίζεται περισσότερο στις αρχές, απαιτώντας «προστασία από κακόβουλο λογισμικό».

- Επικεντρώνεται κυρίως στη θέσπιση πολιτικών, προγραμμάτων και διαδικασιών ασφαλείας. Μια βασική ιδέα σε αυτό το μοντέλο είναι η εκτίμηση του επιπέδου επιπτώσεων που μπορεί να έχει μια παραβίαση ασφαλείας στα περιουσιακά στοιχεία της επιχείρησης. Οι επιχειρήσεις κοινής ωφέλειας πρέπει να προσδιορίσουν σωστά σε ποιο επίπεδο επιπτώσεων ταιριάζει κάθε περιουσιακό στοιχείο, με επίπεδα που ορίζονται ως υψηλά, μεσαία, χαμηλά ή καθόλου επιπτώσεις.

- Απαιτεί συστήματα ανίχνευσης/πρόληψης εισβολών (detection/prevention systems IDS/IPS) ή κάποια μορφή επιθεώρησης πακέτων σε βάθος deep packet inspection (DPI).Το πρότυπο επιβάλλει επίσης τον ορισμό μιας ηλεκτρονικής περιμέτρου ασφαλείας (electronic security perimeter ESP) όταν τα περιουσιακά στοιχεία εντός του EPS προστατεύονται από δύο ξεχωριστά μέτρα ασφαλείας, όπως ένα τείχος προστασίας και ένα IPS. Επιπλέον, ορίζεται μια περίμετρος φυσικής ασφάλειας (physical security perimeter PSP), η οποία περιλαμβάνει άλλες πτυχές, όπως παρακολούθηση βίντεο και συστήματα πρόσβασης κτιρίου, και αποσκοπεί στην προστασία του σταθμού από φυσική επίθεση.

Μια βασική πτυχή του NERC CIP είναι ότι πρέπει να δημιουργηθεί ένα ESP για όλα τα συστήματα κυβερνοχώρου BES υψηλής και μεσαίας πρόσκρουσης που συνδέονται σε δρομολογούμενο δίκτυο, ανεξάρτητα από το αν το τμήμα που περιέχει το κυβερνοσύστημα BES έχει εξωτερική συνδεσιμότητα με οποιοδήποτε άλλο δίκτυο. Το Σχήμα 52 απεικονίζει ένα πρωτεύον δίκτυο υποσταθμών, επισημαίνοντας τα στοιχεία ESP και PSP.



Σχήμα 52: Πρωτεύον δίκτυο υποσταθμών με NERC CIP v6 ηλεκτρονικών και φυσικών περιμέτρων ασφάλειας.

Κεφάλαιο 10 Έξυπνες και συνδεδεμένες πόλεις

Οι περισσότερες πόλεις ξεκίνησαν ως μικρά αστικά κέντρα και αναπτύχθηκαν οργανικά. Πολύ λίγες από αυτές σχεδιάστηκαν αρχικά για να φιλοξενήσουν αμέσως έναν πολύ μεγάλο πληθυσμό. Ο κόσμος αστικοποιείται γρήγορα και αυτή η τάση αναμένεται να συνεχιστεί. Λιγότερο από το ένα τρίτο του παγκόσμιου πληθυσμού ζούσε σε πόλεις το 1950 και υπολογίζεται ότι έως το 2050, τα δύο τρίτα του πληθυσμού του πλανήτη μας θα είναι κάτοικοι πόλεων. Καθώς ο παγκόσμιος πληθυσμός αυξάνεται, αυξάνονται επίσης οι εκπομπές και η κατανάλωση. Σήμερα, οι πόλεις ευθύνονται για το 60% έως 80% των παγκόσμιων εκπομπών ενέργειας και θερμοκηπίου και καταναλώνουν το 60% του συνόλου του πόσιμου νερού. Ένα βασικό μέλημα των ηγετών των πόλεων σε όλο τον κόσμο είναι η βελτιστοποίηση των πόρων (νερό, ενέργεια, αποδοτικότητα υποδομής επικοινωνίας κ.λπ.), επεξεργασία αποβλήτων και εκπομπών. Ωστόσο, οι ηγέτες της πόλης γνωρίζουν επίσης ότι ο αυξανόμενος πληθυσμός σε μια πόλη παρέχει την ευκαιρία να αξιοποιήσουν τις δυνατότητες της πόλης. Ο στόχος η αποτελεσματικότερη διαχείριση της αύξησης του πληθυσμού. Βελτιωμένη αποδοτικότητα διαχείρισης σημαίνει παροχή καλύτερων και αποδοτικότερων αστικών υπηρεσιών και εξασφάλιση καλύτερων εμπειριών ζωής στους κατοίκους της πόλης.

Αυτό το κεφάλαιο εξετάζει τα κύρια στοιχεία του IoT για έξυπνες πόλεις. Τα αστικά κέντρα χαρακτηρίζονται ως «έξυπνα» όταν αξιοποιούν τεχνολογίες για να βελτιώσουν τη διαχείριση κοινών πόρων, όπως ο χώρος του δρόμου ή η συλλογή απορριμμάτων, και να βελτιώσουν την ποιότητα της αστικής ζωής για τους πολίτες. Με την αύξηση της αστικής πυκνότητας, πρέπει να βρεθούν νέες και πιο αποτελεσματικές λύσεις για τη διατήρηση ή την αύξηση της βιωσιμότητας των ταχέως αναπτυσσόμενων αστικών κέντρων. Οι τεχνολογίες IoT αναπτύσσουν αισθητήρες στο επίπεδο του δρόμου για τη συλλογή τοπικών δεδομένων. Ένα τμήμα πόλης μεταφέρει τις συλλεγμένες πληροφορίες στα κέντρα δεδομένων, όπου γίνεται επεξεργασία των πληροφοριών. Στη συνέχεια τα σήματα στέλνονται πίσω στο στρώμα του δρόμου για να τροποποιήσουν την κατάσταση των αισθητήρων, να τροποποιήσουν τα μοτίβα φωτισμού του δρόμου κ.λπ.
Επιπλέον, οι πολίτες ενδέχεται να έχουν πρόσβαση στις πληροφορίες όπως για παράδειγμα, να βρουν θέση στάθμευσης ή να ακολουθήσουν μια εναλλακτική διαδρομή για να αποφύγουν την κυκλοφορία.

Συγκεκριμένα μερικοί τομείς που εξετάζονται στο παρόν κεφάλαιο είναι:

- Η στρατηγική IoT για έξυπνες πόλεις. Καθορίζει πώς μπορούν να αξιοποιηθούν οι τεχνολογίες IoT για τη βελτίωση της ζωής των πολιτών και την αποτελεσματική διαχείριση των αστικών κέντρων.

- Την αρχιτεκτονική IoT μιας έξυπνης πόλης(Smart City IoT Architecture). Περιγράφει τα τέσσερα κύρια επίπεδα για την ενσωμάτωση του IoT για έξυπνες πόλεις.

- Η αρχιτεκτονική ασφάλειας έξυπνης πόλης. Εξετάζει τους βασικούς περιορισμούς και εκτιμήσεις για την εξασφάλιση του IoT για έξυπνες πόλεις, τόσο από την άποψη της επικοινωνίας όσο και από την άποψη της αποδεκτής χρήσης των δεδομένων που συλλέγονται.

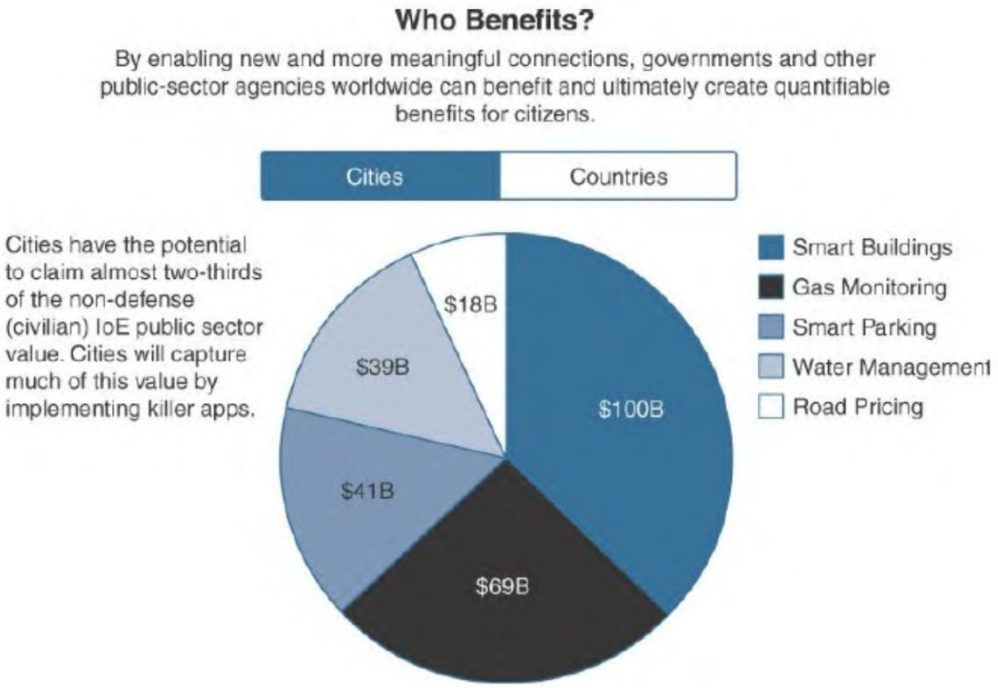
- Παραδείγματα περίπτωσης χρήσης μιας έξυπνης πόλης. Περιγράφει περιπτώσεις χρήσης IoT για έξυπνες πόλεις: φωτισμός δρόμου, έξυπνος χώρος στάθμευσης, κίνηση και έξυπνο περιβάλλον. Το IoT μπορεί να μειώσει δραστικά το ενεργειακό

κόστος της πόλης ενώ χρησιμοποιεί την υπάρχουσα υποδομή φωτισμού. Ο έξυπνος χώρος στάθμευσης είναι μια άλλη περίπτωση όπου το IoT προσφέρει μεγάλο όφελος, μειώνοντας τη συμφόρηση στην πόλη και αυξάνοντας την ποιότητα ζωής για τους πολίτες που οδηγούν. Σε συνδυασμό με το παρκινγκ, ο έξυπνος έλεγχος κυκλοφορίας είναι μια άλλη έξυπνη λύση πόλης που μπορεί να χρησιμοποιηθεί για τη ρύθμιση των ροών των αυτοκινήτων και για να προσφέρει βέλτιστες επιλογές διαδρομής πραγματικός χρόνος. Ο έλεγχος της κυκλοφορίας και η βελτίωση της στάθμευσης ωφελούν επίσης το περιβάλλον.

Κεφάλαιο 10.1 Μια στρατηγική IoT για πιο έξυπνες πόλεις

Η διαχείριση μιας πόλης μοιάζει με τη διαχείριση μιας εταιρικής επιχείρησης. Καθώς αυξάνεται η ανάγκη για αποδοτικότητα, νέα εργαλεία συμβάλλουν στην αύξηση της λειτουργικής αποδοτικότητας. Για τις πόλεις, όπως και για τις επιχειρήσεις, η ψηφιοποίηση μεταμορφώνει την προοπτική των λειτουργιών. Νέες ιδέες αναδύονται, φέρνοντας διαφορετικές προσεγγίσεις στην επίλυση ζητημάτων διαχείρισης. Οι κλιμακούμενες λύσεις που χρησιμοποιούν τεχνολογία πληροφοριών και επικοινωνιών (information and communications technology ICT) μπορούν να ανακουφίσουν πολλά προβλήματα που αντιμετωπίζουν σήμερα τα αστικά κέντρα αυξάνοντας την αποδοτικότητα, η οποία μειώνει το κόστος και βελτιώνει την ποιότητα ζωής. Οι πόλεις που υιοθετούν αυτήν την προσέγγιση αναφέρονται συνήθως ως έξυπνες πόλεις(smart cities), μια έννοια που συχνά συζητείται σε κύκλους πολεοδομίας και πολιτικής πόλεων παγκοσμίως.

Υπάρχουν πολλές διαφορετικές προσεγγίσεις και λύσεις για τη διαχείριση της πόλης. Όλες αυτές οι λύσεις συνήθως ξεκινούν από το επίπεδο δρόμων, με αισθητήρες που συλλέγουν δεδομένα για τα πάντα, από τη διαθεσιμότητα θέσεων στάθμευσης έως την καθαρότητα του νερού. Η ανάλυση δεδομένων χρησιμοποιείται επίσης εκτενώς, για παράδειγμα, για τη βελτίωση της ροής της κυκλοφορίας.
Οι πολίτες μπορούν να χρησιμοποιήσουν εργαλεία για να αξιοποιήσουν τις έξυπνες κινητές συσκευές τους, όπως να αναφέρουν προβλήματα και να κάνουν συστάσεις για τη βελτίωση της αστικής ζωής ή να εντοπίσουν διαθέσιμες θέσεις στάθμευσης. Όταν ενεργοποιούνται μέσω συνδεσιμότητας, αυτές οι έξυπνες λύσεις μπορούν να έχουν αντίκτυπο στην ποιότητα ζωής. Η τεχνολογία πληροφοριών και επικοινωνιών συνδέει ανθρώπους, δεδομένα, πράγματα και διαδικασίες μαζί σε δίκτυα δισεκατομμυρίων ή ακόμη και τρισεκατομμυρίων συνδέσεων. Αυτές οι συνδέσεις δημιουργούν τεράστιο όγκο δεδομένων, μερικά από τα οποία δεν ήταν ποτέ προσιτά στο παρελθόν. Όταν αυτά τα δεδομένα αναλύονται και χρησιμοποιούνται έξυπνα, τότε οι δυνατότητες συσχέτισης, ανάλυσης βελτιστοποίησης υπηρεσιών και διαδικασιών(που προσφέρουν καλύτερη ποιότητα ζωής στους ανθρώπους), είναι πρακτικά ατελείωτες. Έτσι, η ανάπτυξη εφαρμογών IoT για αστικά κέντρα όχι μόνο αποφέρει μοναδικά οφέλη, αλλά παρέχει τη δυνατότητα μία πόλη να προσφέρει αποτελεσματικές υπηρεσίες.
Μια πρόσφατη μελέτη της Cisco, όπως απεικονίζεται στο Σχήμα 53, παρουσιάζει τον οικονομικό αντίκτυπο σε μια περίοδο 10 ετών που θα παρέχουν τα IoTs :



Σχήμα 53: Δυνατότητες για έξυπνες πόλεις.

Έξυπνα κτίρια: έχουν τη δυνατότητα να εξοικονομήσουν 100 δισεκατομμύρια δολάρια μειώνοντας το λειτουργικό κόστος την κατανάλωση ενέργειας μέσω της αποτελεσματικής ενσωμάτωσης των συστημάτων θέρμανσης, εξαερισμού και κλιματισμού (heating, ventilation, and air-conditioning HVAC) και άλλων κτιριακών συστημάτων υποδομής.

Παρακολούθηση αερίου: θα μπορούσε να εξοικονομήσει 69 δισεκατομμύρια δολάρια μειώνοντας το κόστος ανάγνωσης μετρητών και αυξάνοντας την ακρίβεια των ενδείξεων για τους πολίτες και τις δημοτικές υπηρεσίες κοινής ωφέλειας. Επίσης, σημαντικά πλεονεκτήματα όσον αφορά την ασφάλεια.

Έξυπνος χώρος στάθμευσης: θα μπορούσε να εξοικονομήσει 41 δισεκατομμύρια δολάρια, παρέχοντας ορατότητα σε πραγματικό χρόνο στη διαθεσιμότητα χώρων στάθμευσης σε μια πόλη. Οι κάτοικοι μπορούν να προσδιορίσουν και να κρατήσουν τον πλησιέστερο διαθέσιμο χώρο.

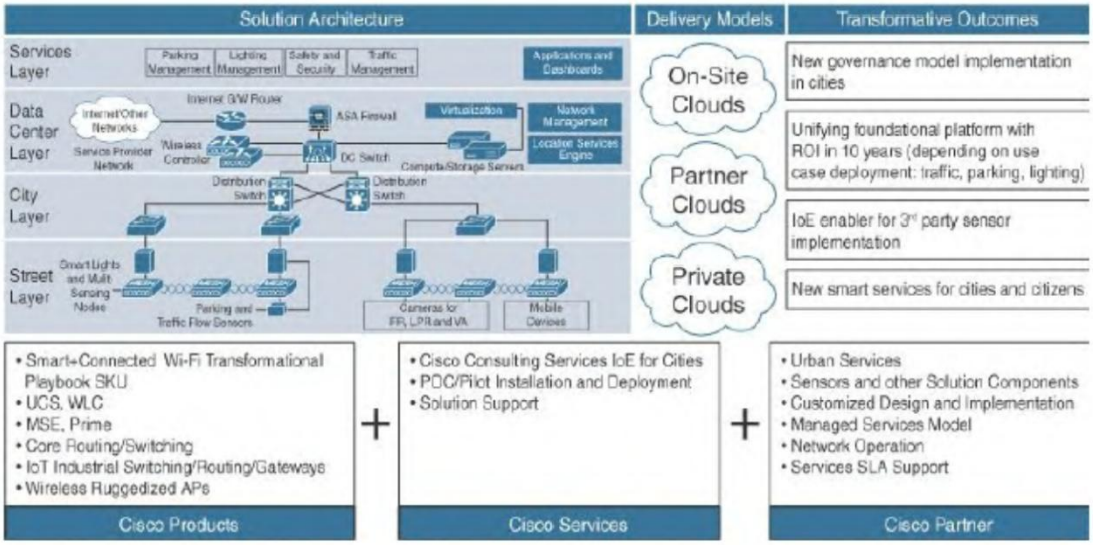
Διαχείριση νερού: θα μπορούσε να εξοικονομήσει 39 δισεκατομμύρια δολάρια συνδέοντας οικιακούς μετρητές νερού μέσω ενός δικτύου IP για την παροχή απομακρυσμένων πληροφοριών χρήσης και κατάστασης. Το όφελος είναι προφανές, με χαρακτηριστικά όπως ορατότητα κατανάλωσης σε πραγματικό χρόνο και ανίχνευση διαρροών. Επιπλέον, οι έξυπνοι μετρητές μπορούν να χρησιμοποιηθούν για τον συντονισμό και την αυτοματοποίηση του ποτίσματος ιδιωτικού και δημόσιου χλοοτάπητα, ξεκινώντας τα προγράμματα ποτίσματος σε περιόδους όταν η κατανάλωση νερού είναι χαμηλότερη ή σύμφωνα με τους περιορισμούς νερού που επιβάλλονται από τις δημόσιες αρχές.

Τιμολόγηση δρόμου: Οι πόλεις θα μπορούσαν να φέρουν κέρδη 18 δισεκατομμύρια δολάρια σε νέα έσοδα εφαρμόζοντας αυτόματες πληρωμές καθώς τα οχήματα εισέρχονται σε πολυσύχναστες ζώνες της πόλης βελτιώνοντας ταυτόχρονα τις συνολικές συνθήκες κυκλοφορίας. Τα δεδομένα για την κατάσταση της κυκλοφορίας σε πραγματικό χρόνο είναι

πολύτιμες και εύχρηστες πληροφορίες που μπορούν επίσης να χρησιμοποιηθούν για τις συγκοινωνίες δημόσιες η ιδιωτικές.

Κεφάλαιο 10.2 IoT-Αρχιτεκτονική έξυπνης πόλης

Κάθε έξυπνη πόλη χρειάζεται ένα προσαρμοσμένο και δομημένο υπολογιστικό μοντέλο που επιτρέπει κατανεμημένη επεξεργασία δεδομένων σε επίπεδο ανθεκτικότητας, κλίμακας, ταχύτητας και κινητικότητας που απαιτούνται για την αποτελεσματική απόδοση που μπορούν να δημιουργήσουν τα δεδομένα που δημιουργούνται όταν υποβάλλονται σε σωστή επεξεργασία σε όλο το δίκτυο. Μια υποδομή έξυπνης πόλης IoT είναι μια αρχιτεκτονική τεσσάρων επιπέδων, όπως φαίνεται στο Σχήμα 54.



Σχήμα 54: Αρχιτεκτονική επίπεδων έξυπνων πόλεων.

Τα δεδομένα ρέουν από συσκευές στο επίπεδο δρόμου στο επίπεδο δικτύου της πόλης και συνδέονται με το επίπεδο του κέντρου δεδομένων, όπου τα δεδομένα συγκεντρώνονται, ομαλοποιούνται(normalized,) και εικονικοποιούνται. Το επίπεδο του κέντρου δεδομένων παρέχει πληροφορίες στο επίπεδο υπηρεσιών, το οποίο αποτελείται από εφαρμογές που παρέχουν υπηρεσίες στην πόλη. Στις έξυπνες πόλεις, πολλές υπηρεσίες ενδέχεται να χρησιμοποιούν λύσεις IoT για πολλούς διαφορετικούς σκοπούς. Αυτές οι υπηρεσίες ενδέχεται να χρησιμοποιούν διαφορετικές λύσεις IoT, με διαφορετικά πρωτόκολλα και διαφορετικές γλώσσες εφαρμογών. Επομένως, η ροή δεδομένων από αισθητήρα σε εφαρμογή περιλαμβάνει μια διαδικασία μετάφρασης σε μια γλώσσα που μπορεί να εκτεθεί μέσω APIs για άλλη κατανάλωση εφαρμογών υπηρεσιών. Αυτή η μετάφραση εξασφαλίζει μια ενιαία γλώσσα για όλες τις συσκευές στο cloud. Αυτή η κοινή γλώσσα απλοποιεί την επικοινωνία και τη διαχείριση δεδομένων και επιτρέπει λύσεις να αλληλοενημερώνονται. Η αξιοποίηση αυτής της ανταλλαγής επιτρέπει στις έξυπνες πόλεις να αναπτύξουν νέες λύσεις που εκτείνονται σε υπηρεσίες, χωρίς να απαιτούνται περαιτέρω υποδομές και μελλοντικές αποδείξεις του συστήματος.

Οι ακόλουθες ενότητες αναφέρονται στην επιλογή αισθητήρων για συγκεκριμένες εφαρμογές και παρέχουν παραδείγματα τεχνολογικών απαιτήσεων δικτύωσης για την υποστήριξη αισθητήρων και την οδήγηση λύσεων σε πραγματικό χρόνο μέσω συνδεσιμότητας τεχνολογίας πληροφοριών και επικοινωνιών (information and communication technology ICT).

Κεφάλαιο 10.2.1 Επιπεδο δρόμου(Street Layer)

Το επίπεδο δρόμου αποτελείται από συσκευές και αισθητήρες που συλλέγουν δεδομένα και λειτουργούν βάσει οδηγιών, καθώς και τα στοιχεία δικτύου που απαιτούνται για τη συγκέντρωση και συλλογή δεδομένων. Ο αισθητήρας είναι μια πηγή δεδομένων που παράγει τα δεδομένα που απαιτούνται για την κατανόηση του φυσικού κόσμου. Οι συσκευές αισθητήρων είναι σε θέση να ανιχνεύουν και να μετρούν γεγονότα στον φυσικό κόσμο. Οι λύσεις συνδεσιμότητας ICT, βασίζονται σε αισθητήρες για τη συλλογή δεδομένων από τον κόσμο γύρω τους, ώστε να μπορούν να αναλυθούν και να χρησιμοποιηθούν για τη λειτουργία των περιπτώσεων χρήσης για πόλεις.
Μια λίστα από αισθητήρες που χρησιμοποιείται στο επίπεδο του δρόμου για μια σειρά περιπτώσεων για έξυπνες πόλεις είναι οι εξής:

- **Μαγνητικός αισθητήρας**: μπορεί να ανιχνεύσει ένα συμβάν στάθμευσης αναλύοντας τις αλλαγές στο γύρω μαγνητικό πεδίο όταν ένα βαρύ μεταλλικό αντικείμενο, όπως ένα αυτοκίνητο ή ένα φορτηγό, πλησιάζει σε αυτό (ή πάνω του).

- **Ελεγκτής φωτισμού**: μπορεί να μειώσει και να φωτίσει ένα φως με βάση ένα συνδυασμό συνθηκών που βασίζονται στο χρόνο και του περιβάλλοντος.

- **Βιντεοκάμερες:** σε συνδυασμό με την ανάλυση βίντεο, μπορούν να ανιχνεύσουν οχήματα, πρόσωπα και συνθήκες κυκλοφορίας για διάφορες περιπτώσεις κυκλοφορίας και χρήσης ασφαλείας.

- **Αισθητήρας ποιότητας αέρα:** μπορεί να ανιχνεύσει και να μετρήσει τις συγκεντρώσεις αερίων και σωματιδίων για να δώσει μια υπέρ-τοπική προοπτική σχετικά με τη ρύπανση σε μια δεδομένη περιοχή. Οι μετρητές συσκευών δίνουν μια εκτίμηση του αριθμού των συσκευών στην περιοχή, η οποία παρέχει μια γενική ιδέα για τον αριθμό των οχημάτων που κινούνται ή σταθμεύουν σε δρόμο ή δημόσιο χώρο στάθμευσης, πεζών σε πεζοδρόμιο ή ακόμη και πουλιών.

Για κάθε τύπο δεδομένων που συλλέγονται, υπάρχει μια ποικιλία λύσεων και πιθανών προσεγγίσεων. Η επιλογή της τεχνολογίας αισθητήρων εξαρτάται από την ακριβή φύση του προβλήματος, την ακρίβεια και τις δαπάνες που είναι κατάλληλες για αυτό, και τυχόν περιορισμούς εγκατάστασης που θέτει το φυσικό περιβάλλον. Ένα άλλο ζήτημα είναι η απαίτηση αλληλεπίδρασης με άλλα συστήματα IoT στον ίδιο φυσικό χώρο.

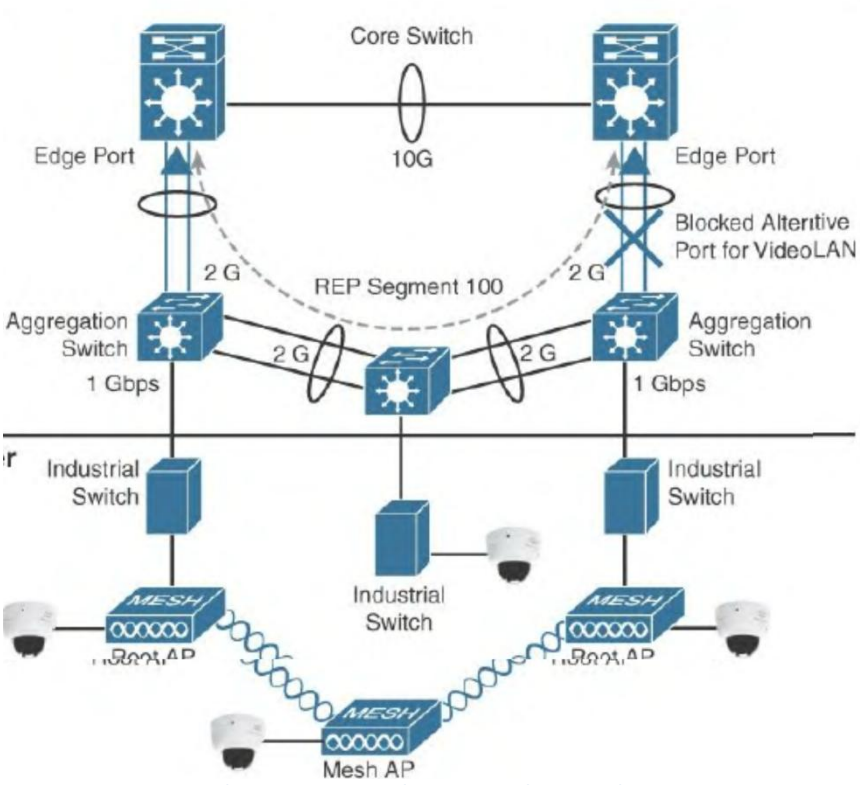
Μια από τις βασικές πτυχές που πρέπει να λάβουμε υπόψη κατά την επιλογή μιας συσκευής ανίχνευσης είναι το κόστος συντήρησης της διάρκειας ζωής της. Ορισμένοι αισθητήρες είναι τοποθετημένοι στην υποδομή της πόλης, άλλοι αισθητήρες μπορεί να εγκατασταθούν στο έδαφος ή σε άλλες απρόσιτες τοποθεσίες. Μια άλλη βασική πτυχή που πρέπει να λάβουμε υπόψη όταν επιλέγουμε τη σωστή τεχνολογία για μια έξυπνη πόλη είναι τα αναλυτικά στοιχεία. Οι πολλοί αισθητήρες και τα δεδομένα τους πρέπει να διαχειρίζονται μέσω του δικτύου με τρόπο που να επεξεργάζεται με ασφάλεια τα δεδομένα με ελάχιστη καθυστέρηση και συχνά σε πραγματικό χρόνο. Η συλλογή και αποθήκευση δεδομένων έχουν επίσης σημαντικό αντίκτυπο στην ιδιωτική ζωή. Ένας αισθητήρας βίντεο που χρησιμοποιείται για την καταμέτρηση οντοτήτων μπορεί να μπορεί να διαβάσει αριθμούς κυκλοφορίας αυτοκινήτων ή να καταγράψει τα πρόσωπα των πεζών. Νομικά θέματα και ζητήματα απορρήτου παίζουν σημαντικό ρόλο στην επιλογή ενός συστήματος. Ενδέχεται να υπάρχει εντολή καταγραφής αυτού του τύπου δεδομένων για λόγους δημόσιας ασφάλειας.

Το εύρος των απαιτήσεων απορρήτου πρέπει να είναι σαφώς κατανοητό και να επεκτείνεται κατά τη στιγμή του σχεδιασμού. Ανεξάρτητα από τον τύπο του συστήματος που επιλέγεται, τα δεδομένα αισθητήρων μεταφέρονται και επεξεργάζονται από το σύστημα IoT.

Κεφάλαιο 10.2.2 Επίπεδο πόλης (City Layer)

Στο επίπεδο της πόλης, το οποίο βρίσκεται πάνω από το επίπεδο του δρόμου, πρέπει να αναπτυχθούν δρομολογητές και διακόπτες δικτύου ώστε να ταιριάζουν με το μέγεθος των δεδομένων της πόλης που πρέπει να μεταφερθούν. Αυτό το επίπεδο συγκεντρώνει όλα τα δεδομένα που συλλέγονται από τους αισθητήρες και το τελικό κόμβο σε ένα δίκτυο μεταφοράς. Το επίπεδο πόλης μπορεί να φαίνεται ότι είναι ένα απλό επίπεδο μεταφοράς μεταξύ των συσκευών άκρης και του κέντρου δεδομένων ή του Διαδικτύου. Ωστόσο, μια βασική θεώρηση του επιπέδου της πόλης είναι ότι πρέπει να μεταφέρει πολλαπλούς τύπους πρωτοκόλλων, για πολλούς τύπους εφαρμογών IoT. Ορισμένες εφαρμογές είναι ευαίσθητες στην καθυστέρηση ενώ άλλες εφαρμογές απαιτούν μια ιδιαίτερη προσέγγιση στην παράδοση του πακέτου. Ένα χαμένο πακέτο μπορεί να οδηγήσει σε μη έγκυρη αναφορά κατάστασης. Ως αποτέλεσμα, το επίπεδο πόλης πρέπει να οικοδομηθεί γύρω από την ανθεκτικότητα, για να διασφαλιστεί ότι ένα πακέτο που προέρχεται από έναν αισθητήρα ή μια πύλη θα προωθείται πάντα με επιτυχία στον κεντρικό σταθμό.

