ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΗΛΕΚΤΡΙΚΩΝ ΒΙΟΜΗΧΑΝΙΚΩΝ ΔΙΑΤΑΞΕΩΝ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΑΠΟΦΑΣΕΩΝ

Μελέτη Υποδομών Έξυπνων Σπιτιών και Εξερεύνηση Συσχέτισης Αυτών με τα Τελευταία Πρωτόκολλα και Πρότυπα του Σημασιολογικού Ιστού

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

ΛΟΪΖΟΥ ΧΡΙΣΤΟΥ

Επιβλέπων : Δημήτριος Ασκούνης
Αν.Καθηγητής Ε.Μ.Π.

Αθήνα, Ιούλιος 2016

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΗΛΕΚΤΡΙΚΩΝ ΒΙΟΜΗΧΑΝΙΚΩΝ ΔΙΑΤΑΞΕΩΝ ΚΑΙ
ΣΥΣΤΗΜΑΤΩΝ ΑΠΟΦΑΣΕΩΝ

Μελέτη Υποδομών Έξυπνων Σπιτιών και Εξερεύνηση Συσχέτισης Αυτών με τα Τελευταία Πρωτόκολλα και Πρότυπα του Σημασιολογικού Ιστού

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

ΛΟΪΖΟΥ ΧΡΙΣΤΟΥ

Επιβλέπων : Δημήτριος Ασκούνης
Αν. Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 13η Ιουλίου 2016.

(Υπογραφή)	*(Υπογραφή)*	*(Υπογραφή)*
.....	.....	.....
Ιωάννης Ψαρράς	Βασίλειος Ασημακόπουλος	Ιωάννης Ψαρράς
Αν.Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.

Αθήνα, Ιούλιος 2016

(Υπογραφή)

.....

ΛΟΪΖΟΣ ΧΡΙΣΤΟΥ

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

Περίληψη

Τα τελευταία χρόνια παρακολουθούμε την ανάπτυξη διαφόρων πρωτοκόλλων και συστημάτων αυτοματισμού από πολλές εταιρίες (ABB, Siemens, Schneider, ELKO) καθώς και διαφόρων έξυπνων συσκευών οι οποίες αποκαλούνται διαδίκτυο των πραγμάτων (IoT , Internet of Things) όπως έξυπνες τηλεοράσεις (Samsung, LG, SONY κτλ), λαμπτήρες (Philips Hue), ψυγεία, πλυντήρια κτλ. Ο στόχος όλων αυτών των προϊόντων και τεχνολογιών είναι διπλός. Από την μια να προσθέσουν περισσότερη άνεση στην καθημερινότητα μας και από την άλλη να πετύχουν εξοικονόμηση ενέργειας. Τα "έξυπνα" κτίρια βρίσκουν σιγά σιγά απήχηση καθώς συμβάλουν στην ορθολογική χρήση της ενέργειας και στην βελτίωση των συνθηκών άνεση και ασφάλειας του κτιρίου.

Στόχος της παρούσας διπλωματικής είναι να παρουσιάσει τα κύρια πρωτόκολλα (KNX, c-bus, Zigbee, zwave) που χρησιμοποιούνται στα συστήματα αυτοματισμού κτιρίων καθώς και την νέα τάση της τεχνολογίας που ονομάζεται διαδίκτυο των πραγμάτων. Επίσης προτείνει και υλοποιεί μια πλατφόρμα που συνδυάζει όλες αυτές τις τεχνολογίες σε ένα ενιαίο σύστημα μέσω του ανοιχτού λογισμικού openHAB. Χρησιμοποιώντας την πλατφόρμα αυτή ο χρήστης θα μπορέσει μέσω ενός φιλικού περιβάλλοντος να αξιοποιήσει όλες τις δυνατότητες που του προσφέρουν οι συσκευές του πετυχαίνοντας την επιθυμητή άνεση , ασφάλεια , προσβασιμότητα και αύξηση της ενεργειακής απόδοσης του κτιρίου του.

Λέξεις κλειδιά:
Διαδίκτυο των πραγμάτων, KNX, c-bus, Zigbee, zwave, Πρωτόκολλα αυτοματισμού κτιρίων, openHAB, Ruspberry Pi.

Abstract

In recent years we are witnessing the development of various protocols and automation systems from many companies (ABB, Siemens, Schneider, ELKO) as well as various smart devices which are called Internet of Things (IoT), such as smart TVs (Samsung, LG, SONY etc.), lamps (Philips Hue), refrigerators, washing machines etc. The objective of all these products and technologies is twofold. From one hand to add more comfort in everyday life and on the other hand to achieve energy savings. The "smart" buildings slowly find resonance as well as contributing to the rational use of energy and improving comfort and safety conditions of the building.

The objective of this diploma thesis is to present the main protocols (KNX, c-bus, Zigbee, zwave) that are used in building automation systems and the new trend of technology called Internet of Things. Also this diploma thesis proposes and implements a platform that combines all these technologies into a single system through the open source software openHAB. Using this platform, the user will be able through a user-friendly environment to exploit the full potential that his devices can offer achieving the desired comfort, safety, accessibility and increase the energy efficiency of the building.

Keywords :
Internet of Things (IoT), KNX, c-bus, Zigbee, zwave, building automation protocols, openHAB, Ruspberry Pi.

Πίνακας περιεχομένων

1

Εισαγωγή

1.1 Αντικείμενο - Σκοπός

Τα τελευταία χρόνια ζούμε την ανατολή μια νέας εποχής της εποχής του διαδικτύου των πραγμάτων (IoT , Internet of Things). Σε γενικές γραμμές αυτό ερμηνεύεται ως η διασύνδεση στο Διαδίκτυο συσκευών καθημερινής χρήσης με ενσωματωμένα ηλεκτρονικά, λογισμικό και αισθητήρες με σκοπό την ανταλλαγή δεδομένων και τον απομακρυσμένο έλεγχο τους.

Το IoT θα αυξήσει την πανταχού παρουσία του Διαδικτύου με την ενσωμάτωση κάθε αντικειμένου που δύναται να αλληλεπιδράσει σε ένα κατανεμημένο δίκτυο συσκευών, το οποίο θα επικοινωνεί με τους ανθρώπους καθώς και με άλλες συσκευές. Χάρη στην ταχεία πρόοδο τεχνολογιών που σχετίζονται με το IoT ανοίγονται τεράστιες ευκαιρίες για ένα μεγάλο αριθμό νέων εφαρμογών σε διάφορους τομείς που υπόσχονται να βελτιώσουν την ποιότητα ζωής μας και να ευκολύνουν την καθημερινότητα μας. Οι τομείς αυτοί περιλαμβάνουν :

- Αυτοματισμούς κτιρίων.
- Αυτοκίνηση.
- Ασφάλεια κτιρίων.

- Φροντίδα υγείας.
- Υποδομή βιομηχανικών εγκαταστάσεων.

και πολλά άλλα.

Μέσα σε αυτό το πλαίσιο έχουν αναπτυχθεί από διάφορες εταιρίες (Samsung, Philips, LG, NEST, Logitech κτλ) ¨έξυπνες¨ συσκευές για το σπίτι. Το πρόβλημα είναι ότι όλες αυτές οι συσκευές λειτουργούν αυτόνομα χωρίς να επικοινωνούν μεταξύ τους χρησιμοποιώντας τις περισσότερες φορές διαφορετικά πρωτόκολλα. Επίσης η κάθε μια από αυτές τις συσκευές χρειάζεται την δική της εφαρμογή για έλεγχο από τον εκάστοτε χρήστη. Όλα αυτά δημιουργούν ένα περιβάλλον καθόλου φιλικό προς τον χρήστη, ο οποίος παρόλο που έχει τεράστιες δυνατότητες στα χέρια του από κάθε συσκευή χωριστά, δεν μπορεί να τις συνδέσει μεταξύ τους και να εφαρμόσει ένα γενικό πλάνο διαχείρισης του σπιτιού του, που θα του αποφέρει την επιθυμητή άνεση σε καθημερινές λειτουργίες, την εξοικονόμηση ενέργειας και άλλα προτερήματα στα οποία προσδοκά από την απόκτηση αυτών των συσκευών.

Σκοπός λοιπόν αυτής της διπλωματικής είναι από την μια να παρουσιάσει αυτή την νέα τάση της τεχνολογίας που ονομάζεται διαδίκτυο των πραγμάτων (IoT) και από την άλλη να προτείνει και να υλοποιήσει μια πλατφόρμα που να αφομοιώνει τις ¨έξυπνές¨ συσκευές διαφορετικών κατασκευαστών και πρωτοκόλλων σε ένα ενιαίο σύστημα το οποίο θα δίνει πλήρη έλεγχο στο χρήστη μέσω της εφαρμογής ανοιχτού λογισμικού openHAB. Με τον τρόπο αυτό ο χρήστης θα μπορέσει μέσω ενός φιλικού περιβάλλοντος να αξιοποιήσει όλες τις δυνατότητες που του προσφέρουν οι συσκευές του πετυχαίνοντας την επιθυμητή άνεση , ασφάλεια , προσβασιμότητα και αύξηση της ενεργειακής απόδοσης του κτιρίου του.

1.2 Διαδίκτυο των πραγμάτων και ¨έξυπνα¨ κτίρια.

Η μετάβαση από το Διαδίκτυο των υπολογιστών στο Διαδίκτυο των πραγμάτων έχει κάνει δυνατή την κατασκευή έξυπνων σπιτιών και κτιρίων τα οποία είναι σχεδιασμένα να παρέχουν ένα αριθμό υπηρεσιών μέσω δικτυακά συνδεδεμένων συσκευών. Η πλατφόρμα του IoT περικλείει ένα αριθμό από πρωτόκολλα και τεχνολογίες που επιτρέπουν τη μετατροπή παραδοσιακών οικιακών συσκευών και συστημάτων σε έξυπνα συστήματα που μπορούν να αλληλεπιδράσουν με το περιβάλλον και να προσαρμόσουν τη λειτουργία τους στις ανάγκες του χρήστη.

Το υλισμικό του IoT επιτρέπει σε όλες τις συσκευές να αποκτήσουν την απαραίτητη διεύθυνση IP και να έχουν πρόσβαση στο εσωτερικό δίκτυο και το Διαδίκτυο. Οι αισθητήρες που ενσωματώνονται στις συσκευές, επιτρέπουν τη συλλογή δεδομένων και πληροφοριών από τον περιβάλλοντα χώρο. Τα δεδομένα αυτά συλλέγονται από ένα λογισμικό το οποίο θα τα επεξεργαστεί και θα επιβάλει τις ανάλογες ενέργειες μέσω των ενεργοποιητών.

Το λογισμικό του IoT, παρέχει στο χρήστη μία πλατφόρμα προσβάσιμη είτε από το εσωτερικό δίκτυο, είτε από το Διαδίκτυο, για να διαχειρίζεται όλες τις συνδεδεμένες συσκευές. Η πρόσβαση στις πλατφόρμες διαχείρισης είναι δυνατή μέσω διαφόρων συσκευών όπως υπολογιστή, tablet και smartphone δίνοντας στο χρήστη την απαραίτητη ευελιξία.

1.3 Πλεονεκτήματα ¨έξυπνων¨ σπιτιών.

Μερικά από τα πιο σημαντικά πλεονεκτήματα των έξυπνων κτιρίων εντοπίζονται στον τομέα της εξοικονόμησης ενέργειας. Τα έξυπνα συστήματα που εγκαθίστανται σε αυτά, αναγνωρίζουν τις αλλαγές που διαμορφώνονται στα κτίρια ανάλογα με την εποχή, τη χρήση και τα άτομα που τα χρησιμοποιούν και αναπροσαρμόζουν τις περιβαλλοντικές συνθήκες, των φωτισμό, τον εξαερισμό κ.τ.λ.. Τα συνηθισμένα κτίρια ψύχονταν ή θερμαίνονταν κατά τη διάρκεια της μέρας ανεξάρτητα από τη χρήση και το βαθμό πληρότητάς τους. Πλέον, μέσω των έξυπνων συστημάτων, ένα κτίριο μπορεί να διαχωριστεί σε ελεγχόμενες ζώνες και η διαχείριση του φωτισμού, θερμοκρασίας και εξαερισμού των ζωνών αυτών να ελέγχεται ανάλογα με τη χρήση τους.

Πιο συγκεκριμένα, τα κύρια πλεονεκτήματα της χρήσης έξυπνων συστημάτων για κατοικίες είναι τα πιο κάτω:

1. Φωτισμός: Τα φώτα σε ένα έξυπνο σπίτι μπορούν να ανάβουν ή να σβήνουν αυτόματα βασιζόμενα σε αισθητήρες. Για παράδειγμα, όταν ένα άτομο εισέρχεται σε ένα δωμάτιο κατά τη διάρκεια της μέρας, το σύστημα φωτισμού μπορεί να δίνει εντολή να ανοίγουν οι κουρτίνες, ενώ αν είναι βράδυ να ανάβουν τα φώτα. Μόλις το δωμάτιο αδειάσει, τα φώτα θα σβήνουν για εξοικονόμηση ενέργειας.
2. Κλιματισμός: Η κατάλληλη τοποθέτηση αισθητήρων θερμοκρασίας και η χρήση χρονομέτρων για τη λειτουργία κλιματιστικών και θέρμανσης μπορεί να συνεισφέρει σημαντικά στον τομέα της εξοικονόμησης ενέργειας.
3. Οικιακές συσκευές: τα έξυπνα κτίρια μπορούν να συνεισφέρουν στον τομέα της μείωσης του κόστους της ενέργειας σε μία οικία ελέγχοντας την κατανάλωση

των οικιακών συσκευών. Το σύστημα ελέγχου του σπιτιού, θα μπορούσε για παράδειγμα να προγραμματίζει τη λειτουργία συσκευών που καταναλώνουν μεγάλα ποσά ενέργειας, όπως για παράδειγμα πλυντήριο πιάτων και στεγνωτήριο, σε ώρες που η χρέωση του παρόχου ηλεκτρικής ενέργειας είναι πιο χαμηλή.

4. Ασφάλεια: Τα έξυπνα σπίτια περιλαμβάνουν επίσης εξελιγμένα συστήματα ασφαλείας με κάμερες, ανιχνευτές κίνησης και σύνδεση είτε με τον τοπικό αστυνομικό σταθμό είτε με ιδιωτική εταιρεία ασφαλείας. Γίνεται επίσης χρήση έξυπνων καρτών ή δακτυλικών αποτυπωμάτων για πρόσβαση στα σπίτια αντί για τις παραδοσιακές κλειδαριές, δυσκολεύοντας έτσι τη διάρρηξη τους.

5. Άνεση και ευκολία: Η παροχή διευκολύνσεων και ανέσεων είναι ένας από τους βασικούς λόγους που οι άνθρωποι επιλέγουν την εγκατάσταση και λειτουργία έξυπνων συστημάτων στις οικίες τους. Τα συστήματα, επιτρέπουν την απομακρυσμένη πρόσβαση και έλεγχο συστημάτων όπως θέρμανσης και ψύξης, μουσικής και πολυμέσων και φωτισμού σε όλο το σπίτι.

6. Προσβασιμότητα: ειδικά για τις κατηγορίες των ηλικιωμένων και ανάπηρων ιδιοκτητών, η εγκατάσταση ενός έξυπνου συστήματος μπορεί να προσφέρει διευκολύνσεις όπως ο φωνητικός έλεγχος του φωτισμού, των πορτών και της χρήσης του τηλεφώνου. Επίσης, τους δίνει το δικαίωμα του προγραμματισμού εργασιών οι οποίες θα ξεκινούν αυτόματα όπως για παράδειγμα το πότισμα του γρασιδιού.

Η χρήση συστημάτων αυτοματισμού και ελέγχου βοηθά στη δημιουργία ενός ασφαλούς και άνετου περιβάλλοντος διαβίωσης και εργασίας καθώς και στην εξοικονόμηση ενέργειας.

1.4 Εξοικονόμηση Ενέργειας.

Η εξοικονόμηση ενέργειας είναι ένα φλέγον ζήτημα που επηρεάζει τόσο τους καταναλωτές όσο και τα εργοστάσια παραγωγής ενέργειας και το παγκόσμιο περιβάλλον. Οι υψηλής κατανάλωσης ηλεκτρικές οικιακές συσκευές, τα συστήματα κλιματισμού και φωτισμού καθιστούν τις κατοικίες σαν μονάδες που επηρεάζουν σημαντικά το ύψος της κατανάλωσης ενέργειας σε μία χώρα. Η υιοθέτηση έξυπνων τεχνολογιών, βοηθά στην ελαχιστοποίηση της χαμένης ενέργειας και προσαρμόζει την κατανάλωση ενέργειας ανάλογα με τις συνήθειες των κατοίκων της οικίας χρησιμοποιώντας ένα αριθμό κατάλληλα τοποθετημένων αισθητήρων.

Ένα έξυπνο σπίτι στηρίζει τη λειτουργία του σε ένα εσωτερικό δίκτυο δεδομένων και έξυπνα συστήματα ελέγχου των διαφόρων λειτουργιών του. Το εσωτερικό δίκτυο λειτουργεί είτε με ασύρματη είτε με ενσύρματη τεχνολογία, βασισμένη σε ένα πρωτόκολλο IEEE 802.1 ή Ethernet αντίστοιχα και διασύνδεει αισθητήρες και ενεργοποιητές (actuators). Τα δεδομένα από τους αισθητήρες και τους ενεργοποιητές αποστέλλονται σε ένα κεντρικό σύστημα ελέγχου και παρακολούθησης το οποίο είναι προσβάσιμο μέσω του εσωτερικού δικτύου ή/και του Διαδικτύου.

Οι εξοικονομήσεις σε ενέργεια στα έξυπνα σπίτια έχουν αποτελέσει αντικείμενο πολλών μελετών. Σε μία από αυτές, η διαχείριση της κατανάλωσης ενέργειας υλοποιήθηκε μέσω αισθητήρων που τοποθετήθηκαν στα δωμάτια του σπιτιού και προσάρμοζαν τις λειτουργίες των διαφόρων συστημάτων ανάλογα με τις συνήθειες των ενοίκων. Οι αισθητήρες τοποθετήθηκαν σε καίρια σημεία ώστε να παρέχουν ακριβή πληροφορία για το που βρίσκονταν οι ένοικοι. Χρησιμοποιήθηκαν δύο είδη αισθητήρων: οι παθητικοί υπέρυθροι αισθητήρες PIR οι οποίοι έλεγχαν το φωτισμό ανιχνεύοντας τη θερμότητα που εξέπεμπαν οι ένοικοι καθώς μετακινούνταν στο χώρο. Οι υπόλοιποι αισθητήρες έπαιρναν μετρήσεις και για τη θερμοκρασία και έδιναν εντολές στο σύστημα κλιματισμού για προσαρμογή της στα επίπεδα που είχε προκαθορίσει ο χρήστης. Εφαρμόζοντας, τις δύο μόνο αυτές τεχνολογίες για έλεγχο του φωτισμού και του κλιματισμού, παρατηρήθηκαν εξοικονομήσεις σε ποσοστό μέχρι και 60% της ημερήσιας κατανάλωσης σε κιλοβατόρες, χωρίς αλλαγές στην ποιότητα ζωής και την άνεση των ενοίκων.

1.5 Οργάνωση κειμένου

Στο Κεφάλαιο 2 επεξηγείται η έννοια του IoT, αναλύοντας τα αρχιτεκτονικά στοιχεία που την αποτελούν, τις τεχνολογίες που χρησιμοποιεί αλλά και τις ελλείψεις και αδυναμίες που υπάρχουν στον τομέα της ασφάλειας και προστασίας Προσωπικών Δεδομένων που συλλέγονται μέσω των έξυπνων συσκευών του IoT. Το Κεφάλαιο 3 ασχολείται με μερικές από τις υπάρχουσες τεχνολογίες στον τομέα του Αυτοματισμού και της Ενεργειακής Διαχείρισης Κτιρίων. Περιγράφονται διάφορα πρωτόκολλα, προϊόντα και συσκευές που χρησιμοποιούνται για το σκοπό αυτό. Το Κεφάλαιο 4 ασχολείται με την τεχνολογία openHAB, την αρχιτεκτονική και τους κανόνες που τη διέπουν καθώς και τις υποστηριζόμενες πλατφόρμες και τεχνολογίες. Τέλος, στο Κεφάλαιο 5 παρουσιάζονται παραδείγματα υλοποίησης σεναρίων αυτοματοποίησης σπιτιού με χρήση openHAB, ενώ στο Κεφάλαιο 6 παρουσιάζονται τα γενικά συμπεράσματα της παρούσας μελέτης.

2

Διαδίκτυο των πραγμάτων

2.1 Εισαγωγή

Το Διαδίκτυο έκανε την εμφάνιση του ως Advanced Research Projects Agency Network (ARPANET) το 1969, συνδέοντας μεταξύ τους μερικά κτίρια, ενώ πλέον, αναμένεται ότι μέχρι το 2020 θα διασυνδέει 50 δισεκατομμύρια συσκευές. Σύμφωνα με την εταιρεία Cisco, έναν από τους μεγαλύτερους κατασκευαστές εξοπλισμού δικτύων παγκοσμίως, η πορεία εξέλιξης του Διαδικτύου μπορεί να χωριστεί σε 4 φάσεις.

Η πρώτη φάση, που ξεκίνησε πριν από 20 και πλέον χρόνια, αναφέρεται ως συνδεσιμότητα (Connectivity) και περιλαμβάνει την χρήση του ηλεκτρονικού ταχυδρομείου, την περιήγηση στο Διαδίκτυο και την εμφάνιση των μηχανών αναζήτησης περιεχομένου. Η δεύτερη φάση, ξεκίνησε στα τέλη της δεκαετίας του 90 και αναφέρεται ως Οικονομία του Διαδικτύου (Networked Economy). Τη δεκαετία αυτή κάνει την εμφάνιση του το ηλεκτρονικό εμπόριο που αλλάζει τον τρόπο που οι καταναλωτές αγοράζουν προϊόντα και ανοίγει καινούργιες αγορές για τις εταιρείες.

Στις αρχές της επόμενης δεκαετίας, 2000, κάνει την εμφάνιση της η επόμενη φάση που αναφέρεται ως φάση Συνεργασίας (Collaborative Experiences) και εισάγει τη χρήση των μέσων κοινωνικής δικτύωσης, του βίντεο, της τηλεδιάσκεψης και του cloud computing

αλλάζοντας εντελώς τον χώρο εργασίας. Η τελευταία και παρούσα φάση ονομάζεται Διαδίκτυο των Πάντων (Internet of Everything) και παρέχει την τεχνολογία για να συνδέσει μεταξύ τους, ανθρώπους, διαδικασίες, δεδομένα και πράγματα. Ένας ακόμα ορισμός της παρούσας φάσης είναι το Διαδίκτυο των Πραγμάτων (Internet of Things).

Η βασική διαφορά είναι ότι ενώ το IoT περιγράφει τη σύνδεση όλων των φυσικών αντικειμένων στο Διαδίκτυο, το IoE περιγράφει τη σύνδεση των αντικειμένων στο Διαδίκτυο, τις διαδικασίες αλληλεπίδρασής τους και την ανταλλαγή δεδομένων και πληροφοριών μεταξύ συσκευών και μεταξύ ανθρώπων και συσκευών. Όπως αναφέρει ο Luke Simmons, διευθυντής μάρκετινγκ στην εταιρεία CloudRail σε ένα από τα άρθρα του, μπορείς να παρομοιάσεις το IoT με μία σιδηροδρομική γραμμή, συμπεριλαμβανομένων των ράγων και των σταθμών, ενώ το IoE με όλα τα πιο πάνω συμπεριλαμβανομένων και των τρένων, των εκδοτηρίων εισιτηρίων, του προσωπικού, των πελατών, των καιρικών συνθηκών κ.τ.λ.

Ο όρος Internet of Things εμφανίζεται για πρώτη φορά σε μία ομιλία του Kevin Ashton, συνιδρυτή του MIT's Auto-ID Lab, το 1999. Σε συνέντευξή του στο RFID Journal, το 2009, ο Ashton δίνει τη δική του ερμηνεία του IoT. Σύμφωνα με τον ίδιο, σήμερα οι υπολογιστές και επομένως το Διαδίκτυο, συλλέγουν πληροφορίες και δεδομένα σχεδόν αποκλειστικά από τους ανθρώπους. Από το σύνολο των δεδομένων που υπάρχει στο Διαδίκτυο και κυμαίνεται στο ύψος των 50 petabytes, σχεδόν όλα έχουν δημιουργηθεί ή εισαχθεί από ανθρώπους, είτε μέσω πληκτρολόγησης, είτε μέσω ηχογράφησης, είτε μέσω φωτογράφησης ή σάρωσης κάποιου ραβδοκώδικα. Το πρόβλημα έγκειται στο ότι οι άνθρωποι έχουν περιορισμένο χρόνο, προσοχή και ακρίβεια, επομένως τα δεδομένα που συλλέγουν δεν είναι απόλυτα ακριβή. Αν υπήρχαν υπολογιστές που να συλλέγουν πληροφορίες, χωρίς την ανθρώπινη παρέμβαση, θα ήταν σε θέση να παρακολουθούν και να μετράνε τα πάντα, μειώνοντας έτσι σημαντικά την απώλεια και το κόστος.

Το IoT περιγράφει ένα κόσμο που οι υπολογιστές θα έχουν τα δικά τους μέσα συλλογής πληροφοριών, ώστε να μπορούν να ¨βλέπουν¨, ¨ακούνε¨ και ¨μυρίζουν¨ τον κόσμο χωρίς τη δική μας βοήθεια. Οι τεχνολογίες των αισθητήρων και του RFID επιτρέπουν στους υπολογιστές να παρατηρούν, να προσδιορίζουν και να κατανοούν τον κόσμο γύρω τους, χωρίς τα λάθη και τους περιορισμούς που εμπεριέχει η ανθρώπινη παρέμβαση.

Το 2015, σε μία έκθεση της Ομοσπονδιακής Επιτροπής Εμπορίου των ΗΠΑ (Federal Trade Commission), το IoT καθορίστηκε ως ένα διασυνδεδεμένο περιβάλλον όπου κάθε λογής

αντικείμενα έχουν μια ψηφιακή παρουσία και την ικανότητα να επικοινωνούν με άλλα αντικείμενα και ανθρώπους.

2.2 Αρχιτεκτονικά στοιχεία

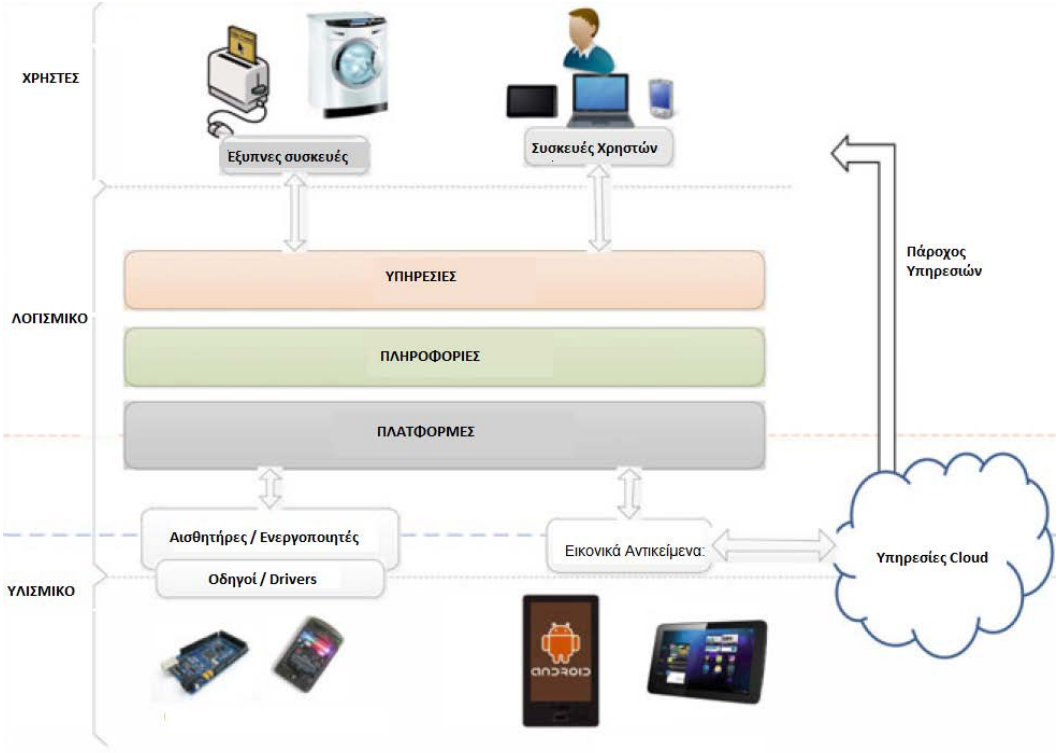
Η ορολογία "Internet of Things" περικλείει μία πληθώρα λύσεων και τεχνολογιών που περιγράφουν την επικοινωνία και αλληλεπίδραση έξυπνων αντικειμένων. Μεταξύ των διαφόρων προτεινόμενων λύσεων δεν υπάρχουν συνήθως δυνατότητες αλληλεπίδρασης καθώς η κάθε μία από αυτές εξελίχθηκε έχοντας ως στόχο την επίλυση ενός συγκεκριμένου προβλήματος και ακολουθώντας συγκεκριμένες απαιτήσεις. Επίσης, καθώς η ομπρέλα του IoT καλύπτει ένα μεγάλο εύρος πεδίων εφαρμογής, οι τεχνολογίες που αναπτύσσονται ποικίλουν και προκύπτουν απομονωνόμενες λύσεις.

Για να μπορέσει το IoT να ωριμάσει και να αποδώσει στο μέγιστο των δυνατοτήτων του, θα πρέπει να βρεθούν κοινές τεχνικές αρχές, πρωτόκολλα και αρχιτεκτονικές που θα διασυνδέσουν τις πιο πάνω λύσεις. Ένα παράδειγμα αυτής της ανάγκης βρίσκεται από την πρόσφατη ιστορία της τεχνολογίας και συγκεκριμένα στον τομέα των δικτύων επικοινωνιών. Οι απομονωμένες τεχνολογίες και λύσεις εγκαταλείφθηκαν και υιοθετήθηκε η σουίτα πρωτοκόλλων TCP/IP που περιγράφει τις γενικές αρχές λειτουργίας κάθε στρώματος του δικτύου. Με τον ίδιο τρόπο, ένα μοντέλο αναφοράς θα πρέπει να αναπτυχθεί για το IoT ώστε μέσω των αρχιτεκτονικών αναφοράς που θα περιγράφει, να επιτευχθεί η ανάπτυξη πιο πολλών και εστιασμένων λύσεων.

Οι περισσότεροι ορισμοί του IoT περιλαμβάνουν την έννοια φυσικών αντικειμένων ή συσκευών που μπορούν να "αισθανθούν" ή να επηρεάσουν το φυσικό περιβάλλον. Επίσης, περιλαμβάνουν εικονικά αντικείμενα όπως ηλεκτρονικές ατζέντες, βιβλία και πορτοφόλια. Το IoT περιλαμβάνει πάντα και την εμπλοκή των ανθρώπων, όπως για παράδειγμα στον τομέα του αυτοματισμού σπιτιών, οι άνθρωποι μπορούν να ελέγξουν το περιβάλλον μέσω μίας εφαρμογής. Μέσω των διαφόρων εφαρμογών και υπηρεσιών, συλλέγεται μεγάλος όγκος δεδομένων που τυχαίνουν επεξεργασίας και μετατρέπονται σε πολύτιμες πληροφορίες. Το IoT χρησιμοποιεί επίσης διάφορες πλατφόρμες, που λειτουργούν ως γέφυρες για να συνδέουν τα διάφορα επιμέρους στοιχεία του IoT (αντικείμενα-συσκευές, ανθρώπους, υπηρεσίες). Οι πλατφόρμες παρέχουν διάφορες λειτουργίες όπως η πρόσβαση στις συσκευές, τη διασφάλιση της σωστής εγκατάστασης και συμπεριφοράς της συσκευής, την ανάλυση δεδομένων και τη διασύνδεση των διάφορων συσκευών στο τοπικό δίκτυο, το cloud ή με άλλες συσκευές.

Τέλος, όλα τα στοιχεία του IoT συνδέονται μεταξύ τους μέσω ενός δικτύου που χρησιμοποιεί ασύρματες ή ενσύρματες τεχνολογίες, πρωτόκολλα και πρότυπα.

Στον σχεδιάγραμμα που ακολουθεί παρατίθενται όλα τα στοιχεία από τα οποία αποτελείται το IoT.



Σχήμα 2.2.1: Συστατικά στοιχεία IoT

Οι αισθητήρες αποτελούν ένα σύστημα συλλογής πληροφοριών από συσκευές. Μετατρέπουν πληροφορίες που συλλέγουν από το φυσικό περιβάλλον σε ηλεκτρικά σήματα τα οποία μπορούν να τύχουν στη συνέχεια επεξεργασίας από υπολογιστές. Μερικά παραδείγματα τέτοιων αισθητήρων είναι οι αισθητήρες υγρασίας, θερμοκρασίας αέρα, ραδιενέργειας και κίνησης. Οι αισθητήρες αυτοί παίζουν σημαντικό ρόλο στη σύνδεση συσκευών που παραδοσιακά δεν είχαν τέτοιες δυνατότητες στο IoT.

Ένα μεγάλο μέρος των αισθητήρων χρησιμοποιούν την τεχνολογία RFID (radio frequency identification). Η τεχνολογία αυτή χρησιμοποιεί τις ραδιοσυχνότητες των ηλεκτρομαγνητικών πεδίων για να ανταλλάζει πληροφορίες μεταξύ κωδικοποιημένων ετικετών (tag) και RFID αναγνωστών. Συνήθως οι ετικέτες RFID χρησιμοποιούνται για να ταυτοποιούν και να παρακολουθούν τα αντικείμενα στα οποία είναι ενσωματωμένες π.χ. βιβλία. Χάρη στο μικρό τους μέγεθος, μπορούν να τοποθετηθούν σε ένα μεγάλο αριθμό

αντικειμένων συμπεριλαμβανομένων ρούχων και μετρητών. Κάποια από αυτά έχουν τη δυνατότητα να λειτουργήσουν και χωρίς μπαταρίες. Η απαραίτητη ενέργεια για να μπορούν να μεταφέρουν την πληροφορία συλλέγεται μέσω του ηλεκτρομαγνητικού πεδίου που εκπέμπει ο αναγνώστης τους. Η ετικέτα λαμβάνει το σήμα από τον αναγνώστη και χρησιμοποιεί ένα μέρος της ενέργειάς του για να αποστείλει τις πληροφορίες που έχει μαζέψει. Η ακτίνα εκπομπής των ετικετών αυτών περιορίζεται σε μερικά μέτρα, ενώ ετικέτες με μπαταρίες φτάνουν σε ακτίνα μέχρι και μερικών εκατοντάδων μέτρων.

Σε αντίθεση με τους ραβδοκώδικες, η τεχνολογία RFID στηρίζεται σε ραδιοσυχνότητες και δεν απαιτεί οπτική επαφή μεταξύ πομπού και δέκτη. Λόγω της ευκαμψίας των ετικετών και των χαμηλών ενεργειακών τους απαιτήσεων, αποτελούν έναν εύκολο και βολικό τρόπο σύνδεσης συσκευών και αντικειμένων στο IoT.

Για παράδειγμα, είναι κοινή πρακτική, εργοστάσια κατασκευής οχημάτων να επικολλούν ετικέτες στο σκελετό των αυτοκινήτων που κατασκευάζουν. Με αυτό τον τρόπο, μπορούν να ανιχνεύουν σε πιο σημείο της γραμμής παραγωγής βρίσκεται το κάθε αυτοκίνητο. Η πρώτη γενιά ετικετών επέτρεπαν την εγγραφή δεδομένων μία φορά και την μετάδοση τους πολλές φορές - “write once read many”. Αυτό σημαίνει ότι μπορούν να προγραμματιστούν στο εργοστάσιο μία φορά αλλά δεν μπορούν να τροποποιηθούν στο χώρο εγκατάστασης τους. Οι καινούργιες ετικέτες έχουν κυκλώματα με κύκλο ζωής 40 έως 50 χρόνια και μπορούν να αλλάξουν τα δεδομένα εγγραφής τους πάνω από 100,000 φορές. Αυτές οι ετικέτες, μπορούν να αποθηκεύσουν με ευκολία όλο το ιστορικό του αντικειμένου στο οποίο είναι εγκατεστημένες όπως την ημερομηνία κατασκευής, το ιστορικό των τοποθεσιών στις οποίες βρέθηκε το αντικείμενο, πότε υπέστη τροποποιήσεις ή επιδιορθώσεις και τον εκάστοτε ιδιοκτήτη του.