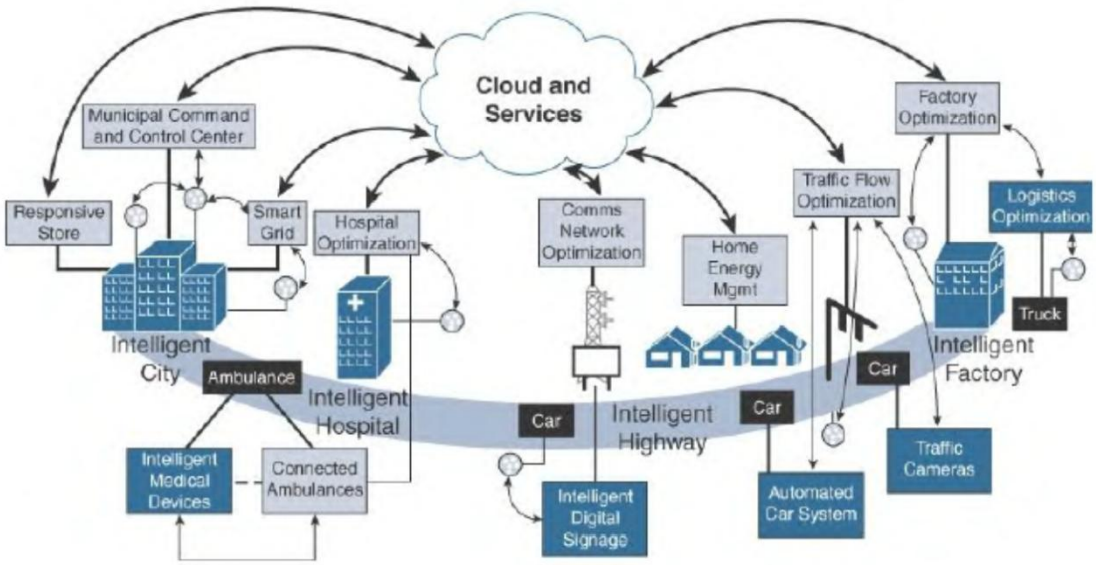
Το Σχήμα 55 δείχνει έναν κοινό τρόπο επίτευξης αυτού του στόχου. Σε αυτό το μοντέλο, υπάρχουν τουλάχιστον δύο διαδρομές από οποιονδήποτε διακόπτη συγκέντρωσης στο επίπεδο του κέντρου δεδομένων. Ένα κοινό πρωτόκολλο που χρησιμοποιείται για να διασφαλιστεί αυτή η ανθεκτικότητα είναι το Resilient Ethernet Protocol (REP).



Σχήμα 55: Ανθεκτικότητα για επίπεδο δρόμου.

Κεφάλαιο 10.2.3 Επίπεδο Κέντρου Δεδομένων (Data Center Layer)

Τα δεδομένα που συλλέγονται από τους αισθητήρες αποστέλλονται σε ένα κέντρο δεδομένων, όπου μπορούν να υποβληθούν σε επεξεργασία. Με βάση αυτήν την επεξεργασία, μπορούν να αντληθούν σημαντικές πληροφορίες και να παρέχονται πληροφορίες. Για παράδειγμα, μια εφαρμογή σε ένα κέντρο δεδομένων μπορεί να παρέχει μια εικόνα της κυκλοφορίας στην πόλη και να βοηθήσει τις αρχές να αποφασίσουν σχετικά με την ανάγκη για περισσότερο ή λιγότερο οχήματα μεταφοράς. Επίσης, οι ίδιες πληροφορίες κυκλοφορίας μπορούν να υποβληθούν σε επεξεργασία για αυτόματη ρύθμιση και συντονισμό της διάρκειας του φωτισμού σε ολόκληρη τη πόλη για τον περιορισμό της κυκλοφοριακής συμφόρησης. Η βασική τεχνολογία για τη δημιουργία οποιασδήποτε ολοκληρωμένης έξυπνης λύσης με υπηρεσίες είναι το cloud. Με μια υποδομή cloud, τα δεδομένα δεν αποθηκεύονται σε κέντρο δεδομένων, αλλά σε rented logical containers με πρόσβαση στο διαδίκτυο. Το μέγεθος αποθήκευσης και η υπολογιστική ισχύς είναι ευέλικτα και μπορούν να προσαρμοστούν στις μεταβαλλόμενες απαιτήσεις ή τις προϋπολογιστικές συνθήκες. Αυτή η ευελιξία διευκολύνουν επίσης την ανταλλαγή πληροφοριών μεταξύ έξυπνων συστημάτων και επιτρέπουν την ανάπτυξη νέων εφαρμογών που μπορούν να αξιοποιήσουν πληροφορίες από διάφορα συστήματα IoT. Το Σχήμα 56 δείχνει το όραμα της χρήσης του cloud σε έξυπνες λύσεις για πόλεις. Το cloud παρέχει μια κλιμακούμενη, ασφαλή και αξιόπιστη μηχανή επεξεργασίας δεδομένων που μπορεί να χειριστεί τον τεράστιο όγκο δεδομένων που διέρχονται από αυτό. Τα ζητήματα των έξυπνων πόλεων δεν απαιτούν μόνο αποτελεσματική χρήση της υποδομής, την οποία βοηθά να ενεργοποιηθεί το cloud, απαιτούν επίσης νέα μοντέλα επεξεργασίας και διαχείρισης δεδομένων.



Σχήμα 56: Ο ρόλος του Cloud για εφαρμογές έξυπνης πόλης.

Κεφάλαιο 10.2.4 Επίπεδο υπηρεσιών ((Services Layer)

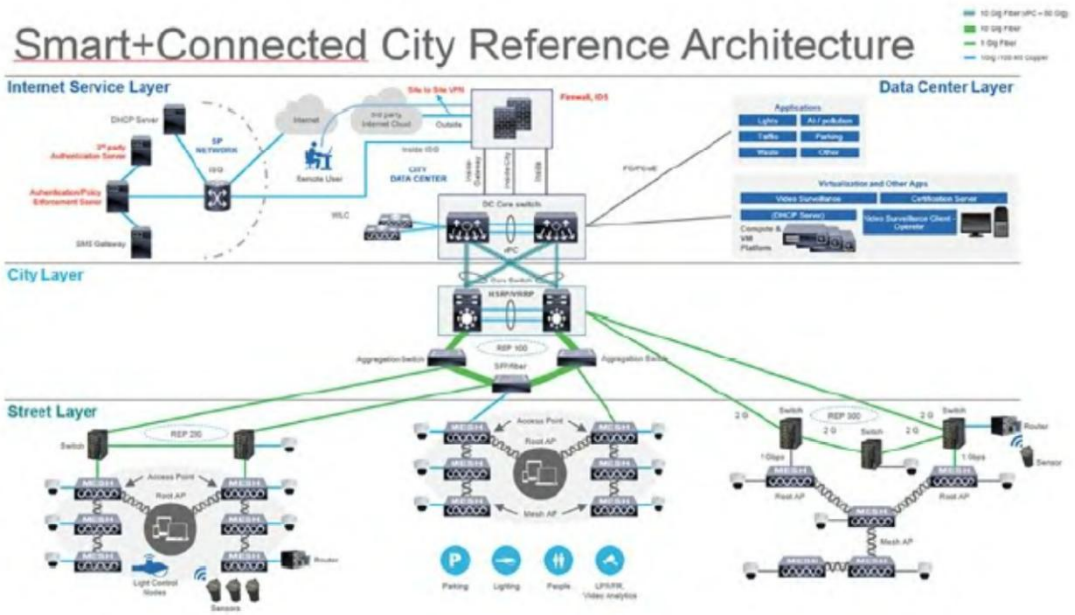
Η πραγματική αξία της συνδεσιμότητας ICT προέρχεται από τις υπηρεσίες που τα δεδομένα μπορούν να παρέχουν σε διαφορετικούς χρήστες που λειτουργούν μέσα σε μια πόλη. Οι εφαρμογές έξυπνων πόλεων μπορούν να παρέχουν αξία και προβολή σε διάφορους τύπους χρηστών, συμπεριλαμβανομένων των φορέων εκμετάλλευσης πόλεων, των πολιτών και των αρχών επιβολής του νόμου.

Τα συλλεγόμενα δεδομένα θα πρέπει να απεικονίζονται σύμφωνα με τις ειδικές ανάγκες κάθε καταναλωτή, τις ιδιαίτερες απαιτήσεις εμπειρίας του χρήστη και τις μεμονωμένες περιπτώσεις χρήσης. Για παράδειγμα, τα δεδομένα στάθμευσης που υποδεικνύουν ποια σημεία είναι και δεν είναι καταχωρημένα, μπορούν να οδηγήσουν μια εφαρμογή στάθμευσης πολιτών με τις διαθέσιμες θέσεις, καθώς και την αντίληψη του υπαλλήλου για την κατάσταση του δημόσιου χώρου στάθμευσης. Ταυτόχρονα βοηθά στην εύρεση και ενημέρωση για τις προβληματικές περιοχές στάθμευσης στην πόλη κάθε δεδομένη στιγμή. Με διαφορετικά επίπεδα ευκρίνειας και κλίμακας, τα ίδια δεδομένα εκτελούν τρεις διαφορετικές λειτουργίες για τρεις διαφορετικούς χρήστες. Κατά τον ίδιο τρόπο, οι πληροφορίες κίνησης μπορούν να χρησιμοποιηθούν από μεμονωμένους οδηγούς αυτοκινήτων για να βρουν τη λιγότερη κυκλοφοριακή συμφόρηση. Μια παραλλαγή των ίδιων πληροφοριών μπορεί να διατεθεί στους χρήστες των δημόσιων συγκοινωνιών για τον υπολογισμό των χρόνων ταξιδιού. Τα συστήματα δημόσιων συγκοινωνιών, όπως τα λεωφορεία, μπορούν να δρομολογηθούν γύρω από γνωστά σημεία συμφόρησης. Ο αριθμός των τρένων του μετρό μπορεί να αυξηθεί δυναμικά για να ανταποκριθεί στην αύξηση της κυκλοφοριακής συμφόρησης, προβλέποντας τις αποφάσεις χιλιάδων ή ακόμη και εκατομμυρίων επιβατών να μετακινούνται με τα μέσα μαζικής μεταφοράς αντί για αυτοκίνητα τις ημέρες που οι δρόμοι είναι πολύ μποτιλιαρισμένοι.

Κεφάλαιο 10.3 Αρχιτεκτονική Ασφάλειας έξυπνης πόλης

Μια ανησυχία των περισσότερων έξυπνων πόλεων και των πολιτών τους είναι η ασφάλεια δεδομένων. Τεράστιες ποσότητες ευαίσθητων πληροφοριών μοιράζονται ανά πάσα στιγμή σε πραγματικό χρόνο και οι πόλεις έχουν καθήκον να προστατεύουν τα δεδομένα των πολιτών τους από μη εξουσιοδοτημένη πρόσβαση, συλλογή και παραποίηση. Σε γενικές γραμμές, οι πολίτες αισθάνονται καλύτερα για την ασφάλεια των δεδομένων όταν η ίδια η πόλη, κατέχει δημόσια ή σχετικά με την πόλη δεδομένα. Εναπόκειται στην πόλη και τους αξιωματούχους που τη διαχειρίζονται να καθορίσουν τον τρόπο χρήσης αυτών των δεδομένων. Όταν μια ιδιωτική οντότητα κατέχει δεδομένα σχετικά με την πόλη, το πεδίο της ιδιοκτησίας μπορεί αρχικά να είναι πολύ σαφές. Ωστόσο, αργότερα εκτιμήσεις ή αλλαγές στη στρατηγική της ιδιωτικής οντότητας μπορεί να αλλάξουν τον τρόπο χρήσης των δεδομένων. Οι ιδιωτικές οντότητες ενδέχεται να έχουν οικονομικά συμφέροντα και πολιτικά κίνητρα και μπορεί να μην έχουν τα πρότυπα ασφάλειας. Παραδοσιακά, οι αναπτύξεις δικτύου χρησιμοποιούν μια προσεγγιστική προσέγγιση και δεν ακολουθούν πάντα τα ανοιχτά πρότυπα ασφαλείας. Οι φορείς μπορούν να εκτελούν εφαρμογές, να εφαρμόζουν περιορισμένες εγγυήσεις ασφαλείας και να χρησιμοποιούν εργαλεία συνεργασίας που βασίζονται σε Cloud χωρίς την κατάλληλη ασφάλεια. Ως εκ τούτου, υπάρχει ανάγκη για έναν κεντρικό, βασισμένο σε cloud, μηχανισμό ασφαλείας που θα βασίζεται στη συμμόρφωση για την αντιμετώπιση των αναγκών των παρόχων υπηρεσιών και των τελικών χρηστών. Η ασφάλεια είναι προφανώς ένα πρόβλημα, ξεκινώντας από το πού και πώς συλλέγονται τα δεδομένα και εκτείνεται σε όλο τον κύκλο της επεξεργασίας δεδομένων.

Μια αρχιτεκτονική ασφαλείας για έξυπνες πόλεις πρέπει να χρησιμοποιεί πρωτόκολλα ασφαλείας για να ενισχύσει κάθε επίπεδο της αρχιτεκτονικής και να προστατεύσει τα δεδομένα της πόλης. Το Σχήμα 57 δείχνει μια αρχιτεκτονική αναφοράς, με επισημασμένα τα συγκεκριμένα στοιχεία ασφαλείας.



Σχήμα 57: Αρχιτεκτονική αναφοράς βασικών έξυπνων και συνδεδεμένων πόλεων.

Τα πρωτόκολλα ασφαλείας πρέπει να επαληθεύουν τα διάφορα στοιχεία και να προστατεύουν τη μεταφορά δεδομένων καθ 'όλη τη διάρκεια. Για παράδειγμα, το «χακάρισμα» αισθητήρων κυκλοφορίας για την αποστολή ψευδών δεδομένων κίνησης στο σύστημα που ρυθμίζει τα φώτα του δρόμου μπορεί να οδηγήσει σε σημαντικά προβλήματα συμφόρησης. Το συνολικό αποτέλεσμα θα ήταν τυπικά επικίνδυνο και επιζήμιο για την πόλη. Η αρχιτεκτονική ασφαλείας θα πρέπει να μπορεί να εξελίσσεται με την τελευταία λέξη της τεχνολογίας και να ενσωματώνει περιφερειακές οδηγίες.

Ξεκινώντας από το επίπεδο του δρόμου, οι αισθητήρες θα πρέπει να έχουν τα δικά τους πρωτόκολλα ασφαλείας. Ορισμένες βασικές βιομηχανικές λειτουργίες ασφαλείας περιλαμβάνουν συσκευή/αισθητήρα αναγνώρισης και εξουσιοδότησης, συσκευή/αισθητήρα κρυπτογράφησης δεδομένων. Μια άλλη σκέψη μπορεί να είναι ο τύπος δεδομένων που ο αισθητήρας είναι σε θέση να συλλέξει και να επεξεργαστεί. Οι εκτιμήσεις ασφαλείας θα πρέπει να καθορίζουν εάν αυτές οι πληροφορίες πρέπει να συλλέγονται. Εάν συλλεχθούν, θα πρέπει να ληφθεί απόφαση για το αν αυτά τα δεδομένα υποβάλλονται σε επεξεργασία χρησιμοποιώντας μια «διαδικτυακή διαδικασία» ή μια πιο κλασική διαδικασία ανάλυσης. Κατά την αποθήκευση των δεδομένων, απαιτείται πρόσθετη ασφάλεια για να διασφαλιστεί ότι οι πληροφορίες δεν θα παραβιαστούν και δεν θα κλαπούν. Αυτό ισχύει ανεξάρτητα από τη θέση όπου αποθηκεύονται τα δεδομένα(στην πύλη ή στο cloud).

Το επίπεδο πόλης μεταφέρει δεδομένα μεταξύ του επιπέδου δρόμου και του επιπέδου του κέντρου δεδομένων και λειτουργεί ως επίπεδο δικτύου. Μερικά κοινά στοιχεία της βιομηχανίας για ασφάλεια στο επίπεδο δικτύου είναι τα εξής:

Τείχος προστασίας: βρίσκεται στην άκρη και θα πρέπει να είναι έτοιμο για IPsec και VPN. Επίσης, πρέπει να περιλαμβάνει έλεγχο πρόσβασης βάσει χρηστών και ρόλων και να ενσωματωθεί με την αρχιτεκτονική για να δώσει στους χειριστές της πόλης απομακρυσμένη πρόσβαση στο κέντρο δεδομένων της πόλης.

VLAN: παρέχει τμηματοποίηση από άκρο σε άκρο της μετάδοσης δεδομένων, προστατεύοντας περαιτέρω τα δεδομένα από κακόβουλες επεμβάσεις. Κάθε υπηρεσία / τομέας έχει ένα ειδικό VLAN για μετάδοση δεδομένων.

Κρυπτογράφηση: Η προστασία της επισκεψιμότητας από τον αισθητήρα στην εφαρμογή είναι μια κοινή απαίτηση για να αποφευχθεί η παραποίηση και η υποκλοπή δεδομένων. Στις περισσότερες περιπτώσεις, η κρυπτογράφηση ξεκινά σε επίπεδο αισθητήρα.

Πολλά συγκεκριμένα στοιχεία (όπως κρυπτογράφηση) ενδέχεται να απαιτούνται από κάθε αναπτυγμένη λύση IoT για να αυξήσουν την αξιοπιστία του συστήματος. Στο επίπεδο του κέντρου δεδομένων, η κατοχή ασφαλών εικονικών ιδιωτικών cloud είναι μια κοινή απαίτηση. Η δημιουργία δυναμικών περιμέτρων γύρω από εφαρμογές, πελάτες, κεντρικούς υπολογιστές και κοινόχρηστους πόρους μπορεί να αποκρύψει περαιτέρω τα δεδομένα. Η ενσωμάτωση πλαισίων τελευταίας τεχνολογίας, όπως η αμοιβαία ασφάλεια επιπέδου μεταφοράς (mutual Transport Layer Security mTLS) ή το OAuth 2.0 για τη βεβαίωση συσκευών και την πρόσβαση βάσει ταυτότητας, είναι το κλειδί για τη διασφάλιση της ακεραιότητας μιας λύσης πόλης. Η παρακολούθηση και η ιεράρχηση της λογικής ασφαλείας στην πολυεπίπεδη αρχιτεκτονική θα μειώσει τις πιθανότητες σοβαρής παραβίασης της ασφάλειας δικτύου ή παραβίασης απορρήτου των δεδομένων της πόλης.

Κεφάλαιο 10.4 Έξυπνες πόλεις- Περιπτώσεις- Παραδείγματα

Υπάρχουν πολλοί τρόποι που μια έξυπνη πόλη μπορεί να βελτιώσει την αποτελεσματικότητά της και τη ζωή των πολιτών της. Οι παρακάτω υπό-ενότητες εξετάζουν μερικές από τις εφαρμογές που χρησιμοποιούνται συνήθως ως σημεία εκκίνησης για την εφαρμογή του IoT σε έξυπνες πόλεις. Συγκεκριμένα παρατίθενται τα εξής :

- Συνδεδεμένος φωτισμός δρόμου.
- Έξυπνος χώρος στάθμευσης.
- Έξυπνος έλεγχος κυκλοφορίας.
- Συνδεδεμένο περιβάλλον.

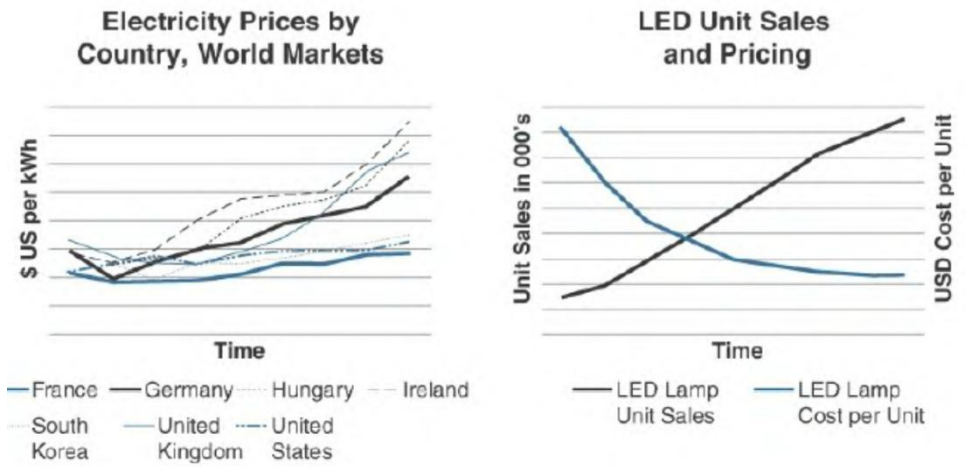
Κεφάλαιο 10.4.1 Συνδεδεμένος φωτισμός δρόμου

Από το σύνολο των αστικών υπηρεσιών κοινής ωφελείας(utilities), ο φωτισμός του δρόμου αποτελεί ένα από τις μεγαλύτερες δαπάνες, σύμφωνα με το Υπουργείο Περιβάλλοντος της Νέας Υόρκης. Η συντήρηση των φώτων του δρόμου είναι μια επιχειρησιακή πρόκληση, δεδομένου του μεγάλου αριθμού των φώτων και της τεράστιας γεωγραφικής τους κατανομής.

Λύση συνδεδεμένου φωτισμού δρόμου

Οι πόλεις συνήθως αναζητούν λύσεις που θα βοηθήσουν στη μείωση των εξόδων φωτισμού και ταυτόχρονα στη βελτίωση της αποδοτικότητας λειτουργίας, ελαχιστοποιώντας ταυτόχρονα τις αρχικές επενδύσεις. Η εγκατάσταση μιας έξυπνης λύσης φωτισμού δρόμου μπορεί να προσφέρει σημαντική εξοικονόμηση ενέργειας και μπορεί επίσης να αξιοποιηθεί για την παροχή πρόσθετων υπηρεσιών. Από αυτή την άποψη, η τεχνολογία LED(light-emitting diode) οδηγεί τη μετάβαση από τον παραδοσιακό φωτισμό του δρόμου στον έξυπνο φωτισμό δρόμου.
Τα LEDs απαιτούν λιγότερη ενέργεια για να παράγουν περισσότερο φως από τα παλιά φώτα και έχουν πολύ μεγαλύτερη διάρκεια ζωής και μεγαλύτερο κύκλο συντήρησης. Μια κορυφαία εταιρεία φωτισμού εκτιμά ότι μια πλήρης μετάβαση στην τεχνολογία LED μπορεί να μειώσει τους μεμονωμένους λογαριασμούς φωτισμού έως και 70%. Τα LEDs είναι κατάλληλα για περιπτώσεις χρήσης έξυπνων λύσεων.

Το Σχήμα 58 δείχνει πώς αυξάνονται οι τιμές ηλεκτρικής ενέργειας, ενώ οι τιμές LED μειώνονται και οι πωλήσεις μονάδων αυξάνονται.

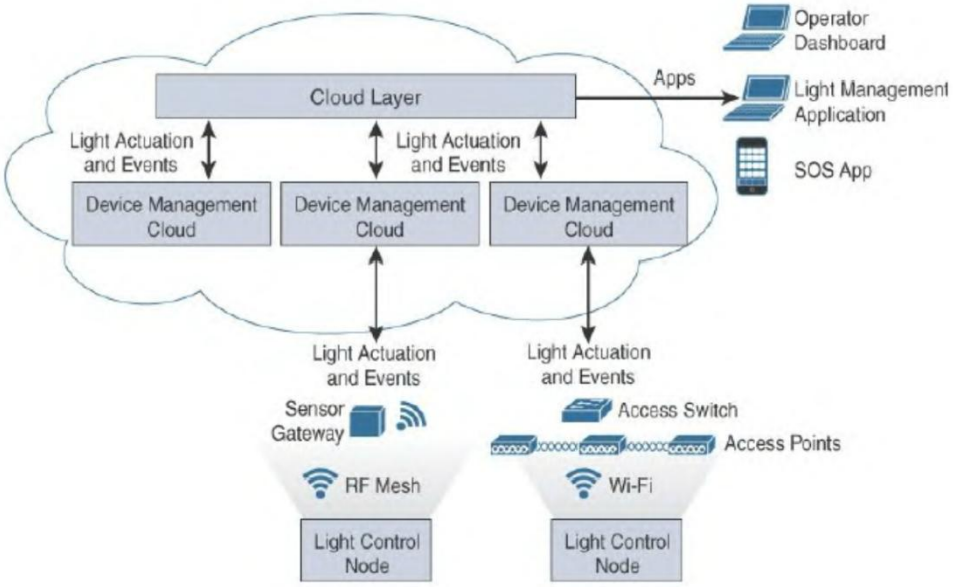


Σχήμα 58: Κόστος ηλεκτρικής ενέργειας έναντι Κόστος LED και πωλήσεις.

Η μετάβαση σε LED είναι ένας βασικός παράγοντας για τις έξυπνες πόλεις να ξεκινήσουν την πορεία προς λύσεις ICT. Καθώς οι λογαριασμοί ηλεκτρικής ενέργειας αυξάνονται και οι τιμές των LEDs μειώνονται, αυτή η μετάβαση υλικού μπορεί να ανοίξει την πόρτα σε μια ολοκληρωμένη λύση έξυπνου φωτισμού. Μια ολοκληρωμένη λύση έξυπνου φωτισμού επιτρέπει ένα δικτυωμένο σύστημα που ενσωματώνει φωτιστικά που βασίζονται σε LED και δυναμικό έλεγχο φωτισμού, υποστηριζόμενο από την πολυεπίπεδη αρχιτεκτονική της έξυπνης πόλης που συζητήθηκε νωρίτερα και είναι εύκολα επεκτάσιμο για να υποστηρίξει άλλες περιπτώσεις χρήσης και λύσεις προς όφελος της πόλης.

Αρχιτεκτονική φωτισμού δρόμου

Ο συνδεδεμένος φωτισμός χρησιμοποιεί μια εφαρμογή διαχείρισης φωτός για τη διαχείριση των φώτων του δρόμου από απόσταση, συνδέοντας την υποδομή της έξυπνης πόλης. Αυτή η εφαρμογή συνδέεται με φώτα LED, παρακολουθεί τη διαχείριση και τη συντήρησή τους και μας επιτρέπει να δούμε την κατάσταση λειτουργίας κάθε φωτός. Στις περισσότερες περιπτώσεις, μια πύλη αισθητήρα λειτουργεί ως ενδιάμεσο σύστημα μεταξύ της εφαρμογής και των φώτων (κόμβοι ελέγχου φωτός).Η πύλη μεταδίδει οδηγίες από την εφαρμογή στα φώτα και αποθηκεύει τις εκδηλώσεις του φωτισμού. Το χειριστήριο και τα φώτα LED χρησιμοποιούν το cloud για σύνδεση με την υποδομή της έξυπνης πόλης, όπως φαίνεται στο Σχήμα 59.



Σχήμα 59: Συνδεδεμένη αρχιτεκτονική φωτισμού.

Ένας ανθρώπινος ή αυτοματοποιημένος χειριστής μπορεί να χρησιμοποιήσει μια εφαρμογή cloud για να εκτελέσει αυτοματοποιημένο προγραμματισμό φώτων και ακόμη και να λάβει αισθητήρες φωτός για αυτόματη εξασθένηση ή φωτεινότητα, όπως απαιτείται. Το πρόγραμμα μπορεί επίσης να επηρεάσει το επίπεδο έντασης φωτός και πιθανώς το χρώμα, ανάλογα με τις περιβαλλοντικές συνθήκες, δηλαδή τον καιρό, την εποχή του χρόνου, την ημέρα, την τοποθεσία εντός της πόλης κ.λπ.
Ο φωτισμός, ως λύση συνδεσιμότητας ICT, χρησιμοποιεί ένα υπάρχον στοιχείο της πόλης με μια υπάρχουσα πηγή ενέργειας. Η ενεργοποίηση αυτού του στοιχείου με τεχνολογίες συνδεσιμότητας ICT όχι μόνο αυξάνει τα έσοδα από μόνη της, αλλά μπορεί επίσης να οδηγήσει σε μια λύση συνδεσιμότητας ICT, καθώς αποτελεί το πλεονέκτημα που χρησιμοποιούν διαφορετικά τεχνολογικά κομμάτια για να λειτουργήσουν.
Για παράδειγμα, οι λαμπτήρες LED είναι συνήθως εξοπλισμένοι με βασικούς αισθητήρες που μπορούν να ανιχνεύσουν φως (οδήγηση τοπικής ενεργοποίησης / απενεργοποίησης) και μπορούν επίσης να ανιχνεύσουν πολλές άλλες περιβαλλοντικές παραμέτρους, όπως θερμοκρασία, κίνηση, πίεση ή υγρασία. Η προσθήκη τέτοιων λειτουργιών στους αισθητήρες προσθέτει συνήθως μόνο κόστος. Το μεγάλο πλεονέκτημα είναι ότι τα φώτα του δρόμου μπορούν επίσης να γίνουν τοπικοί σταθμοί αναφοράς καιρού. Αυτές οι πληροφορίες είναι χρήσιμες για τους πολίτες και επίσης για συστήματα αστικών συγκοινωνιών που πρέπει να εντοπίζουν συνθήκες οδήγησης σε πραγματικό χρόνο.
Λειτουργίες όπως η παρακολούθηση της ισχύος, η μέτρηση των επιπέδων οξυγόνου και διοξειδίου του άνθρακα, η μέτρηση της ποσότητας ρύπανσης ή σωματιδίων και η ανίχνευση επιπέδων υπεριώδους ακτινοβολίας long-wave (ultraviolet A UVA) και υπεριώδους ακτινοβολίας short-wave (ultraviolet B UVB) μπορούν επίσης να προστεθούν και να παρέχουν πρόσθετες αξίες και υπηρεσίες (για παράδειγμα, παρακολούθηση της ρύπανσης, παρακολούθηση ενεργειακού δικτύου).