Οι αισθητήρες μπορούν να προγραμματιστούν για να παίρνουν διάφορες μετρήσεις, να μεταφράζουν τα δεδομένα που συλλέγουν σε σήματα και να στέλνουν τα σήματα αυτά σε μια κεντρική ομάδα ελέγχου. Η μονάδα αυτή είναι υπεύθυνη να συλλέγει τα δεδομένα και να παρέχει πρόσβαση στο Διαδίκτυο. Μπορεί επίσης να λαμβάνει άμεσες αποφάσεις με βάση τα δεδομένα που λαμβάνει ή να τα προωθεί για ανάλυση σε άλλους υπολογιστές. Αυτοί οι υπολογιστές μπορεί να είναι εγκατεστημένοι είτε στο ίδιο τοπικό δίκτυο LAN είτε να είναι προσβάσιμοι μέσω Διαδικτύου.

Μία ακόμα τεχνολογία αισθητήρων που χρησιμοποιείται τα τελευταία χρόνια είναι η NFC (Near-Field Communications). Η NFC αποτελεί έναν τρόπο μεταφοράς περιορισμένου όγκου δεδομένων, μεταξύ συσκευών, σε μικρή ακτίνα και με χαμηλή κατανάλωση ενέργειας. Η τεχνολογία αυτή μπορεί να ενεργοποιηθεί σε ένα μεγάλο ποσοστό κινητών τηλεφώνων και συνήθως χρησιμοποιείται για υπηρεσίες πληρωμών μέσω κινητού όπως για παράδειγμα το Google Wallet.

Μια άλλη συσκευή που χρησιμοποιείται για την υλοποίηση του IoT είναι ο ενεργοποιητής (actuator). Ο ενεργοποιητής είναι ένας κινητήρας/μοτέρ που χρησιμοποιείται για να μετακινήσει ή να ελέγξει έναν άλλο μηχανισμό ή σύστημα, βασιζόμενος σε συγκεκριμένες οδηγίες. Υπάρχουν τρεις τύποι ενεργοποιητών στο IoT:

- Υδραυλικός – Χρησιμοποιεί την πίεση υγρών για να εκτελέσει μηχανική κίνηση.
- Pneumatic - Χρησιμοποιεί αέρα σε υψηλή πίεση για να επιτρέψει τη μηχανική λειτουργία
- Ηλεκτρικός – Τροφοδοτείται από ένα μοτέρ και μετατρέπει την ηλεκτρική ενέργεια σε μηχανική λειτουργία.

Ανεξάρτητα από το είδος του ενεργοποιητή που θα χρησιμοποιηθεί, η βασική του λειτουργία είναι να λαμβάνει ένα σήμα με οδηγίες και βάση αυτών των οδηγιών να εκτελεί κάποιες εργασίες. Συνήθως δεν είναι ικανοί να επεξεργαστούν δεδομένα. Οι ενέργειες που εκτελεί ένας ενεργοποιητής βασίζονται στο σήμα που λαμβάνει. Υπεύθυνος για την αποστολή του σήματος, είναι κατά κανόνα η κεντρική ομάδα ελέγχου.

Στο IoT θα είναι δυνατή η απευθείας επικοινωνία μεταξύ συστημάτων και συσκευών. Τα ακρωνύμια M2M (machine to machine) αναφέρονται σε αυτού του είδους επικοινωνία, όπως για παράδειγμα ένα έξυπνο ρολόι και μια εφαρμογή κινητού τηλεφώνου που διαβάζει δεδομένα από αυτό. Όταν δύο συσκευές επικοινωνούν μεταξύ τους, συλλέγουν δεδομένα μέσω ενός αισθητήρα και τα μεταδίδουν στη συνέχεια μέσω του ενσύρματου ή ασύρματου δικτύου. Πρωτόκολλα που αφορούν την κινητή τηλεφωνία και την μεταφορά δεδομένων όπως LTE, 4G, GSM και CDMA μπορούν επίσης να χρησιμοποιηθούν. Συστήματα που ανταλλάζουν μεγάλο όγκο δεδομένων επικοινωνούν μεταξύ τους με ενσύρματες τεχνολογίες όπως το Ethernet και οι οπτικές ίνες. Ο πιο εύχρηστος τρόπος επικοινωνίας παραμένει η ασύρματη σύνδεση μέσω ασύρματων καρτών που ενσωματώνονται στις συσκευές και χρησιμοποιούν πρωτόκολλα όπως το Wi-Fi, το Bluetooth, το ZigBee, το Z-Wave, το NFC και το RFID που αναφέρθηκε πιο πάνω. Οι πάροχοι υπηρεσιών κινητής τηλεφωνίας και mobile

date παρατηρούν αυξημένοι χρήση των τεχνολογιών αυτών με τη Verizon να δηλώνει αύξηση των κερδών της στον τομέα των τεχνολογιών που υποστηρίζουν το IoT κατά 45% και αύξηση στην ενεργοποίηση της υπηρεσίας 4GLTE κατά 135%.

Τέλος, σημαντικό ρόλο στην υιοθέτηση του IoT θα παίξει και η χρήση του πρωτοκόλλου IPv6. Σε αντίθεση με το IPv4 το IPv6 έχει θεωρητικά ανεξάντλητες διευθύνσεις IP που αρκούν για να συνδεθεί οποιαδήποτε συσκευή και υπηρεσία στο Διαδίκτυο. Πειράματα έχουν αποδείξει την επιτυχή χρήση των διευθύνσεων IPv6 σε μεγάλη κλίμακα αναπτύξεις όπως για αισθητήρες σε έξυπνα κτίρια ή έξυπνες πόλεις, ακόμα και με τα βοοειδή.

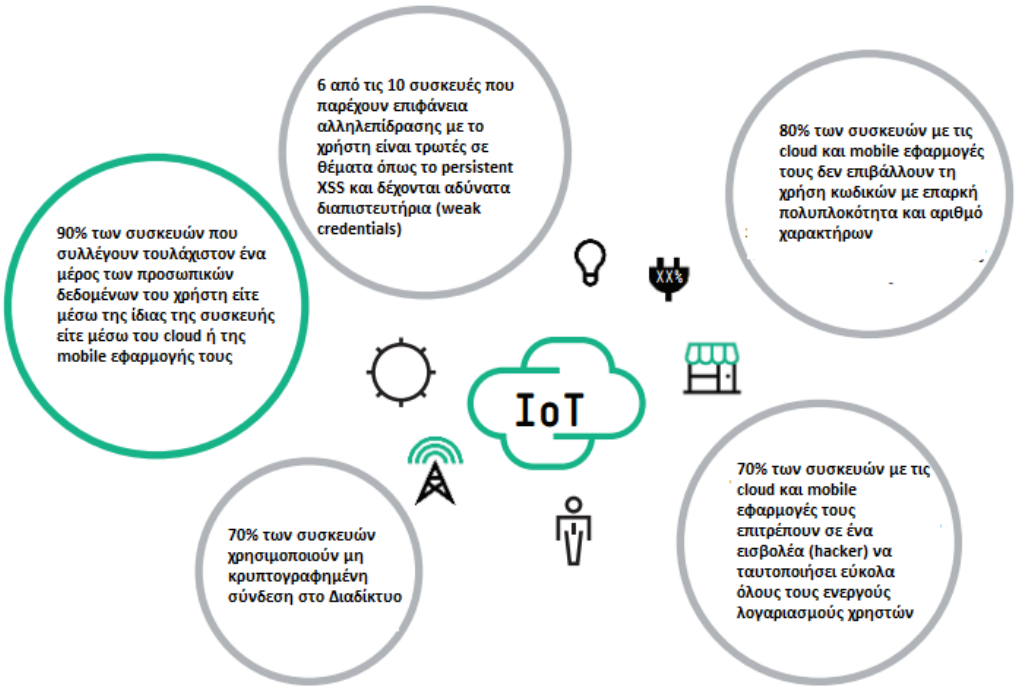
2.3 Ασφάλεια και Προστασία Προσωπικών Δεδομένων

Οι ανησυχίες για την προστασία της ιδιωτικής ζωής και της ασφάλειας, που σχετίζονται με τις νέες τεχνολογίες, αυξάνονται με απαράμιλλο ρυθμό. Όλο και περισσότερες συσκευές και αντικείμενα καθημερινής χρήσης έχουν ενσωματωμένους αισθητήρες για τη συλλογή δεδομένων σχετικά με το περιβάλλον γύρω τους και τα άτομα που τα χρησιμοποιούν. Ενώ το IoT υπόσχεται πως μέσω αυτών των δεδομένων θα ενισχύσει την άνεση και την αποτελεσματικότητα στις διάφορες καθημερινές λειτουργίες, εντούτοις, η συλλογή τους εμπεριέχει σημαντικές επιπτώσεις στην ιδιωτική ζωή και την προστασία της. Ούτε στην Ευρώπη αλλά ούτε και στις ΗΠΑ δεν υπάρχει ακόμα καθορισμένο νομικό πλαίσιο που να επιβάλλει την προστασία του τεράστιου όγκου προσωπικών δεδομένων που συλλέγονται μέσω των διαφόρων συσκευών, ούτε να αναγκάζει τους κατασκευαστές των συσκευών αυτών να υιοθετούν ικανοποιητικά πρωτόκολλα ασφαλείας. Εναπόκειται στη διακριτική ευχέρεια του κάθε κατασκευαστή κατά πόσον θα λάβει οποιεσδήποτε ενέργειες προς αυτή την κατεύθυνση.

Οι κατασκευαστές των “παραδοσιακών” οικιακών συσκευών, που τώρα μεταμορφώνονται σε “έξυπνες” συσκευές, δεν έχουν ιδιαίτερη πείρα στον τομέα της ασφάλειας καθώς ποτέ παλαιότερα δε συνέλεγαν δεδομένα. Η χρήση όμως συσκευών ικανών να συλλέγουν, να αποθηκεύουν και να μεταδίδουν προσωπικά δεδομένα, αυξάνει τον αριθμό των σεναρίων που μπορεί να εξελιχθούν εις βάρος του χρήστη. Σε άρθρο που δημοσιεύτηκε το Δεκέμβριο του 2014 στην ιστοσελίδα Slate με τίτλο “Σχεδόν οποιαδήποτε έξυπνη οικιακή συσκευή που μπορείς να σκεφτείς έχει παραβιαστεί η ασφάλειά της” ("Pretty Much Every Smart Home Device You Can Think of Has Been Hacked"), παρατίθεται μία λίστα με τις συσκευές των

οποίων η ασφάλεια έχει παραβιαστεί και περιλαμβάνει συσκευές όπως εκτυπωτές, λαμπτήρες, ηλεκτρονικά τσιγάρα, θερμοστάτες και κάμερες.

Επίσης, η ομάδα ασφαλείας της εταιρείας HP, ανακοίνωσε τα ευρήματα μίας μελέτης το Νοέμβριο του 2015, που καταδεικνύουν ότι το 60% των πιο κοινών συσκευών που χρησιμοποιεί το IoT εμπεριέχουν σοβαρούς κινδύνους ασφαλείας. Η HP εξέτασε επίσης τις 10 πιο ευρέως διαδεδομένες συσκευές του IoT και βρήκε ένα μεγάλο αριθμό τρωτών σημείων ανά συσκευή. Σε αυτά περιλαμβάνονται ζητήματα προστασίας της ιδιωτικής ζωής , η έλλειψη κρυπτογράφησης κατά τη μεταφορά δεδομένων, η μη ασφαλής σύνδεση στο Διαδίκτυο και η ανεπαρκής προστασία του λογισμικού των συσκευών. Στο σχεδιάγραμμα που ακολουθεί, απεικονίζονται περιληπτικά τα ευρήματα της έρευνας.



Σχήμα 2.3.1: Κίνδυνοι στην ασφάλεια των συσκευών IoT

Πολλές από τις συσκευές συλλέγουν προσωπικά δεδομένα, όπως όνομα, διεύθυνση, ημερομηνία γέννησης, πληροφορίες για την υγεία, ακόμα και αριθμούς πιστωτικών καρτών των χρηστών. Οι ανησυχίες για την ασφάλεια εντείνονται καθώς πολλές συσκευές έχουν cloud ή mobile εφαρμογές για τον έλεγχό τους και η πλειοψηφία από αυτές μεταδίδουν την πληροφορία μη κρυπτογραφημένο στο τοπικό δίκτυο των χρηστών. Καθώς οι χρήστες διαχειρίζονται τα δικά τους οικιακά τοπικά δίκτυα, εύκολα μπορεί να παραλείψουν την περιφρούρηση του δικτύου και τα δεδομένα αυτά να εκτεθούν σε μη εξουσιοδοτημένους χρήστες μέσω του ασύρματου τους δικτύου.

Οι χάκερς επίσης, μπορούν να εκμεταλλευτούν αδύναμους κωδικούς και μη ασφαλείς μεθόδους επανάκτησης κωδικού για να αποκτήσουν πρόσβαση στις διάφορες συσκευές. Οι κατασκευαστές, δεν αναγκάζουν τους χρήστες να χρησιμοποιούν περίπλοκους κωδικούς και επιτρέπουν τόσο στις cloud όσο και στις mobile εφαρμογές κωδικούς του τύπου "1234" ή "password". Επιπρόσθετα, οι περισσότερες συσκευές, μεταδίδουν δεδομένα χωρίς κρυπτογράφηση τόσο στο Διαδίκτυο όσο και στο τοπικό δίκτυο. Η κρυπτογράφηση στη μεταφορά δεδομένων είναι ακόμα πιο αναγκαία όταν τα δεδομένα μεταφέρονται στο cloud.

Όπως φαίνεται και στο σχεδιάγραμμα, έξι από τις δέκα συσκευές που εξετάστηκαν παρουσιάζουν αδυναμίες ασφαλείας και στη διεπαφή Διαδικτύου που χρησιμοποιείται από τους χρήστες (web interface). Σε αυτές περιλαμβάνονται η κακή διαχείριση των session του χρήστη και η χρήση αδύναμων προεπιλεγμένων διαπιστευτηρίων (default credentials). Η πλειοψηφία των συσκευών που εξετάστηκαν και οι cloud και mobile εφαρμογές τους επιτρέπουν σε ένα χάκερ να ανακαλύψει έγκυρους λογαριασμούς χρηστών μέσω μηχανισμών για επανέκδοση κωδικού. Ακόμα, το λογισμικό και το firmware του 60% των συσκευών που εξετάστηκαν εμφανίζουν προβλήματα ασφαλείας καθώς δεν χρησιμοποιούν κρυπτογράφηση όταν "κατεβάζουν" τις αναβαθμίσεις τους και τα αρχεία της αναβάθμισης δεν προστατεύονται με κανένα τρόπο. Σε ένα πείραμα που έγινε, ήταν δυνατή η υποκλοπή του αρχείου αναβάθμισης κατά τη διάρκεια της λήψης, η μετατροπή του και η εισαγωγή κακόβουλου κώδικα που επέτρεπε την υποκλοπή δεδομένων.

Ο Sanjay Sarma, ένας από τους ιδρυτές του MIT Auto-ID Center, εξηγεί ότι η υποδομή του IoT εμπεριέχει ρίσκα ασφαλείας καθώς είναι δύσκολο να αναβαθμιστεί ή να βελτιωθεί η λειτουργία της. Όπως αναφέρθηκε και πιο πάνω πολλές συσκευές δεν υποστηρίζουν κρυπτογράφηση επειδή δεν έχουν την αναγκαία υπολογιστική δύναμη και ισχύ στις μπαταρίες τους. Οι προγραμματιστές που σχεδιάζουν IoT συσκευές που στοχεύουν εκατομμύρια καταναλωτές, έχουν σημαντικούς περιορισμούς ως προς το κόστος τους και τον αναγκαίο χρόνο κατασκευής τους. Κάθε επιπρόσθετο bit μνήμης ή χώρου αποθήκευσης flash, κάθε προσθήκη υπολογιστικής ισχύς ή λογισμικού προστασίας μεταφράζεται σε κόστος. Σε μία αγορά όπου ο χρόνος και το κόστος είναι κρίσιμα, οι προγραμματιστές δεν βάζουν ως προτεραιότητα την ασφάλεια.

Έχουν ήδη αναφερθεί δεκάδες παραβιάσεις ασφαλείας της τεχνολογίας RFID που χρησιμοποιείται ευρέως από το IoT. Τα ηλεκτρονικά της RFID τεχνολογίας μπορούν να γίνουν hacked, να πλαστογραφηθούν και να μπλοκαριστούν (spoofed and jammed). Η πλειοψηφία των RFID ετικετών (tags) δεν περιλαμβάνει αποτελεσματικά μέτρα ασφαλείας.

Οι ελλείψεις αυτές επέτρεψαν στο hacker Francis Brown να αναπτύξει τους δικούς του αναγνώστες RFID (readers), με κόστος κάτω από $400 που μπορούν να σκανάρουν, να αντιγράψουν και να υποκλέψουν δεδομένα από αντικείμενα που χρησιμοποιούν την τεχνολογία RFID όπως οι ταυτότητες ασφαλείας (security IDs), οι πιστωτικές κάρτες εγγύτητας και οι κάρτες-κλειδιά των ξενοδοχείων. Οι συνέπειες της κατασκευής αυτού του αναγνώστη για τη φυσική και τεχνολογική ασφάλεια είναι τεράστιες. Η τεχνολογία NFC έχει δεχθεί επίσης επιθέσεις με εφαρμογές που κατάφεραν σε αρκετές περιπτώσεις να αντιγράψουν στοιχεία πιστωτικών καρτών σε πραγματικό χρόνο και να τα χρησιμοποιήσουν αργότερα για αγορές. Με τα διάφορα IoT συστήματα να συνδέονται και να ανταλλάζουν πληροφορίες, η παραβίαση της ασφάλειας μίας τουλάχιστον συσκευής θα δώσει στο hacker τη δυνατότητα να αποκτήσει πρόσβαση σε κάθε λογής προσωπικά δεδομένα που βρίσκονται αποθηκευμένα σε οποιαδήποτε συνδεδεμένη συσκευή.

Οι αδυναμίες που εμφανίζουν οι συσκευές του IoT, δεν περιορίζονται μόνο στον τομέα της προστασίας των προσωπικών δεδομένων αλλά και της φυσικής ασφάλειας. Μελετητές έχουν αποδείξει ότι η λειτουργία τόσο των αντλιών ινσουλίνης όσο και των βηματοδοτών μπορεί να επηρεαστεί από μη εξουσιοδοτημένους χρήστες. Το 2014, ο Kim Zetter, δημοσιογράφος στο Wired, κατέγραψε τα αποτελέσματα μελέτης που έγινε από τον Scott Erven, επικεφαλή του τομέα ασφαλείας στην εταιρεία Essentia Health, που λειτουργεί σε περισσότερους από 100 χώρους παροχής υπηρεσιών υγείας. Η μελέτη καταδείκνυε ότι οι συσκευές χορήγησης φαρμάκων (για χορήγηση μορφίνης, χημειοθεραπείας και αντιβιοτικών) μπορούσαν να ελεγχτούν εξ αποστάσεως και να αλλαχθεί η δοσολογία που έπρεπε να χορηγηθεί στους ασθενείς. Ακόμα, οι απινιδωτές με Bluetooth τεχνολογία θα μπορούσαν να δεχθούν παρεμβάσεις που να επηρεάσουν τη λειτουργία τους. Τέλος, τα ψηφιακά ιατρικά αρχεία του ασθενή θα μπορούσαν να αλλαχθούν και να οδηγήσουν τους γιατρούς σε λάθος διάγνωση και θεραπεία. Όπως αναφέρει ο Erven, πολλοί οργανισμοί ιατρικής περίθαλψης δεν εξετάζουν επαρκώς την ασφάλεια των συσκευών που χρησιμοποιούν και πολλά νοσοκομεία δεν γνωρίζουν το υψηλό ρίσκο που συνδέεται με τη χρήση έξυπνων συσκευών.

Μία ακόμα επιπλοκή του IoT αποτελεί το γεγονός ότι δεν οριοθετείται ξεκάθαρα ο τρόπος χρήσης των δεδομένων που συλλέγονται από τους χρήστες. Παρόλο που οι εταιρείες υπόσχονται ότι θα αποθηκεύουν τα δεδομένα που χρειάζονται και μόνο για όσο καιρό είναι απαραίτητα, εντούτοις η πολιτική αυτή ακολουθείται στην πράξη μόνο από τη μειοψηφία των εταιρειών. Στην πραγματικότητα, τα δεδομένα που συλλέγονται πωλούνται συχνά σε διαφημιστικές ή μάρκετινγκ εταιρείες. Έχει προβλεφθεί ότι, τα δεδομένα που συλλέγονται μέσω των έξυπνων συσκευών θα είναι σύντομα προσβάσιμα σε εργοδότες ώστε να μπορούν

να εξάγουν συμπεράσματα για την καταλληλότητα των υποψηφίων σε θέσεις εργασίας, τράπεζες για να διαπιστώνεται η πιστοληπτική ικανότητα των πελατών τους και ασφαλιστικές εταιρείες για να ενημερώνονται για την κατάσταση της υγείας των ασφαλιζόμενων. Νομικοί μελετητές έχουν προβλέψει ότι τέτοια δεδομένα θα μπορούν να χρησιμοποιηθούν στο εγγύς μέλλον σε μία δικαστική μάχη για διαζύγιο ως απόδειξη μιας εξωσυζυγικής σχέση.

Τέλος, τα δεδομένα που συλλέγονται ως επί τω πλείστο αποθηκεύονται στο cloud. Προβλέπεται ότι μέχρι το 2020 ποσοστό μεγαλύτερο του 90% των δεδομένων του IoT θα αποθηκεύεται εκεί. Αυτό πολλαπλασιάζει τους κινδύνους για την ασφάλεια και προστασία της ιδιωτικής ζωής καθώς οι διακομιστές που περιέχουν μεγάλο όγκο προσωπικών δεδομένων είναι πιο ελκυστικοί στόχοι για κακόβουλους χάκερς παρά οι μεμονωμένες συσκευές επομένως θα δέχονται πιο πολλές επιθέσεις.

Σύμφωνα με την Ευρωπαϊκή Επιτροπή, οι κρατικοί και ευρωπαϊκοί φορείς χάραξης πολιτικής θα πρέπει να εμπλακούν στην ανάπτυξη του πλαισίου λειτουργίας του IoT σε συνεργασία με τον ιδιωτικό τομέα. Μερικές από τις προκλήσεις που εμφανίζονται σχετίζονται με πολιτικές που θα υιοθετηθούν, συζητήθηκαν στην Παγκόσμια Σύσκεψη Κορυφής για την Κοινωνία της Πληροφορίας (World Summit on the Information Society), κατά την οποία ενθαρρύνθηκε όπως η διακυβέρνηση του IoT να σχεδιαστεί και να ασκείται κατά τρόπο συνεκτικό με όλες τις πολιτικές που βρίσκονται ήδη σε εφαρμογή και σχετίζονται με τη διακυβέρνηση του Διαδικτύου. Μερικά από τα ερωτήματα που προκύπτουν σε σχέση με τη σύνδεση συσκευών/αντικειμένων στο IoT είναι:

- Πως θα ονομάζονται οι συσκευές ώστε να υπάρχει μια γενική αντίληψη σχετικά με το είδος και τις λειτουργίες του κάθε αντικειμένου. (Naming scheme convention)
- Ποια αρχή θα είναι υπεύθυνη για να χορηγεί αναγνωριστικά για κάθε συσκευή.
- Με ποιο τρόπο θα μπορούν να αναζητηθούν πληροφορίες για την κάθε συσκευή.
- Πως οι πληροφορίες που συλλέγονται ή αποθηκεύονται σε κάθε συσκευή καθίστανται ασφαλής.
- Ποιο είναι το ηθικό και νομικό πλαίσιο λειτουργίας του IoT.
- Ποιοι είναι οι διαθέσιμοι μηχανισμοί ελέγχου.

Αναγνωρίζοντας τις πιο πάνω προκλήσεις η Ε.Ε. πρότεινε την δημιουργία μίας ομάδας που θα καθορίζει την διακυβέρνηση του IoT και δε θα επιτρέπει την κατάργηση της ιδιωτικότητας ή της προστασίας των προσωπικών δεδομένων. Επίσης, η Ε.Ε. προτίθεται να

ξεκινήσει ένα διάλογο σχετικά με την ελευθερία και το δικαίωμα των ατόμων να αποσυνδέονται από το δίκτυο όποια στιγμή το επιθυμούν.

Η Ευρωπαϊκή Επιτροπή πραγματοποίησε το έτος 2012 μία δημόσια διαβούλευση με θέμα το Internet of Things, στην οποία έλαβαν μέρος 600 άτομα, Σύνδεσμοι, διάφορες ομάδες ακαδημαϊκών και πολιτών αλλά και φορείς της βιομηχανίας. Παράλληλα διεξήχθη μία μελέτη από ομάδα ειδικών. Ο συνδυασμός των δύο, θα χρησιμοποιηθεί για να καθοριστεί η μελλοντική πολιτική για το IoT.

Στόχος είναι η πολιτική που θα αναπτυχθεί να παρέχει αποτελεσματική προστασία των προσωπικών δεδομένων και της ασφάλειας των πληροφοριών (διαθεσιμότητα, εχεμύθεια, ακεραιότητα) η οποία θα επιτυγχάνεται μέσω της εφαρμογή των αρχών του Ευρωπαϊκού δικαίου. Ακόμα ένα ενδιαφέρον συμπέρασμα της διαβούλευσης είναι η ανάγκη για μια καθολική προσέγγιση στο θέμα της προστασίας δεδομένων. Το IoT δεν έχει γεωγραφικά πλαίσια αλλά είναι εκ φύσεων μία τεχνολογία που επεκτείνεται παγκοσμίως. Θα πρέπει οι νομοθεσίες όλων των χωρών να εναρμονιστούν ώστε να υπάρχει η ίδια αντιμετώπιση στα θέματα που αφορούν την προστασία δεδομένων. Επίσης, το IoT θα πρέπει να σχεδιαστεί ώστε εξ αρχής να παρέχει στους χρήστες το δικαίωμα να διαγράφουν τα δεδομένα τους και το ιστορικό τους και να θέτει κανόνες σχετικά με τη φορητότητα των δεδομένων (data portability) και την ασφάλεια και την προστασία δεδομένων.

Τέλος, δύο γενικές αρχές πρέπει να ληφθούν υπόψη κατά τον καθορισμό της πολιτικής:

- Το IoT δεν θα πρέπει να παραβιάζει την ταυτότητα του κάθε ανθρώπου, την ακεραιότητά του, τα ανθρώπινα δικαιώματα, την ιδιωτική ζωή και τις δημόσιες ή ιδιωτικές ελευθερίες.
- Το κάθε άτομο θα μπορεί να ελέγχει τα προσωπικά δεδομένα που παράγονται ή επεξεργάζονται από τις τεχνολογίες του IoT εκτός κι αν αυτό έρχεται σε αντίθεση με την πρώτη αρχή.

2.4 Μελέτες και Εφαρμογές.

Τα τελευταία χρόνια έχει αναπτυχθεί πληθώρα IoT υπηρεσιών και εφαρμογών που εξυπηρετούν όχι μόνο τις ανάγκες τις βιομηχανίας και των μεγάλων εργοστασίων παραγωγής προϊόντων αλλά και τις καθημερινές ανάγκες, ανησυχίες και ασχολίες του μέσου ανθρώπου. Μερικά παραδείγματα περιγράφονται πιο κάτω.

Η εταιρεία Hilton, έχει δημιουργήσει μία εφαρμογή με το 'HHhonors', μέσω της οποίας διευκολύνεται η διαμονή του χρήστη. Μερικά χαρακτηριστικά της σπουδαίας αυτής IoT εφαρμογής είναι ότι ο πελάτης θα μπορεί μέσω κινητού τηλεφώνου να αποκτήσει πρόσβαση στο δωμάτιο του, το γυμναστήριο, την πισίνα και άλλους χώρους του ξενοδοχείου, να ζητήσει υπηρεσίες καθαρισμού για το δωμάτιο του ή να κάνει κράτηση για μια θέση στάθμευσης.

Άλλη μία εφαρμογή του IoT εντοπίζεται στον τομέα της ασφάλειας και αυτοματοποίησης κατοικίας. Οι εταιρείες AT&T και Cisco έχουν κατασκευάσει μία σειρά προϊόντων που προσφέρουν υπηρεσίες ασφαλείας και αυτοματισμών και ονομάζεται Digital Life. Το Digital Life προσφέρει 24 προστασία οικίας, μέσω τον εξειδικευμένων κέντρων της AT&T, μέσω των οποίων, σε περίπτωση κινδύνου ειδοποιείται η πυροσβεστική, την αστυνομία ή ασθενοφόρο. Το σύστημα συνδέεται με το ασύρματο δίκτυο ή με δίκτυο 3G και οι χρήστες του μπορούν να το διαχειριστούν μέσω του κινητού τους τηλεφώνου ή υπολογιστή. Η πρόσβαση στο Digital Life γίνεται μέσω ενός φυλλομετρητή ενώ υπάρχουν διαθέσιμες εφαρμογές για λειτουργικά κινητών τηλεφώνων iOS, Android και Windows.

Η Cisco παρέχει την πλατφόρμα ελέγχου των υπηρεσιών του Digital Life. Η πλατφόρμα χρησιμοποιεί διάφορες τεχνολογίες για να ελέγχει και να διαχειρίζεται οικιακές συσκευές, φώτα και συστήματα ψύξης/θέρμανσης αλλά και για να κλειδώνει και να ξεκλειδώνει πόρτες και να ανιχνεύει διαρροές νερού. Επίσης, με την τεχνολογία GSM/HSPA συνδέει το οικιακό Digital Life με το δίκτυο της AT&T. Ακόμα, η πλατφόρμα περιλαμβάνει το λογισμικό Home Plug AV για να επικοινωνεί με συσκευές που συνδέονται στο IP δίκτυο μέσω του οικιακού δικτύου παροχής ρεύματος, για 24ωρο έλεγχο και διαγνωστικά τεστ. .

Μια εταιρεία που εισήγαγε τεχνολογίες IoT για τη διαφήμιση και προώθηση των προϊόντων της είναι η Johnnie Walker. Τον Μάρτιο του 2015, η εταιρεία Diageo ανακοίνωσε ότι σε συνεργασία με την εταιρεία Thinfilm Electronics θα εισάγει το "έξυπνο μπουκάλι" για το ουίσκι της με την μπλε ετικέτα (blue label). Το έξυπνο μπουκάλι, θα έχει ενσωματωμένο ένα αισθητήρα, που θα φέρει την υπογραφή της Thinfilm's OpenSense technology. Ο αισθητήρας θα μπορεί να ανιχνεύσει κατά πόσο ένα μπουκάλι είναι σφραγισμένο ή έχει ανοιχθεί. Επίσης, θα χρησιμοποιεί το πρωτόκολλο NFC για να στέλνει εξατομικευμένες ανακοινώσεις προς τους καταναλωτές που προσπαθούν να διαβάσουν την ετικέτα του προϊόντος με τα έξυπνα τους τηλέφωνα.

Σύμφωνα με εκπρόσωπο παρόλο που τα προϊόντα τους δεν ανήκουν στην κατηγορία των "έξυπνων" προϊόντων, εντούτοις υπάρχει αρκετή ψηφιακή αλληλεπίδραση με τα προϊόντα καθώς οι άνθρωποι κοιτάζουν τις διάφορες κατηγορίες ποτών στο κατάστημα και ψάχνουν στο Διαδίκτυο πληροφορίες για αυτές. Γίνονται εκατομμύρια αναζητήσεις για τα προϊόντα αυτά στο Διαδίκτυο και περισσότερο από το 50% αυτών γίνεται μέσω κινητού τηλεφώνου σε καταστήματα που τα πουλούν.

Με την εισαγωγή των έξυπνων μπουκαλιών η εταιρεία θέλει να επιτύχει δύο στόχους: πρώτον να κατευθύνει τον καταναλωτή στην αγορά του σωστού προϊόντος και δεύτερον, μετά το άνοιγμα του προϊόντος να του παρουσιάζει επιλογές σχετικά με το πώς θα το απολαύσει καλύτερα. Πέρα από τις προοπτικές που έχει στον τομέα του μάρκετινγκ το καινούργιο αυτό μπουκάλι μπορεί να βρει και άλλες εφαρμογές στην αλυσίδα παραγωγής του προϊόντος καθώς μέσω των ετικετών που θα εφαρμόζονται στα μπουκάλια θα μπορεί να παρακολουθείται η πορεία του από την αλυσίδα παραγωγής , στο κατάστημα και μέχρι το σημείο της κατανάλωσης. Σύμφωνα με την εταιρεία θα παρέχει και μία μέθοδο ελέγχου της νόθευσης και της αυθεντικότητας του ποτού.

Το IoT βρίσκει εφαρμογή ακόμα και στη ψυχαγωγία με την Disney να ανακοινώνει την χρήση ενός έξυπνου βραχιολιού ή κάρτας με το όνομα Magic Band. Το Magic Band, είναι μία συσκευή, που επιτρέπει στους χρήστες της να αποκτούν εύκολη πρόσβαση στις εγκαταστάσεις αλλά και στις επιλογές διασκέδασης για τις οποίες έκαναν κράτηση μέσω της εφαρμογής My Disney Experience. Μπορεί να χρησιμοποιηθεί ως κάρτα πρόσβασης σε δωμάτια ξενοδοχείου της Disney, ως κάρτα πρόσβασης στα θεματικά πάρκα καθώς και για αγορά φαγητού και άλλων εμπορευμάτων. Τέλος, το Magic Band συνδέεται με την εφαρμογή PhotoPass, μέσω της οποίας, οι φωτογραφίες που θα τραβηχτούν από τους φωτογράφους του πάρκου θα συνδεθούν με το προσωπικό προφίλ του χρήστη και θα μπορεί να τις σώσει ή να τις εκτυπώσει.

2.5 Περίληψη

Η εποχή του IoT είναι ήδη εδώ. Σύμφωνα και με τα στατιστικά του Internet World Stats (www.internetworldstats.com), τον Ιούνιο του 2012 υπήρχαν τουλάχιστον 2.4 δισεκατομμύρια χρήστες συνδεδεμένοι στο Διαδίκτυο, αριθμός που αποτελεί το 34% περίπου του συνολικού πληθυσμού. Ο αριθμός των συνδεδεμένων συσκευών από την άλλη, υπερέβαινε τον συνολικό πληθυσμό. Στις μετρήσεις συμπεριλήφθηκαν υπολογιστές και

κινητά τηλέφωνα, αλλά και καινούργιες βιομηχανικές και οικιακές συσκευές που δεν είχαν μέχρι πρόσφατα τέτοιες δυνατότητες. Ο αριθμός των συσκευών αυτών που συνδέεται μέχρι τώρα στο Διαδίκτυο ισοδυναμεί με ποσοστό λιγότερο του 1% των αντικειμένων που θα μπορούσαν να συνδεθούν. Για παράδειγμα, το IoT περιλαμβάνει τη σύνδεση συσκευών όπως φούρνοι μικροκυμάτων, ξυπνητήρια, πλυντήρια κ.τ.λ.

Έχοντας παρατηρήσει τη θεαματική ανάπτυξη του IoT οι νομοθετικές και άλλες αρχές σε Ευρώπη και Αμερική κινητοποιήθηκαν και αποφάσισαν να λάβουν δράση ώστε η χρήση των τεχνολογιών αυτών να μην γίνεται ανεξέλεγκτα αλλά να προστατεύονται τα προσωπικά δεδομένα των χρηστών και η προσωπική τους ζωή. Η ψήφιση κατάλληλων νομοθετημάτων είναι ακόμα σε νηπιακά στάδια αλλά τουλάχιστον άρχισαν να γίνονται βήματα προς τη σωστή κατεύθυνση.