Μπορούν επίσης να ενσωματωθούν πιο εξειδικευμένες δυνατότητες, όπως η βασική λειτουργία ήχου ή βίντεο με ανάλυση για τον εντοπισμό κυκλοφοριακής συμφόρησης ή τροχαίων ατυχημάτων σε πραγματικό χρόνο. Σε αυτή την περίπτωση, οι τεχνολογίες συνδεσιμότητας δικτύου είναι σημαντικές καθώς αυξάνεται η κατανάλωση και το εύρος ζώνης. Η αποδοτικότητα είναι ένα βασικό χαρακτηριστικό των έξυπνων πόλεων, συμπεριλαμβανομένου του συνδεδεμένου φωτισμού. Για παράδειγμα, η ποσότητα

φωτισμού μπορεί να μειωθεί σε αυτοκινητόδρομους όπου δεν ανιχνεύονται αυτοκίνητα. Τα φώτα μπορούν να ρυθμιστούν ώστε να αναβοσβήνουν με ένα συγκεκριμένο μοτίβο για να βοηθήσουν την αστυνομία να εντοπίσει γρήγορα μια συγκεκριμένη τοποθεσία GPS.

Η χρήση του IoT για φωτισμό επιτρέπει πληθώρα χρήσιμων εφαρμογών και για το λόγο αυτό, ο φωτισμός χρησιμοποιείται συχνά ως εισαγωγική λειτουργία IoT για εφαρμογές έξυπνων πόλεων. Οι δήμοι συχνά ξεκινούν με την εξοικονόμηση κόστους ενέργειας ως πρωταρχική προτεραιότητα και σύντομα συνειδητοποιούν ότι οι αισθητήρες που προστίθενται στην ήδη εγκατεστημένη υποδομή φωτισμού IoT μπορούν να προσθέσουν σημαντικά οφέλη και πλεονεκτήματα στη διαχείριση της πόλης.

Κεφάλαιο 10.4.2 Έξυπνος χώρος στάθμευσης

Ο χώρος στάθμευσης είναι μια πρόκληση για τις πόλεις, σε όλο τον κόσμο. Σύμφωνα με τους ερευνητές πολεοδομίας, έως και το 30% των αυτοκινήτων που οδηγούν σε κυκλοφοριακή συμφόρηση στο κέντρο της πόλης αναζητούν θέσεις στάθμευσης. Η αναποτελεσματική πρόσβαση στο πάρκινγκ και η διαχείριση καθιστούν τη στάθμευση στις αστικές περιοχές μόνιμο αγώνα και επηρεάζει τις πόλεις με πολλούς τρόπους.

Περιπτώσεις έξυπνης στάθμευσης

Μία πολύ σημαντική αιτία της αυξημένης κυκλοφοριακής συμφόρησης είναι η αναζήτηση χώρου στάθμευσης από τους οδηγούς. Συνέπειες του φαινομένου αυτού είναι οι εξής:

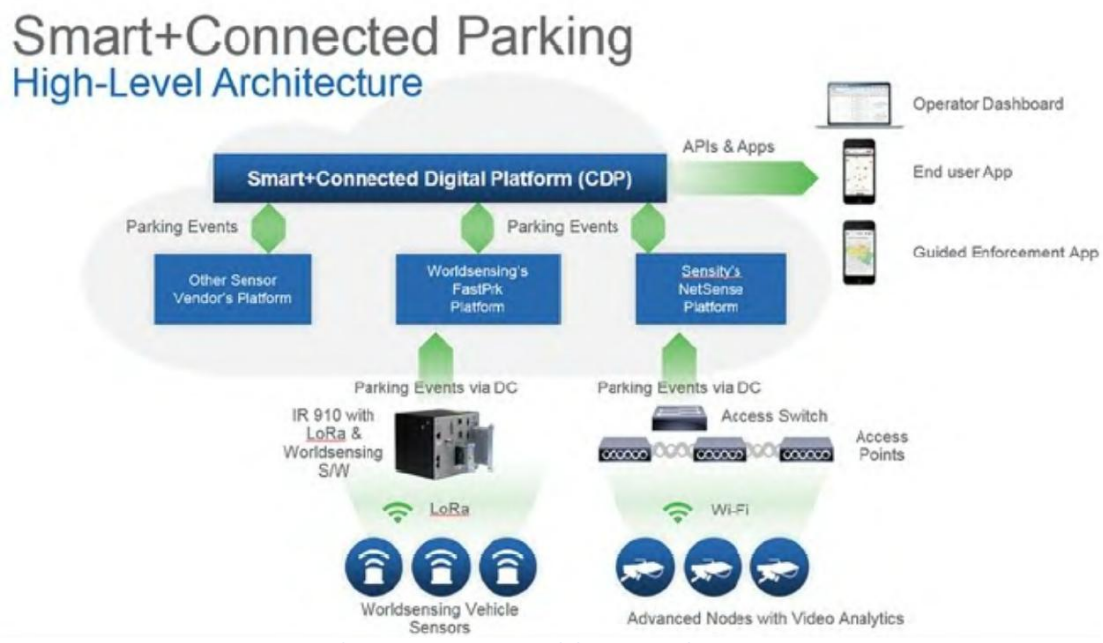
- Συμβάλλει στη ρύπανση. Τόνοι επιπλέον εκπομπών διοξειδίου του άνθρακα απελευθερώνονται στο περιβάλλον της πόλης λόγω των αυτοκινήτων που κυκλοφορούν αναζητώντας θέσεις στάθμευσης όταν θα μπορούσαν να σταθμεύσουν.
- Προκαλεί την απογοήτευση των οδηγών. Στις περισσότερες πόλεις, η έλλειψη θέσης στάθμευσης οδηγεί τους οδηγούς να χάσουν την υπομονή τους και να χάσουν χρόνο, οδηγώντας με οργή στο δρόμο, απροσεξία και άλλους παράγοντες όπως το στρες.
- Αυξάνει τα περιστατικά κυκλοφορίας. Οι οδηγοί που αναζητούν θέσεις στάθμευσης προκαλούν αυξημένη συμφόρηση στους δρόμους και αυτό, με τη σειρά του, προκαλεί αυξημένα ατυχήματα και άλλα τροχαία περιστατικά.
- Η απώλεια εσόδων. Είναι μία άλλη συνέπεια των οδηγών που αναζητούν ανεπιτυχώς χώρο στάθμευσης και έχει επίσης διάφορες αρνητικές παρενέργειες.
- Οι πόλεις συχνά χάνουν έσοδα. Ως αποτέλεσμα της ανεπαρκούς τέλους στάθμευσης και της απαγόρευσης στάθμευσης, οι πόλεις χάνουν έσοδα.
- Η παραγωγικότητα των υπαλλήλων της διοίκησης στάθμευσης υποφέρει. Οι εργαζόμενοι χάνουν χρόνο περιφέροντας στους δρόμους, προσπαθώντας να εντοπίσουν παραβάτες των κανόνων στάθμευσης.
- Η διαθεσιμότητα στάθμευσης επηρεάζει το εισόδημα. Τα τοπικά καταστήματα και οι επιχειρήσεις χάνουν πελάτες λόγω της μειωμένης προσβασιμότητας που προκαλείται από τις ελλείψεις χώρων στάθμευσης.

Αρχιτεκτονική έξυπνης στάθμευσης

Μια ποικιλία αισθητήρων στάθμευσης είναι διαθέσιμες στην αγορά και έχουν διαφορετικές προσεγγίσεις για την ανίχνευση πληρότητας για θέσεις στάθμευσης.
Τέτοια ποικιλία είναι η εξής:

- Μαγνητικοί αισθητήρες στο έδαφος, οι οποίοι χρησιμοποιούν ενσωματωμένους αισθητήρες για να δημιουργήσουν ένα μαγνητικό πεδίο ανίχνευσης σε ένα χώρο στάθμευσης.
- Αισθητήρες που βασίζονται σε βίντεο, οι οποίοι ανιχνεύουν γεγονότα με βάση τον υπολογισμό βίντεο (κινήσεις ή παρουσία οχημάτων).
- Αισθητήρες ραντάρ που ανιχνεύουν την παρουσία οχημάτων (ογκομετρική ανίχνευση).

Οι περισσότεροι αισθητήρες που είναι εγκατεστημένοι στο έδαφος πρέπει να βασίζονται στην ισχύ της μπαταρίας. Συνήθως αντιδρούν σε αλλαγές, όπως μια αλλαγή στο μαγνητικό πεδίο, προκαλώντας έναν αισθητήρα να αφυπνίσει και να στείλει μια αναφορά συμβάντος. Επειδή αυτά τα γεγονότα δεν είναι πολύ συχνά, η μπαταρία μπορεί να διαρκέσει πολύ. Για έναν τυπικό αισθητήρα στάθμευσης, με βάση την ενέργεια που καταναλώνει κάθε συμβαν, μια διάρκεια ζωής 600.000 συμβάντων δεν είναι ασυνήθιστη. Ένα πολύ πολυσύχναστο σημείο στάθμευσης, όπου ένα αυτοκίνητο εισέρχεται ή βγαίνει κάθε 10 λεπτά, θα επέτρεπε 10 χρόνια μπαταρίας-και είναι ασυνήθιστο να βλέπουμε θέσεις στάθμευσης με τόσο βαριά χρήση. Σε περιβάλλοντα υψηλής πυκνότητας (για παράδειγμα, εσωτερικός χώρος στάθμευσης, καταστρώματα στάθμευσης), μία ή περισσότερες πύλες ανά όροφο ενδέχεται να συνδεθούν με τους αισθητήρες στάθμευσης, χρησιμοποιώντας πρωτόκολλα μικρότερης εμβέλειας, όπως το ZigBee ή το Wi-Fi. Στη συνέχεια, η πύλη μπορεί να χρησιμοποιήσει άλλο πρωτόκολλο (ενσύρματο ή ασύρματο) για σύνδεση με το σταθμό ελέγχου. Σε μεγαλύτερα (για παράδειγμα, εξωτερικά) περιβάλλοντα, ένα πρωτόκολλο μεγαλύτερης εμβέλειας Low Power Wide Area (LPWA) είναι κοινό, όπως φαίνεται στο Σχήμα 60.



Σχήμα 60: Αρχιτεκτονική έξυπνης στάθμευσης.

Οι τεχνολογικές καινοτομίες συμβαίνουν συνεχώς, καθιστώντας την αρχιτεκτονική συνδεσιμότητας ICT ακόμη πιο σημαντική. Για παράδειγμα, οι νέες τεχνολογίες ανίχνευσης βασίζονται στην ανίχνευση των εκπομπών ραδιοφώνου (Bluetooth και άλλων) που προέρχονται από ένα όχημα. Η υιοθέτηση τέτοιων νέων τεχνολογιών συνεπάγεται ότι η αρχιτεκτονική επικοινωνίας είναι αρκετά ανοιχτή για να καλύψει τις ανάγκες αυτών των νέων συστημάτων. Ο συνδυασμός αυτών των τεχνολογιών με καινοτόμους τρόπους διευρύνει επίσης τις δυνατότητες των υπηρεσιών που μπορούν να προσφέρουν τα συστήματα IoT, για τον έξυπνο χώρο στάθμευσης.

Για παράδειγμα, οι αισθητήρες μπορούν να εγκατασταθούν σε θέσεις στάθμευσης με ειδικές ανάγκες. Μια εφαρμογή μπορεί να χρησιμοποιηθεί για τους οδηγούς να καταχωρήσουν την αναπηρία τους και στη συνέχεια να εντοπίσουν αυτά τα σημεία πιο εύκολα. Όταν ένας χρήστης σταθμεύει, ο αισθητήρας μπορεί να επικοινωνήσει με την εφαρμογή στο έξυπνο τηλέφωνο του οδηγού για να επικυρώσει την κατάσταση αναπηρίας και να περιορίσει τη παράνομη χρήση αυτών των θέσεων στάθμευσης από οδηγούς που δεν έχουν αναπηρία.

Ανεξάρτητα από την τεχνολογία που χρησιμοποιείται, οι αισθητήρες στάθμευσης είναι συνήθως αντικείμενα που οδηγούνται από συμβάντα. Ένας αισθητήρας ανιχνεύει ένα συμβάν και το προσδιορίζει με βάση το χρόνο ή την ανάλυση. Το συμβάν μεταδίδεται μέσω του πρωτοκόλλου επικοινωνίας της συσκευής σε ένα σημείο πρόσβασης ή πύλη, η οποία προωθεί τα δεδομένα συμβάντων μέσω του επιπέδου της πόλης. Η πύλη το στέλνει στο σε μια εφαρμογή cloud. Μια εφαρμογή εμφανίζει το συμβάν στάθμευσης σε smart phones, όπου μπορεί να γίνει κάποια ενέργεια. Για παράδειγμα, ένας οδηγός μπορεί να κλείσει ένα κοντινό σημείο στάθμευσης ή ένας χειριστής στάθμευσης μπορεί να το αφαιρέσει από τη λίστα των διαθέσιμων θέσεων στάθμευσης . Αυτή η ενέργεια ενεργοποιεί την αποστολή δεδομένων στον αισθητήρα στάθμευσης για να τροποποιήσει την κατάσταση διαθεσιμότητάς του με βάση τις ληφθείσες οδηγίες. Με τη σειρά του, ο αισθητήρας μπορεί να αλληλεπιδρά με κοντινά συστήματα.

Για παράδειγμα, σε απάντηση αυτών των οδηγιών, τα φώτα πάνω από τις θέσεις στάθμευσης μπορούν να γίνουν κόκκινα, πορτοκαλί ή πράσινα για να εμφανιστεί ένα ελεύθερο, κρατημένο ή κατειλημμένο σημείο, διευκολύνοντας έτσι την αναζήτηση του οδηγού για ένα διαθέσιμο σημείο στάθμευσης. Ομοίως, ένας αισθητήρας στάθμευσης μπορεί να στείλει μια κατάσταση σε έναν μετρητή θέσης στάθμευσης στην είσοδο του στρώματος στάθμευσης για να εμφανίσει πόσα σημεία είναι διαθέσιμα σε μια δεδομένη περιοχή, όπως σε έναν συγκεκριμένο όροφο ενός επιπέδου στάθμευσης. Αυτή η επικοινωνία μπορεί να είναι άμεση αλλά συχνά περνάει από μια πύλη, το δίκτυο και την εφαρμογή που επικοινωνεί με τα άλλα συστήματα μέσω APIs. Ο χρήστης μπορεί επίσης να έχει πρόσβαση στα δεδομένα από εφαρμογές cloud για να δει τη λίστα των διαθέσιμων σημείων σε μια συγκεκριμένη περιοχή της πόλης ή της γειτονιάς. Μπορούν επίσης να ενσωματωθούν έξυπνα δεδομένα όπως για παράδειγμα, να αυξηθεί η έκπτωση σε πιο μακρινά σημεία στάθμευσης ή να αυξηθεί το κόστος των θέσεων στάθμευσης σε χώρους κοντινούς σε συγκεκριμένες ώρες (όπως αθλητικές εκδηλώσεις ή συναυλίες).

Κεφάλαιο 10.4.3 Έλεγχος έξυπνης κυκλοφορίας

Η κίνηση είναι η κύρια αιτία τυχαίου θανάτου παγκοσμίως, προκαλεί τεράστια απογοήτευση και συμβάλλει σημαντικά στη ρύπανση σε όλο τον κόσμο. Μια λύση έξυπνης κυκλοφορίας στις πόλεις θα συνδυάζει πληροφορίες συγκοινωνίας, καταμέτρηση οχημάτων και θα στέλνει ενημερώσεις σχετικές με περιστατικά στο δρόμο, έτσι ώστε άλλοι ελεγκτές στο δρόμο να μπορούν να αναλάβουν δράση.

Αρχιτεκτονική ελέγχου έξυπνης κυκλοφορίας

Στην αρχιτεκτονική που φαίνεται στο Σχήμα 61. ένας αισθητήρας ανάλυσης βίντεο υπολογίζει συμβάντα επισκεψιμότητας με βάση μια ροή βίντεο και προωθεί μόνο συμβάντα (τον αριθμό αυτοκινήτου), μέσω του δικτύου. Αυτά τα συμβάντα περνούν από τα αρχιτεκτονικά επίπεδα και φτάνουν στις εφαρμογές που μπορούν να οδηγήσουν τις υπηρεσίες κίνησης. Αυτές οι υπηρεσίες περιλαμβάνουν συντονισμό φαναριών και επίσης αναγνώριση πινακίδων για δρόμους με διόδια. Ορισμένοι αισθητήρες μπορούν επίσης να αναγνωρίσουν μη φυσιολογικά συμβάντα, όπως οχήματα που κινούνται σε λάθος κατεύθυνση.
Άλλοι τύποι αισθητήρων που αποτελούν μέρος των λύσεων ελέγχου της κυκλοφορίας περιλαμβάνουν Bluetooth μετρητές οχημάτων, μετρητές ταχύτητας και συστήματα ελέγχου φωτισμού. Αυτοί οι αισθητήρες παρέχουν μια προοπτική σε πραγματικό χρόνο.
Οι τεχνικές επικοινωνίας είναι τόσο διαφορετικές όσο οι παράγοντες μορφής αισθητήρα. Για παράδειγμα, οι μετρητές που είναι εγκατεστημένοι σε φανάρια ενδέχεται να χρησιμοποιούν ενσύρματη ή ασύρματη τεχνολογία και οποιονδήποτε αριθμό πρωτοκόλλων επικοινωνίας. Όταν ένας αισθητήρας δεν συνδυάζεται με άλλη αστική εφαρμογή IoT, συνήθως χρησιμοποιούνται ασύρματες τεχνολογίες.

Εφαρμογές έξυπνης κυκλοφορίας

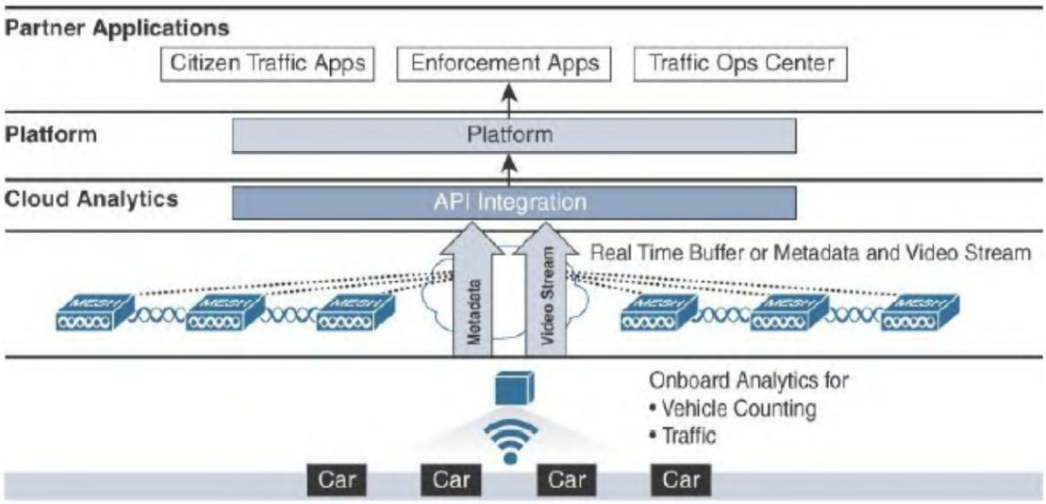
Οι εφαρμογές κυκλοφορίας μπορούν να ενεργοποιηθούν για άμεση δράση με άλλους αισθητήρες για τη διαχείριση της κυκλοφορίας. Τα δεδομένα μπορούν να χρησιμοποιηθούν για την ανάπτυξη πιο αποτελεσματικού πολεοδομικού σχεδιασμού για τη μείωση του όγκου κίνησης που βιώνει μια πόλη.
Η εντύπωση είναι ότι η κίνηση είναι αργή αλλά κινούμενη και το συνολικό αποτέλεσμα είναι μια καλύτερη εμπειρία μετακίνησης, με μειωμένο και λιγότερο αγχωτικό χρόνο μετακίνησης, καθώς και μειωμένο αριθμό ατυχημάτων.
Αμέτρητες εφαρμογές αξιοποιούν πληροφορίες που προέρχονται από αισθητήρες για να παρέχουν εκτιμήσεις χρόνου ταξιδιού σε πραγματικό χρόνο, προτείνουν επιλογές για την αποφυγή σημείων κυκλοφοριακής συμφόρησης ή απλά βρίσκουν τον καλύτερο τρόπο μεταξύ δύο σημείων, λαμβάνοντας υπόψη την κίνηση, τις οδικές εργασίες κ.λπ.
Η κατανόηση των τρόπων κίνησης σε πραγματικό χρόνο μιας πόλης και η ικανότητα αποτελεσματικού περιορισμού των προβλημάτων κυκλοφορίας μπορεί να αποφέρει τεράστια αξία για μια πόλη. Αισθητήρες που μετρούν συσκευές ή αυτοκίνητα, αισθητήρες ανίχνευσης κινήσεων και αισθητήρες που μετρούν τη συγκέντρωση αερίου στον αέρα μπορούν όλα να αξιοποιηθούν για να παρέχουν μια εκτίμηση των συνθηκών κυκλοφορίας. Η εκτίμηση που προκύπτει μπορεί να αξιοποιηθεί με πολλούς τρόπους, όπως σε επίπεδο πόλης για τη ρύθμιση της ροής της κυκλοφορίας και σε επίπεδο πολιτών για καλύτερη εμπειρία οδήγησης.

Κεφάλαιο 10.4.4 Συνδεδεμένο Περιβάλλον(Connected Environment)

Περισσότερο από το 90% του παγκόσμιου αστικού πληθυσμού αναπνέει αέρα με επίπεδα ρύπων που είναι πολύ υψηλότερα από τα συνιστώμενα όρια και ένας στους οκτώ θανάτους παγκοσμίως είναι αποτέλεσμα μολυσμένου αέρα. Οι περισσότερες μεγάλες πόλεις παρακολουθούν την ποιότητα του αέρα τους. Τα δεδομένα συχνά προέρχονται από τεράστιους σταθμούς παρακολούθησης της ποιότητας του αέρα που είναι ακριβοί και υπάρχουν εδώ και δεκαετίες. Αυτοί οι σταθμοί είναι εξαιρετικά ακριβείς στις μετρήσεις τους αλλά και πολύ περιορισμένοι στην εμβέλειά τους και μια πόλη είναι πιθανό να έχει πολλά τυφλά σημεία στην κάλυψη. Δεδομένης της τιμής και του μεγέθους των σταθμών παρακολούθησης της ποιότητας του αέρα, οι πόλεις δεν μπορούν να αγοράσουν τον αριθμό των σταθμών που απαιτούνται για την παροχή ακριβών αναφορών σε τοπικό επίπεδο και την παρακολούθηση των ροών ρύπανσης.

Αρχιτεκτονική Συνδεδεμένου Περιβάλλοντος

Το Σχήμα 61 δείχνει μια αρχιτεκτονική στην οποία όλα τα συνδεδεμένα στοιχεία περιβάλλοντος επικαλύπτονται με τη γενικευμένη αρχιτεκτονική IoT έξυπνης πόλης τεσσάρων επιπέδων που παρουσιάστηκε νωρίτερα σε αυτό το κεφάλαιο.



Σχήμα 61: Αρχιτεκτονική Συνδεδεμένου Περιβάλλοντος.

Όπως φαίνεται στο Σχήμα 61 στο στρώμα του δρόμου, υπάρχει μια ποικιλία από αισθητήρες πολλαπλών χρήσεων, χρησιμοποιώντας μια ποικιλία πρωτοκόλλων επικοινωνίας. Οι συνδεδεμένοι αισθητήρες περιβάλλοντος ενδέχεται να μετρούν διαφορετικά αέρια, ανάλογα με τα ιδιαίτερα προβλήματα ποιότητας της πόλης και μπορεί να περιλαμβάνουν αισθητήρες καιρού και θορύβου. Αυτοί οι αισθητήρες μπορεί να βρίσκονται σε μια ποικιλία αστικών εγκαταστάσεων, όπως στα φώτα του δρόμου. Μπορούν επίσης να ενσωματωθούν στο έδαφος ή σε άλλες δομές ή υποδομές έξυπνων πόλεων. Οι τεχνολογίες επικοινωνίας εξαρτώνται από τη θέση των αισθητήρων. Οι αισθητήρες που είναι εγκατεστημένοι σε αστικά συστήματα χρησιμοποιούν επίσης μια ποικιλία τεχνολογιών επικοινωνίας. Οι αισθητήρες που περιλαμβάνονται στα συστήματα φωτισμού του δρόμου ενδέχεται να χρησιμοποιούν την ίδια υποδομή επικοινωνίας με την εφαρμογή ελέγχου φωτισμού δρόμου.

Οι ανεξάρτητοι αισθητήρες συνήθως χρησιμοποιούν ασύρματες τεχνολογίες. Εκτός από όλους τους αισθητήρες ποιότητας του αέρα, το επίπεδο του κέντρου δεδομένων ή το

επίπεδο εφαρμογής που απεικονίζεται στην αριστερή πλευρά του Σχήματος 61 λαμβάνει επίσης τα ανοιχτά δεδομένα από τους υπάρχοντες μετεωρολογικούς σταθμούς ως πρόσθετη εισαγωγή δεδομένων. Όλες αυτές οι εισαγωγές δεδομένων συγκεντρώνονται για να παρέχουν μια πολύ ακριβή αίσθηση της ποιότητας του αέρα στην πόλη ανά πάσα στιγμή. Διαφορετικά επίπεδα ρύπανσης μπορούν να κοινοποιηθούν και τα αέρια μπορούν να εντοπιστούν καθώς κινούνται σε όλη την πόλη, είτε λόγω του ανέμου είτε λόγω της κίνησης των πηγών αερίου (για παράδειγμα, η συστηματική ταλάντευση του εκκρεμούς των μετακινήσεων των επιβατών το πρωί και το βράδυ δημιουργεί πρότυπα ρύπανσης κατά μήκος των πυκνότερων οδών κυκλοφορίας).
Από τα περιβαλλοντικά δεδομένα και τις αναλύσεις που εφαρμόζονται σε αυτήν, η πόλη μπορεί να εντοπίσει προβληματικές περιοχές και με ένα μακροπρόθεσμο πολεοδομικό σχεδιασμό να ξεκινήσει η διαδικασία για τη μείωση των επιπτώσεων των διαταραχών της ποιότητας του αέρα. Στρατηγικές και συντονισμένες κοινές δράσεις, όπως ο περιορισμός της κυκλοφορίας σε συγκεκριμένες διαδρομές ή σε ορισμένες ημέρες και η ενθάρρυνση των πολιτών να χρησιμοποιούν τις δημόσιες μεταφορές, είναι δυνατές.

Κεφάλαιο 11 Μέσα Μεταφοράς

Η αποτελεσματική μεταφορά έχει φέρει επανάσταση στον τρόπο επικοινωνίας και αλληλεπίδρασης των ανθρώπων. Με ισχυρότερους και φθηνότερους κινητήρες, ο αριθμός των - διαφόρων μεγεθών - επαγγελματικών οχημάτων, επιβατικών αυτοκινήτων, λεωφορείων και τρένων (συμπεριλαμβανομένων των υπόγειων και των τραμ), όλα αυτά τα μέσα αυξήθηκαν σημαντικά κατά τον εικοστό αιώνα. Αυτή η αύξηση, έφερε αυξημένη συμφόρηση, ατυχήματα και ρύπανση. Επίσης, αυτή η εκρηκτική ανάπτυξη των συστημάτων ιδιωτικών και δημόσιων μεταφορών συνοδεύτηκε από αυξανόμενες προκλήσεις που σχετίζονται με την ασφάλεια, την ταξιδιωτική εμπειρία και την προβλεψιμότητα του ταξιδιού γενικά.
Σε επίπεδο οχήματος, πολλαπλοί αισθητήρες μπορούν να παρέχουν μια προληπτική εικόνα των συνθηκών του οχήματος, περιορίζοντας τον αριθμό των αιφνιδιαστικών βλαβών. Ταυτόχρονα, τα έξυπνα ενσωματωμένα συστήματα επιτρέπουν μια καλύτερη εμπειρία ταξιδιού επιτρέποντας στο όχημα να αντιδρά δυναμικά και να προσαρμόζεται στις περιβαλλοντικές συνθήκες. Ακόμα οι ταξιδιώτες μπορούν να έχουν άμεσα οφέλη μέσω πιο αποτελεσματικών συστημάτων συγκοινωνίας και μέσω έξυπνων πινάκων σε σταθμούς λεωφορείων ή τρένων που παρέχουν μια έξυπνη εικόνα του ταξιδιού μέσω του συστήματος μεταφοράς.
Το IoT και ο αυτοματισμός μπορούν να βοηθήσουν οδηγούς παρέχοντας πληροφορίες σε πραγματικό χρόνο για την απόδοση του οχήματος και τις αναμενόμενες συνθήκες ταξιδιού. Επίσης μπορεί να βοηθήσει ολόκληρες πόλεις και χώρες να βελτιστοποιήσουν την κυκλοφορία και τις μεταφορές

Αυτό το κεφάλαιο περιλαμβάνει τις ακόλουθες ενότητες:

- Μεταφορές: Παρέχει μια εικόνα της βιομηχανίας μεταφορών και των τομέων της.
- Προκλήσεις μεταφορών: Περιγράφει προκλήσεις που επηρεάζουν τα ταξίδια που γίνονται με χρήση δρόμου(Connected Cars).
- IoT- Περιπτώσεις για μαζική μεταφορά: Παρέχει πληροφορίες για το πώς το IoT μπορεί να αλλάξει σημαντικά τη βιομηχανία μέσων μεταφορών και την ταξιδιωτική εμπειρία.

Κεφάλαιο 11.1 Μεταφορές και Μεταφορικά Μέσα

Ο κλάδος των μεταφορών περιλαμβάνει πολλούς τομείς. Τέτοιοι μπορεί να είναι τα μέσα μεταφοράς(μετρό, τραμ, τρόλεϊ, φέρυ-μποτ και λεωφορεία), σιδηρόδρομος, οδικοί άξονες, αεροπορία, ναυτιλία και επιβατικά οχήματα. Κάθε τομέας ή τρόπος μεταφοράς μπορεί επίσης να περιλαμβάνει πολλαπλούς εξειδικευμένους τομείς. Για παράδειγμα, οι αεροπορικές μεταφορές περιλαμβάνουν αεροδρόμια, περιφερειακές ή εθνικές αρχές ελέγχου εναέριας κυκλοφορίας, αεροπορικές εταιρείες, εταιρείες συντήρησης πολλαπλών ειδών και, φυσικά, κατασκευαστές αεροσκαφών. Το Σχήμα 62 απεικονίζει τους κοινούς τομείς μεταφοράς.

Σχήμα 62: Τομείς Μεταφορών.