Εφαρμογές του IoT μπορείς να βρεις σε όλους τους τομείς της ζωής. Από τις γραμμές παραγωγής μιας αυτοκινητοβιομηχανίας μέχρι τον τρόπο εισόδου σε ένα θεματικό πάρκο. Θεωρητικά οι εφαρμογές που μπορούν να αναπτυχθούν είναι απεριόριστες και μπορούν να παρέχουν διευκολύνσεις

3

Τεχνολογίες Αυτοματισμού και Ενεργειακής Διαχείρισης Κτιρίων

3.1 Εισαγωγή

Τα συστήματα αυτοματισμού και τα πρωτόκολλα τους μπορούν να χωριστούν σε πολλές κατηγορίες, χρησιμοποιώντας διαφορετικά κριτήρια. Σε αυτό το ευρύ σύνολο ιδιοτήτων ταξινόμησης μπορούμε να προσδιορίσουμε κάποιες βασικές και ενδιαφέρουσες κατηγοριοποιήσεις: ανοιχτού κώδικα, κεντρική διαχείριση και η ευελιξία του συστήματος. Οι κατηγορίες αυτές μας παρέχουν σημαντικές πληροφορίες που είναι ζωτικής σημασίας για την αξιολόγηση της ευχρηστίας ενός πρωτοκόλλου ή ενός συστήματος για ένα έργο.

3.1.1 Συστήματα-πρωτόκολλα ανοιχτού κώδικα

Ο χαρακτηρισμός ανοιχτό ή κλειστό πρωτόκολλο, χρησιμοποιείται για να περιγράψει την εξάρτηση ενός συστήματος από τον κατασκευαστή του. Υπάρχουν δύο βασικές κατηγορίες:

- Ανοιχτά πρωτόκολλα
- Κλειστά συστήματα

Τα ανοικτά πρωτόκολλα βασίζονται σε ανοικτά πρότυπα και προδιαγραφές, τα οποία είναι προσβάσιμα για όλους όχι μόνο από τον κατασκευαστή, ο οποίος ανέπτυξε το πρωτόκολλο. Το σημαντικότερο πλεονέκτημα αυτής της προσέγγισης είναι προφανές: οι ανοιχτές προδιαγραφές εξασφαλίζουν μεγάλη ευελιξία στον σχεδιαστή ενός συστήματος ελέγχου κτιρίου, διότι μπορεί να χρησιμοποιήσει συσκευές που να εκτελούν μια επιθυμητή λειτουργία από διάφορους κατασκευαστές. Οι διαφορές μεταξύ των συσκευών διαφορετικών κατασκευαστών είναι στην τιμή, το σχεδιασμό ή στις πρόσθετες λειτουργίες που μπορούν να εκτελέσουν. Τα ανοιχτά πρωτόκολλα δίνουν στο σχεδιαστή την ευελιξία να επιλέξει συσκευές ανάλογα με τις ανάγκες του έργου.

Ένα άλλο πλεονέκτημα είναι ότι για τα πρωτόκολλα αυτά υπάρχει σημαντική ακαδημαϊκή έρευνα για την ανάπτυξη νέων χαρακτηριστικών και δυνατοτήτων. Ένα από τα μειονεκτήματα των ανοικτών πρωτοκόλλων, είναι συνήθως η αυξημένη τιμή του συστήματος για σπίτια. Τα συστήματα αυτά είναι οικονομικά αποδοτικά για μεγάλα κτίρια, όπως κτίρια γραφείων, νοσοκομεία, ξενοδοχεία ή αεροδρόμια.

Οι προδιαγραφές (π.χ. πρωτόκολλο επικοινωνίας) ενός κλειστού συστήματος είναι, σε αντίθεση με τα ανοιχτά πρωτόκολλα, δεν είναι διαθέσιμες για όλους αλλά αναπτύσσονται από συγκεκριμένες εταιρείες. Το πλεονέκτημα των κλειστών συστημάτων είναι το κόστος των εξαρτημάτων που το αποτελούν αλλά και του ολόκληρο του συστήματος για εγκαταστάσεις σε μονοκατοικίες, διαμερίσματα ή μικρά σπίτια. Επίσης, συνήθως τα συστήματα αυτά είναι πολύ εύκολα στην εγκατάσταση και τον προγραμματισμό. Τα κλειστά συστήματα, στις περισσότερες των περιπτώσεων, είναι σε θέση να εξυπηρετήσουν όλες τις βασικές ανάγκες ενός οικιακού αυτοματισμού. Αλλά δεν προσφέρουν μεγάλη ευελιξία, καθώς ο χρήστης μπορεί να επιλέξει μόνο από μια πολύ μικρή ομάδα συσκευών και σχεδίων μιας συγκεκριμένης εταιρείας. Ένα άλλο πρόβλημα είναι ότι οι χρήστες εξαρτώνται από έναν μόνο κατασκευαστή που όταν σταματήσει την παραγωγή των συγκεκριμένων συσκευών, δε θα μπορούν να επεκτείνουν μία υφιστάμενη εγκατάσταση ή να αντικαταστήσουν χαλασμένες συσκευές.

3.1.2 Κεντρικά συστήματα

Μια άλλη ιδιότητα που χωρίζει τα πρωτόκολλα και τα συστήματα σε διαφορετικές ομάδες είναι η τοπολογία και η λογική συγκέντρωσης. Υπάρχου οι πιο κάτω κατηγορίες:

- Συγκεντρωτικά συστήματα.
- Αποκεντρωμένα/κατανεμημένα συστήματα.

- Υβριδικά συστήματα.

Ένα συγκεντρωτικό σύστημα αποτελείται από μια κεντρική μονάδα η οποία ελέγχει τις λειτουργίες ολόκληρου του συστήματος. Έτσι, το σύστημα δεν χρειάζεται έξυπνους αισθητήρες και ενεργοποιητές, αλλά εξαρτάται πλήρως από τη λειτουργία της κεντρικής μονάδας. Αν αυτή αποτύχει, τότε το όλο σύστημα θα τεθεί εκτός λειτουργίας. Σήμερα, τα συστήματα αυτά χρησιμοποιούν επί τω πλείστο τοπολογία διαύλου, αλλά υπάρχουν ακόμα συστήματα που εξακολουθούν να χρησιμοποιούν απευθείας συνδέσεις με αισθητήρες και ενεργοποιητές. (Τοπολογία αστέρα - κάθε συσκευή έχει τη δική της σύνδεση με την κεντρική μονάδα).

3.1.3 Κατανεμημένα συστήματα

Τα κατανεμημένα συστήματα δεν έχουν κεντρική μονάδα. Αυτό σημαίνει ότι κάθε μονάδα είναι ευφυής/έξυπνη και ξέρει τι να κάνει (π.χ. πότε και πού να στείλει δεδομένα). Αυτό είναι φυσικά ένα μεγάλο πλεονέκτημα, διότι το σύστημα είναι ανθεκτικό και ασφαλές έναντι αστοχίας καθώς και πιο αξιόπιστο - όταν μία μονάδα αποτύχει, τότε οι άλλες εξακολουθούν να λειτουργούν. Τα κατανεμημένα συστήματα χρησιμοποιούν πάντα τοπολογία διαύλου. Το μειονέκτημα είναι ότι οι συσκευές του συστήματος είναι πιο ακριβές από ότι οι συσκευές ενός κεντρικού συστήματος.

3.1.4 Υβριδικά συστήματα

Τα υβριδικά συστήματα είναι κάπου στη μέση , όπου οι είσοδοι (αισθητήρες) συνδέεται με τη χρήση ενός διαύλου και οι έξοδοι (ενεργοποιητές) συνδέονται απευθείας με τη χρήση τοπολογίας αστέρα σε ημι-κεντρικές μονάδες. Σε αυτό το κεφάλαιο θα εξετάσουμε κάποια από τα πιο γνωστά και διαδεδομένα συστήματα αυτοματισμού κτιρίων όπως το KNX, το C-bus, το Zigbee και το Z-wave. Στο εμπόριο υπάρχουν αρκετά άλλα τέτοια συστήματα η λειτουργία των οποίων παρομοιάζει με τα παραδείγματα που θα αναφέρουμε.

3.2 KNX

Το KNX είναι ένα σύστημα διαύλου για έλεγχο κτιρίων. Αυτό σημαίνει ότι όλες οι συσκευές σε ένα σύστημα KNX χρησιμοποιούν την ίδια μέθοδο μετάδοσης και είναι σε θέση να ανταλλάσσουν δεδομένα μέσω ενός κοινού διαύλου. Αυτό έχει τις ακόλουθες συνέπειες:

- Η πρόσβαση στο δίκτυο διαύλου χρειάζεται να ρυθμίζεται με σαφήνεια (bus access method).

- Τα περισσότερα από τα δεδομένα που μεταδίδονται δεν είναι ωφέλιμα φορτία (π.χ. σήμα για φως on / off φως), αλλά αφορούν διευθυνσιοδότηση (δηλαδή από που προέρχονται τα δεδομένα; Πού θα πάνε;)

Ένα άλλο σημαντικό χαρακτηριστικό του συστήματος διαύλου KNX είναι η αποκεντρωμένη δομή του: δεν υπάρχει ανάγκη για μια κεντρική μονάδα ελέγχου, επειδή η "νοημοσύνη" του συστήματος είναι κατανεμημένη σε όλες τις συσκευές του. Οι κεντρικές μονάδες είναι πιθανές, για την πραγματοποίηση πολύ εξειδικευμένων εφαρμογών. Κάθε συσκευή έχει το δικό της μικροεπεξεργαστή. Ένα σημαντικό πλεονέκτημα της αποκεντρωμένης δομής του KNX είναι ότι, αν μία συσκευή αποτύχει, οι άλλες συνεχίζουν να λειτουργούν.

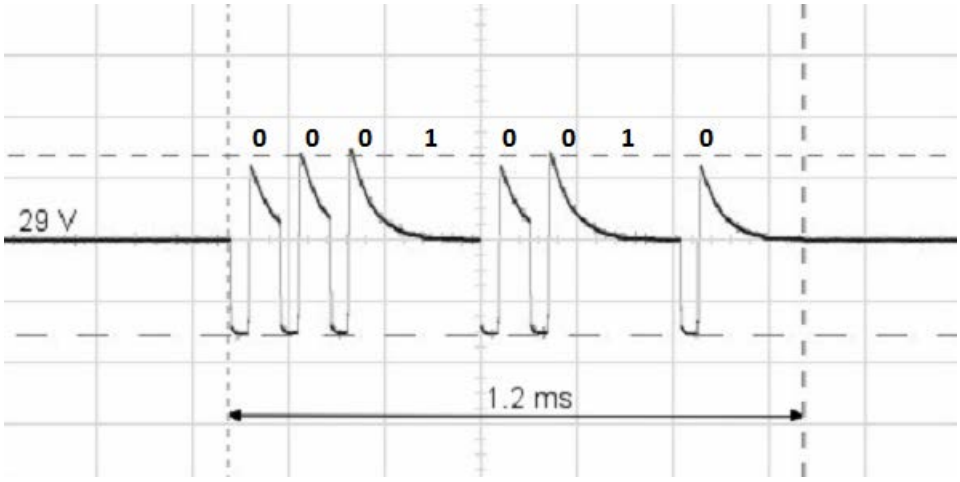
Γενικά σε ένα σύστημα KNX, οι συσκευές εμπίπτουν σε τρεις κατηγορίες: συσκευές του συστήματος (Τροφοδοτικό, διεπαφή προγραμματισμού, κ.λπ.), αισθητήρες και ενεργοποιητές. Χάρη στην αποκεντρωμένη τους δομή, τα συστήματα διαύλου KNX μπορούν να τροποποιηθούν και να επεκταθούν ακριβώς όπως απαιτείται. Θεωρητικά ένα σύστημα KNX μπορεί να αποτελείται από περισσότερες από 50.000 συσκευές. Διάφορα μέσα επικοινωνίας (και ως εκ τούτου μέθοδοι μετάδοσης) μπορούν να χρησιμοποιηθούν για την ανταλλαγή δεδομένων μεταξύ συσκευών σε ένα σύστημα KNX:

- KNX Twisted Pair (KNX TP) - επικοινωνία μέσω ενός καλωδίου δεδομένων συνεστραμμένου ζεύγους (καλώδιο διαύλου).
- KNX Powerline (KNX PL) - χρησιμοποιεί το υπάρχον δίκτυο ρεύματος 230V.
- KNX Radio Frequency (KNX RF) - επικοινωνία μέσω ασύρματου σήματος.
- KNX IP - επικοινωνία μέσω Ethernet.

3.2.1 KNX Twisted Pair (TP)

Το καλώδιο δεδομένων συνεστραμμένου ζεύγους (καλώδιο διαύλου) είναι το πιο κοινό μέσο επικοινωνίας για τις εγκαταστάσεις KNX. Εδώ όλες οι συσκευές συνδέονται μεταξύ τους μέσω του καλωδίου διαύλου. Στο KNX TP το καλώδιο διαύλου παρέχει σε όλες τις συσκευές τα δεδομένα και το ρεύμα λειτουργίας. Η ονομαστική τάση του συστήματος διαύλου είναι 24V, ενώ η τάση που παρέχεται από τα τροφοδοτικά είναι 30V. Οι συσκευές διαύλου λειτουργούν χωρίς σφάλμα σε τάσεις μεταξύ 21 V και 30 V, έτσι ένα εύρος ανοχής 9 V είναι διαθέσιμο για να αντισταθμίσει τις πτώσεις τάσης στο καλώδιο, και την αντίσταση επαφής. Στις συσκευές, αρχικά διαχωρίζεται η τάση τροφοδοσίας DC από τα δεδομένα που μεταφέρονται στην τάση AC. Η τάση τροφοδοσίας DC δημιουργείται από έναν πυκνωτή, ενώ ένας μετασχηματιστής διαχωρίζει τα δεδομένα που μεταφέρει τάση AC. Σε συσκευές μετάδοσης, ο μετασχηματιστής χρησιμεύει επίσης για την υπέρθεση των εξερχόμενων

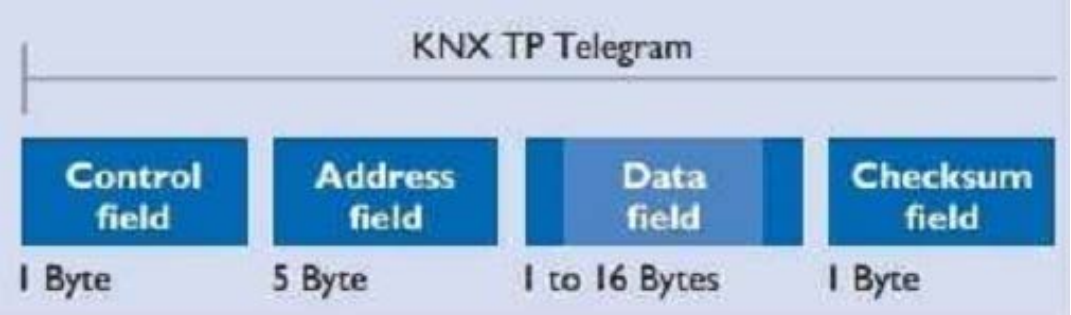
δεδομένων πάνω στην τάση διαύλου. Η ταχύτητα μεταφοράς δεδομένων είναι 9.600 bit / s, και τα δεδομένα μεταδίδονται σειριακά, ένα byte κάθε φορά, μέσω ασύγχρονης μεταφοράς δεδομένων. Όταν μεταδίδεται ένα λογικό μηδέν, η τάση πέφτει στιγμιαία και κατόπιν, μετά από όχι περισσότερο από 104 μs, αυξάνεται και πάλι για να εξισορροπήσει τελικά στην αρχική τάση. Η μετάδοση των λογικών ένα αντιστοιχεί στην κατάσταση ηρεμίας του διαύλου (Σχήμα 3.2.1.1).



Σχήμα 3.2.1.1: Μετάδοση λογικών 1 και 0 για το KNX TP

Η ανταλλαγή πληροφοριών μεταξύ των συσκευών του συστήματος, γίνεται με τη μορφή των λεγόμενων τηλεγραφημάτων. Ένα τηλεγράφημα αποτελείται από μια ακολουθία χαρακτήρων, του ενός byte. Διάφοροι χαρακτήρες σε συνδυασμό μεταξύ τους σχηματίζουν ένα πεδίο. Τα τηλεγραφήματα στο σύστημα KNX-TP έχουν τέσσερα πεδία (Σχήμα 3.2.1.2):

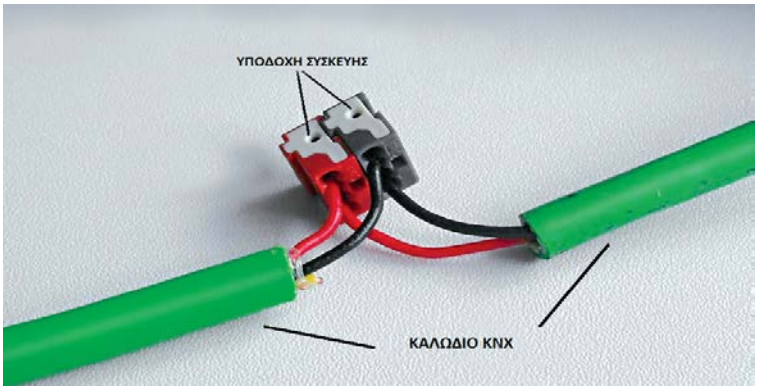
- Το πεδίο ελέγχου (Control field) καθορίζει την προτεραιότητα του τηλεγραφήματος και κατά πόσον ή όχι η μετάδοση του τηλεγραφήματος επαναλήφθηκε (αν ο δέκτης δεν ανταποκρίθηκε).
- Το πεδίο διεύθυνσης (Address field) προσδιορίζει την διεύθυνση του αποστολέα και τη διεύθυνση προορισμού (Ατομική Διεύθυνση ή Ομάδα Διευθύνσεων) του δέκτη.
- Το πεδίο δεδομένων(Data field), το οποίο μπορεί να έχει μήκος έως 16 bytes, περιέχει το ωφέλιμο φορτίο του τηλεγραφήματος.
- Το πεδίο αθροίσματος ελέγχου (Checksum field) χρησιμοποιείται για τον έλεγχο ισοτιμίας.



Σχήμα 3.2.1.2: Δομή τηλεγραφήματος στο KNX TP

Η πρόσβαση στο δίαυλο KNX, όπως και σε πολλά άλλα συστήματα διαύλου, είναι τυχαία και καθοδηγείται από κάποιο γεγονός. Ένα τηλεγράφημα μπορεί να μεταδοθεί μόνο εφόσον δεν υπάρχει άλλο τηλεγράφημα να μεταδίδεται ταυτόχρονα. Για την αποφυγή συγκρούσεων κατά τη διάρκεια της μετάδοσης, οι προτεραιότητες των διαφόρων συσκευών αποστολής ρυθμίζονται από την μέθοδο CSMA/CA (Carrier Sense Multiple Access/ Collision Avoidance).

Οι συσκευές διαύλου συνδέονται στο καλώδιο του διαύλου μέσω υποδοχών που μπορούν να φιλοξενήσουν μέχρι τέσσερα καλώδια KNX. Οι υποδοχές αυτές (Σχήμα 3.2.1.3) καθιστούν δυνατή την αποσύνδεση συσκευών από τον δίαυλο χωρίς να διακόπτεται η λειτουργία του. Αυτό αποτελεί και ένα βασικό πλεονέκτημα του συστήματος διαύλου KNX: αφαίρεση μιας μόνο συσκευής από το σύστημα δεν σταματά τις άλλες συσκευές από το να επικοινωνούν μεταξύ τους.



Σχήμα 3.2.1.3: Υποδοχή Συσκευής

3.2.2 KNX Powerline (KNX PL)

Η χρήση των υπαρχουσών καλωδίων της ηλεκτρικής εγκατάστασης σε ένα κτίριο ως μέσο επικοινωνίας για το KNX είναι ένας οικονομικά αποδοτικό τρόπος για την εκ των υστέρων εφαρμογή σε ένα κτίριο ενός συστήματος KNX. Τα σήματα δεδομένων υπερτίθενται στην

τάση του δικτύου. Δεν απαιτούνται επιπλέον τροφοδοτικά στο KNX PL; η ισχύς που απαιτείται από τις συσκευές διαύλου προέρχεται από την παροχή 230V του υφιστάμενου ηλεκτρικού δικτύου. Για να εξασφαλιστεί ότι η επικοινωνία δεδομένων μπορεί να λάβει χώρα μέσω και των τριών φάσεων, χρησιμοποιούνται συζεύκτες φάσεων, ενώ φίλτρα προλαμβάνουν την διάδοση των σημάτων δεδομένων μέσω της σύνδεσης του κτιρίου προς το δίκτυο διανομής ηλεκτρικού ρεύματος.

Στο KNX PL η ταχύτητα μεταφοράς δεδομένων είναι 1.200 bits. Τα λογικά μηδενικά και μονάδες μεταδίδονται μέσω διαμόρφωσης μετατόπισης συχνότητας (S-FSK). Σήμα συχνότητας 105,6 kHz που αποστέλλεται από έναν πομπό αντιστοιχεί σε λογικό μηδέν, ενώ το λογικό ένα αντιπροσωπεύεται από σήμα συχνότητας 115,2 kHz. Τα σήματα υπερτίθενται πάνω στη τάση δικτύου. Χάρη σε συγκριτικές τεχνικές και μια έξυπνη διορθωτική διαδικασία, τα σήματα που λαμβάνονται μπορούν να αποτιμηθούν ακόμη και όταν υπάρχουν παρεμβολές. Η κεντρική συχνότητα των δύο κυμάτων είναι 110 kHz, και αυτός είναι ο λόγος που το σύστημα KNX PL είναι επίσης γνωστό ως PL110. Η ισχύς εκπομπής των υπερτεθειμένων σημάτων είναι συχνά ίση με το επίπεδο του θορύβου στα σημερινή δίκτυα ρεύματος. Ως αποτέλεσμα, τα σήματα μπορούν να αποτιμηθούν μόνο με τη χρήση ειδικών μεθόδων επεξεργασίας ψηφιακού σήματος, κατά την οποία η ισχύς εκπομπής και ευαισθησία του δέκτη των συσκευών του διαύλου συνεχώς προσαρμόζονται στις συνθήκες του δικτύου.

Τα τηλεγραφήματα του KNX PL είναι ουσιαστικά επέκταση των τηλεγραφημάτων του KNX TP. Τα τηλεγραφήματα του KNX PL έχουν τέσσερα πεδία (Σχήμα 3.2.2.1:):

- Το πεδίο κατάρτισης (training field) συγχρονίζει και καθορίζει τα επίπεδα των αποστολέων και των παραληπτών.
- Τα πεδία προοιμίου (preamble fields) υποδηλώνουν την έναρξη της μετάδοσης, ελέγχουν την πρόσβαση στο δίαυλο, και είναι αναγκαία για την πρόληψη σύγκρουσης των τηλεγραφημάτων.
- Το τρίτο πεδίο περιέχει το τηλεγράφημα KNX TP.
- Το πεδίο ID (system ID) περιέχει ένα αναγνωριστικό για τη διατήρηση των σημάτων των διαφορετικών συστημάτων KNX PL χωριστά, έτσι ώστε μόνο συσκευές που χρησιμοποιούν το ίδιο σύστημα ID μπορούν να επικοινωνούν μεταξύ τους.

Σχήμα 3.2.2.1: Τηλεγράφημα KNX PL

Όπως το KNX TP, έτσι και το KNX PL απαιτεί τη χρήση μιας μεθόδου πρόσβασης στον δίαυλο για την αποφυγή συγκρούσεων μεταξύ των τηλεγραφημάτων. Αυτό μπορεί να γίνει μόνο με την καθυστέρηση αποστολής τηλεγραφημάτων από τις συσκευές του διαύλου. Η προεπιλεγμένη κατάσταση όλων των συσκευών του διαύλου είναι η λειτουργία λήψης, μόνον αν συντρέχουν ορισμένες προϋποθέσεις μπορούν να μεταβούν στη λειτουργία αποστολής. Εάν μια συσκευή ανιχνεύσει μια σειρά δυαδικών ψηφίων από ένα προοίμιο, αυτό της υποδεικνύει ότι ο δίαυλος είναι κατειλημμένος από μια άλλη συσκευή. Διαφοροποίηση γίνεται μεταξύ των δύο καταστάσεων, διαύλου κατειλημμένος και δίαυλος αποκλεισμένος. Εάν μια συσκευή λάβει ένα σήμα ¨δίαυλος κατειλημμένος¨, η μετάδοση του τηλεγραφήματος της αναβάλλεται μέχρι μία μεταγενέστερη χρονική στιγμή, η οποία επιλέγεται τυχαία από επτά πιθανές επιλογές. Αυτό μειώνει σημαντικά την πιθανότητα συγκρούσεων.

3.2.3 KNX Radio Frequency (KNX RF)

Ο ραδιοδίαυλος είναι ένα κατάλληλο μέσο επικοινωνίας για το KNX σε εκείνες τις περιπτώσεις όπου δεν είναι δυνατόν να τοποθετηθούν νέα καλώδια στο κτίριο (π.χ. όταν είναι απαραίτητη η εγκατάσταση αισθητήρων σε δυσπρόσιτες περιοχές). Το KNX RF είναι επίσης κατάλληλο για την επέκταση υφιστάμενων εγκαταστάσεων KNX TP. Θεωρητικά το KNX RF θα μπορούσε να επιτρέψει σε όλες τις τεχνολογίες σε ένα κτίριο να ελέγχονται ασύρματα, αλλά στην πράξη η χρήση του ραδιοδιαύλου παραμένει η εξαίρεση παρά ο κανόνας. Για να καταστεί δυνατή η τοποθέτηση αισθητήρων RF σε σημεία όπου δεν υπάρχει πρόσβαση στο δίκτυο ηλεκτρικής ενέργειας, οι αισθητήρες εξοπλίζονται με μπαταρίες.

Το KNX RF χρησιμοποιεί διαμόρφωση συχνότητας. Οι λογικές καταστάσεις μηδέν και ένα παράγονται τροποποιώντας ελαφρώς τη συχνότητα του φέροντος κύματος, επίσης γνωστή ως κεντρική συχνότητα. Ένας σημαντικός παράγοντας που καθορίζει την απόδοση της μετάδοσης είναι η επιλογή σωστής κεντρικής συχνότητας. Υπάρχουν δύο εκδόσεις του KNX RF - KNX RF Ready και KNX RF Multi. Στο KNX RF Ready η κεντρική συχνότητα είναι 868,3 MHz, και μόνο ένα κανάλι επικοινωνίας είναι διαθέσιμο. Ωστόσο, ραδιοεπικοινωνία

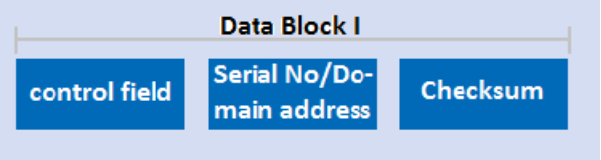
στην οποία μόνο ένα κανάλι είναι διαθέσιμο είναι ευάλωτη σε παρεμβολές από συστήματα ραδιοεπικοινωνιών στην ίδια ή σε γειτονική ζώνη που χρησιμοποιούν διαφορετικές μεθόδους πρόσβασης στο μέσο επικοινωνίας.

Το KNX RF Multi ξεπερνά αυτές τις παρεμβολές επιτρέποντας στη συσκευή να μεταβαίνει από ένα κατειλημμένο κανάλι σε ένα εναλλακτικό ελεύθερο κανάλι. Όπως και με όλα τα μέσα επικοινωνίας KNX, έτσι και στο KNX RF τα χρήσιμα δεδομένα αποστέλλονται μέσω τηλεγραφημάτων πολλαπλής διανομής (multicast). Αυτό σημαίνει ότι ένα τηλεγράφημα μπορεί να ληφθεί από πολλές συσκευές ταυτόχρονα και έτσι π.χ. να ανάψουν διάφορα φώτα συγχρόνως. Τα τηλεγραφήματα KNX-RF αποτελούνται από πολλά τμήματα δεδομένων (Σχήμα 3.2.3.1:) που χωρίζονται από πεδία αθροίσματος ελέγχου (CRC). Τα τμήματα δεδομένων περιέχουν το πραγματικό φορτίο καθώς και διάφορες πληροφορίες διαύλου όπως δεδομένα διευθυνσιοδότησης.

Σχήμα 3.2.3.1: Τηλεγράφημα KNX-RF

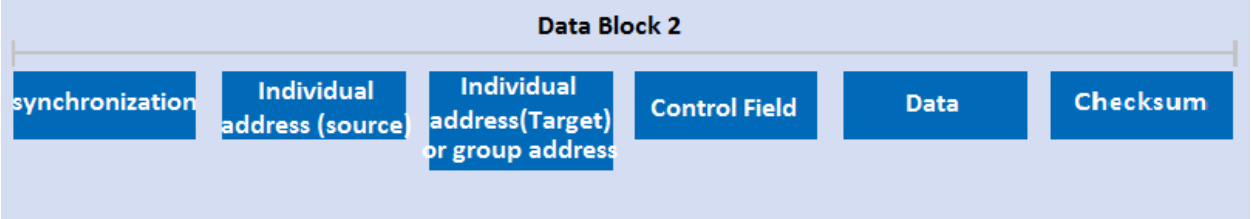
Το πρώτο τμήμα δεδομένων αποτελείται από τρία πεδία (Σχήμα 3.2.3.2):

- Το πεδίο ελέγχου που περιέχει πληροφορίες σχετικά με το μήκος του τηλεγραφήματος, την ποιότητα μετάδοσης (απόδοση λήψης), την κατάσταση της μπαταρίας για τις συσκευές KNX RF που λειτουργούν με μπαταρία και αν η συσκευή είναι μιας κατεύθυνσης.
- Το δεύτερο πεδίο περιέχει είτε το σειριακό αριθμό KNX ή τη διεύθυνση του τομέα. Ο σειριακός αριθμός εκχωρείται από τον κατασκευαστή και δεν μπορεί να αλλάξει.
- Το πεδίο αθροίσματος ελέγχου (Checksum field) χρησιμοποιείται για τον έλεγχο ισοτιμίας και επιτρέπει στον παραλήπτη να καθορίσει εάν ένα τηλεγράφημα εστάλη χωρίς λάθος.



Σχήμα 3.2.3.2 : Τμήμα δεδομένων 1

Εκτός από τα παραπάνω πεδία ελέγχου και αθροίσματος ελέγχου, το δεύτερο τμήμα δεδομένων (Σχήμα 3.2.3.3) αποτελείται από πεδία που περιέχουν την ατομική διεύθυνση προέλευσης (φυσική διεύθυνση), τη διεύθυνση προορισμού και το ωφέλιμο φορτίο. Το ωφέλιμο φορτίο είναι η πραγματική πληροφορία που πρέπει να σταλεί. Ανάλογα με το μήκος του ωφέλιμου φορτίου, ένα τηλεγράφημα KNX μπορεί επίσης να περιέχει περαιτέρω τμήματα δεδομένων.



Σχήμα 3.2.3.3 : Τμήμα δεδομένων 2

3.2.4 KNX IP

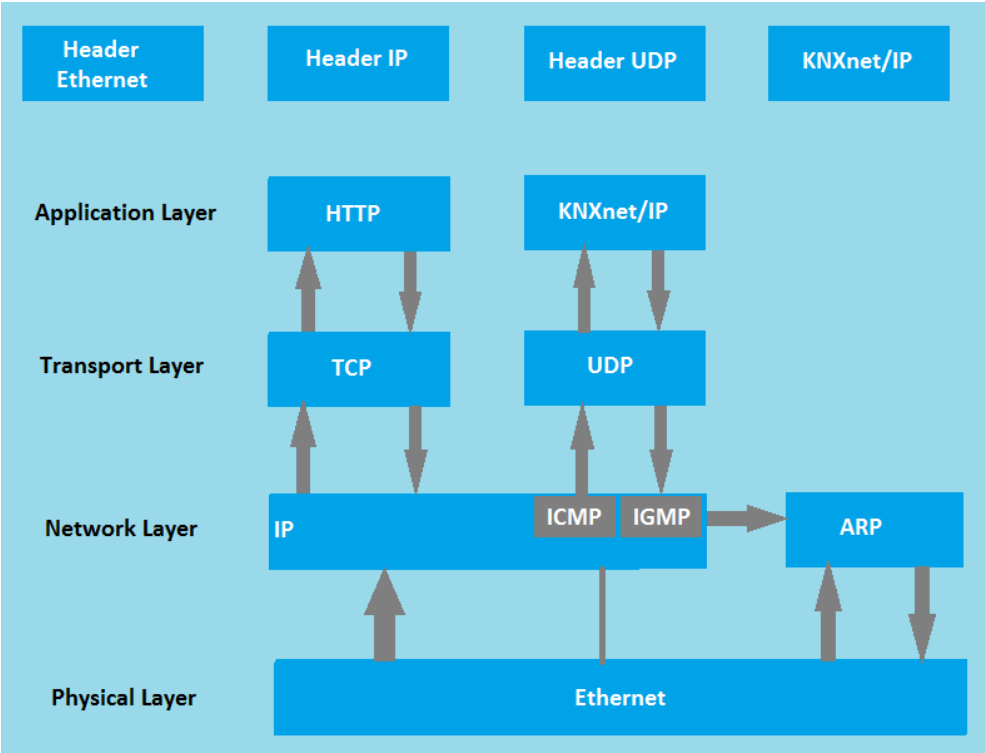
Το Ethernet χρησιμοποιείται για τοπικά δίκτυα καθώς και για πρόσβαση προς το Διαδίκτυο. Απαιτούνται διάφορα πρωτόκολλα, προκειμένου οι υπολογιστές να επικοινωνούν μεταξύ τους στο δίκτυο. Το TCP / IP - μια ομάδα πρωτοκόλλων και κανόνων (οικογένεια πρωτοκόλλων) που θεσπίστηκε το 1984 - χρησιμοποιείται σήμερα ευρύτατα. Αν και συνήθως αναφέρονται με τη μορφή "TCP / IP", TCP (Transmission Control Protocol) και IP (Internet Protocol) είναι στην πραγματικότητα δύο ξεχωριστά πρωτόκολλα. Αυστηρά μιλώντας, το πρωτόκολλο TCP/IP περιλαμβάνει επίσης ένα τρίτο, εξίσου σημαντικό πρωτόκολλο το UDP (User Datagram Protocol).

Το πρωτόκολλο IP, εξυπηρετεί στο να εξασφαλιστεί ότι τα πακέτα δεδομένων αποστέλλονται από τη μία συσκευή στην άλλη ακολουθώντας τις βέλτιστες διαδρομές. Το πρωτόκολλο TCP δημιουργεί μια μόνιμη σύνδεση μεταξύ των συσκευών, που ελέγχει για σφάλματα και διασφαλίζει ότι όλα τα πακέτα δεδομένων αποστέλλονται με τη σωστή σειρά και ανακατασκευάζονται με επιτυχία από τον δέκτη (connection-oriented Protocol). Το πρωτόκολλο UDP χρησιμοποιείται για εφαρμογές (π.χ. ήχου και βίντεο συνεχούς ροής), στις

οποίες είναι αποδεκτό μερικές φορές να χάνονται κάποια πακέτα δεδομένων. Η σύνδεση δεν ελέγχει για λάθη και η παράδοση των πακέτων δεδομένων είναι ανεξέλεγκτη, καθώς τα πακέτα δεν είναι αριθμημένα (πρωτόκολλο χωρίς σύνδεση). Το UDP είναι πολύ πιο ευέλικτο και γρήγορα από ό, τι το πρωτόκολλο TCP. Χρησιμοποιείται συχνά στην κατασκευή αυτοματισμών κτιρίων. Η σύνδεση του KNX μέσω Ethernet έχει τα εξής πλεονεκτήματα:

- Μπορεί να χρησιμοποιηθεί η υπάρχουσα υποδομή δικτύου του κτηρίου για το δίκτυο του KNX (υψηλότερη ταχύτητα, πιο οικονομικό και πιο εύκολη εγκατάσταση).
- Τα κτήρια μπορούν να παρακολουθούνται και να ελέγχονται μέσω Διαδικτύου από οπουδήποτε στον κόσμο.
- Διάφορες μεμονωμένες τοποθεσίες μπορούν παρατηρούνται και να συντηρούνται από μια κεντρική τοποθεσία μέσω του διαδικτύου.
- Εγκαταστάσεις KNX πελατών μπορούν να αναλυθούν και να προγραμματιστούν από απόσταση μέσω του διαδικτύου από το σχεδιαστή του συστήματος KNX.