Καθώς τα μεταφορικά μέσα πολλαπλασιάστηκαν, εμφανίστηκαν προκλήσεις που σχετίζονται με την κλίμακα που αφορά τον χρήστη ή γενικά έναν οργανισμό. Με περισσότερα οχήματα, η διαχείριση και η συντήρηση δρόμων και σιδηροδρόμων γίνεται πιο δύσκολη. Η διατήρηση υψηλών επιπέδων ασφάλειας ενώ αυξάνεται η κίνηση απαιτεί βελτιστοποιημένη αποδοτικότητα διαχείρισης. Όσον αφορά τη κλίμακα χρήστη, η συντήρηση ενός οχήματος είναι μάλλον εύκολη. Όμως σε κλίμακα μιας μεγάλης επιχείρησης ή ενός οργανισμού δημόσιων συγκοινωνιών, η διατήρηση είναι πολύ πιο δύσκολη. Η παρακολούθηση της θέσης και της συντήρησης κάθε οχήματος απαιτεί προληπτικούς τρόπους παρακολούθησης κάθε οχήματος. Αυτές οι προκλήσεις είναι κοινές για όλα τα οχήματα και τα μέσα μεταφοράς (αεροπορικά, θαλάσσια, σιδηροδρομικά ή οδικά). Ωστόσο, κάθε τομέας μεταφορών έχει μοναδικές προκλήσεις. Τρεις τομείς μεταφορών χρησιμοποιούνται ως απεικονίσεις του τρόπου με τον οποίο το IoT μεταμορφώνει αυτόν τον κλάδο:

1.Οδικός Άξονας. Περιλαμβάνει τα οχήματα και ολόκληρη την υποδομή των δρόμων όπως είναι τα φανάρια, οι κάμερες, οι αισθητήρες δρόμου, τα διόδια, τη ψηφιακή σήμανση κ.λπ. Λόγω της ισχυρής και άμεσης επίδρασης στη ζωή των ατόμων, οι βελτιώσεις του IoT στους δρόμους είναι τεράστιες και πολύ ορατές.
Οι προκλήσεις στους δρόμους είναι ίσως οι πιο γνωστές επειδή τα οδικά ζητήματα αναφέρονται συχνά στις ειδήσεις. Μερικές από τις μεγαλύτερες προκλήσεις που αντιμετωπίζουν σήμερα οι φορείς εκμετάλλευσης οδών είναι στους τομείς της ασφάλειας, της κινητικότητας και του περιβάλλοντος:

Ασφάλεια: Σύμφωνα με το Υπουργείο Μεταφορών των ΗΠΑ, 6,3 εκατομμύρια ατυχήματα αναφέρθηκαν στις Ηνωμένες Πολιτείες το 2015, με αποτέλεσμα περισσότερους από 33.000 νεκρούς και 2,4 εκατομμύρια τραυματίες.

Κινητικότητα: Με πάνω από 1 δισεκατομμύριο αυτοκίνητα στους δρόμους παγκοσμίως, η συμφόρηση έχει γίνει μείζον ζήτημα. Ο Παγκόσμιος Οργανισμός Υγείας (ΠΟΥ, ο φορέας δημόσιας υγείας των Ηνωμένων Εθνών) έχει υπολογίσει ότι 5,5 δισεκατομμύρια ώρες καθυστερήσεων ταξιδιού προκαλούνται παγκοσμίως από τη συμφόρηση. Αυτές οι καθυστερήσεις αντιπροσωπεύουν κόστος 101 δισεκατομμυρίων δολαρίων μόνο στις ΗΠΑ.

Περιβάλλον: Σύμφωνα με την Αμερικανική Ένωση Δημοσίων Μεταφορών, κάθε χρόνο η συμφόρηση δημιουργεί πάνω από 3 δισεκατομμύρια σπατάλη καυσίμου στις Ηνωμένες Πολιτείες. Επιπλέον, οι μεταφορές δημιουργούν σχεδόν το ένα τρίτο των εκπομπών αερίων θερμοκηπίου.

Η οδήγηση τη νύχτα ή σε δύσκολες καιρικές συνθήκες είναι επικίνδυνη. Η έλλειψη ορατότητας, τα αργά οχήματα, τα απρόσμενα εμπόδια και άλλοι οδηγοί προσθέτουν τις προκλήσεις. Γενικά οι άνθρωποι θεωρούν και αναμένουν ότι τα αυτοκίνητα και οι μοτοσικλέτες θα έχουν το ίδιο επίπεδο ευφυΐας που βλέπουν σε ένα έξυπνο τηλέφωνο ή σε συστήματα πλοήγησης. Τα αυτοκίνητα αναμένεται να είναι έξυπνα εργαλεία. Σε αυτόν τον τομέα, το IoT μπορεί να βοηθήσει στη βελτίωση της εμπειρίας ταξιδιού, παρέχοντας λεπτομερείς πληροφορίες σχετικά με την κατάσταση του οχήματος και προβλέποντας την κούραση ή την αποτυχία οποιουδήποτε στοιχείου. Τα έξυπνα αντικείμενα μπορούν επίσης να βοηθήσουν ένα όχημα και τον οδηγό του να επικοινωνούν με την ευρύτερη υποδομή των οδικών οδών, να προβλέπουν εμπόδια ή να έχουν καλύτερη ορατότητα στις συνθήκες του ταξιδιού. Αυτή η βελτιωμένη ορατότητα διευκολύνει την κινητικότητα, μειώνει τη ρύπανση και επίσης αυξάνει την ασφάλεια με μηχανισμούς αποφυγής σύγκρουσης και προειδοποίησης αστοχίας. Αυτή η προσδοκία για έξυπνα οχήματα την έχει επίσης και κάθε οργανισμός. Με εκατοντάδες ή χιλιάδες ανεπτυγμένα οχήματα και πληρώματα, οι οργανισμοί πρέπει να είναι σε θέση να γνωρίζουν πού βρίσκεται κάθε όχημα, να προειδοποιούνται για μηχανικά προβλήματα.

2.Μεταφορικά μέσα. Περιλαμβάνει τα οχήματα στις συλλογικές μεταφορές. Αυτός ο τομέας είναι πολύ σημαντικός, για αλλαγές στους άλλους τομείς. Η μαζική μεταφορά, είναι ένα σύστημα συλλογικών μεταφορών που συνδέει διαφορετικές τοποθεσίες μιας δεδομένης αστικής περιοχής. Μπορεί να αναφέρεται σε λεωφορεία, τραμ, τρόλεϊ, μετρό ακόμα σε ράγες(να περιλαμβάνει δηλαδή και τα τρένα). Η μαζική μεταφορά (λεωφορεία, τραμ) μπορεί να μοιράζεται το δρόμο με άλλα οχήματα και ως εκ τούτου συχνά υπόκειται στις ίδιες προκλήσεις σε σχέση με τη συμφόρηση. Το κίνητρο να αφήσουμε το αυτοκίνητο στο σπίτι μας για να πάρουμε το λεωφορείο δεν είναι τόσο σημαντικό εάν το λεωφορείο έχει κολλήσει στην ίδια κυκλοφοριακή συμφόρηση(που θα είχαμε και με το αυτοκίνητο μας). Αντίθετα, τα τρένα καλύπτουν πολλαπλές πραγματικότητες. Μερικά από αυτά ταξιδεύουν μεταξύ πόλεων. Τα συστήματα μαζικής μεταφοράς(συμπεριλαμβανομένων σιδηροτροχιών, μετρό, λεωφορείων) ταξιδεύουν σε μικρότερες αποστάσεις αλλά με πολύ μεγαλύτερη συχνότητα. Οι επιβάτες μαζικής μεταφοράς μπορούν να χρησιμοποιούν περισσότερα από ένα συστήματα μεταφοράς ή μία γραμμή μεταφοράς όταν ταξιδεύουν. Για παράδειγμα, το ταξίδι με προαστιακό τρένο και στη συνέχεια με λεωφορείο (ή αντίστροφα) μπορεί να είναι ένα φυσιολογικό μέρος μιας καθημερινής μετακίνησης. Το μέλημα του ταξιδιώτη είναι να βρει την ταχύτερη διαδρομή μεταξύ δύο σημείων. Όταν τα γεγονότα επηρεάζουν την αποδοτικότητα ενός συστήματος, ο ταξιδιώτης πρέπει να είναι σε θέση να αξιολογήσει εναλλακτικές λύσεις και να προσαρμοστεί σε πραγματικό χρόνο.

3.Σιδηρόδρομος: Παρόλο που τα μεταφορικά μέσα περιλαμβάνουν το μετρό και συστήματα του σιδηροδρομικού άξονα η κυκλοφορία των τρένων εντός των πόλεων περιλαμβάνει επίσης και τα φορτηγά τρένα, τα οποία μπορεί να αποτελούν μεγάλο μέρος της σιδηροδρομικής δραστηριότητας.
Η διασφάλιση ότι ένα τρένο φτάνει στον προορισμό του με ασφάλεια και εγκαίρως συνεπάγεται το συντονισμό πολλαπλών σημάτων και συστημάτων. Μια σημαντική πρόκληση είναι να διασφαλιστεί η αποτελεσματικότητα όλων αυτών των συστημάτων και να διασφαλιστεί ότι οι πληροφορίες είναι διαθέσιμες με συντονισμένο τρόπο. Για παράδειγμα, εάν ένα τρένο πρέπει να σταματήσει λόγω προβλήματος στις ράγες, πρέπει το τρένο πίσω να λάβει αυτές τις πληροφορίες για να σταματήσει; Εάν το ζήτημα της σιδηροδρομικής γραμμής απαιτεί βαριές επισκευές, μπορούν τα τρένα να δρομολογηθούν σε μια πιθανή εναλλακτική διαδρομή γύρω από το επηρεαζόμενο τμήμα;
Για τέτοιους σκοπούς, το IoT μπορεί να βελτιώσει σημαντικά την ασφάλεια και την αποτελεσματικότητα των εργασιών, παρακολουθώντας τις θέσεις των τρένων και την ταχύτητά τους και συλλέγοντας δεδομένα σχετικά με την κατάσταση των γραμμών, των σημάτων, των γραμμών ρεύματος και άλλων στοιχείων υποδομής κατά μήκος των γραμμών. Η άποψη σε πραγματικό χρόνο για την κατάσταση των σιδηροδρομικών υποδομών μειώνει σημαντικά τους κινδύνους καθυστερήσεων ή ατυχημάτων.

Ο σιδηρόδρομος αποτελεί αφορά επίσης και το κομμάτι του ταξιδιού για την αποστολή εμπορευμάτων. Το φορτίο πρέπει να παραδοθεί εγκαίρως, διαφορετικά μπορεί να επηρεαστεί ολόκληρη η αλυσίδα εφοδιασμού. Ομοίως, ένας επιβάτης που φτάνει σε ένα σιδηροδρομικό σταθμό αναμένει ένα ενημερωμένο και ακριβές χρονοδιάγραμμα τρένων. Μόλις επιβιβαστεί, ο επιβάτης αναμένει επίσης μια ποικιλία υπηρεσιών που ξεπερνούν τις απλές μεταφορές (για παράδειγμα, καθαρές τουαλέτες, φαγητό, άνετη θερμοκρασία, σύνδεση στο Διαδίκτυο). Το IoT μπορεί να χρησιμοποιηθεί για την παρακολούθηση αγαθών, την προβολή πραγματικού χρόνου στο ταξίδι (καθυστερήσεις, αναμενόμενη άφιξη), καθώς και τη βελτιστοποίηση της ταξιδιωτικής εμπειρίας παρακολουθώντας και αναφέροντας τις συνθήκες του εξοπλισμού του τρένου για να επιτρέψουν αποτελεσματική και στοχευμένη συντήρηση στον επόμενο σταθμό.

Κεφάλαιο 11.2 Συνδεδεμένα Αυτοκίνητα(Connected Cars)

Μια τοποθεσία όπου το IoT μπορεί να βελτιστοποιήσει τη μεταφορά είναι το ίδιο το όχημα. Τα σύγχρονα αυτοκίνητα είναι πολύ μηχανογραφημένα, με εκατοντάδες αισθητήρες να αξιολογούν τα πάντα, από την πίεση των ελαστικών έως το χαλαρό καπάκι αερίου. Αυτές οι πληροφορίες εμφανίζονται στο ταμπλό για να βοηθήσουν τον οδηγό να έχει μια καλύτερη ταξιδιωτική εμπειρία. Αυτό είναι ένα παράδειγμα έξυπνων αντικειμένων αλλά όχι IoT. Ένας περιορισμός αυτής της εφαρμογής είναι ότι οι πληροφορίες είναι διαθέσιμες μόνο τοπικά. Επομένως, δεν μπορεί να συσχετιστεί με πληροφορίες που προέρχονται από άλλα οχήματα για να σχεδιάσουμε μια καλύτερη και μεγαλύτερη εικόνα.

Το IoT επιτρέπει στα έξυπνα αντικείμενα να επικοινωνούν και να παρέχουν πολύτιμες υπηρεσίες με βάση αυτή την επικοινωνία. Οποιεσδήποτε πληροφορίες ανακαλύπτονται από τους αισθητήρες του αυτοκινήτου μπορούν να κοινοποιηθούν σε συστήματα εκτός του αυτοκινήτου. Όταν οι πληροφορίες ισχύουν τοπικά, θα πρέπει να είναι διαθέσιμες τοπικά.
Όταν άλλα αυτοκίνητα πλησιάζουν σε μια συγκεκριμένη περιοχή, προειδοποιούνται για συμφόρηση λόγω τοπικού ατυχήματος, ολισθηρών συνθηκών λόγω πετρελαιοκηλίδων στο πεζοδρόμιο ή δυσκολίας στην κυκλοφορία λόγω σπασμένου φωτισμού του δρόμου ή

ελαττωματικού συστήματος διασταύρωσης σιδηροδρόμων. Αυτή η επικοινωνία συνεπάγεται ότι πρέπει να υπάρχει σύστημα ανταλλαγής πληροφοριών από αυτοκίνητο σε αυτοκίνητο ή όχημα σε όχημα (vehicle-to-vehicle V2V). Το σύστημα αυτό, προστατεύει το απόρρητο και συγχρόνως παρέχει χρήσιμες πληροφορίες. Επίσης προσφέρει ανταλλαγή πληροφοριών από όχημα σε υποδομή (vehicle-to- infrastructure V2I), έτσι ώστε οι τοπικές πληροφορίες να είναι διαθέσιμες όπου είναι σχετικές.
Όταν οι πληροφορίες αφορούν αποκλειστικά το αυτοκίνητό μας, μπορούν να διατίθενται τοπικά, αλλά ενδέχεται να κοινοποιηθούν σε συστήματα τρίτων. Μια τέτοια επικοινωνία απαιτεί μια συνεχόμενη σύνδεση μεταξύ του οχήματος και του διαδικτύου. Ο λόγος που οι εφαρμογές στο τηλέφωνό είναι σε θέση να παρέχουν τη βέλτιστη πλοήγηση είναι επειδή το τηλέφωνό είναι συνδεδεμένο στο διαδίκτυο και τα δεδομένα κίνησης ενημερώνονται σε πραγματικό χρόνο. Ωστόσο, το τηλέφωνό δεν έχει καμία σύνδεση με τα συστήματα του αυτοκινήτου. Η σύνδεση του αυτοκινήτου απευθείας στο διαδίκτυο ή στο τηλέφωνό φέρνει όλα τα πλεονεκτήματα της συνδεσιμότητας στην ταξιδιωτική εμπειρία και οι εφαρμογές είναι ατελείωτες. Για παράδειγμα, ο κατασκευαστής του αυτοκινήτου μπορεί να χαρτογραφήσει τις προβλέψεις καιρού σε πολύ λεπτομερή επίπεδο και να προσαρμόσει δυναμικά τις ρυθμίσεις του κινητήρα του αυτοκινήτου ώστε να προσαρμόζεται στις τοπικές συνθήκες και να εξοικονομεί καύσιμο. Επίσης, όταν δύο εξοπλισμένα αυτοκίνητα αντικρίζουν το ένα το άλλο, συγχρονίζουν τα φώτα και τις οθόνες τους. Όταν τα φώτα του αυτοκινήτου που έρχονται προς την κατεύθυνση μας είναι αναμμένα, η οθόνη μας σκοτεινιάζει και γίνεται διαφανές όταν σβήνουν τα φώτα. Το αποτέλεσμα είναι ότι και οι δύο οδηγοί βλέπουν το δρόμο να φωτίζεται, αλλά κανένας δεν τυφλώνεται από τα φώτα που έρχονται. Αυτή η τεχνολογία βελτιστοποιεί την εμπειρία οδήγησης και εστιάζεται σημαντικά στην ασφάλεια.

Κεφάλαιο 11.3 Υποδομές και Μαζική Μεταφορά

Για να μπορεί μία υποδομή να επικοινωνεί με οχήματα θα πρέπει να υπάρχει ένα σύστημα ανταλλαγής πληροφοριών. Να μπορεί να συλλέγει πληροφορίες από αυτά (για παράδειγμα, τοποθεσία, ταχύτητα, κατάσταση λειτουργίας του οχήματος) με βάση εκατοντάδες αισθητήρες και να τις μεταφέρει στο διαδίκτυο. Όταν και η ίδια η υποδομή περιλαμβάνει αισθητήρες, οι πληροφορίες μπορεί να είναι πιο πλούσιες (συμπεριλαμβανομένων των καιρικών συνθηκών, ανιχνευόμενης αυξημένης κυκλοφορίας, ανίχνευση ατυχημάτων κ.λπ.) και διαθέσιμες για πολλές εφαρμογές. Στη συνέχεια αποστέλλονται στο cloud, όπου μπορούν να εξαχθούν χρήσιμα μοτίβα. Οι ζώνες και οι ώρες συμφόρησης μπορούν να μετρηθούν και να επιστρέψουν στην εφαρμογή για να εμφανιστεί ο αναμενόμενος χρόνος ταξιδιού. Ωστόσο, αυτές οι εφαρμογές είναι περιορισμένες όσον αφορά τα οφέλη για τους τοπικούς χρήστες.
Ενώ μπορούν να ενημερώσουν την τρέχουσα κατάσταση της επισκεψιμότητας, να ενσωματώσουν προγνωστικές αλλαγές στην κατάσταση της κυκλοφορίας και να τροποποιήσουν ανάλογα τις προβλέψεις τους, όμως δεν μπορούν να τροποποιήσουν τις καταστάσεις των δρόμων ή να συντονίσουν τις απαντήσεις που αποστέλλονται σε πολλούς χρήστες.

Με το IoT, οι πληροφορίες για κάθε αυτοκίνητο, καθώς και τα προγραμματισμένα ταξίδια από κάθε σύστημα πλοήγησης σε κάθε αυτοκίνητο, μπορούν να αναλυθούν με συντονισμένο τρόπο στο cloud. Το αποτέλεσμα είναι καλύτερη πρόβλεψη επισκεψιμότητας που μπορεί επίσης να επιστρέψει διαφορετικές πληροφορίες σε διαφορετικούς χρήστες. Αυτή η νοημοσύνη IoT έχει επίσης άμεση επίδραση σε χρήστες μαζικής μεταφοράς. Για παράδειγμα, όταν περπατάμε προς έναν σταθμό λεωφορείων, ένα μήνυμα κειμένου σε

έναν ειδικό αριθμό (αναφέροντας το αναγνωριστικό λεωφορείου) ή μια εφαρμογή τηλεφώνου μπορεί να εμφανίσει την πλησιέστερη τοποθεσία στάσης λεωφορείου και τον εκτιμώμενο χρόνο αναμονής. Όταν περιμένουμε στη στάση του λεωφορείου, ένα έξυπνο πλαίσιο μπορεί να εμφανίσει τον αναμενόμενο χρόνο αναμονής μέχρι το επόμενο λεωφορείο και μια εκτίμηση του χρόνου ταξιδιού σε οποιονδήποτε προορισμό. Αυτή η εκτίμηση αναφέρεται σε πραγματικό χρόνο και είναι έξυπνη (με βάση τις τρέχουσες συνθήκες κυκλοφορίας και επίσης λαμβάνοντας υπόψη τις αναμενόμενες αλλαγές στην πυκνότητα κίνησης τις επόμενες ώρες). Σε κλίμακα πόλης, ένας προγραμματιστής ταξιδιού μας ενημερώνει για τις συνθήκες ταξιδιού στην πόλη και σε όλα τα συστήματα συγκοινωνίας και μπορεί να μας προτείνει την καλύτερη διαδρομή προς τον προορισμό μας. Πολλές άλλες περιπτώσεις χρήσης IoT επιτρέπουν την καλύτερη διαχείριση της συμφόρησης στην πόλη.

Μια άλλη επίδραση του IoT στην επικοινωνία μεταξύ οχήματος και υποδομής είναι η αυξημένη ασφάλεια. Για παράδειγμα, ένας σημαντικός συντελεστής σε τροχαία ατυχήματα σε κυκλοφοριακή συμφόρηση είναι οι συνθήκες στάσης και μετάβασης (όταν η κυκλοφορία είναι με μέτρια ή υψηλή ταχύτητα και στη συνέχεια σταματά ξαφνικά και γίνεται πάλι γρήγορη). Τα αίτια του stop-and-go είναι γνωστά: πυκνότητα κυκλοφορίας (συγχώνευση λωρίδων), περισπασμοί στην άκρη του δρόμου (τροχαία ατυχήματα, ασυνήθιστα φαινόμενα στην άκρη του δρόμου), κακοκαιρία (κομμάτια βροχής ή ομίχλης), κακός συντονισμός φώτων του δρόμου κ.λπ. Η συνδυασμένη επίδραση αυτών των αιτιών μπορεί να δημιουργήσει εφέ stop-and-go για πολλά χιλιόμετρα. Ένας κοινός τρόπος για να μειωθεί η κυκλοφορία ενδιάμεσων μετακινήσεων είναι η προσεκτική ρύθμιση της ροής των αυτοκινήτων που εισέρχονται στα διάφορα τμήματα του δρόμου.

Το IoT σε συνδυασμό με τη μηχανική εκμάθηση(machine learning) είναι ένας τρομερός συνδυασμός για την επίτευξη αυτού του στόχου. Πληροφορίες πυκνότητας κυκλοφορίας που συλλέγονται από αισθητήρες στα οχήματα και στην υποδομή(για παράδειγμα, κάμερες καταμέτρησης οχημάτων, καλώδια πίεσης που καταγράφουν οχήματα και ταχύτητα ή οπτικά καλώδια στην άσφαλτο που μπορούν να μετρήσουν την πυκνότητα κυκλοφορίας) μπορούν να προσαρμοστούν δυναμικά στις τοπικές συνθήκες για την επίλυση προβλημάτων στάσης και μετάβασης. Ταυτόχρονα, μια ξαφνική πτώση της ροής της κυκλοφορίας (που μπορεί να υποδηλώνει ατύχημα) μπορεί να ενημερώσει τα κέντρα ελέγχου της αρχής κυκλοφορίας. Αυτός η ενημέρωση(ο συναγερμός) μπορεί να μεταδοθεί σε κέντρα έκτακτης ανάγκης, επιτρέποντας την ταχύτερη αποστολή οχημάτων έκτακτης ανάγκης.

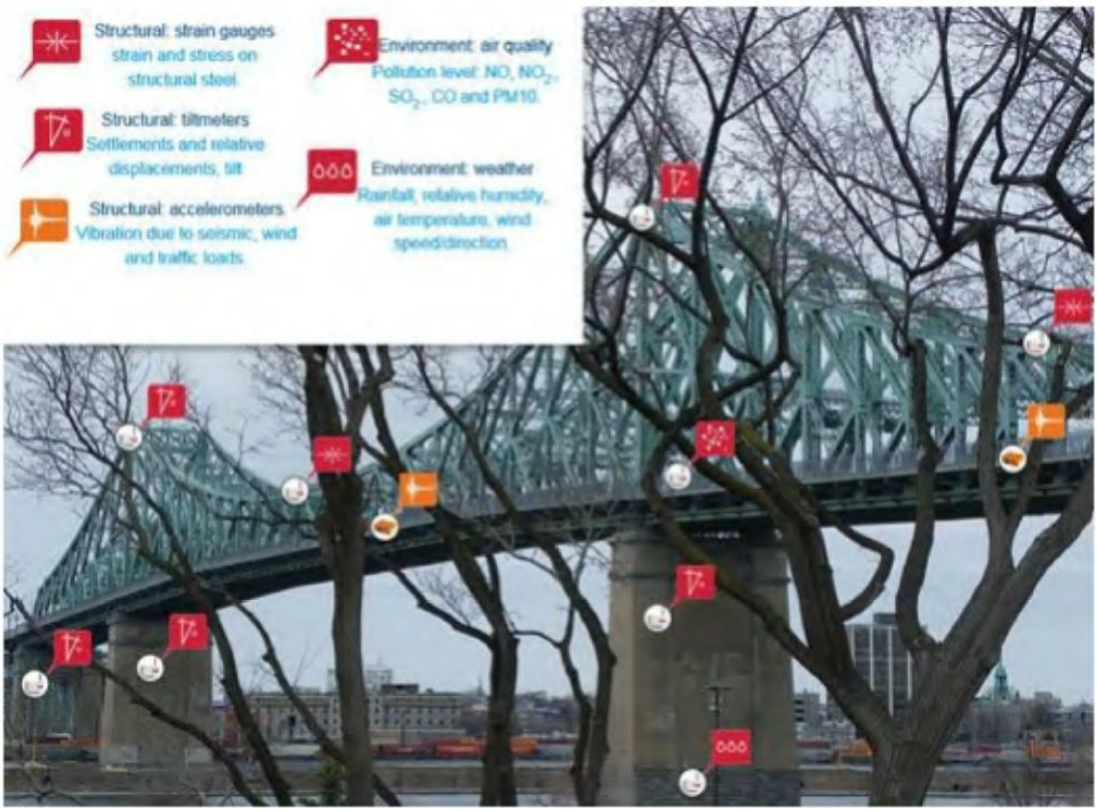
Συνοπτικά το IoT που εφαρμόζεται σε οχήματα μαζικής μεταφοράς μπορεί να βελτιώσει μαζικά την ταξιδιωτική εμπειρία. Οι οδηγοί μπορούν να επωφεληθούν ένα ασφαλέστερο και πιο προβλέψιμο ταξίδι. Οι αρχές κυκλοφορίας μπορούν να ρυθμίζουν καλύτερα τη ροή των οχημάτων και να διαχειρίζονται καλύτερα την υποδομή του οδικού άξονα. Ωφελούν επίσης τους ταξιδιώτες αστικών λεωφορείων παρέχοντας ακριβείς πληροφορίες συγκοινωνίας, έξυπνους χάρτες και σχέδια ταξιδιών.

Άλλες εφαρμογές και οφέλη που παρέχουν τα IoT είναι οι αισθητήρες δρόμου, οι οποίοι μπορούν να κάνουν πολλά περισσότερα από την καταμέτρηση αυτοκινήτων.
Συγκεκριμένα μπορούν να:

- Μετρήσουν την ποιότητα του αέρα, καθώς και να προβλέψουν τις καιρικές συνθήκες. Αυτές οι πληροφορίες μπορούν να μεταδοθούν σε κεντρικά συστήματα για παρακολούθηση και προειδοποίηση.

- Εφαρμοστούν στην οδική υποδομή και σε αντικείμενα για τη βελτίωση της συντήρησης και της ασφάλειας. Για παράδειγμα, οι αισθητήρες δρόμου μπορούν να μετρήσουν την ποσότητα νερού που διαπερνά την άσφαλτο και να αξιολογήσουν τη φθορά της επιφάνειας.
- Αξιολογήσουν στις γέφυρες(οι δομικοί αισθητήρες) τις καταπονήσεις στα δομικά χαλύβδινα μέλη, την κλίση των πυλώνων και των στηριγμάτων και να μετρήσουν την καθίζηση και τη σχετική μετατόπιση μιας γέφυρας. Σε συνδυασμό με τα επιταχυνσιόμετρα μπορούν να μετρήσουν τους κραδασμούς και τις δυναμικές αντιδράσεις στην κίνηση, τον άνεμο ή ακόμη και σεισμική δραστηριότητα.

Το Σχήμα 63 δείχνει ένα παράδειγμα αυτών των αισθητήρων που εφαρμόζονται σε μια γέφυρα.



Σχήμα 63: Παρακολούθηση έξυπνων αντικειμένων σε γέφυρα.

Κεφάλαιο 12 Εξόρυξη(Mining)

Εξόρυξη είναι η διαδικασία εξαγωγής ορυκτών από τη γη. Πολλοί τύποι ορυκτών εξάγονται σήμερα, συμπεριλαμβανομένων των: χαλκού, χρυσού, αργύρου, λιθίου, μολυβδαινίου, σιδήρου, αλατιού, άνθρακα, ουρανίου και των πολύτιμων λίθων. Τα περισσότερα από αυτά τα μέταλλα(ιδιαίτερα τα πολύτιμα μέταλλα), σπάνια απλώνονται στο έδαφος σε μεγάλα κομμάτια. Αντίθετα, αναμειγνύονται με άλλα υλικά κάτω από την επιφάνεια της γης. Για να διαχωριστούν και εξαχθούν τα επιθυμητά ορυκτά, πρέπει να διασπαστούν μεγάλες ποσότητες γης και να μεταφερθούν σε μια εγκατάσταση επεξεργασίας, όπου διασπούνται περαιτέρω και χρησιμοποιούνται διάφορες τεχνικές για την απομόνωση του επιθυμητού

υλικού. Οι τεχνικές και οι τεχνολογίες που χρησιμοποιούνται στις εργασίες εξόρυξης έχουν πολλές ομοιότητες με άλλες βιομηχανίες.

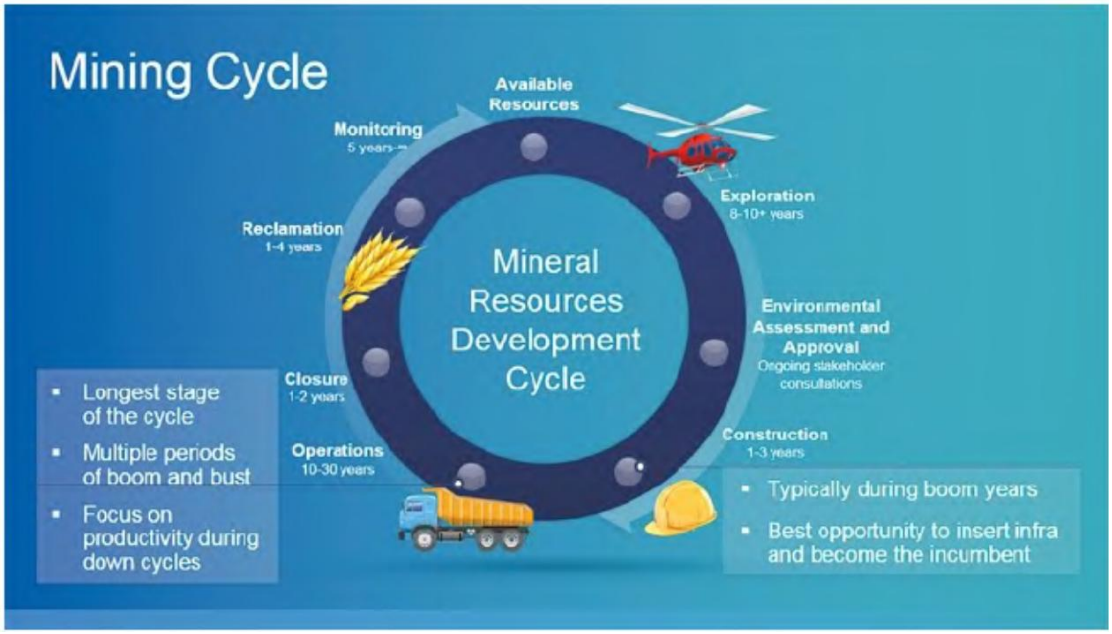
Τα ορυχεία μπορούν γενικά να ταξινομηθούν σε τρεις μεγάλες κατηγορίες:

- Επιφανειακής εξόρυξης.
- Υπόγεια εξόρυξη.
- Υποβρύχια εξόρυξη.

Υπάρχουν επίσης τρεις κύριοι τύποι ορυκτών που εξορύσσονται, και στις τρεις κατηγορίες εξόρυξης:

- Ανθρακας.
- Μέταλλο.
- Μη μέταλλο.

Στις περισσότερες χώρες, οι δραστηριότητες εξόρυξης ρυθμίζονται. Η εργασία σε ορυχείο απαιτεί συνήθως εξειδικευμένη εκπαίδευση και πιστοποίηση από εθνικούς ρυθμιστικούς οργανισμούς, όπως το MSHA(Mine Safety and Health Administration MSHA). Σε άλλες χώρες, ο τύπος ορυχείου και οι διαδικασίες εκμετάλλευσης ρυθμίζονται επίσης.
Ο κύκλος ζωής ενός ορυχείου, ο οποίος υπερβαίνει κατά πολύ την εξόρυξη ορυκτών, φαίνεται στο Σχήμα 64



Σχήμα 64: Κύκλος ζωής ορυχείων.

Το IoT αλλάζει ταχύτατα τον τρόπο λειτουργίας των ορυχείων. Επιτρέπει στα ορυχεία να λειτουργούν πιο αποτελεσματικά και με μεγαλύτερη ασφάλεια από ποτέ, παρέχοντας αποτελέσματα τόσο στους φορείς εκμετάλλευσης εξόρυξης, όσο και στις επιχειρήσεις και στους καταναλωτές. Παρέχοντας κρίσιμες πληροφορίες σε πραγματικό χρόνο σε συστήματα και χειριστές ορυχείων, το IoT μειώνει τους κινδύνους που θεωρούνταν μια ατυχής αλλά φυσική συνέπεια της δραστηριότητας μόλις πριν από 10 χρόνια. Τα έξυπνα αντικείμενα μπορούν να αυτοματοποιήσουν τις διαδικασίες και να κάνουν την εξόρυξη ευκολότερη και ασφαλέστερη.

Αυτό το κεφάλαιο περιλαμβάνει τις ακόλουθες ενότητες:

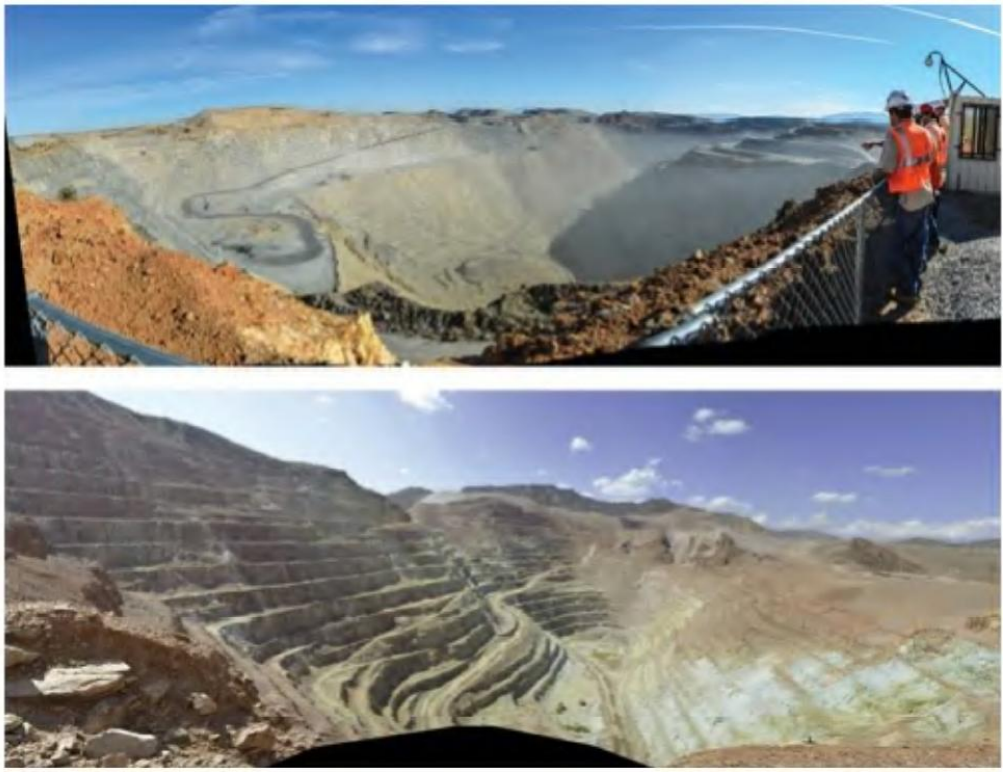
- Εξόρυξη σήμερα και οι προκλήσεις της: παρέχει μια επισκόπηση της μεταλλευτικής βιομηχανίας και θα βοηθήσει να γίνουν κατανοητά τα εργαλεία, οι κλίμακες, οι περιορισμοί και οι προκλήσεις αυτής της βιομηχανίας.

- Προκλήσεις για το IoT στη σύγχρονη εξόρυξη: εξετάζει συγκεκριμένες προκλήσεις στην ανάπτυξη λύσεων IoT σε περιβάλλοντα εξόρυξης.
- Μία στρατηγική IoT για εξόρυξη: αναφέρει πολλαπλούς τρόπους με τους οποίους το IoT μπορεί να βελτιώσει τις εργασίες εξόρυξης όπως, αυξημένη ασφάλεια και αποτελεσματικότητα άμεση ασφάλεια επικίνδυνων αερίων, παρακολούθηση περιβάλλοντος και υπηρεσίες εντοπισμού.

- Μία αρχιτεκτονική IoT για εξόρυξη: περιγράφει την αρχιτεκτονική ενός δικτύου IoT για εξόρυξη.

Κεφάλαιο 12.1 Η εξόρυξη σήμερα και οι προκλήσεις της

Τα τελευταία 50 χρόνια, το μέγεθος και η κλίμακα των εργασιών εξόρυξης έχουν αυξηθεί πάρα πολύ, ενώ ταυτόχρονα οι διαδικασίες και η αποτελεσματικότητα της εξόρυξης ορυκτών έχουν βελτιωθεί σημαντικά. Η σύγχρονη εξόρυξη είναι η ασφαλέστερη που υπήρξε ποτέ. Ωστόσο, οι χειριστές σύγχρονων ορυχείων εξακολουθούν να αντιμετωπίζουν πολλές προκλήσεις. Στην εξόρυξη, οι τοποθεσίες μπορούν να καλύψουν εκατοντάδες τετραγωνικά μίλια και μπορούν να περιέχουν λάκκους βάθους άνω των 2500 ποδιών, με πλάτος που εκτείνεται σε αρκετά μίλια (Σχήμα 65) σε αντίθεση με μια μεγάλη κοιλάδα.



Σχήμα 65: Ανοικτό ορυχείο στην Αριζόνα.

Πολλά επιφανειακά ορυχεία έχουν αρκετά βαθιά κοιλώματα (Σχήμα 66) το ένα δίπλα στο άλλο, με μεγάλους, ελικοειδείς δρόμους μεταφοράς που διασχίζονται από γιγάντια φορτηγά.

Σχήμα 66: Ανοικτό ορυχείο με μεγάλα φορτηγά.

Τα υπόγεια ορυχεία μπορούν να έχουν εκατοντάδες μίλια τούνελ, που εκτείνονται σε μεγάλες κάθετες αποστάσεις κάτω από την επιφάνεια. Από την άποψη του IoT, αυτό σημαίνει ότι θα χρειαστούν αρκετές ώρες για να μεταφερθεί ένας τεχνικός σε τοποθεσίες εξοπλισμού σε έναν ιστότοπο. Τα ορυχεία βρίσκονται συχνά σε απομακρυσμένες τοποθεσίες που μπορεί να είναι δύσκολο να προσεγγιστούν, τόσο σωματικά όσο και ηλεκτρονικά. Αυτό σημαίνει ότι η υποδομή που απαιτείται για τη στήριξη ορυχείου μεγάλης κλίμακας (ηλεκτρική ενέργεια, νερό, επικοινωνίες, σιδηροδρομικές / οδικές / θαλάσσιες μεταφορές) συχνά δεν υπάρχει ή δεν είναι διαθέσιμη στην κλίμακα που απαιτείται για τη διευκόλυνση των δραστηριοτήτων εξόρυξης. Αυτή η υποδομή πρέπει να δημιουργηθεί από τον διαχειριστή ορυχείου ή έναν πληρεξούσιο. Μερικές φορές πολλές τοποθεσίες εξόρυξης βρίσκονται σε περιοχές όπου πρέπει να αντιμετωπιστούν ακραίες περιβαλλοντικές συνθήκες, όπως υψόμετρο, υγρασία και θερμοκρασία και όπου οι ασθένειες και η πανίδα μπορεί επίσης να προκαλέσουν κινδύνους.

Κεφάλαιο 12.2 Προκλήσεις για το IoT στη σύγχρονη εξόρυξη

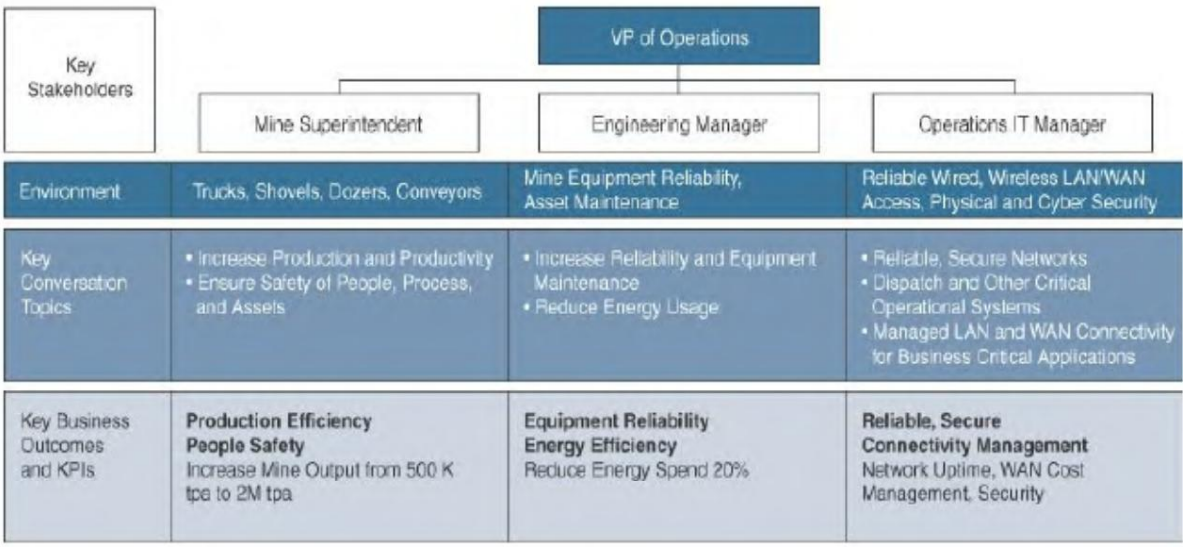
Η ασφάλεια είναι ένα από τα σημαντικότερα ζητήματα στον τομέα της εξόρυξης. Συγκεκριμένα:

- Ο κίνδυνος κατάρρευσης είναι πάντα ανησυχητικός και η παρακολούθηση της δομής της σήραγγας είναι πάντα πρωταρχική προτεραιότητα.
- Οι εκρήξεις αποτελούν επίσης κίνδυνο.
- Τα ανοιχτά ορυχεία μπορεί να φαίνονται ασφαλέστερα από τα υπόγεια ορυχεία. Ωστόσο, τα μέσα που εμπλέκονται στη μεταφορά τόνων γης και οι διαδικασίες που απαιτούνται για την εξαγωγή ορυκτών μπορεί να είναι πολύ επικίνδυνες.

- Οι κατολισθήσεις μπορεί να είναι θανατηφόρες και η παρακολούθηση των κλίσεων των ανοικτών ορυχείων αποτελεί βασική απαίτηση ασφάλειας.
- Η εργασία γύρω από γιγαντιαίους κινητήρες(φορτηγά) είναι επικίνδυνη. Από την καμπίνα αυτών των πολύ μεγάλων οχημάτων, οι οδηγοί μπορεί να μην μπορούν να δουν πεζούς ή ακόμη και φορτηγά.
- Οι καιρικές συνθήκες μπορούν επίσης να δημιουργήσουν προκλήσεις.
- Πολλά ορυχεία βρίσκονται σε περιοχές με ακραίες καιρικές συνθήκες. Ξαφνικές βίαιες βροχές μπορεί να γεμίσουν γρήγορα λάκκους και τρύπες. Όταν ξεσπούν καταιγίδες, οι εργαζόμενοι εκτίθενται και μπορεί να απέχουν μίλια από ασφαλή, προστατευμένα κτίρια.

Οι μεταλλευτικοί οργανισμοί έχουν καθήκον να προστατεύουν το περιβάλλον από τις επιπτώσεις των δραστηριοτήτων τους. Αυτές οι επιπτώσεις περιλαμβάνουν φυσικά τη ρύπανση του εδάφους και των υδάτων, καθώς και τον θόρυβο, τη σκόνη και τις επιπτώσεις των εξορυκτικών εργασιών στη χλωρίδα και την πανίδα.

Η σύγχρονη κοινωνία μας εξαρτάται από την εξόρυξη για να παρέχει τα ορυκτά που χρειάζονται σχεδόν για όλους τους τομείς όπως είναι: ηλεκτρικά καλώδια σε κτίρια, εξαρτήματα που χρησιμοποιούνται σε κάθε ηλεκτρονική συσκευή, μπαταρίες που λειτουργούν τα gadget μας, μέταλλα που μπαίνουν στα κτίριά μας, αυτοκίνητα, αεροσκάφη, πλοία, γέφυρες, κοσμήματα κ.λπ.
Πολλές από τις προκλήσεις στη σύγχρονη εξόρυξη μπορούν να αντιμετωπιστούν με λύσεις IoT. Ωστόσο, η ανάπτυξη λύσεων IoT σε περιβάλλον εξόρυξης είναι δύσκολη. Όπως και με άλλες βιομηχανίες, οι στόχοι και οι απαιτήσεις για τα παραδοσιακά εταιρικά δίκτυα IT στη βιομηχανία εξόρυξης είναι πολύ διαφορετικοί από εκείνους του OT. Τα ορυχεία έχουν συνήθως τεχνικούς ρόλους επικεντρωμένους στην πλευρά OT (Σχήμα 67).



Σχήμα 67: Βασικοί ρόλοι εξόρυξης.

Συγκεκριμένα αναφέρονται στον:

Επιθεωρητή ορυχείου(Mine superintendent): είναι υπεύθυνος για τις λειτουργίες και την κερδοφορία του ορυχείου. Για την εξισορρόπηση των επενδύσεων (σε IoT, μηχανές και άτομα) και την αναμενόμενη παραγωγή από το ορυχείο. Ενδιαφέρεται για οποιαδήποτε λύση IoT για την αύξηση της κερδοφορίας και της ασφάλειας ή τη μείωση του κόστους.

Μηχανικό διευθυντή(Engineering manager): Ο επιθεωρητής εργάζεται σε συντονισμό με τον διευθυντή μηχανικής. Ο διευθυντής μηχανικής είναι υπεύθυνος για τον εξοπλισμό του ορυχείου. Ενδιαφέρεται για οποιαδήποτε λύση που μπορεί να αυξήσει την αξιοπιστία του εξοπλισμού παρέχοντας καλύτερη παρακολούθηση, επιτρέποντας την προληπτική συντήρηση και μειώνοντας την κατανάλωση ενέργειας που σχετίζεται με τις εξορυκτικές εργασίες.

Διαχειριστής λειτουργιών IT(Operations IT manager): Είναι υπεύθυνος για το δίκτυο IT. Κάθε συσκευή που θα χρειαστεί να συνδεθεί μέσω του δικτύου IT πρέπει να αναθεωρηθεί και να εγκριθεί από την ομάδα του διαχειριστή IT.

Το IoT εξαρτάται από τη συνδεσιμότητα((Connectivity) και στον τομέα της εξόρυξης, είναι ιδιαίτερα σημαντική. Η ίδια η φύση της εξόρυξης σημαίνει ότι το φυσικό στρώμα είναι εξαιρετικά δυναμικό και το δίκτυο μπορεί να βρίσκεται σε συνεχή κατάσταση αλλαγής για να ικανοποιήσει τις απαιτήσεις ενός συνεχώς μεταβαλλόμενου ορυχείου.
Συνολικά, αυτές οι προκλήσεις μπορούν συνήθως να χωριστούν σε τρεις κύριες κατηγορίες:

Απόσταση: Σε απομακρυσμένες περιοχές όπου λειτουργούν πολλά ορυχεία, η σύνδεση WAN μπορεί να είναι δύσκολη και συχνά είναι εξαιρετικά δαπανηρή. Έχει σχετικά χαμηλό εύρος ζώνης και συχνά υπόκειται σε μεγάλη καθυστέρηση και μεγάλη απώλεια πακέτων. Αυτό ισχύει ιδιαίτερα όταν τα παραδοσιακά κυκλώματα δεν είναι διαθέσιμα και πρέπει να χρησιμοποιούνται δορυφορικές συνδέσεις. Για πολλές εφαρμογές, αυτά τα ζητήματα μπορούν να αντιμετωπιστούν με τεχνολογίες WAN. Ωστόσο, αυτές οι τεχνολογίες συνήθως δεν είναι αποτελεσματικές για εφαρμογές επικοινωνίας σε πραγματικό χρόνο, όπως η τηλεδιάσκεψη VoIP και IP. Επιπλέον, πολλά ορυχεία βρίσκονται σε μέρη όπου δεν υπάρχει κάλυψη, πράγμα που σημαίνει ότι οι φορείς εκμετάλλευσης ορυχείων πρέπει συχνά να αναπτύξουν τη δική τους ασύρματη υποδομή επικοινωνιών και μπορεί να εξαρτώνται από δορυφορικές επικοινωνίες για ορισμένες υπηρεσίες δεδομένων.

Ακραίες περιβαλλοντικές συνθήκες: Τα ορυχεία παρουσιάζουν μεγάλη ποικιλία ακραίων συνθηκών στις οποίες πρέπει να λειτουργεί ο εξοπλισμός. Ορισμένες από αυτές τις συνθήκες σχετίζονται με την απόσταση των ορυχείων, ενώ άλλες συνδέονται με τη φύση της διαδικασίας. Οι εργασίες εξόρυξης πάνω από το έδαφος συχνά αντιμετωπίζουν εξαιρετική υγρασία, θερμοκρασίες ζεστές και κρύες, καθώς και ακραίες καιρικές συνθήκες(κεραυνοί, καταρρακτώδεις βροχές έως και άνεμοι). Πολλά ορυχεία, ειδικά στη Νότια Αμερική, λειτουργούν σε μεγάλα υψόμετρα, συχνά πάνω από 15.000 πόδια, όπου ο αέρας είναι πολύ λιγότερο πυκνός και πρέπει να ληφθεί υπόψη η αποτελεσματικότητα ψύξης του εξοπλισμού. Ορισμένες διαδικασίες εξόρυξης περιλαμβάνουν διαβρωτικές χημικές ουσίες ή εύφλεκτες και εκρηκτικές ατμόσφαιρες. Απαιτούνται κατάλληλες πιστοποιήσεις εξοπλισμού ή περιβλήματα για τη διατήρηση της ασφάλειας του εξοπλισμού και την αποφυγή πυρκαγιών και εκρήξεων. Τέτοια περιβάλλοντα απαιτούν δημιουργικότητα κατά την τοποθέτηση εξοπλισμού

Ο πίνακας 8 συνοψίζει μερικές από τις περιβαλλοντικές προκλήσεις στην εξόρυξη και πιθανές λύσεις.

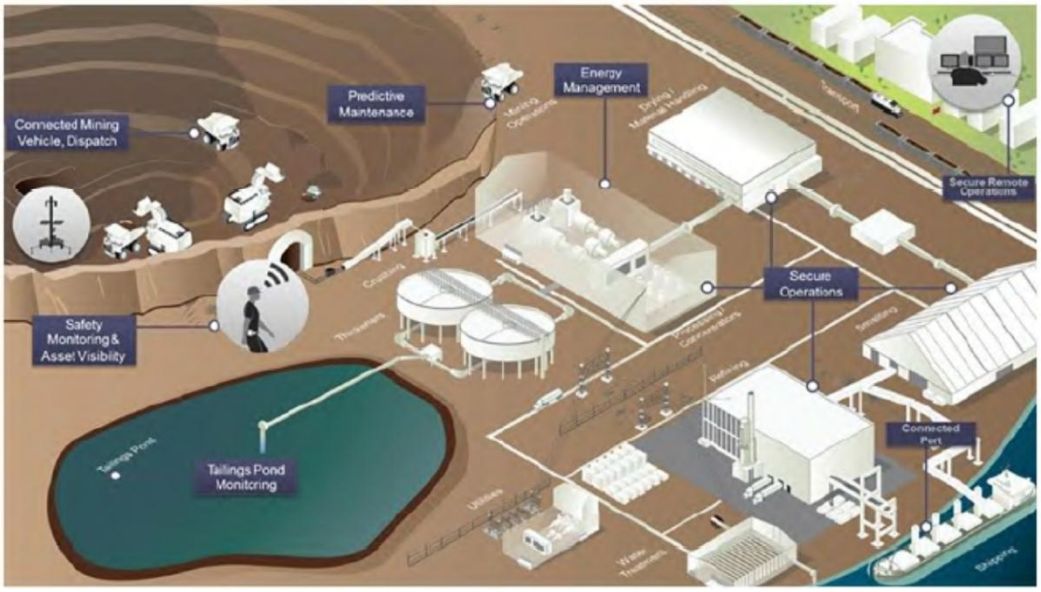
Environmental Consideration	Potential Solutions
Moisture and dust	Use equipment or enclosures with appropriate ingress protection (IP) rating, such as IP54 or IP68.
Corrosive	Use "conformal coating" equipment or an enclosure with an appropriate rating.
Lightning	Use appropriate lightning protection equipment, such as lightning arrestors, proper grounding, and electrical isolation via fiber-optic interconnects.
Extreme heat/ cold/altitude	Use equipment designed for extended temperature ranges and/or appropriate enclosures that can keep equipment within operating specifications.
Vibration	Use vibration-dampening mounts and enclosures.
Flammable or explosive atmosphere	Use equipment or enclosures rated intrinsically safe for the specific hazard(s) that received HazLoc certifications (for example, Class 1 Div 2).

Πίνακας 8: Περιβαλλοντικές εκτιμήσεις και πιθανές λύσεις.

Κλίμακα: Οι εργασίες εξόρυξης έχουν εντελώς διαφορετικό μέγεθος και κλίμακα από τις περισσότερες βιομηχανίες. Αυτό συχνά σημαίνει ότι ένα δίκτυο πρέπει να παρέχει συνδεσιμότητα σε εκατοντάδες τετραγωνικά μίλια. Ορισμένες εφαρμογές εξόρυξης δεν βασίζονται σε IP και δεν μπορούν να δρομολογηθούν. Η συνδεσιμότητα επιπέδου 2(Layer 2) πρέπει μερικές φορές να είναι διαθέσιμη σε μια ευρεία γεωγραφία. Η τοπογραφία του ορυχείου αλλάζει καθημερινά, πράγμα που σημαίνει ότι η λογική και φυσική τοπολογία του δικτύου πρέπει να προσαρμόζεται ανάλογα. Λόγω της εξαιρετικά ρευστής φύσης των τοπολογιών δικτύου σε ένα ορυχείο εργασίας, η ασύρματη συνδεσιμότητα χρησιμοποιείται συχνά.

Κεφάλαιο 12.3 Μια στρατηγική IoT για την εξόρυξη

Το IoT παρουσιάζει μία μεγάλη ποικιλία ευκαιριών για την εξόρυξη, από νέες λειτουργικές αποδόσεις έως την ασφάλεια της ζωής και την παρακολούθηση του περιβάλλοντος. Το Σχήμα 64 παρέχει αρκετά παραδείγματα.



Σχήμα 68: Παραδείγματα Εφαρμογών IoT σε Μεταλλευτικές Λειτουργίες.

Οι υπηρεσίες και λύσεις που προσφέρουν τα IoTs παρέχουν σημαντικά οφέλη στη λειτουργία των ορυχείων. Συγκεκριμένα εστιάζουν:

1.Στις βελτιωμένες υπηρεσίες ασφάλειας και τοποθεσίας. Μεταξύ όλων των πιθανών εφαρμογών του IoT για εργασίες εξόρυξης, η πρώτη υπηρεσία που προσφέρει είναι η ασφάλεια. Η εξόρυξη είναι επικίνδυνη λόγω του περιβάλλοντος όπου λαμβάνει χώρα και της τεράστιας ποσότητας υλικού που μετακινείται από πολύ μεγάλα οχήματα. Το IoT παρέχει πολύ ισχυρά μέσα για τη βελτίωση της ασφάλειας εξόρυξης, σε πολλαπλά επίπεδα όπως.:

2.Στην Ασφάλεια του οδηγού. Η ασφάλεια ενός φορτηγού μεταφοράς μπορεί να διακυβευθεί πολύ εάν ο οδηγός παρουσιάσει υπνηλία. Τα συστήματα IoT μπορούν να χρησιμοποιηθούν για τη μέτρηση του επιπέδου υπνηλίας ενός οδηγού φορτηγού. Αυτά τα συστήματα μπορούν να λειτουργούν με βάση τρεις τύπους μέτρων:

- Φυσιολογικά μέτρα: Ενδέχεται να απαιτείται από τους οδηγούς να φορούν ένα βραχιολάκι που μετρά τον καρδιακό ρυθμό, τα μοτίβα αναπνοής και άλλους παράγοντες και δημιουργεί συναγερμό όταν αυτά τα πρότυπα υποδηλώνουν υπνηλία.
- Μέτρα συμπεριφοράς: Μια κάμερα τοποθετημένη στο ταμπλό ή στον πίσω καθρέφτη μπορεί να μετρήσει το κλείσιμο των ματιών, το μοτίβο που αναβοσβήνουν, το χασμουρητό, τη θέση του κεφαλιού κ.λπ.
- Μέτρα τροχιάς οχήματος: Οι αισθητήρες στο φορτηγό μπορούν να μετρήσουν τις κινήσεις του τιμονιού, τη θέση στη λωρίδα, την πίεση στο πεντάλ γκαζιού και άλλους παράγοντες. Οι ξαφνικές αλλαγές υποδηλώνουν υπνηλία. Όταν ανιχνεύεται υπνηλία, μπορεί να ενεργοποιηθεί συναγερμός στο φορτηγό ή στο κέντρο ελέγχου και το φορτηγό μπορεί να σταματήσει αυτόματα.

3.Στον Καιρό και στις ακραίες καιρικές συνθήκες. Στην επιφανειακή εξόρυξη, οι κεραυνοί και οι κακές καιρικές συνθήκες αποτελούν σοβαρό κίνδυνο. Τα συστήματα παρακολούθησης κεραυνών και οι μικροί μετεωρολογικοί σταθμοί μπορούν να αναπτυχθούν σε μια περιοχή ορυχείου και να συνδεθούν στο δίκτυο για να παρέχουν πληροφορίες καιρού σε πραγματικό χρόνο στους χειριστές ορυχείων. Όταν ο κεραυνός εντοπίζεται σε απόσταση μικρότερη από 5 μίλια, οι εργαζόμενοι μπορούν να λάβουν μια ειδοποίηση στα κινητά τους τηλέφωνα, δίνοντάς τους οδηγίες να καλυφθούν μέχρι να περάσει η καταιγίδα.

4.Στην παρακολούθηση κλίσης ορυχείων. Τα ανοικτά ορυχεία κινδυνεύουν ιδιαίτερα από αστοχίες της κλίσης των ορυχείων, τα οποία μπορούν να οδηγήσουν σε μαζικές θανατηφόρες κατολισθήσεις. Αρκετές εταιρείες έχουν αναπτύξει συστήματα για την παρακολούθηση της ακεραιότητας των τοιχωμάτων, που συχνά ονομάζονται συστήματα παρακολούθησης κλίσης(slope monitoring systems). Τοποθετούνται στρατηγικά σε ανοικτό ορυχείο και απαιτούν συνδεσιμότητα δικτύου για τη μετάδοση των πληροφοριών στους χειριστές του ορυχείου. Επίσης, μπορούν να χρησιμοποιήσουν μια ποικιλία αισθητήρων.

5.Στις υπηρεσίες τοποθεσίας. Οι υπηρεσίες ασύρματης τοποθεσίας έχουν το πλεονέκτημα ότι δεν απαιτούν σήμα GPS και μπορούν να αναφέρουν τη θέση μιας κατάλληλα εξοπλισμένης συσκευής ή εργαζομένου μέσω ενός δικτύου ορυχείων. Είναι χρήσιμες για τον εντοπισμό περιουσιακών στοιχείων ή εργαζομένων όπου τα σήματα GPS δεν είναι διαθέσιμα. Αυτό είναι εξαιρετικά σημαντικό κατά τη διάρκεια έκτακτης ανάγκης, καθώς επιτρέπει στους πρώτους ανταποκριτές να γνωρίζουν αμέσως πού βρίσκονται οι εργαζόμενοι και να συγκεντρώνουν τις προσπάθειές τους για τη διάσωση, με βάση τον τόπο του συμβάντος. Πέρα από τις περιπτώσεις έκτακτης ανάγκης, η παρακολούθηση εργαζομένων μπορεί να είναι χρήσιμη για την ειδοποίηση οδηγού φορτηγού όταν εντοπιστεί εργαζόμενος στο έδαφος. (Τα φορτηγά συνήθως περιλαμβάνουν αισθητήρες και ραντάρ για να ειδοποιούνται όταν εντοπίζονται μικρότερα αντικείμενα, όπως οχήματα ή άτομα στην περιοχή.) Μια ειδική προειδοποίηση μπορεί επίσης να εμφανιστεί στην αίθουσα ελέγχου όταν οι εργαζόμενοι λειτουργούν σε επικίνδυνο σημείο.