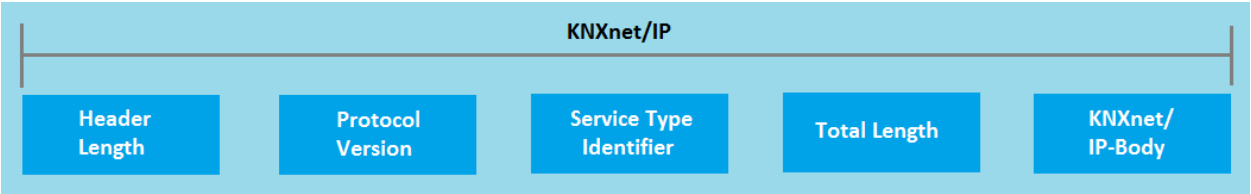
Το σύστημα KNX χρησιμοποιεί δύο μεθόδους επικοινωνίας Ethernet -σήραγγας και δρομολόγησης (tunneling and routing) εκ των οποίων και οι δύο χρησιμοποιούν το πρωτόκολλο UDP. Το Tunneling χρησιμοποιείται για πρόσβαση στο δίαυλο από ένα τοπικό δίκτυο ή από το διαδίκτυο για διάφορους σκοπούς όπως προγραμματισμό της εγκατάστασης KNX, ενώ δρομολόγηση χρησιμοποιείται για την ανταλλαγή τηλεγραφημάτων μέσω ενός δικτύου Ethernet, π.χ. για να συνδεθούν δύο συστήματα KNX TP μέσω Ethernet. Τα πρωτόκολλα KNX για τις δύο αυτές μεθόδους επικοινωνίας ονομάζονται KNXnet / IP δρομολόγησης και KNXnet / IP σήραγγας. Η επικοινωνία IP στο KNX μπορεί να εξηγηθεί με τη χρήση του μοντέλου αναφοράς OSI (Σχήμα 3.2.4.1).



Σχήμα 3.2.4.1: KNXnet/IP στο μοντέλο αναφοράς OSI

Η επικοινωνία πραγματοποιείται μέσω του στρώματος εφαρμογής (το οποίο παράγει το τηλεγράφημα KNXnet / IP), το στρώμα μεταφοράς (UDP), το στρώμα δικτύου (IP), και το φυσικό στρώμα (Ethernet). Όπως και με το πρωτόκολλο TCP, πρόσθετες πληροφορίες για το αντίστοιχο στρώμα (επικεφαλίδα) προστίθεται πάντα στις πληροφορίες KNXnet/IP. Το τηλεγράφημα KNXnet / IP περιέχει κάποιες περαιτέρω πληροφορίες πέρα από ότι στο τηλεγράφημα KNX TP (Σχήμα 3.2.4.2):

- Header Length: Το μήκος της επικεφαλίδας είναι πάντα το ίδιο. Αυτή η πληροφορία ωστόσο εξακολουθεί να αποστέλλεται, επειδή το μήκος της επικεφαλίδας μπορεί να αλλάξει σε μια νεότερη έκδοση του πρωτοκόλλου. Ο σκοπός της επικεφαλίδας είναι να προσδιορίζει την έναρξη του τηλεγραφήματος.
- Protocol Version: Δηλώνει την παρούσα έκδοση του πρωτοκόλλου KNXnet / IP.
- KNXnet/IP Service Type Identifier: Το αναγνωριστικό αυτό υποδεικνύει την δράση που πρόκειται να πραγματοποιηθεί.
- Total Length: Αυτό το πεδίο δείχνει το συνολικό μήκος του τηλεγραφήματος KNXnet / IP.
- KNXnet/IP-Body: Το πεδίο αυτό περιέχει το ωφέλιμο φορτίο.



Σχήμα 3.2.4.2: Τηλεγράφημα KNXnet/IP

3.3 C-BUS

Το C-BUS είναι ένα έξυπνο σύστημα βασισμένο σε ένα μικροεπεξεργαστή που χρησιμοποιείται για τον έλεγχο και τη διαχείριση του φωτισμού, και άλλων ηλεκτρικών εφαρμογών σε κατοικίες ή εμπορικά κτίρια. Το C-BUS μπορεί να ελέγξει σχεδόν οποιοδήποτε τύπο ηλεκτρικού φορτίου. Κάθε συσκευή C-BUS έχει το δικό της ενσωματωμένο μικροεπεξεργαστή, ο οποίος επιτρέπει σε όλες τις μονάδες σε μια εγκατάσταση να προγραμματιστούν ανεξάρτητα. Το σύστημα δεν απαιτεί έναν κεντρικό υπολογιστή ή κεντρική μονάδα ελέγχου για να χειριστεί βάσεις δεδομένων ή για την αναζήτηση σε μεγάλους πίνακες λειτουργίας.

Μεγάλες ποσότητες δεδομένων μπορούν να μεταδοθούν αποτελεσματικά και αξιόπιστα σε όλο το δίκτυο C-BUS σε ελάχιστο χρονικό διάστημα πράγμα που οδηγεί σε χαμηλές απαιτήσεις εύρους ζώνης και χαμηλά έξοδα επεξεργασίας. Η επικοινωνία μεταξύ των συσκευών εισόδου και εξόδου σε ένα συγκεκριμένο δίκτυο πραγματοποιείται από ένα σύστημα καλωδίωσης διαύλου με τη χρήση αθωράκιστου καλωδίου συνεστραμμένου ζεύγους (UTP). Αυτός ο δίαυλος φέρει μία μικρή τάση (36V DC) για τη λειτουργία του κυκλώματος μέσα σε κάθε μονάδα C-BUS. Τα δίκτυα C-BUS είναι προγραμματισμένα έτσι ώστε συγκεκριμένες δράσεις εντός του δικτύου ενεργοποιούν αντιδράσεις από μία ή περισσότερες μονάδες εντός του δικτύου.

Όταν μια συσκευή εισόδου ενεργοποιείται, ένα κατάλληλο μήνυμα διαβιβάζεται σε όλο το δίκτυο και στη συνέχεια, η κατάλληλη συσκευή εξόδου, εκτελεί το απαιτούμενο έργο της. Υπάρχουν διάφοροι τρόποι καλωδίωσης ενός δικτύου C-BUS αλλά ανεξάρτητα από τη μέθοδο που χρησιμοποιείται το δίκτυο πρέπει να συμμορφώνεται με τις παραμέτρους λειτουργίας.

Το μέγεθος μιας εγκατάστασης C-BUS είναι πρακτικά απεριόριστο. Υπάρχουν περιορισμοί σχετικά με το μέγεθος ενός δικτύου, ωστόσο, πολλά επιμέρους δίκτυα μπορούν να συσταθούν ώστε να σχηματίσουν ένα μεγάλο δίκτυο. Αυτά τα υποδίκτυα μπορεί να είναι

ηλεκτρικά απομονωμένα, εάν απαιτείται (Για παράδειγμα, ένα πολυώροφο κτίριο που ελέγχεται από C-BUS). Το C-BUS έχει πολλά πλεονεκτήματα σε σχέση με μια συμβατική εγκατάσταση καλωδίωσης. Από άποψη καλωδίωσης του C-BUS, είναι λιγότερο περίπλοκη και απαιτεί λιγότερη καλωδίωση κατά την εγκατάσταση. Μια μόνο σύνδεση C-BUS μπορεί να ελέγχει έναν απεριόριστο αριθμό συσκευών. Κάθε συσκευή εισόδου, υφιστάμενη ή που θα προστεθεί αργότερα, σε ένα δίκτυο C-BUS μπορεί να δει όλες οι συσκευές εντός του δικτύου χωρίς την ανάγκη νέας καλωδίωσης. Ως εκ τούτου, αλλάζοντας τον τρόπο που συμπεριφέρεται το δίκτυο δεν σημαίνει αλλαγή και στην καλωδίωση.

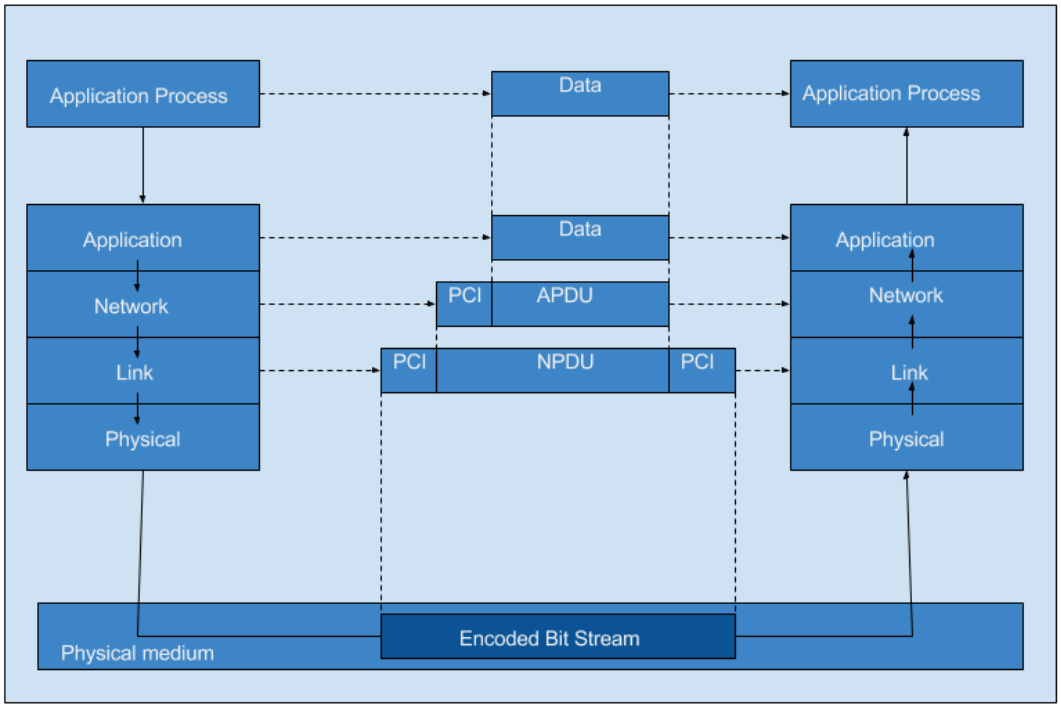
Το C-BUS δεν είναι απλά ένα σύστημα για έλεγχο του φωτισμού. Μέρος της ευελιξίας του συστήματος αυτού είναι ότι μπορεί να χρησιμοποιηθεί με πολλούς διαφορετικούς τρόπους. Υπάρχει ένα ευρύ φάσμα διαθέσιμων εργαλείων, ώστε το σύστημα να μπορεί να διασυνδεθεί με προϊόντα τρίτων. Το C-BUS μπορεί να ελέγξει σχεδόν οποιαδήποτε συσκευή ψηφιακή και αναλογική. Κάθε διακόπτης έχει τη δυνατότητα να εκτελεί πολλές λειτουργίες. Σε αντίθεση με την συμβατική καλωδίωση όπου απαιτείται πρόσθετος εξοπλισμός για λειτουργίες όπως dimming και χρονοδιαγράμματα στις υλοποιήσεις με C-BUS οι δυνατότητες αυτές μπορούν να υλοποιηθούν γρήγορα και εύκολα.

Όπως οι διακόπτες, έτσι και οι αισθητήρες μπορούν να εκτελέσουν πολλές λειτουργίες. Ένας αισθητήρας που μπορεί να λειτουργεί φωτισμό σε μια περιοχή με χαμηλή κυκλοφορία τη μέρα, μπορεί επίσης να είναι μέρος του συστήματος ασφαλείας του κτιρίου τη νύχτα.

3.3.1 Μοντέλο πρωτόκολλου

Το C-Bus έχει σχεδιαστεί σύμφωνα με το πρότυπο ISO 7498. Στο Σχήμα 3.3.1.1 βλέπουμε το μοντέλο πρωτόκολλου δικτύου που χρησιμοποιείται για το C-Bus. Σε αυτό το σχήμα, το Πρωτόκολλο Ελέγχου Πληροφοριών (PCI, Protocol Control Information) χρησιμοποιείται από διαφορετικά στρώματα πρωτοκόλλου για να προσθέσει ειδικές πληροφορίες που χρησιμοποιούνται για να βοηθήσουν στην μεταφορά των πληροφοριών. Μια μονάδα δεδομένων πρωτοκόλλου (PDU, Protocol Data Unit) αναφέρεται στο περιεχόμενο των πληροφοριών που διακινούνται από ένα στρώμα.

Για παράδειγμα, το στρώμα ζεύξεως μεταφέρει ένα PDU δικτύου (NPDU). Αυτό περιέχει ενσωματωμένες πληροφορίες που χρησιμοποιούνται από το στρώμα δικτύου, αλλά το στρώμα σύνδεσης δεν ξέρει ή δεν νοιάζεται για αυτές.



Σχήμα 3.3.1.1: Στρώματα Πρωτόκολλου C-Bus

3.3.2 Τύποι πληροφοριών C-Bus

Ένα δίκτυο C-Bus μπορεί να μεταφέρει τους ακόλουθους τύπους μηνυμάτων:

- Από σημείο σε σημείο (Point to Point): Χρησιμοποιείται για να μεταφέρει ένα μήνυμα μεταξύ δύο μεμονωμένων μονάδων στο δίκτυο. Συνήθως χρησιμοποιείται για την φόρτωση δεδομένων διαμόρφωσης σε μια μονάδα, ή για τη διαχείριση και τον έλεγχο του δικτύου. Μηνύματα από σημείο σε σημείο μπορούν επίσης να μεταδοθούν μέσω ενός ή περισσότερων γεφυρών C-Bus. Σε αυτήν την περίπτωση, ένα PCI δικτύου χρησιμοποιείται για να καθορίσει μια διαδρομή μέσο γεφυρών στο δίκτυο προορισμού. Τα δεδομένα που μεταφέρονται (τα APDU) είναι γνωστά ως C-Bus Common Application Language (CAL)
- Από σημείο σε πολλά σημεία (Point to Multi-Point): Χρησιμοποιείται για να μεταφέρει ένα μήνυμα από μια μονάδα μετάδοσης σε πολλές μονάδες λήψης, ταυτόχρονα.

Μηνύματα από σημείο σε πολλά σημεία επιτρέπουν τη δημιουργία μεταβλητών δικτύου, και διασφαλίζουν ότι οι μεταβλητές δικτύου ενημερώνονται ταυτόχρονα σε όλες τις μονάδες. Τα μηνύματα από σημείο σε πολλά σημεία απευθύνονται σε κάποια εφαρμογή προορισμού. Οι μονάδες μπορούν να συμμετέχουν σε μια ή περισσότερες εφαρμογές, ανάλογα με το σκοπό

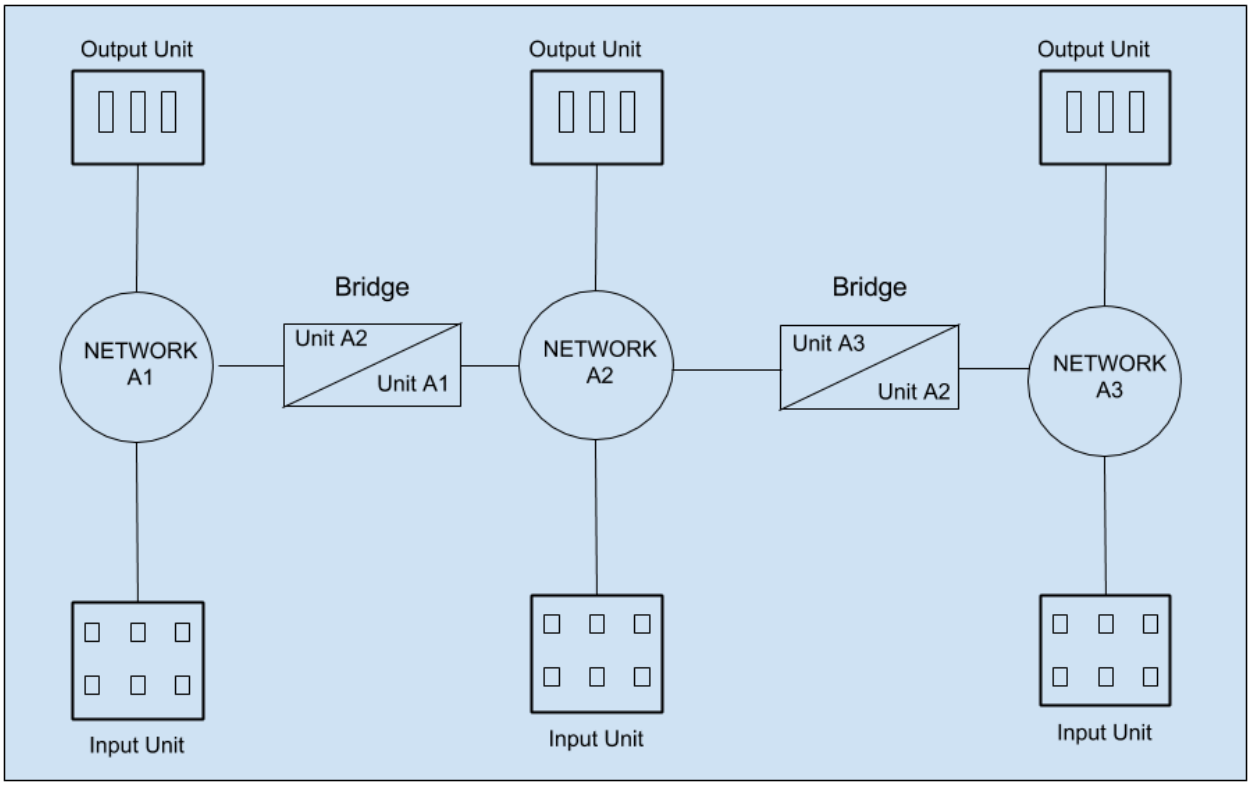
τους. Τα δεδομένα που μεταφέρονται (τα APDU) είναι γνωστά ως C-Bus Specific Application Language (SAL).