Το μονοξείδιο του άνθρακα (CO) αποτελεί σημαντικό κίνδυνο στα υπόγεια ορυχεία. Είναι ένα άχρωμο, άοσμο, άοσμο τοξικό αέριο που παράγεται από την ατελή καύση υλικού που περιέχει άνθρακα, όπως άνθρακα ή ξύλο. Για πολλά χρόνια, οι εργαζόμενοι κουβαλούσαν συσκευές για τον εντοπισμό CO. Σήμερα, οι αισθητήρες IoT μπορούν να ειδοποιούν τους χειριστές για την παρουσία CO οπουδήποτε στο ορυχείο, σε πραγματικό χρόνο, και επίσης δείχνουν τάσεις συσσώρευσης CO. Ένα σύστημα IoT μπορεί επίσης να ρυθμίσει τον εξαερισμό με βάση την ανίχνευση CO και να τον διαμορφώσει περαιτέρω, ανάλογα με την παρουσία φορτηγών (που παράγουν μονοξείδιο του άνθρακα) και ανθρώπων. Αυτά τα συστήματα εντοπισμού συνήθως απαιτούν συνδεσιμότητα στο δίκτυο.

6.Στην ανίχνευση επικίνδυνων αερίων. Τόσο στην υπόγεια όσο και στην επιφανειακή εξόρυξη, μπορεί να υπάρχει μεγάλη ποικιλία θανατηφόρων ή επικίνδυνων αερίων, ανάλογα με τα ορυκτά που εξορύσσονται και τον τρόπο επεξεργασίας τους. Στα σημεία όπου αποτελούν κίνδυνο για τους εργαζόμενους αυτά τα αέρια είναι τοποθετημένα σταθερά συστήματα ανίχνευσης αερίου όσο και φορητές λύσεις για εργαζόμενους που εισέρχονται σε αυτές τις περιοχές. Αρκετά από αυτά τα φορητά συστήματα είναι ικανά να συνδεθούν στο δίκτυο είτε άμεσα είτε με τη χρήση μιας πύλης ικανής να υποστηρίζει βιομηχανικά ασύρματα πρωτόκολλα όπως το ISAlOO.lla και το WirelessHART.

7.Στην περιβαλλοντική παρακολούθηση. Ο συγκεκριμένος τύπος περιβαλλοντικής παρακολούθησης μπορεί να διαφέρει πολύ, ανάλογα με τον τύπο του ορυχείου, τη θέση και τους περιφερειακούς κανονισμούς. Ωστόσο, είναι πολύ συνηθισμένο τα συστήματα αυτά να είναι συνδεδεμένα στο δίκτυο. Περιλαμβάνουν οθόνες ποιότητας αέρα, και βιντεοκάμερες για την παρακολούθηση σκόνης, σωματιδίων και ποιότητας νερού. Ένας τομέας μεγάλης περιβαλλοντικής ανησυχίας που σχετίζεται με την εξόρυξη είναι η διασφάλιση της ακεραιότητας των λιμνών. Οι λίμνες δεξαμενής(Tailing Pond) είναι πολύ μεγάλες λίμνες που συγκρατούν τα απόβλητα της εξόρυξης, συνήθως ψιλοτριμμένα πετρώματα, νερό και χημικά που χρησιμοποιούνται στη διαδικασία εξόρυξης. Το Σχήμα 69 δείχνει ένα παράδειγμα.

Σχήμα 69: Άποψη ενός χωμάτινου φράγματος από το εξωτερικό (επάνω) και μια λίμνη αποθήκευσης απόβλητων με ένα χωμάτινο φράγμα (κάτω).

Κεφάλαιο 12.4 Μια αρχιτεκτονική για το IoT στην εξόρυξη

Οι εφαρμογές που χρησιμοποιούνται για τη λειτουργία εξοπλισμού σε ένα ορυχείο μπορεί να έχουν συγκεκριμένες απαιτήσεις δικτύου που πρέπει να αντιμετωπιστούν. Το δίκτυο σε ένα ορυχείο πρέπει να υποστηρίζει μια μεγάλη ποικιλία εφαρμογών και περιπτώσεων χρήσης και πρέπει να έχει σχεδιαστεί τόσο για προσαρμοστικότητα όσο και για αξιοπιστία. Λόγω του συνεχούς προγράμματος λειτουργίας πολλών ορυχείων(24 ώρες την ημέρα όλο το χρόνο), η ανθεκτικότητα και η ανοχή σε σφάλματα είναι επίσης πολύ σημαντικοί παράγοντες στο σχεδιασμό του δικτύου. Δεν είναι ασυνήθιστο να διακόπτεται ένας σύνδεσμος μεταξύ ενδιάμεσων πλαισίων διανομής (intermediate distribution frames IDFs) και ενός κύριου πλαισίου διανομής (main distribution frame MDF) ως αποτέλεσμα της συνήθους εξορυκτικής δραστηριότητας. Τα ορυχεία είναι πολύ δυναμικά μέρη όπου το φυσικό περιβάλλον βρίσκεται σε συνεχή κατάσταση αλλαγής. Το δίκτυο πρέπει να προσαρμόσει αυτή τη συνεχή αλλαγή και να επιτρέψει εξαιρετικά γρήγορη σύγκλιση στο πιθανό ενδεχόμενο βλάβης φυσικής σύνδεσης. Επιπλέον, η ισχύς σε ένα ορυχείο μπορεί να είναι πολύ δυναμική.

Σε περιβάλλοντα εξόρυξης, τα μεγάλα αντικείμενα, συμπεριλαμβανομένων των φορτηγών και ηλεκτρικών φτυαριών, γίνονται πλέον έξυπνα αντικείμενα. Επειδή αυτά τα μεγάλα αντικείμενα χειρίζονται συχνά από έναν άνθρωπο, οι αισθητήρες συνήθως συνδέονται με μια διεπαφή ανθρώπου-μηχανής (human-machine interface HMI) μέσω ενσύρματης διασύνδεσης. Ο χειριστής μπορεί να αξιοποιήσει άμεσα τις παρεχόμενες πληροφορίες. Ωστόσο, σε πολλές περιπτώσεις, το έξυπνο αντικείμενο χρειάζεται επίσης να παρέχει πληροφορίες στον απομακρυσμένο χειριστή. Σε αυτήν την περίπτωση, η συνδεσιμότητα δικτύου είναι απαραίτητη. Λόγω του συνεχώς μεταβαλλόμενου τοπίου τους, τα περισσότερα ορυχεία επιλέγουν ασύρματες τεχνολογίες για τη σύνδεση ανθρώπων και έξυπνων αντικειμένων. Μία ποικιλία ασύρματων τεχνολογιών μπορεί να χρησιμοποιηθεί σε εργασίες εξόρυξης για την ενεργοποίηση των επικοινωνιών για το IoT. Το ασύρματο είναι εξαιρετικά σημαντικό στις περισσότερες τοποθεσίες ορυχείων καθώς είναι μοναδικά ικανό να συνδέει σταθερό -κινητό εξοπλισμό και άτομα. Οι περισσότερες τεχνολογίες ασύρματης δικτύωσης λειτουργούν σε συχνότητες στη ζώνη μικροκυμάτων, όπου συνήθως απαιτείται οπτική επαφή για αξιόπιστες επικοινωνίες.

Οι ασύρματες δικτυώσεις χωρίζονται σε δύο κύριες κατηγορίες:

1.Ασύρματες δικτυώσεις με άδεια. Όπως υποδηλώνει το όνομα, για άδεια ασύρματου φάσματος απαιτείται κρατική άδεια για τη λειτουργία εξοπλισμού σε καθορισμένη συχνότητα ή ζώνη. Αυτές οι άδειες συνδέονται συνήθως με μια φυσική τοποθεσία ή γεωγραφική τοποθεσία. Στις εργασίες εξόρυξης, η άδεια ασύρματου δικτύου χρησιμοποιείται συχνά για:

- LMR (γνωστά ως walkie-talkies ή handie-talkies).
- Ασύρματες συνδέσεις μεγάλων αποστάσεων backhaul (γνωστές και ως συνδέσεις μικροκυμάτων).
- Παραδοσιακές συνδέσεις τύπου 3G / 4G / LTE.

2.Ασύρματες δικτυώσεις χωρίς άδεια. Το ασύρματο φάσμα χωρίς άδεια ρυθμίζεται από τον ίδιο κυβερνητικό φορέα με το αδειοδοτημένο ασύρματο φάσμα, αλλά ο εξοπλισμός αυτής της κατηγορίας δεν απαιτεί από τον ιδιοκτήτη ή τον χειριστή να αναζητήσει ατομικά άδεια χρήσης του εξοπλισμού σύμφωνα με τους κανόνες. Στις Ηνωμένες Πολιτείες, η Ομοσπονδιακή Επιτροπή Επικοινωνιών (Federal Communications Commission FCC) είναι ο ρυθμιστικός φορέας και ο δικτυώσεις χωρίς άδεια πρέπει να συμμορφώνονται με τους κανόνες FCC. Αυτή η κατηγορία περιλαμβάνει τεχνολογίες όπως το
IEEE 802.11a/b/g/n/ac/ah και το IEEE 802.15.4, το οποίο περιλαμβάνει ISAlOO.lla, ZigBee και WirelessHART.

Λόγω του σχετικά χαμηλού κόστους και της ευκολίας χρήσης τους, οι ασύρματες τεχνολογίες χωρίς άδεια είναι πολύ συχνές σε εφαρμογές εξόρυξης για επικοινωνίες δεδομένων, συμπεριλαμβανομένου του IoT. Ενώ οι αδειοδοτημένες συχνότητες είναι βολικές, πρέπει να ληφθεί μέριμνα για τον συντονισμό της χρήσης συχνοτήτων σε ένα ορυχείο για την αποφυγή παρεμβολών. Μία από τις πιο συνηθισμένες πηγές αστοχίας επικοινωνιών σε ένα ορυχείο είναι οι παρεμβολές που προκαλούνται από την υποδομή που εγκαταστάθηκε από δύο διαφορετικές ομάδες που δεν συντόνισαν την προγραμματισμένη χρήση συχνοτήτων τους.

Κεφάλαιο 13 Δημόσια ασφάλεια

Οι πρωταρχικοί στόχοι των οργανισμών δημόσιας ασφάλειας είναι να διατηρήσουν τους πολίτες, τις κοινότητες και τους δημόσιους χώρους ασφαλείς με ταχύτερη απόκριση, βελτιωμένη λειτουργική αποδοτικότητα και μειωμένο κόστος. Οι προκλήσεις δημόσιας ασφάλειας και αντιμετώπισης έκτακτης ανάγκης αυξάνονται σε πολυπλοκότητα και οι προσδοκίες μεγαλώνουν.
Το κύριο μέλημα της δημόσιας ασφάλειας είναι η δυνατότητα ταχείας χρήσης δεδομένων Το IoT έχει βαθύ αντίκτυπο στη δημόσια ασφάλεια, όσον αφορά τις πληροφορίες που απαιτούνται σε πραγματικό χρόνο. Συγκεκριμένα:

- Είναι ένα δίκτυο φυσικών αντικειμένων που μπορούν να ανιχνεύσουν και να επικοινωνήσουν δεδομένα.
- Βοηθά στη βελτίωση της επικοινωνίας μεταξύ των ανθρώπων.
- Βοηθά τους φορείς δημόσιας ασφάλειας με την προεπεξεργασία των συλλεγμένων δεδομένων, καθιστώντας τις ενέργειες των ανταποκριτών έκτακτης ανάγκης πιο αποτελεσματικές.
- Με την τεχνολογία αυτή επιτρέπει στους χρήστες να αναλαμβάνουν δράση με βάση έξυπνα δεδομένα.

Η δημόσια ασφάλεια είναι ένας ευρύς τομέας που περιλαμβάνει διάφορους τομείς με σκοπό τη διασφάλιση της ασφάλειας και της προστασίας. Ανταποκριτές πυρκαγιάς και έκτακτης ανάγκης, δυνάμεις επιβολής του νόμου και ασφάλειας σε δημόσιους χώρους και συγκεκριμένες τοποθεσίες, όπως είναι τα σχολεία, ακτοφυλακή και άμυνα, προστασία των συνόρων είναι μερικοί από αυτούς τους τομείς.

Αυτό το κεφάλαιο επικεντρώνεται στην επίδραση του IoT σε τυπικές περιπτώσεις αναγκών δημόσιας ασφάλειας όπως: της επιβολής του νόμου, της πυρόσβεση, τις ιατρικές υπηρεσίες έκτακτης ανάγκης (emergency medical services EMS) και τα σχολικά λεωφορεία.
Ειδικότερα, το κεφάλαιο αυτό περιλαμβάνει:

- Μία επισκόπηση της δημόσιας ασφάλειας. Εξετάζει τις διαφορετικές περιπτώσεις χρήσης για συνδεδεμένη δημόσια ασφάλεια, συμπεριλαμβανομένων των διαφορετικών αντικειμένων, οχημάτων και υπηρεσιών που αλληλεπιδρούν για να επιτρέψουν μια αποτελεσματική αντιμετώπιση έκτακτης ανάγκης.

- Ένα σχέδιο IoT για τη δημόσια ασφάλεια. Εξηγεί την έννοια της αποστολής και απαριθμεί τα διάφορα στοιχεία που απαιτούνται για τη διασφάλιση της αποστολής δημόσιας ασφάλειας.

- Μία αρχιτεκτονική IoT για έκτατη ανάγκη. Περιγράφει αρχιτεκτονικές IoT και επικοινωνίας που απαιτούνται για διάφορα οχήματα απόκρισης έκτακτης ανάγκης.

- IoT επεξεργασία πληροφοριών δημόσιας ασφάλειας. Παρέχει μια επισκόπηση του τρόπου με τον οποίο η επεξεργασία μεγάλων δεδομένων και πληροφοριών βελτιώνει την αποτελεσματικότητα της απόκρισης σε καταστάσεις έκτακτης ανάγκης.

- Την ασφάλεια σχολικών λεωφορείων. Αναφέρεται σε περαιτέρω εφαρμογές δημόσιας ασφάλειας και συγκεκριμένα στα σχολικά λεωφορεία για να δείξει πώς τα συνδεδεμένα δημόσια οχήματα μπορούν να βελτιώσουν τις δημόσιες υπηρεσίες και την ασφάλεια.

Κεφάλαιο 13.1 Μία επισκόπηση της δημόσιας ασφάλειας

Ένα κοινό θέμα για τη δημόσια ασφάλεια είναι η ανάγκη συλλογής, ανάλυσης και διανομής πληροφοριών που θα επιτρέψουν σε άτομα, ομάδες εργασίας, επιθεωρητές και στελέχη να εκτελέσουν τις αποστολές των αντίστοιχων οργανισμών τους. Αυτοί οι οργανισμοί εξαρτώνται από τη συνεργασία μεταξύ διαφόρων ομάδων ανθρώπων, που συνήθως αναφέρεται ως η ιεραρχία διοίκησης(chain of command), για την υποστήριξη των δημόσιων αναγκών. Ανεξάρτητα από τον τύπο της εκδήλωσης, η ασφάλεια του κοινού και του προσωπικού της υπηρεσίας εξαρτάται από την αξιοπιστία, την εμπιστευτικότητα και την ακεραιότητα των επικοινωνιών τους.
Το IoT ανοίγει νέες δυνατότητες για τη σύνδεση οργανισμών και ενισχύει τις δυνατότητες επίγνωσης και απόκρισης της κατάστασης σε όλο το περιβάλλον αποστολής, βοηθώντας στην παροχή των ακόλουθων:

- Επίγνωση της κατάστασης σε πραγματικό χρόνο.
- Ενδοεταιρική επικοινωνία και συνεργασία (για παράδειγμα, φωνή, δεδομένα, βίντεο).
- Ανάλυση δεδομένων και ανταλλαγή πληροφοριών.
- Αυξημένη συμμετοχή της κοινότητας και προσέγγιση ενδιαφερομένων.

Η δημόσια ασφάλεια απαιτεί την αλληλεπίδραση σε πραγματικό χρόνο μεταξύ πολιτών, προσωπικού πεδίου, επιβολής του νόμου, ευφυών αισθητήρων και ευφυών συστημάτων ανάλυσης. Αυτό έχει ως αποτέλεσμα, μια ποικιλία λύσεων IoT να εφαρμόζεται σε περιπτώσεις δημόσιας ασφάλειας. Οι έξυπνοι αισθητήρες και οι συναγερμοί επιτρέπουν στους οργανισμούς να συλλαμβάνουν δεδομένα και να δημιουργούν έναν σύνδεσμο μεταξύ αισθητήρων και σημείων συλλογής δεδομένων. Τα εργαλεία ανάλυσης, επεξεργάζονται δεδομένα και γεγονότα στο άκρο(tactical edge) ή στο cloud και παρέχουν μια οπτική παρουσίαση δεδομένων και γεγονότων για ανάλυση και λήψη αποφάσεων. Οι εφαρμογές IoT για τη δημόσια ασφάλεια περιλαμβάνουν ευρέως τρεις τύπους έξυπνων αντικειμένων:

Αντικείμενα που μεταφέρονται από τους πρώτους ανταποκριτές. Είναι εξειδικευμένοι αισθητήρες, όπως καταγραφείς και πομποί ζωτικών σημείων πρώτης απόκρισης και αισθητήρες περιβάλλοντος που συλλέγουν πληροφορίες σχετικά με τη θερμοκρασία, την παρουσία χημικών ουσιών και οποιαδήποτε άλλη παράμετρο που πιθανόν να βοηθήσει τον πρώτο ανταποκριτή να εκτιμήσει τους κινδύνους για άμεση δράση ή ανάλυση μετά το συμβάν. Μπορούν επίσης να είναι γενικά αντικείμενα όπως κάμερες σώματος (ηχογράφηση σε τοπικό επίπεδο ή παροχή ζωντανής τροφοδοσίας σε κεντρικό σταθμό συντονισμού και εντολών) ή ακόμη και έξυπνα τηλέφωνα. Τα δεδομένα που συλλέγονται από αυτά τα αντικείμενα μπορούν επίσης να υποβληθούν σε επεξεργασία τοπικά ή στο cloud.

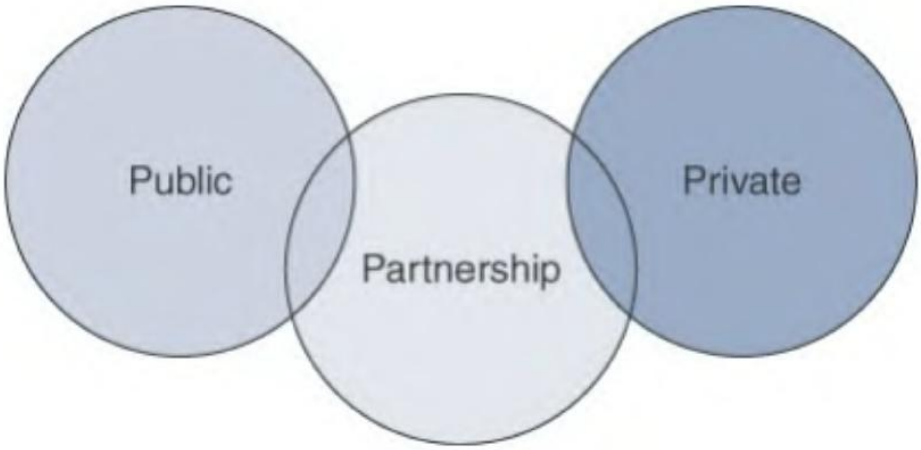
Αντικείμενα που βοηθούν τους καλούντες ή τα θύματα των υπηρεσιών έκτακτης ανάγκης. Περιλαμβάνει μια μεγάλη ποικιλία συσκευών υγείας, από βασικά κουμπιά πανικού (συνδεδεμένα με συστήματα κλήσης ανταπόκρισης έκτακτης ανάγκης) έως προηγμένους αισθητήρες υγείας (για παράδειγμα, οθόνες υγείας που μπορούν να ενεργοποιήσουν συναγερμούς και αυτοματοποιημένες κλήσεις σε ανταποκριτές έκτακτης ανάγκης μέσω κινητού τηλεφώνου με λεπτομερείς πληροφορίες σχετικά με το εντοπισμένο ζήτημα).

Αντικείμενα που υπάρχουν στο περιβάλλον. Είναι έξυπνα αντικείμενα που υπάρχουν σε δημόσιο περιβάλλον. Αυτοί οι αισθητήρες βελτιώνουν τη δημόσια ασφάλεια παρακολουθώντας το περιβάλλον (για παράδειγμα, κάμερες δρόμου, χειριστήρια φωτισμού δρόμου, αισθητήρες περιβάλλοντος και καπνού, τοποθεσία κυκλοφορίας και πυκνότητα). Τα δεδομένα τους μπορούν να έχουν πρόσβαση από μεμονωμένους ανταποκριτές έκτακτης ανάγκης ή μπορούν να χρησιμοποιηθούν για να τροφοδοτήσουν μια υπηρεσία αντιμετώπισης έκτακτης ανάγκης για να βελτιώσουν την επίγνωση της κατάστασης ή την αποτελεσματικότητα της απόκρισης.

Ένας άλλος αντίκτυπος του IoT στη δημόσια ασφάλεια είναι η αυξανόμενη απαίτηση συλλογής, αποθήκευσης και επεξεργασίας πλούσιων πληροφοριών φωνής, βίντεο και δεδομένων σε πραγματικό χρόνο ή για ανάλυση μετά το συμβάν. Οι λύσεις IoT απαιτούνται για τη συλλογή και επεξεργασία δεδομένων στην άκρη (fog computing), ενώ προωθούν μόνο στο cloud σε πραγματικό χρόνο ένα υποσύνολο των δεδομένων που συλλέγονται και επεξεργάζονται. Ένα μεγαλύτερο ή πλήρες σύνολο δεδομένων μπορεί να προωθηθεί σε μια κεντρική εγκατάσταση αποθήκευσης και επεξεργασίας όταν οι ανταποκριτές έκτακτης ανάγκης έχουν πρόσβαση σε μια γρήγορη σύνδεση. Ο όγκος των διαθέσιμων πληροφοριών είναι ήδη συντριπτικός και το IoT οδηγεί στην ανάγκη για προηγμένα εργαλεία και αναλύσεις (για παράδειγμα, μεγάλα δεδομένα, μηχανική εκμάθηση) για να διασφαλιστεί ότι τα γεγονότα και τα πρότυπα προσδιορίζονται για έγκαιρη και ακριβή απάντηση. Όταν απαιτείται ανταπόκριση, το IoT συντελεί σημαντικά για να προστατεύει και να βοηθά το κοινό, να αποκρούει και να περιορίζει απειλές και καταστροφές.

Η επιτυχία ενός οργανισμού δημόσιας ασφάλειας εξαρτάται σε μεγάλο βαθμό από την ικανότητά του να συνεργάζεται με άλλους οργανισμούς και να ανταλλάσσει πληροφορίες. Η πιο κοινή ανάγκη για ανταλλαγή πληροφοριών είναι ο συντονισμός των πόρων του πεδίου(coordination of field resources). Αυτός ο συντονισμός μπορεί να λάβει πολλές μορφές, συμπεριλαμβανομένης της άμεσης επικοινωνίας, της φωνής, του βίντεο και των δεδομένων. Διαφορετικές υπηρεσίες μπορούν επίσης να επωφεληθούν από την ανταλλαγή πληροφοριών εκτός πλαισίου αντιμετώπισης έκτακτης ανάγκης. Πολλοί οργανισμοί μπορεί επίσης να συμμετέχουν στη συλλογή ή την παροχή πληροφοριών σχετικά με τις μεταφορές, τις υπηρεσίες κοινής ωφέλειας, τα σχολεία ή οποιοδήποτε άλλο πεδίο ενδιαφέροντος για το ευρύ κοινό, όπως οδικούς κινδύνους, καιρικές συνθήκες, ημερολογιακές εκδηλώσεις και χρονοδιαγράμματα, καθώς και διαθεσιμότητα ενέργειας και νερού.

Η εταιρική σχέση ανταλλαγής πληροφοριών εκτείνεται πέρα από τη δημόσια ασφάλεια και περιλαμβάνει πολλούς άλλους κυβερνητικούς οργανισμούς. Η δημόσια ασφάλεια βασίζεται στην πραγματικότητα σε μια ολοκληρωμένη σχέση μεταξύ κυβερνητικών υπηρεσιών, μη κυβερνητικών οργανώσεων (ΜΚΟ) και ιδιωτών. Αυτός ο δεσμός είναι κοινώς γνωστός ως σύμπραξη δημόσιου-ιδιωτικού τομέα(public-private partnership). Τόσο οι ΜΚΟ όσο και οι ιδιώτες αλληλεπιδρούν και εξαρτώνται από τις υπηρεσίες δημόσιας ασφάλειας για να υποστηρίξουν το κοινό σε πολλά διαφορετικά περιβάλλοντα, από δρόμους και αυτοκινητόδρομους, κτίρια γραφείων και πανεπιστημιουπόλεις, εμπορικά κέντρα και τοπικές επιχειρήσεις, μέχρι πάρκα και χώρους αναψυχής. Η σύμπραξη δημόσιου-ιδιωτικού τομέα που φαίνεται στο Σχήμα 70 είναι ένα οικοσύστημα. Αυτό σημαίνει ότι η επιτυχία της εταιρικής σχέσης εξαρτάται από τη συμμετοχή και των δύο πλευρών. Ένα μεγάλο μέρος αυτού του οικοσυστήματος είναι η δυνατότητα να συνδέονται μεταξύ τους μέσω της ανταλλαγής πληροφοριών.

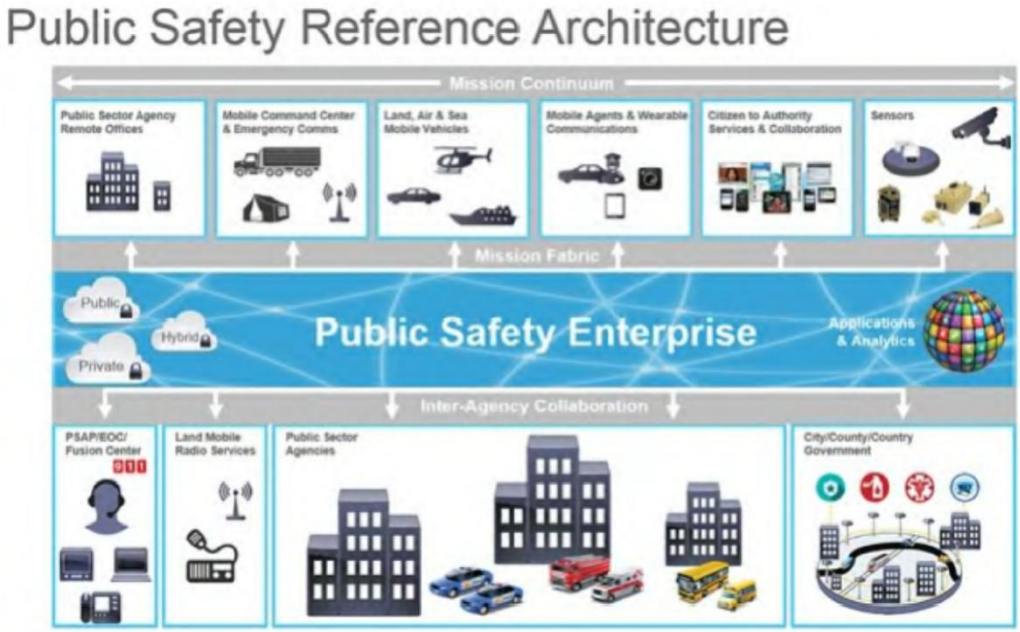


Σχήμα 70: Συνεργασία δημόσιου-ιδιωτικού τομέα.

Καθώς το IoT αναπτύσσεται, ο αντίκτυπος της ανταλλαγής πληροφοριών στη δημόσια ασφάλεια και τη συνεργασία δημόσιου-ιδιωτικού τομέα θα επεκταθεί εκθετικά. Ως αποτέλεσμα αυτής της διευρυνόμενης συνεργασίας, θα εμφανιστούν πολλές νέες καινοτομίες και περιπτώσεις χρήσης, αξιοποιώντας νέες πηγές δεδομένων και τύπους αισθητήρων, οδηγώντας στην ανάγκη για καλύτερη αποθήκευση, ανάλυση και ανταλλαγή πληροφοριών.

Κεφάλαιο 13.2 Ένα IoT σχέδιο για τη δημόσια ασφάλεια

Ο IoT σχεδιασμός για τον δημόσιο χώρο ασφάλειας συνεπάγεται ομαδοποίηση αντικειμένων και τύπους δεδομένων σε κατηγορίες με δυνατότητα δράσης. Κάθε περίπτωση χρήσης και κάθε περιβάλλον μπορεί να έχει μια μοναδική αρχιτεκτονική. Πάνω από όλες αυτές τις αρχιτεκτονικές, το IoT για τη δημόσια ασφάλεια χρειάζεται ένα γενικό πλαίσιο. Το σχέδιο IoT που φαίνεται στο Σχήμα 71 παρέχει ένα πλαίσιο για την επιχείρηση δημόσιας ασφάλειας. Αυτό το πλαίσιο μπορεί να επεκταθεί για να περιγράψει ένα πλαίσιο IoT για σχεδόν οποιοδήποτε φορέα δημόσιας ασφάλειας, μεγάλο ή μικρό.



Σχήμα 71: IoT σχέδιο για τη δημόσια ασφάλεια.

Περιγραφή πλαισίου για τη δημόσια ασφάλεια:

Συνεχής αποστολή(Mission Continuum). Στην κορυφή του σχεδίου,βρίσκονται έξι τύποι τοποθεσιών και συσκευών επικοινωνίας που εξασφαλίζουν τη συνέχεια της αποστολής. Συγκεκριμένα υπάρχουν:

- Απομακρυσμένα γραφεία και σταθεροί χώροι. Πρόκειται για σταθερές τοποθεσίες, όπως αστυνομικός χώρος, πυροσβεστικός σταθμός, αποθήκη οχημάτων, σχολικό κτίριο ή διοικητικό κτίριο που υποστηρίζει την αποστολή. Εκεί βρίσκονται οι παραδοσιακές λύσεις δικτύωσης για δρομολόγηση, εναλλαγή, ασφάλεια και εφαρμογές. Αυτά τα δίκτυα μεταφέρουν δεδομένα IT και OT.

- Κινητό κέντρο εντολών και τοποθεσίες επικοινωνίας έκτακτης ανάγκης. Είναι προσωρινές τοποθεσίες που πρέπει να αναπτυχθούν, για να παρέχουν υποστήριξη (για τη διοίκηση συμβάντων και στις εξειδικευμένες ομάδες) και λειτουργίες που αποτελούν αναπόσπαστο μέρος της αποστολής δημόσιας ασφάλειας. Η επικοινωνία IT και OT για αυτούς τους ιστότοπους μπορεί να υποστηριχθεί από ειδικά σχεδιασμένες λύσεις για συνδεσιμότητα και λειτουργία. Αυτοί οι ιστότοποι ενδέχεται να επεξεργαστούν τοπικά δεδομένα που συλλέγονται από το πεδίο για να αναφέρουν μια συλλογική επίγνωση της κατάστασης.

- Κινητά οχήματα ξηράς, αέρος και θάλασσας. Αυτές οι πλατφόρμες κινητών οχημάτων απαιτούν συνδεσιμότητα σε κίνηση. Παραδείγματα είναι αυτοκίνητα, φορτηγά, λεωφορεία, σκάφη και αεροσκάφη που υποστηρίζουν την αποστολή δημόσιας ασφάλειας. Αυτά τα οχήματα είναι συνήθως εξοπλισμένα με πολλαπλούς αισθητήρες και έξυπνα αντικείμενα, όπως κάμερες, tablet και εξειδικευμένες συσκευές. Οι τεχνολογίες για αυτά τα οχήματα έχουν σχεδιαστεί για να αντιμετωπίζουν σκληρά περιβάλλοντα όπου η θερμοκρασία, οι κραδασμοί και η υγρασία μπορεί να κυμαίνονται ευρέως. Αυτές οι τοποθεσίες δίνουν επίσης ιδιαίτερη προσοχή στις απαιτήσεις μεγέθους, βάρους και ισχύος (size, weight, and power SWaP), οι οποίες μπορεί να είναι πολύ περιορισμένες.

- Κινητοί πράκτορες(Mobile agents) και φορητές επικοινωνίες. Αυτές οι τοποθεσίες είναι οι ίδιοι οι πράκτορες πεδίου ή το άμεσο περιβάλλον τους, που συνήθως σχηματίζουν ένα προσωπικό δίκτυο περιοχής (personal area network PAN). Οι λύσεις επικοινωνίας για αυτές τις τοποθεσίες είναι λύσεις φορητές.

- Υπηρεσίες και συνεργασία από πολίτη σε αρχή. Αυτή είναι η διεπαφή όπου η δημόσια ασφάλεια και το κοινό συνεργάζονται μέσω ανταλλαγής πολιτών-αρχών. Μια κοινή ανταλλαγή είναι η επείγουσα κλήση και η αποστολή γραπτών μηνυμάτων. Πολλά άλλα παραδείγματα υπάρχουν, επιτρέποντας αυτήν την ανταλλαγή ή να είναι πιο ισχυρή, υποστηρίζοντας πλούσια φωνή, βίντεο και δεδομένα σε αλληλεπιδράσεις σε πραγματικό χρόνο.

- Αισθητήρες. Πρόκειται για συσκευές και πράγματα που συλλέγουν πληροφορίες για την αποστολή δημόσιας ασφάλειας. Οι δυνατότητες αυτής της κατηγορίας διευρύνονται. Οι αισθητήρες μπορούν να είναι στατικοί ή κινητοί, τοποθετημένοι σε περιβάλλον εξωτερικό της ομάδας αποστολής δημόσιας ασφάλειας ή ενσωματωμένα στον εξοπλισμό της ομάδας. Το αποτέλεσμα είναι ένα πλέγμα αισθητήρων ικανό να συλλέγει πληροφορίες που μπορούν να συνδυαστούν με

εφαρμογές, αναφορές και αναλύσεις για να οδηγήσουν την επίγνωση της κατάστασης.

Ιστός αποστολής(mission fabric). Είναι η διαδικτυακή σύνδεση που συνδέει τη συνέχεια της αποστολής μαζί με την επιχείρηση δημόσιας ασφάλειας. Ο ιστός της αποστολής πρέπει να παρέχει μια απρόσκοπτη ολοκλήρωση που είναι ανεξάρτητη από τα χαρακτηριστικά τοποθεσίας (σταθερή ή κινητή πλατφόρμα). Στο πλαίσιο της επιχείρησης δημόσιας ασφάλειας, η συνέχεια της αποστολής και οι διάφορες πλατφόρμες συνδέονται μεταξύ τους με τον ιστό της αποστολής. Είναι μια δυναμική και ευέλικτη έννοια που επιτρέπει στις σταθερές και κινητές πλατφόρμες να παραμένουν συνδεδεμένες. Παρέχει μια ομοιόμορφη μέθοδο που επιτρέπει στα διάφορα άτομα, διαδικασίες και πράγματα να μοιράζονται ένα κοινό σύνολο πολιτικών ασφαλείας και πρόσβαση σε εφαρμογές και πόρους, καθώς και είναι αγνωστικιστική για τη μεταφορά φυσικού επιπέδου.
Συγκεκριμένα:

- Οι πολιτικές ασφαλείας είναι σημαντικές και ενδέχεται να διαφέρουν ανάλογα με το φυσικό ή λογικό περιβάλλον κάθε πλατφόρμας. Για παράδειγμα, σε μια σταθερή τοποθεσία, η φυσική ασφάλεια αυτών των τοποθεσιών θα πρέπει να είναι καλά καθορισμένη και θα πρέπει να μειώνει τον κίνδυνο μη εξουσιοδοτημένης φυσικής πρόσβασης και έκθεσης.

- Οι απαιτήσεις για πολιτικές ασφαλείας αλλάζουν σε όλη τη συνέχεια της αποστολής. Οι εξωτερικές επιρροές και η πρόσβαση αυξάνονται σημαντικά από αριστερά προς τα δεξιά όπως φαίνεται στο Σχήμα 71. Αυτό συμβαίνει επειδή οι πλατφόρμες λειτουργούν εντός της κοινότητας και σε ορισμένες περιπτώσεις λειτουργούν εντελώς χωρίς επίβλεψη (όπως στην περίπτωση των απομακρυσμένων αισθητήρων).

- Η πρόσβαση σε εφαρμογές και πόρους θα πρέπει επίσης να είναι απρόσκοπτη όλη τη διάρκεια, επιτρέποντας στο προσωπικό οπουδήποτε στην αποστολή να εκτελεί τα καθήκοντά του. Αυτή η ικανότητα μπορεί να αλλάξει καθώς αλλάζει το εύρος ζώνης και η διαθεσιμότητα δικτύου, αλλά δεν πρέπει να αποκλείει ή να εμποδίζει μια ομοιόμορφη και συνεχή ικανότητα συνεργασίας μέσω εφαρμογών φωνής, βίντεο και δεδομένων.

- Οποιαδήποτε μεταφορά φυσικού στρώματος θα πρέπει να είναι συμβατή με τον ιστό της αποστολής για να διασφαλιστεί ότι, ανεξάρτητα από το πού πρέπει να λειτουργήσει η αποστολή, είναι διαθέσιμη συνδεσιμότητα. Αυτό σημαίνει ότι μπορεί να υποστηριχθεί οποιαδήποτε σύγχρονη ενσύρματη ή ασύρματη τεχνολογία όπως είναι τα ακόλουθα Ethernet, σειριακή τεχνολογία, οπτικές ίνες SONET και DWDM, MPLS, WiFi, εμπορικές ή ιδιωτικές συσκευές, μικροκύματα point-to-point και multipoint, ad hoc δικτύωση για κινητά.

Εσωτερική υπηρεσία και συνεργασία(Inter-agency Collaboration).Το περισσότερο του σχεδίου IoT για τη δημόσια ασφάλεια σχετίζεται με την εσωτερική υπηρεσία και τη συνεργασία μεταξύ πολιτών και αρχών. Το λιγότερο από το μισό του σχεδίου IoT αφορά την αλληλεπίδραση μεταξύ των οργανισμών.

Πολλές χώρες διαθέτουν διάφορους οργανισμούς δημόσιας ασφάλειας, όπως τα:

- PSAPs (public safety answering points). Είναι σημεία ανταπόκρισης δημόσιας ασφάλειας όπου απαντώνται κλήσεις έκτακτης ανάγκης.
- EOCs(emergency operations centers). Είναι κέντρα επιχειρήσεων έκτακτης ανάγκης, όπου εκπρόσωποι από έναν ή περισσότερους οργανισμούς συναντώνται για να συντονίσουν τις ενέργειές τους σε καταστάσεις έκτακτης ανάγκης.
- Κέντρα σύντηξης(fusion centers). Είναι κέντρα πληροφοριών που συλλέγουν, αναλύουν και διαδίδουν πληροφορίες σε τοπικές υπηρεσίες.
- LMRS(land mobile radio services). Είναι υπηρεσίες κινητής ραδιοεπικοινωνίας, που διαχειρίζονται φωνητικές επικοινωνίες κρίσιμες για την αποστολή σε έναν ή περισσότερους τοπικούς οργανισμούς.

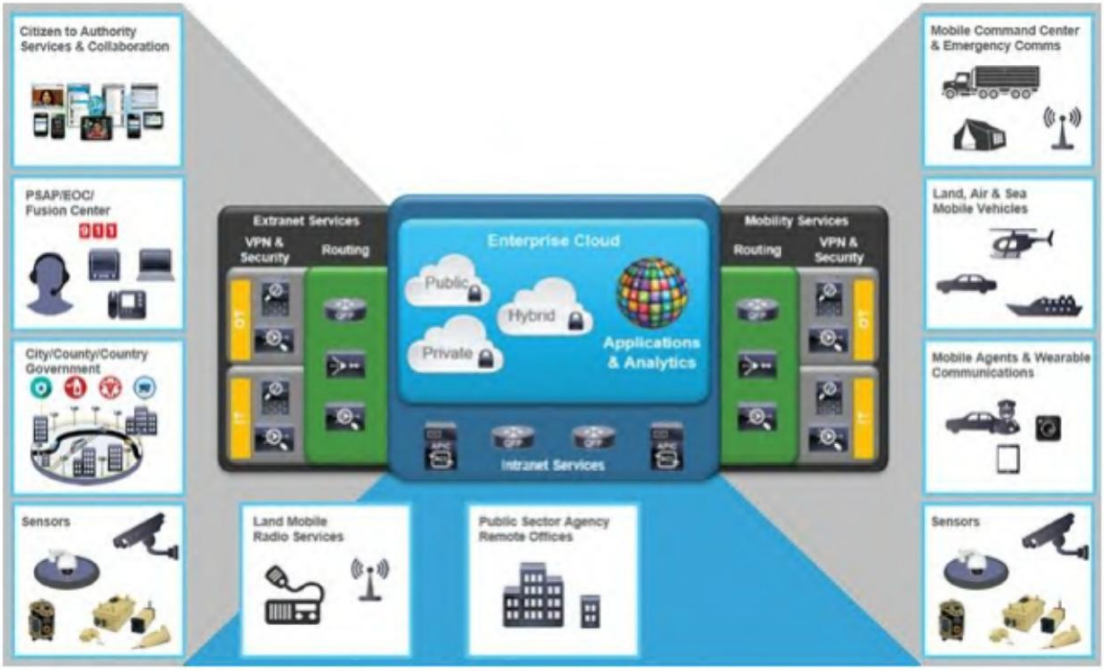
Αυτά τα κρίσιμα στοιχεία της υποδομής δημόσιας ασφάλειας αποτελούν κοινό σημείο συντονισμού και συνεργασίας μεταξύ δημόσιων και ιδιωτικών οργανισμών. Έχοντας μια ισχυρή διασύνδεση για συνεργασία σημαίνει ότι οι έγκαιρες, ακριβείς και ουσιαστικές πληροφορίες μπορούν να ανταλλαχθούν με μεγαλύτερη ακρίβεια. Μια άλλη αξιοσημείωτη παρατήρηση έχει σχέση με το πώς αλλάζει η δημόσια ασφάλεια σε συνδιασμό με κινητά οχήματα. Οι περισσότερες υπηρεσίες δημόσιας ασφάλειας θεωρούν ότι το όχημα είναι επέκταση του χώρου γραφείων της υπηρεσίας. Ωστόσο, τα συστήματα και οι δυνατότητες σε αυτά τα οχήματα έχουν εφαρμοστεί διαφορετικά με την πάροδο του χρόνου. Σε αντίθεση με ένα απομακρυσμένο γραφείο, το οποίο διαθέτει εξοπλισμό που μοιράζεται υποδομές και υπηρεσίες, καθένα από αυτά τα συστήματα λειτουργεί σαν πελάτης απομακρυσμένης πρόσβασης, με αποτέλεσμα την απόκλιση της τεχνολογίας του οχήματος και την αύξηση των κινδύνων ασφαλείας.

Για παράδειγμα, στα περισσότερα αστυνομικά αυτοκίνητα σήμερα, ο φορητός υπολογιστής με δυνατότητα CAD / RMS διαθέτει ένα κινητό(cellular) μόντεμ. Η συσκευή εγγραφής βίντεο στο αυτοκίνητο μπορεί επίσης να διαθέτει ραδιόφωνο Wi-Fi και κινητό μόντεμ. Το σύστημα LPR ενδέχεται να διαθέτει ραδιόφωνο Wi-Fi. Το σύστημα παρακολούθησης AVF μπορεί να λειτουργεί μέσω του φορητού υπολογιστή ή μέσω του FMR που είναι τοποθετημένο στο αυτοκίνητο, ή μπορεί να είναι ανεξάρτητο και να έχει τη δική του κινητή σύνδεση. Το αποτέλεσμα είναι μια συνεχής επίδραση στο λειτουργικό κόστος και τη δυσκολία κεντρικής και ομοιόμορφης διαχείρισης και ασφάλειας αυτών των συστημάτων. Αυτή η κατάσταση δεν είναι μόνο για τα αστυνομικά οχήματα και υπάρχει σε πυρκαγιά, EMS και σχολικά λεωφορεία.

Αυτό το γενικό σχέδιο IoT για τη δημόσια ασφάλεια μπορεί στη συνέχεια να εφαρμοστεί στους διάφορους φορείς και τα διάφορα λειτουργικά μοντέλα τους. Η αναφορά στο σχέδιο μπορεί να διασφαλίσει ότι κάθε μεμονωμένη λύση και αρχιτεκτονική ταιριάζει στο μεγαλύτερο μοντέλο. Αυτό θα διευκολύνει την επικοινωνία και την ανταλλαγή πληροφοριών μεταξύ λύσεων και αρχιτεκτονικών.

Κεφάλαιο 13.3 Αρχιτεκτονική IoT για περιπτώσεις έκτακτης ανάγκης(Response Emergency)

Οι ανταποκριτές έκτακτης ανάγκης, σε αντίθεση με τους εργαζόμενους σε άλλα επαγγέλματα, λειτουργούν σε απρόβλεπτα περιβάλλοντα. Γνωρίζουν επίσης ότι δεν μπορούν να εργαστούν ανεξάρτητα. Πρέπει να συνεργαστούν με άλλους ανταποκριτές, για να εκτελέσουν το καθήκον τους με επιτυχία. Η περίπτωση της αρχιτεκτονικής IoT αντιμετώπισης έκτακτης ανάγκης είναι ελαφρώς διαφορετική επειδή οργανώνεται γύρω από κινητά ή στατικά κέντρα εντολών έκτακτης ανάγκης. Η συνδεσιμότητα είναι επομένως το πρώτο μέλημα αυτής της τοπολογίας και οδηγεί την αρχιτεκτονική των διαφόρων στοιχείων που διασυνδέονται με το κέντρο εντολών. Το Σχήμα 72 δείχνει τις διάφορες κινητές πλατφόρμες πιθανής αντιμετώπισης έκτακτης ανάγκης και πώς συνδέονται με το cloud μέσω μιας πύλης υπηρεσιών κινητικότητας.



Σχήμα 72: Αρχιτεκτονική αντιμετώπισης έκτακτης ανάγκης.

Υπάρχουν τρεις συνηθισμένοι τύποι κινητών πλατφορμών σε αυτό το περιβάλλον:

- Ο φορέας κινητής τηλεφωνίας(mobile agent).
- Το κινητό κέντρο εντολών (the mobile command center).
- Το κινητό όχημα(mobile vehicle).

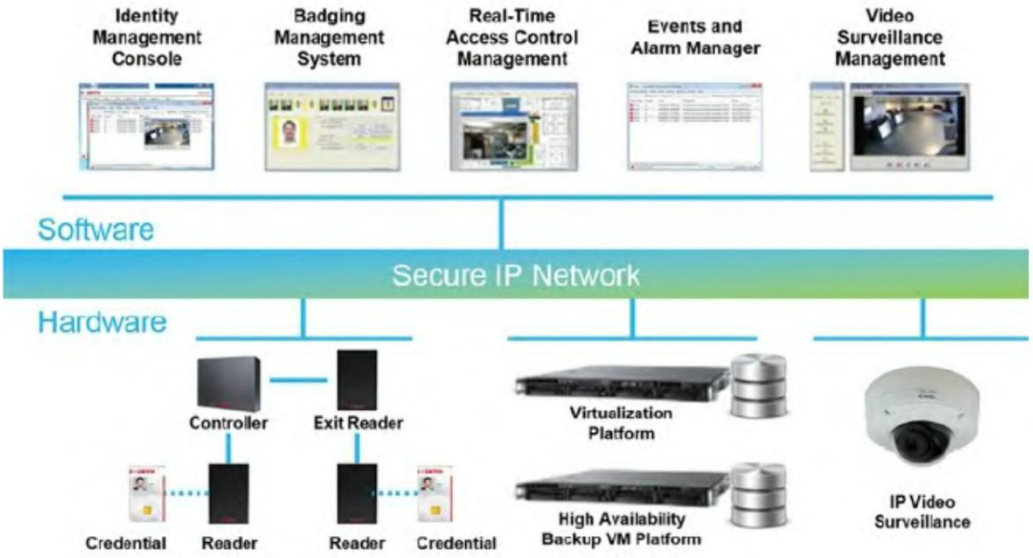
Το κινητό κέντρο εντολών(Mobile command center), είναι μια επέκταση του σταθερού γραφείου. Χρησιμεύει ως κέντρο επικοινωνίας σε καταστάσεις έκτακτης ανάγκης, όπως απειλές για βόμβες, διαδηλώσεις, πυρκαγιές ή φυσικές καταστροφές και μπορεί επίσης να χρησιμοποιηθεί για τη διεξαγωγή συναντήσεων στρατηγικής και άλλων τακτικών επιχειρήσεων. Αναπτύσσεται κοντά στην τοποθεσία της έκτακτης ανάγκης ή στον ίδιο τον τόπο για να βοηθήσει στην αξιολόγηση της έκτακτης ανάγκης και επίσης να διευκολύνει τη φυσική αλληλεπίδραση με τους τοπικούς ενδιαφερόμενους φορείς. Κατά συνέπεια, οι απαιτήσεις του κινητού κέντρου εντολών είναι ίδιες με αυτές ενός στατικού γραφείου.

Υπηρεσίες Δικτύου και Ασφάλειας(Network and Security Services): Το κινητό κέντρο εντολών τυπικά διαθέτει αρκετό χώρο για να υποστηρίξει τον παραδοσιακό εξοπλισμό IT. Αυτό καθιστά δυνατή τη χρήση πολλών τυπικών προϊόντων για δρομολόγηση, μεταγωγή, ασύρματο έλεγχο, ασφάλεια και υπολογιστικές υπηρεσίες. Εκεί που το κέντρο εντολών διαφέρει από το τυπικό απομακρυσμένο γραφείο είναι ότι όλη η συνδεσιμότητά του με το cloud είναι ασύρματη. Η αρχιτεκτονική του κινητού οχήματος βασίζεται στην ιδέα ότι κάθε τεχνολογία uplink θα πρέπει να είναι ένα χρήσιμο εργαλείο για την επίτευξη του επιχειρησιακού cloud. Αυτό σημαίνει ότι σχεδόν οποιαδήποτε ενσύρματη ή ασύρματη τεχνολογία είναι αποδεκτή. Ως μέρος της επιχείρησης δημόσιας ασφάλειας, ένα κινητό κέντρο εντολών πρέπει να παρέχει ασφαλείς επικοινωνίες και να υποστηρίζει το απόρρητο δεδομένων παρόμοια με αυτό των απομακρυσμένων γραφείων της υπηρεσίας. Επειδή το κινητό κέντρο εντολών χρησιμοποιεί παρόμοιο εξοπλισμό με αυτόν στα απομακρυσμένα γραφεία, οι ίδιες πολιτικές και δυνατότητες ασφαλείας μπορούν να εφαρμοστούν και στις δύο πλευρές.

Η ασφάλεια σε αυτήν την περίπτωση μπορεί να εξεταστεί σε δύο τομείς:

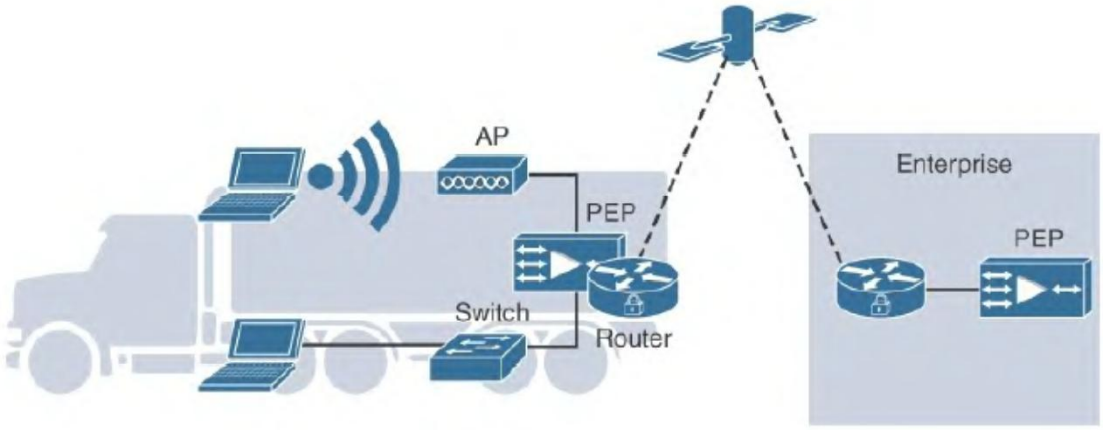
- Την φυσική ασφάλεια, η οποία μπορεί να αντιμετωπιστεί όπως και στο απομακρυσμένο γραφείο μιας υπηρεσίας, χρησιμοποιώντας συστήματα ελέγχου πρόσβασης, συναγερμού και παρακολούθησης βίντεο. Μια ποικιλία λύσεων φυσικής ασφάλειας παρέχουν τυπικούς αναγνώστες φυσικής πρόσβασης και ενεργοποιητές πόρτας, όπως φαίνεται στο Σχήμα 73. Ο φυσικός έλεγχος πρόσβασης μπορεί επίσης να περιλαμβάνει μια μεγάλη ποικιλία από ετικέτες ελέγχου στοιχείων, λύσεις διαχείρισης ταυτότητας και πίνακες συναγερμού. Οι βιντεοκάμερες IP είναι κατάλληλες για τη συλλογή ροών βίντεο από γύρω από ένα όχημα, την καταγραφή του περιεχομένου για έλεγχο και αναπαραγωγή και τη διανομή βίντεο στο προσωπικό της περιοχής συμβάντων.

- Την ασφάλεια δικτύου. Η ασφάλεια δικτύου για κινητό κέντρο εντολών θα πρέπει να πληροί ή να υπερβαίνει τις πολιτικές και τις διαδικασίες που χρησιμοποιούνται σε απομακρυσμένα γραφεία πρακτορείων.



Σχήμα 73: Έλεγχος πρόσβασης και ενσωμάτωση βίντεο επιτήρησης.

Στην αρχιτεκτονική του κινητού κέντρου εντολών, ο δρομολογητής είναι το κοινό σημείο ολοκλήρωσης μεταξύ του οχήματος και του εξωτερικού κόσμου της συνδεσιμότητας. Συνεπώς, ο δρομολογητής(router), πρέπει να προσφέρει προηγμένες υπηρεσίες ασφαλείας (για παράδειγμα, προηγμένη κρυπτογράφηση, υπηρεσίες τείχους προστασίας, προστασία από απειλές, VPN) για την προστασία των δεδομένων. Επίσης, απαιτείται η προστασία τοπικής συνδεσιμότητας πρόσβασης στο διαδίκτυο. Η εξασφάλιση ανοικτών θυρών Ethernet και ασύρματης πρόσβασης είναι ένα σημαντικό ζήτημα για ένα κινητό κέντρο εντολών. Σε μια πλατφόρμα για κινητές συσκευές, αυτό είναι ιδιαίτερα σημαντικό επειδή η έκθεση της υποδομής IT στο προσωπικό(εκτός της υπηρεσίας δημόσιας ασφάλειας), είναι δεδομένη. Το Σχήμα 74 παρέχει ένα δείγμα χρήσης.



Σχήμα 74: Αρχιτεκτονική επικοινωνίας Wi-Fi.

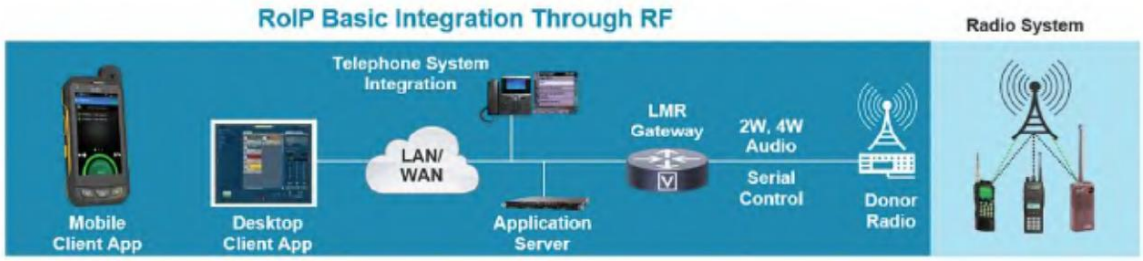
Ένα κινητό κέντρο εντολών δεν έχει την ίδια προστασία φυσικής ασφάλειας με ένα σταθερό γραφείο. Οποιοδήποτε άτομο στην περιοχή του κέντρου εντολών μπορεί να εντοπίσει το δίκτυο Wi-Fi και να προσπαθήσει να παρακολουθήσει ή να καταλάβει ή να διακόψει τις επικοινωνίες. Ένα κοινό μοντέλο ανάπτυξης χρησιμοποιεί αρχιτεκτονική βασισμένη σε ελεγκτή WFAN, όπου το AP βρίσκεται στο κέντρο εντολών, αλλά ο ελεγκτής WFAN παραμένει στο στατικό γραφείο. Το AP συνδέεται με τον ελεγκτή WFAN μέσω της σύνδεσης WAN uplink. Ο έλεγχος ταυτότητας χρήστη πραγματοποιείται μέσω του κεντρικού ελεγκτή WFAN και ενός διακομιστή RADIUS.
Οποιαδήποτε θύρα στο διακόπτη στο κέντρο εντολών προστατεύεται επίσης με έλεγχο ταυτότητας 802.1x. Εάν ένα αίτημα πρόσβασης δεν μπορεί να πιστοποιηθεί, οι πολιτικές στον τοπικό διακόπτη ή στο σημείο πρόσβασης Wi-Fi μπορούν να αποτρέψουν την πλήρη πρόσβαση ή να περιορίσουν την πρόσβαση έως ότου παρέχεται έλεγχος ταυτότητας. Αυτή η προσέγγιση διασφαλίζει ότι η πρόσβαση σε ενσύρματες και ασύρματες συνδέσεις διαχειρίζεται ομοιόμορφα και μετριάζει τις απειλές με βάση τη φυσική πρόσβαση στο όχημα.

Υπηρεσίες υπολογιστών και εφαρμογών: Ένα κινητό κέντρο εντολών πρέπει να είναι ευέλικτο και ικανό να υποστηρίζει τη δυναμική φύση της αποστολής. Οι υπηρεσίες υπολογιστών και εφαρμογών πρέπει να λειτουργούν διαδραστικά και απρόσκοπτα με τους πόρους της επιχείρησης και της περιοχής συμβάντων. Αυτές οι υπηρεσίες πρέπει επίσης να είναι αυτάρκες σε περιόδους που το εταιρικό cloud δεν είναι διαθέσιμο και το κινητό κέντρο εντολών είναι η μόνη διαθέσιμη αναπαράσταση της δομής εντολών μιας υπηρεσίας σε ένα συμβάν.

Αυτά αναφέρονται ως εξαρτημένοι και ανεξάρτητοι τρόποι λειτουργίας. Για υποστήριξη εξαρτημένων και ανεξάρτητων λειτουργιών, το κινητό κέντρο εντολών θα πρέπει να διαθέτει τοπικές δυνατότητες υπολογισμού με δυνατότητα φιλοξενίας εικονικών μηχανών και εφαρμογών. Η αποτελεσματικότητα ενός κινητού κέντρου εντολών εξαρτάται σε μεγάλο βαθμό από τις δυνατότητες IT και OT. Οι παραδοσιακές δυνατότητες IT για φωνή, τηλεδιάσκεψη και κοινή χρήση δεδομένων αποτελούν τη βάση για το κέντρο εντολών. Εφαρμογές ειδικές για την OT όπως CAD, RMS, COP, διαχείριση προσωπικού και παρόμοια εργαλεία, αντιμετωπίζουν περιπτώσεις για τη δημόσια ασφάλεια.

Ο τοπικός έλεγχος για φωνητικές κλήσεις και βιντεοκλήσεις είναι ο πυρήνας της συνεργασίας. Επιτρέπει σε ένα κινητό κέντρο εντολών να λειτουργεί με ή χωρίς σύνδεση με το εταιρικό cloud. Όταν το κέντρο εντολών μπορεί να έχει πρόσβαση στο εταιρικό cloud, υπηρεσίες όπως η φωνητική κλήση στο διαδίκτυο και η βιντεοκλήση, μπορούν να διασφαλίσουν την ασφάλεια και να μειώσουν το κόστος των λειτουργιών. Σε ανεξάρτητη λειτουργία, μπορούν να δημιουργηθούν υπηρεσίες φωνητικής επικοινωνίας μέσω IP VoIP(voice over IP), μεταξύ του κέντρου εντολών και ενός παρόχου φωνητικών υπηρεσιών μέσω απευθείας σύνδεσης στο διαδίκτυο. Η φωνή **push to talk** αποτελεί βασικό εργαλείο OT για τις υπηρεσίες δημόσιας ασφάλειας. Ένα κινητό κέντρο εντολών βασίζεται στην πρόσβαση στα συστήματά του LMR για να αλληλεπιδρά αποτελεσματικά με το προσωπικό πεδίου. Μια βασική προσέγγιση είναι η τοποθέτηση παραδοσιακών κινητών ραδιοφώνων που είναι τοποθετημένα στο όχημα στο κέντρο εντολών. Αυτό μπορεί να γίνει σε κάθε γραφείο με ηχεία και μικρόφωνα. Αυτή η προσέγγιση είναι κοινή αλλά έχει προβλήματα. Σε ένα πολυάσχολο περιβάλλον, το να ακούγονται πολλά ηχεία μπορεί να αυξήσει το επίπεδο θορύβου(noise floor) και μπορεί να αποσπά την προσοχή, μειώνοντας την αποτελεσματικότητα της λειτουργίας. Επίσης, η απόφαση ποια ραδιόφωνα να εγκατασταθούν σε κάθε γραφείο μπορεί να είναι δύσκολη, επειδή ο λειτουργικός ρόλος κάθε θέσης γραφείου μπορεί να αλλάξει με βάση την αποστολή.

Η χρήση ενός προηγμένου συστήματος ραδιοελέγχου, όπως φαίνεται στο Σχήμα 75 για την κεντρική διαχείριση των ραδιοφώνων σε ένα κέντρο εντολών και τη δυναμική διανομή της πρόσβασης στους χρήστες, είναι μια κλιμακούμενη και ευέλικτη προσέγγιση. Επιτρέπει σε κάθε χρήστη να έχει πρόσβαση σε οποιοδήποτε ραδιόφωνο στο όχημα χρησιμοποιώντας mobile client, εγκατεστημένο σε smartphone ή tablet Android ή Apple. Ένα τέτοιο σύστημα μπορεί επίσης να ενσωματωθεί με την υπάρχουσα ραδιοφωνική υποδομή μέσω σύνδεσης IP στην επιχείρηση.



Σχήμα 75: Παράδειγμα ραδιοφώνου μέσω IP.

Αυτό είναι σημαντικό επειδή μπορεί να ελαχιστοποιήσει τον αριθμό των ραδιοφώνων που απαιτούνται. Μπορεί επίσης να αυξήσει την προσβασιμότητα του κέντρου διοίκησης, συμπεριλαμβανομένων των τοπικών πόρων δημόσιας ασφάλειας που διατίθενται σε αυτόν τον οργανισμό και σε άλλους συνεργαζόμενους οργανισμούς.

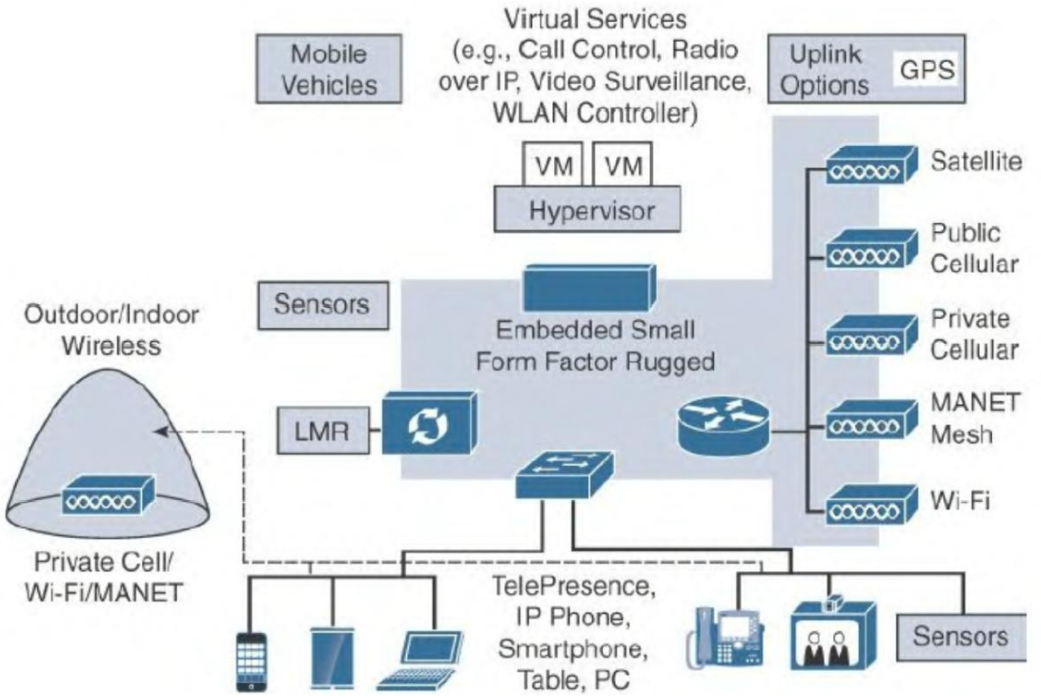
Η IT τηλεδιάσκεψη, η βίντεο-τηλεδιάσκεψη και η συνεργασία μέσω διαδικτύου, είναι εργαλεία που χρησιμοποιούν οι περισσότεροι άνθρωποι, συμπεριλαμβανομένης της δημόσιας ασφάλειας, για να συνεργαστούν σήμερα. Οι λύσεις λογισμικού που παρέχουν σε αυτήν την υπηρεσία είναι κοινές σε ένα κινητό κέντρο εντολών. Επίσης, μπορούν να φιλοξενήσουνε ή / και να παρέχουν πρόσβαση σε εφαρμογές OT που σχετίζονται με δημόσιες υπηρεσίες μέσω κινητού κέντρου εντολών. Αυτά τα εργαλεία CAD, RMS, αποστολής LMR, διαχείρισης κλήσεων PSAP και διαχείρισης EOC μπορούν να χρησιμοποιηθούν κατά τη διάρκεια της ανάπτυξης.

Μια άλλη εφαρμογή που αρχίζει να εμφανίζεται σε αυτά τα οχήματα ονομάζεται κοινή εικόνα λειτουργίας (common operating picture COP), που φαίνεται στο Σχήμα 76.

Σχήμα 76: Κοινή λειτουργική εικόνα (common operating picture COP) σε ένα έξυπνο τηλέφωνο.

Ένα COP έχει σχεδιαστεί για να εμφανίζει τακτικές λειτουργίες σε πραγματικό χρόνο με διάφορα στοιχεία, όπως άτομα, οχήματα, drones και αισθητήρες. Τα περισσότερα εργαλεία COP ενσωματώνονται με πλούσια μέσα, όπως ροές βίντεο και μπορούν να κατευθύνουν άλλους χρήστες του COP να δουν κάτι ενδιαφέρον. Μπορούν επίσης να υποστηρίξουν την τηλεμεταφορά και τη δυνατότητα να σχεδιάζουμε ελεύθερα .Τέλος μπορούν να υποστηρίξουν εικόνα ή ακόμα και προβολή βίντεο. Μια σημαντική πτυχή των εργαλείων COP είναι ότι όλοι στην αποστολή βλέπουν μια κοινή εικόνα. Τα προηγούμενα εργαλεία επίγνωσης της κατάστασης επέτρεπαν μόνο στον υπεύθυνο να δει ολόκληρη την εικόνα. Έχοντας αυτήν την ευελιξία σε ένα κινητό κέντρο εντολών μπορεί να επιτρέψει στην πλατφόρμα να αναλάβει μια ποικιλία ρόλων, με βάση το περιστατικό, όπως λύση αποκατάστασης PSAP, σταθμό διοίκησης συμβάντων, κοινό κέντρο επιχειρήσεων και συντονισμού ή αποστολή ειδικής ομάδας εργασίας.

Η αρχιτεκτονική κινητών οχημάτων(mobile vehicle) δημόσιας ασφάλειας, που φαίνεται στο Σχήμα 77 περιγράφει μια ποικιλία από πλατφόρμες κινητών που χρησιμοποιούνται στη δημόσια ασφάλεια.



Σχήμα 77: Κινητά οχήματα ξηράς, αέρος και θαλάσσης.

Αυτή η αρχιτεκτονική είναι παρόμοια με το κινητό κέντρο εντολών, αλλά με αρκετές σημαντικές διαφορές. Η πιο σημαντική διαφορά είναι ότι η αρχιτεκτονική του κινητού κέντρου εντολών βασίζεται στην έννοια των επικοινωνιών όταν το όχημα είναι σταθμευμένο. Ένα κινητό κέντρο εντολών μπορεί επίσης να λειτουργεί αυτόνομα από το εταιρικό δίκτυο και τις υπηρεσίες cloud. Η αρχιτεκτονική των χερσαίων, εναέριων και θαλάσσιων κινητών οχημάτων έχει σχεδιαστεί για επικοινωνίες εν κινήσει και λειτουργεί επίσης ως επέκταση της επιχείρησης δημόσιας ασφάλειας. Επομένως, τυπικά εξαρτάται από εταιρικές υπηρεσίες. Αυτές οι πλατφόρμες δεν χρησιμοποιούν ενσύρματες επικοινωνίες, αλλά εξαρτώνται από ασύρματους συνδέσμους και συνδέσεις από ομότιμους, καθώς τα οχήματα κινούνται στην ξηρά, στον αέρα και στη θάλασσα. Μια άλλη σημαντική διαφορά είναι τα φυσικά και περιβαλλοντικά χαρακτηριστικά των κινητών οχημάτων. Αυτά τα οχήματα έχουν σχεδιαστεί για αποστολή. Για παράδειγμα, ένα πυροσβεστικό όχημα διαθέτει πολλά τμήματα για εξειδικευμένο εξοπλισμό. Ο χώρος που διατίθεται για επικοινωνίες, αισθητήρες ή μονάδες επεξεργασίας δεδομένων πρέπει να είναι όσο το δυνατόν μικρότερος. Περιβαλλοντικά, αυτά τα οχήματα λειτουργούν σε υψηλές και χαμηλές θερμοκρασίες, αντιμετωπίζουν κραδασμούς και εκτίθενται σε υγρασία, και σκόνη. Ενώ ο εξοπλισμός γενικής χρήσης μπορεί να χρησιμοποιηθεί σε αυτά τα οχήματα, όμως οι περιβαλλοντικές συνθήκες μπορούν να μειώσουν σημαντικά τη διάρκεια ζωής του ηλεκτρονικού εξοπλισμού. Ορισμένα εξειδικευμένα οχήματα, όπως αεροσκάφη ή θαλάσσια σκάφη, ενδέχεται να απαιτούν εξοπλισμό πιστοποιημένο για χρήση σε δύσκολες συνθήκες.

Τα χερσαία, εναέρια και θαλάσσια οχήματα έχουν διαφορετικές ανάγκες υπολογιστικών υπηρεσιών και εφαρμογών από ό, τι το κινητό κέντρο εντολών. Τα κινητά οχήματα εστιάζουν περισσότερο στην εκτέλεση μιας συγκεκριμένης και τυπικά βραχυπρόθεσμης αποστολής.

Ένα μεγάλο μέρος της αποστολής είναι η συνεργασία με την επιχείρηση, πράγμα που σημαίνει ότι οι επικοινωνίες και οι εφαρμογές πρέπει να μοιραστούν. Οι φορητές και οι συσκευές LMR που είναι τοποθετημένες στο όχημα είναι μια μακροχρόνια κύρια μέθοδος επικοινωνίας δημόσιας ασφάλειας. Αυτές οι συσκευές χρησιμοποιούν την υποδομή επικοινωνίας για να μιλούν σε μεγάλες αποστάσεις. Η υποδομή περιλαμβάνει σταθμούς βάσης, διασυνδέσεις και κεντρική δυνατότητα μεταγωγής, όπως ακριβώς παρέχει το μοντέλο του επιχειρησιακού cloud.

Κεφάλαιο 13.4 IoT Επεξεργασία πληροφοριών δημόσιας ασφάλειας

Στην περίπτωση της δημόσιας ασφάλειας, τα έξυπνα αντικείμενα διευκολύνουν την άμεση ανταπόκριση σε κατάσταση έκτακτης ανάγκης. Για παράδειγμα, οι ανιχνευτές καπνού και οι συναγερμοί πυρκαγιάς είναι τέτοια πολύ γνωστά αντικείμενα. Με το IoT, αυτά τα αντικείμενα μπορούν να συνδεθούν στο διαδίκτυο και να στείλουν σήμα(να εκέψουν συναγερμό), στην πλησιέστερη πυροσβεστική υπηρεσία. Ομοίως, αυτοί οι αισθητήρες μπορούν να επικοινωνούν μεταξύ τους. Μια τέτοια επικοινωνία επιτρέπει την ενεργοποίηση συναγερμού πυρκαγιάς με ένα συγκεκριμένο μοτίβο ήχου ή κουδουνίσματος εάν ένα γειτονικό σπίτι ή κτίριο καίγεται, επιτρέποντας τη λήψη προληπτικών μέτρων. Σε σχολεία, πανεπιστήμια και γειτονιές που είναι ευάλωτες σε εγκληματικότητα, συχνά χρησιμοποιούνται ανιχνευτές πυροβολισμών. Αυτοί οι αισθητήρες επεξεργάζονται ήχους για να αναζητήσουν το συγκεκριμένο μοτίβο ενός ήχου πυροβολισμού. Εάν εντοπιστεί αυτό το μοτίβο, ένας συναγερμός αποστέλλεται αυτόματα στο πλησιέστερο αστυνομικό τμήμα μέσω ενσύρματου ή ασύρματου συνδέσμου επικοινωνιών. Η μείωση του χρόνου ανίχνευσης συμβάντων με τη σειρά του μειώνει τον συνολικό χρόνο απόκρισης.

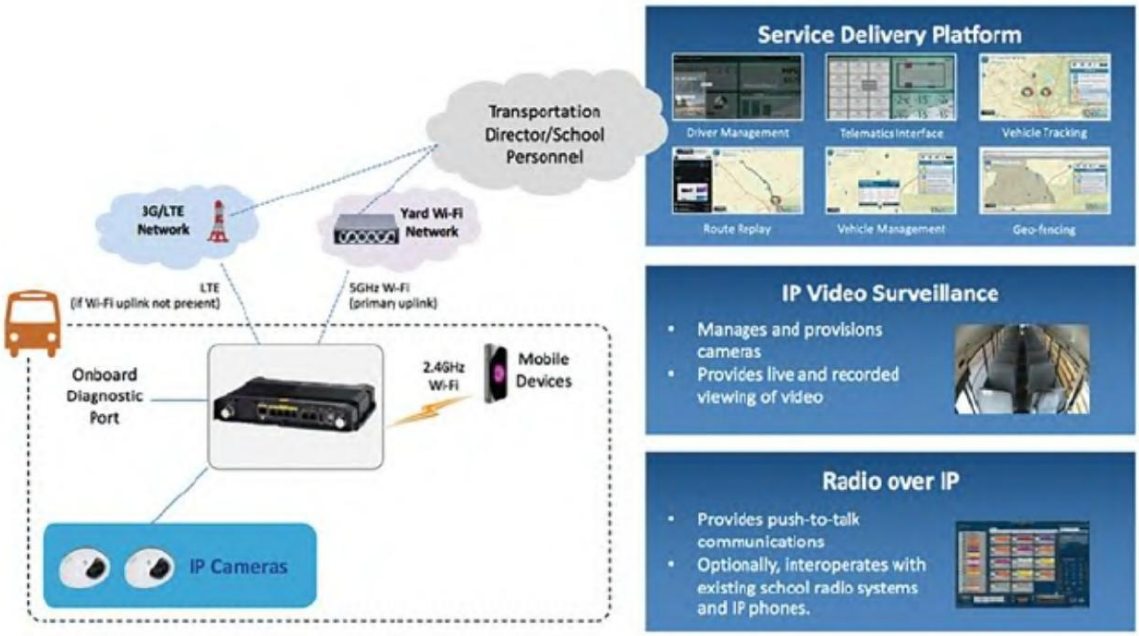
Η επεξεργασία βίντεο είναι πλέον μια κοινή εφαρμογή για τη δημόσια ασφάλεια. Οι νέοι αλγόριθμοι μηχανικής μάθησης αυξάνουν τα ποσοστά επιτυχίας αναγνώρισης προσώπου και η επεξεργασία εικόνων από σκηνές εγκλήματος έχει γίνει μια κοινή εφαρμογή IoT. Το βίντεο σε πραγματικό χρόνο χρησιμοποιείται επίσης συνήθως για να επιτρέψει τη βοήθεια εξειδικευμένων ειδικών σε πολλά σενάρια έκτακτης ανάγκης, συμπεριλαμβανομένων εκείνων που αφορούν ατυχήματα. Το βίντεο χρησιμοποιείται επίσης για περιπτώσεις δημόσιας ασφάλειας που δεν σχετίζονται με καταστάσεις έκτακτης ανάγκης για τη βελτίωση της αποδοτικότητας και τη μείωση των κινδύνων που σχετίζονται με τη μεταφορά. Για παράδειγμα, οι συνομιλίες μέσω βίντεο περιορίζουν το κόστος και τον κίνδυνο μεταφοράς καταδίκων.

Τα μεγάλα δεδομένα χρησιμοποιούνται επίσης για τη δημόσια ασφάλεια. Για παράδειγμα, τα εγκληματικά δεδομένα μπορούν να αναλυθούν λεπτομερώς για να παρέχουν μια προοπτική άποψη για την πιθανότητα εγκληματικότητας. Τα μεγάλα συστήματα δεδομένων δεν μπορούν να προβλέψουν το μέλλον. Ωστόσο, αυτά τα εργαλεία μπορούν να αναλύσουν χαρακτηριστικά εγκλημάτων του παρελθόντος και να χαρτογραφήσουν μοτίβα εγκληματικής συμπεριφοράς για να συμπεράνουν την πιθανότητα μελλοντικής εγκληματικής δραστηριότητας. Οι αστυνομικές δυνάμεις μπορούν να χρησιμοποιήσουν αυτές τις πληροφορίες για να αναπτύξουν τον σωστό αριθμό αξιωματικών στις σωστές τοποθεσίες για να αποτρέψουν την εκδήλωση εγκλημάτων.

Η ίδια λογική χρησιμοποιείται από πολλούς άλλους φορείς δημόσιας ασφάλειας. Για παράδειγμα, ο τομέας της πυροσβεστικής χρησιμοποιεί μηχανική μάθηση για τη διασταύρωση δεδομένων και την πρόβλεψη πυρκαγιών. Οι πληροφορίες μπορεί να περιλαμβάνουν προφανή στοιχεία όπως ιστορικό πυρκαγιάς. Στη συνέχεια, μπορούν να ληφθούν προληπτικά μέτρα για την αποφυγή πυρκαγιών πριν προκύψουν συνθήκες πυρκαγιάς.

Κεφάλαιο 13.5 Ασφάλεια σχολικού λεωφορείου

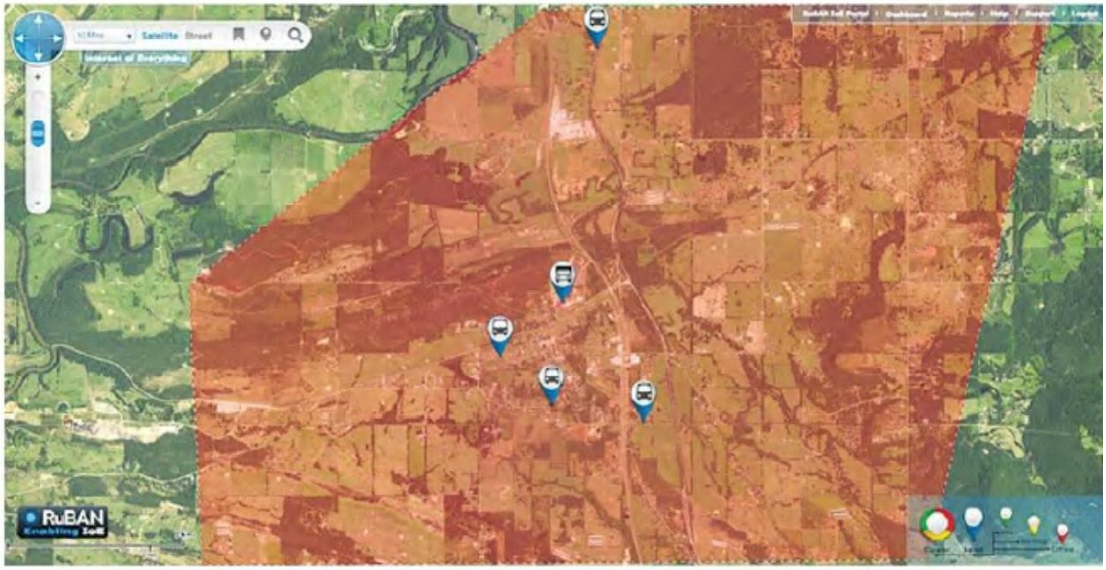
Η δημόσια ασφάλεια εκτείνεται και πέρα από τις υπηρεσίες έκτακτης ανάγκης και περιλαμβάνει κάθε τομέα όπου διακυβεύεται το ευρύ κοινό και η ασφάλειά τους. Σήμερα, το IoT εφαρμόζεται και στα σχολικά λεωφορεία, για να παρέχει νέες δυνατότητες και γνώσεις στους υπεύθυνους μεταφορών, στους γονείς, στους διευθυντές και στους μαθητές. Ένα μεγάλο μέρος της αρχιτεκτονικής αφορά άμεσα την ασφάλεια των μαθητών. Το Σχήμα 78, δείχνει ένα διάγραμμα υψηλού επιπέδου της αρχιτεκτονικής και επικοινωνίας ασφάλειας σχολικών λεωφορείων καθώς και των προσφερόμενων υπηρεσιών τους.



Σχήμα 78: Αρχιτεκτονική Επικοινωνίας - Ασφάλειας Σχολικών Λεωφορείων.

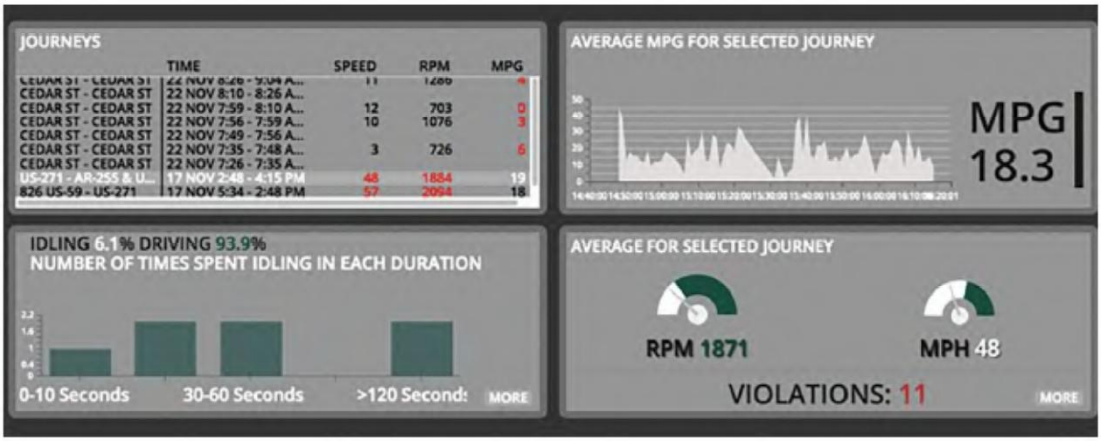
Ένα μεγάλο πρόβλημα που αντιμετωπίζουν καθημερινά οι γονείς και το προσωπικό του σχολείου είναι να γνωρίζουν πού βρίσκεται το λεωφορείο και αν ένας μαθητής βρίσκεται στο λεωφορείο. Σε πολλές περιπτώσεις, ένας γονιός και ενώ περιμένει το παιδί του να είναι στο σπίτι, καλεί το γραφείο μεταφορών αναζητώντας μαθητή. Χωρίς τη βοήθεια του IoT, το προσωπικό του γραφείου μεταφορών πρέπει να πραγματοποιεί τηλεφωνικές ή ραδιοφωνικές κλήσεις για να καθορίσει εάν ένας μαθητής βρίσκεται στο λεωφορείο.
Με τη βοήθεια του IoT, ο υπεύθυνος μεταφοράς μπορεί να γνωρίζει, σε πραγματικό χρόνο, την ακριβή τοποθεσία του λεωφορείου, ποιοι μαθητές βρίσκονται στο λεωφορείο και από ποιο σημείο βγήκαν ή μπήκαν μαθητές στο λεωφορείο. Αυτή η απλή γνώση του πού βρίσκονται τα λεωφορεία μπορεί να είναι μεγάλη βοήθεια για τους υπεύθυνους των μεταφορών κυρίως όταν ένα σχολικό λεωφορείο έχει διανύσει μεγάλη απόσταση από το σχολείο.

Έτσι σε περίπτωση κάποιου συμβάντος(που σχετίζεται με την ασφάλεια), ο υπεύθυνος μεταφοράς μπορεί να γνωρίζει πού ακριβώς να κατευθύνει τους ανταποκριτές έκτακτης ανάγκης. Ο υπεύθυνος μεταφορών δύναται να γνωρίζει περίπου πότε ένα λεωφορείο πρέπει να φτάσει σε μια δεδομένη τοποθεσία και μπορεί να ειδοποιηθεί εάν το λεωφορείο έχει ταξιδέψει έξω από ένα καθορισμένο όριο διαδρομής. Το Σχήμα 79, δείχνει ένα παράδειγμα στο οποίο η επικαλυμμένη περιοχή με κόκκινο χρώμα αντιπροσωπεύει τις θέσεις όπου μπορεί να βρεθεί ένα λεωφορείο κατά τη διάρκεια μιας κανονικής ημέρας.
Εάν το λεωφορείο ταξιδεύει εκτός αυτής της περιοχής, το προσωπικό του σχολείου ειδοποιείται.



Σχήμα 79: Τοποθεσία λεωφορείου εντός συγκεκριμένου ορίου μεταφοράς.

Ένα άλλο πλεονέκτημα της πληροφορίας θέσης και τηλεματικής είναι η παρακολούθηση της συμπεριφοράς του οδηγού λεωφορείου. Για παράδειγμα, εάν ένας οδηγός λεωφορείου υπερβεί μια ασφαλή ταχύτητα, μπορεί να ειδοποιηθεί ο υπεύθυνος μεταφοράς.
Το Σχήμα 80, δείχνει ένα άλλο παράδειγμα αναφοράς συμπεριφοράς οδηγού. Αυτός ο τύπος αναφοράς είναι χρήσιμος για να διαπιστωθεί εάν ένας συγκεκριμένος οδηγός δεν περιμένει αρκετό χρόνο στη στάση του λεωφορείου ώστε να κάθονται με ασφάλεια οι μαθητές ή εάν ένας συγκεκριμένος οδηγός περνά το όριο ταχύτητας κατά τη διάρκεια μιας διαδρομής. Αυτός ο τύπος αναφοράς μπορεί να οδηγήσει σε ασφαλέστερη οδήγηση.



Σχήμα 80: Αναφορά συμπεριφοράς οδηγού λεωφορείου.

Ένα από τα πιο ευρέως χρησιμοποιούμενα χαρακτηριστικά της λύσης ασφάλειας των σχολικών λεωφορείων είναι η παρακολούθηση βίντεο. Η παρακολούθηση βίντεο μπορεί να χρησιμοποιηθεί για την παρακολούθηση της ασφάλειας των μαθητών στο λεωφορείο. Επίσης χρησιμεύει είτε για την καταγραφή του τι συμβαίνει έξω από το λεωφορείο σε περίπτωση ατυχήματος είτε για την καταγραφή ενός οδηγού που παράνομα πέρασε ένα σχολικό λεωφορείο που είχε σταματήσει. Σε πολλές χώρες, οι οδηγοί δεν επιτρέπεται να περάσουν ένα σχολικό λεωφορείο που έχει σταματήσει, καθώς τα παιδιά μπορεί να περπατούν γύρω από το λεωφορείο ή να διασχίζουν το δρόμο χωρίς να δίνουν ιδιαίτερη προσοχή στην πιθανή κίνηση του δρόμου. Βίντεο, που αποτυπώνουν τα χαρακτηριστικά ταυτοποίησης του παραβατικού οχήματος μπορούν να παρασχεθούν στο προσωπικό επιβολής του νόμου.

Ένα ακόμα χαρακτηριστικό των σχολικών λεωφορείων είναι το Wi-Fi. Συγκεκριμένα, μπορεί να παρασχεθεί για να επιτρέψει στους μαθητές να κάνουν εργασίες στο λεωφορείο ή απλώς να τους απασχολήσουν για να αποτρέψουν προβλήματα συμπεριφοράς. Μερικοί μαθητές βρίσκονται σε λεωφορείο για περισσότερες από δύο ώρες την ημέρα, κάτι που μπορεί να είναι πολύτιμος χρόνος μελέτης. Τέλος, η φωνητική επικοινωνία μεταξύ του προσωπικού του σχολείου και των οδηγών λεωφορείων είναι μια συνηθισμένη περίπτωση χρήσης IoT. Το σχολείο μπορεί είτε να παρέχει συσκευές έξυπνου τηλεφώνου ή tablet στους οδηγούς λεωφορείων είτε να ζητήσει από τους οδηγούς του λεωφορείου να εγκαταστήσουν μια εφαρμογή σε προσωπικές συσκευές. Σε κάθε περίπτωση, η συσκευή συνδέεται με το δίκτυο Wi-Fi του λεωφορείου, αποφεύγοντας έτσι την ανάγκη χρήσης δεδομένων κινητής τηλεφωνίας στη συσκευή του έξυπνου τηλεφώνου.

Συμπέρασμα

Η τεχνολογία του «Διαδικτύου των Πραγμάτων» αναμένεται τα επόμενα χρόνια να γνωρίσει ιδιαίτερη άνθηση σε όλους τους τομείς της ανθρώπινης δραστηριότητας. Υπάρχουν πολλές προσεγγίσεις οι οποίες μπορούν να εξυπηρετήσουν αυτό το σκοπό ώστε όσο το δυνατόν μικρότερα λειτουργικά και οικονομικά κόστη να επιβαρύνουν τον άνθρωπο. Στα κεφάλαια που προηγήθηκαν αναλύθηκαν βασικές προσεγγίσεις του IoT στο τομέα της τεχνολογίας και το συμπέρασμα που μπορεί να προκύψει είναι πως το «Διαδίκτυο των πραγμάτων», δεν είναι σενάριο επιστημονικής φαντασίας και παράλληλα η τεχνογνωσία και η μεθοδολογία για να γίνει πραγματικότητα, υπάρχει ήδη.

Οι τεχνολογίες του «Διαδικτύου των Πραγμάτων» θα εισχωρήσουν αρκετά εύκολα στην καθημερινότητα, και αναμένεται η εξοικείωση των ανθρώπων με αυτό το κομμάτι της τεχνολογίας. Σαν συνέπεια όλων των παραπάνω, η τεχνολογία του «Διαδικτύου των Πραγμάτων», δεν είναι μόνο ένα αντικείμενο το οποίο μπορεί να χαρακτηρίσει την βασική έννοια και τους σκοπούς λειτουργικότητας που προσφέρει αυτή η τεχνολογία. Το «Διαδίκτυο των Πραγμάτων» αποτελείται από ένα σύνολο ιδεών που σταδιακά θα καλύψει και θα δημιουργήσει ανάγκες, για μια καλύτερη ποιότητα ζωής. Πολλές τεχνολογίες, εταιρίες και διαφορετικές αντιλήψεις, στο τέλος θα ενοποιηθούν για να δημιουργήσουν την εικόνα του αύριο, που μελετάμε σήμερα, με το όνομα «Διαδίκτυο των Πραγμάτων».

Βιβλιογραφία

IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things (Copyright© 2017 Cisco Systems, Inc.)