- Σημείο σε σημείο σε πολλά σημεία (Point to Point to Multi-Point): Χρησιμοποιείται για να μεταφέρει ένα μήνυμα από μια μονάδα μετάδοσης σε πολλές μονάδες λήψης, ταυτόχρονα, όπου οι μονάδες λήψης είναι σε ένα απομακρυσμένο δίκτυο. Ομοίως με τα μηνύματα από σημείο σε σημείο, οι Μεταβλητές Δικτύου μπορούν να δημιουργηθούν και να ενημερώνονται ταυτόχρονα σε όλες τις μονάδες λήψης. Τα μηνύματα από σημείο σε σημείο σε πολλά σημεία απευθύνονται σε γέφυρα C-Bus, και περιέχει ένα PCI Δικτύου που καθορίζει τη διαδρομή στο δίκτυο προορισμό και τη εφαρμογή. Όπως και παραπάνω τα δεδομένα που μεταφέρονται (τα APDU) είναι γνωστά ως C-Bus Specific Application Language (SAL).

3.3.3 Διευθύνσεις

Όλες οι διευθύνσεις C-Bus είναι 1 byte, και κωδικοποιούνται από 00 έως FF στο δεκαεξαδικό σύστημα.

- Διεύθυνση Μονάδας (Unit Address): Κάθε μονάδα που συνδέεται με ένα δίκτυο C-Bus έχει μια μοναδική διεύθυνση μονάδας, που χρησιμοποιείται αποκλειστικά κατά τη διαβίβαση πληροφοριών στην εν λόγω μονάδα. Οι πληροφορίες που διαβιβάζονται αναφέρονται ως ΔΕΔΟΜΕΝΑ CAL και χρησιμοποιούνται για τη ρύθμιση της μονάδας και τη διαχείριση του δικτύου. Όλες οι μονάδες αποστέλλονται από το εργοστάσιο με την Διεύθυνση μονάδας ορισμένη σε $ FF. Το λογισμικό εγκατάστασης του C-Bus είναι σε θέση να ανιχνεύσει ένα δίκτυο, να εντοπίσει μονάδες που έχουν την ίδια διεύθυνση, και στη συνέχεια μπορεί να εκχώρηση εκ νέου διεύθυνση σε κάθε μονάδα.
- Διεύθυνση εφαρμογής (Application Address): Οι διευθύνσεις εφαρμογής χρησιμοποιούνται για να καθορίσουν την μεταφορά σχετικών πληροφοριών μέσω του δικτύου. Διαφορετικές εφαρμογές μπορεί να μεταβιβάζουν διαφορετικούς τύπους πληροφοριών, ανάλογα με την εφαρμογή. Για παράδειγμα, οι εντολές ελέγχου φωτισμού είναι άσχετες με τις εντολές ενημέρωσης του ρολογιού. Αυτές οι δύο τοποθετούνται σε ξεχωριστές εφαρμογές. Μια μονάδα μπορεί να είναι αποτελεί μέρος σε περισσότερες από μία εφαρμογές.
- Διεύθυνση δικτύου (Network Address): Κατά συνθήκη, η διεύθυνση δικτύου αντιστοιχεί στην διεύθυνση μονάδας στην άλλη πλευρά της γέφυρας, όπως φαίνεται στο σχήμα 2. Μια γέφυρα έχει δύο διευθύνσεις μονάδας, μια σε κάθε δίκτυο. Στο Σχήμα 3.3.3.1, το δικτύου A1 μπορεί να στείλει δεδομένα στο δίκτυο A3.



Σχήμα 3.3.3.1: Διευθύνσεις δικτύου (Network Address):

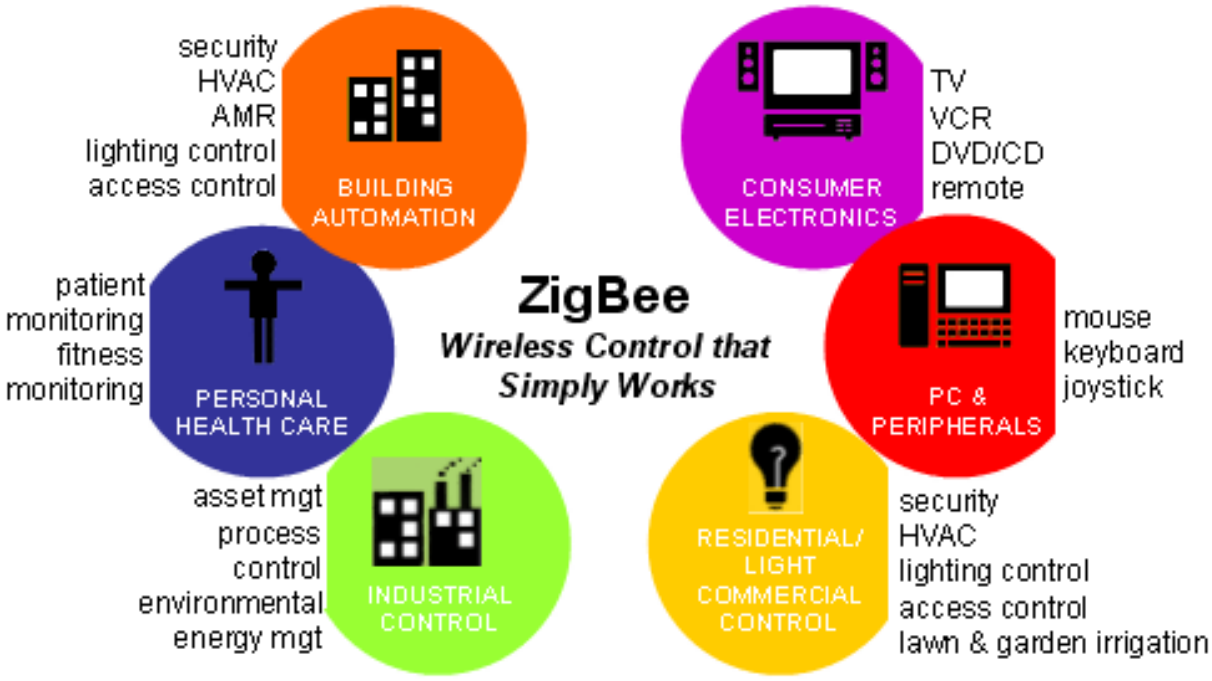
3.4 ZigBee

Το ZigBee είναι ένα ανοιχτό πρωτόκολλο σχεδιασμένο έτσι ώστε να παρέχει μια εύκολη στη χρήση αρχιτεκτονική για ασφαλή, αξιόπιστα, χαμηλής ισχύος ασύρματα δίκτυα. Μαζί με το IEEE 802.15.4 είναι πρότυπα χαμηλού ρυθμού δεδομένων τα οποία μπορούν να εξαλείψουν τις δαπανηρές και επιρρεπείς σε βλάβες καλωδιώσεις για εφαρμογές βιομηχανικού ελέγχου. Ο εξοπλισμός ελέγχου ροής και διεργασιών μπορεί να τοποθετηθεί οπουδήποτε και να εξακολουθεί να επικοινωνεί με το υπόλοιπο σύστημα. Μπορεί επίσης να μετακινηθεί αφού το δίκτυο δεν ενδιαφέρεται για την φυσική τοποθεσία του κάθε αισθητήρα, αντλίας ή βαλβίδας.

Το πρότυπο ZigBee προσφέρει ένα απλό στρώμα δικτύου και τυποποιημένα προφίλ εφαρμογής τα οποία μπορούν να χρησιμοποιηθούν για την δημιουργία διαλειτουργικών λύσεων μεταξύ συσκευών διαφορετικών κατασκευαστών. Τα πλεονεκτήματα αυτής της τεχνολογίας εκτείνονται πολύ πιο πέρα. Το πρότυπο ZigBee μπορεί να υλοποιήσει τις εξής εφαρμογές :

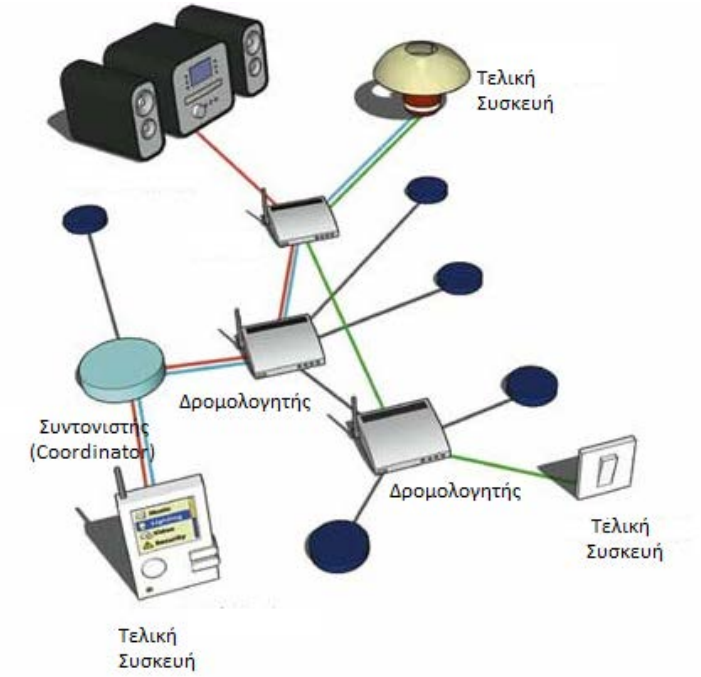
- Αυτοματισμούς για σπίτια και γραφεία.
- Βιομηχανικούς αυτοματισμούς.

- Ιατρική παρακολούθηση.
- Αισθητήρες χαμηλής ισχύος.
- Συστήματα ελέγχου HVAC (Heating, Ventilating and Air Contitioning).
- Πολλές άλλες επιπλέον χρήσεις ελέγχου και παρακολούθησης.



Σχήμα 3.4.1: Εφαρμογές ZigBee

Το ZigBee στοχεύει στην υλοποίηση εφαρμογών για συσκευές χαμηλής ισχύος και χαμηλού ρυθμού δεδομένων. Στο παρακάτω σχήμα (Σχήμα 3.4.2) βλέπουμε ένα παράδειγμα δικτύου ZigBee.



Σχήμα 3.4.2 : Δίκτυο ZigBee

3.4.1 Τύποι συσκευών ZigBee

Οι συσκευές ZigBee αποτελούνται από το συνδυασμό λογικών συσκευών ZigBee (συντονιστές, δρομολογητές , τερματικές συσκευές), δύο τύποι φυσικών συσκευών ZigBee (πλήρους και μειωμένης λειτουργικότητας συσκευές) και εφαρμογών (όπως αισθητήρες φωτός , έλεγχος φωτισμού κτλ).

3.4.1.1 Τύποι λογικών συσκευών ZigBee

Υπάρχουν τρεις κατηγορίες κόμβων σε ένα σύστημα ZigBee, ο συντονιστής οι δρομολογητές και οι τερματικές συσκευές.

- Συντονιστής (Coordinator) : Αποτελεί την ρίζα του δέντρου του δικτύου και μπορεί να γεφυρωθεί με άλλα δίκτυα. Υπάρχει ακριβώς ένας συντονιστής σε κάθε δίκτυο. Είναι υπεύθυνος για την έναρξη του δικτύου και για την επιλογή κάποιων παραμέτρων του δικτύου όπως την συχνότητα του ραδιοκαναλιού, το μοναδικό αναγνωριστικό κώδικα του δικτύου και τον καθορισμό άλλων λειτουργικών παραμέτρων.
- Δρομολογητές (Router) : Οι δρομολογητές λειτουργούν ως ενδιάμεσοι κόμβοι, διαβιβάζοντας δεδομένα από άλλες συσκευές. Οι δρομολογητές μπορούν να συνδεθούν με ένα ήδη υπάρχον δίκτυο, επίσης είναι σε θέση να δεχτούν συνδέσεις από άλλες συσκευές και να αποτελέσουν ένα είδος πομπού αναμετάδοσης στο

δίκτυο. Με την χρήση δρομολογητών ZigBee είναι δυνατή και η επέκταση του δικτύου.

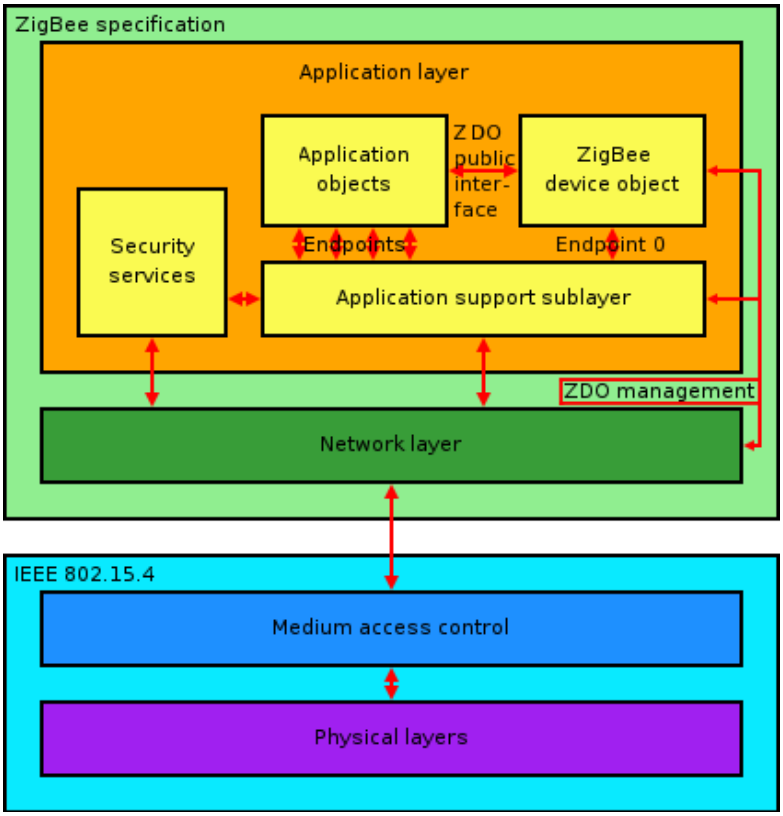
- Τερματικές συσκευές (End Devices) : Οι τερματικές συσκευές μπορεί να είναι χαμηλής ισχύος συσκευές μπαταρίας. Μπορούν να συλλέξουν διάφορες πληροφορίες από αισθητήρες και διακόπτες. Έχουν επαρκή λειτουργικότητα για να επικοινωνήσουν με τους γονείς τους (είτε τον συντονιστή είτε τον δρομολογητή) αλλά δεν μπορούν να αναμεταδίδουν δεδομένα από άλλες συσκευές . Αυτή η μειωμένη λειτουργικότητα επιτρέπει και την μείωση του κόστους τους. Αυτές οι συσκευές δεν χρειάζεται να είναι ξύπνιες όλη την ώρα όπως οι συσκευές που ανήκουν στις άλλες δύο κατηγορίες. Κάθε τερματική συσκευή μπορεί να έχει μέχρι 240 τερματικούς κόμβους οι οποίοι είναι διαφορετικές εφαρμογές που μοιράζονται την ίδια ραδιοσυχνότητα.

3.4.1.2 Τύποι φυσικών συσκευών ZigBee

Το πρότυπο IEEE 802.15.4 παρέχει δύο τύπους φυσικών συσκευών με βάση τις δυνατότητες τους στην επεξεργασία δεδομένων : Συσκευές πλήρους λειτουργικότητας FFD (Full Function Devices) και συσκευές μειωμένης λειτουργικότητας RFD (Reduced Function Devices). Οι συσκευές πλήρους λειτουργικότητας μπορούν να εκτελέσουν όλες τις διαθέσιμες λειτουργίες που περιγράφονται από το πρότυπο συμπεριλαμβανομένων του μηχανισμού δρομολόγησης, καθήκοντα συντονισμού και καθήκοντα ανίχνευσης. Μπορούν να παίξουν τον ρόλο είτε του συντονιστή είτε του δρομολογητή είτε τον ρόλο της τερματικής συσκευής. Η τροφοδοσία μιας τυπικής FFD σε ένα δίκτυο ZigBee γίνεται από συνεχή παροχή ρεύματος καθώς η συσκευή πρέπει να είναι πάντα ενεργή και να ακούει το δίκτυο.

Από την άλλη οι συσκευές μειωμένης λειτουργικότητας υλοποιούν μόνο ένα μέρος του προτύπου IEE 802.15.4. Οι συσκευές RFD δεν δρομολογούν πακέτα και για αυτό το λόγο πρέπει να συνδέονται με κάποια συσκευή FFD. Αυτές είναι τερματικές συσκευές όπως αισθητήρες, ενεργοποιητές οι οποίες εκτελούν περιορισμένα καθήκοντα, όπως η καταγραφή θερμοκρασιών, η παρακολούθηση της κατάστασης του φωτισμού ή ο έλεγχος άλλων εξωτερικών συσκευών.

3.4.2 Αρχιτεκτονική πρωτοκόλλου ZigBee

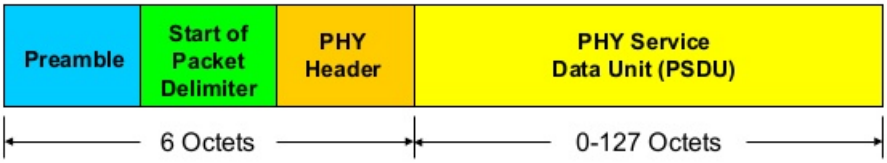


Σχήμα 3.4.2.1: Αρχιτεκτονική πρωτοκόλλου ZigBee

3.4.2.1 Το Φυσικό Στρώμα

Το φυσικό στρώμα του προτύπου IEEE802.15.4 είναι το πιο κοντινό στρώμα στο υλικό, το οποίο ελέγχει και επικοινωνεί άμεσα με τον πομποδέκτη. Χειρίζεται όλες τις διεργασίες που αφορούν την πρόσβαση στο υλικό του ZigBee συμπεριλαμβανομένης της αρχικοποίησης του υλικού, επιλογή καναλιού, εκτίμηση της ποιότητας της σύνδεσης, και σαφή εκτίμηση του καναλιού για να βοηθήσει στην επιλογή του. Υποστηρίζει τρεις ζώνες συχνοτήτων, την ζώνη των 2,4GHz χρησιμοποιώντας 16 κανάλια, την ζώνη των 915MHz χρησιμοποιώντας 10 κανάλια και την ζώνη των 868MHz χρησιμοποιώντας 1 κανάλι. Και οι τρεις χρησιμοποιούν ως τρόπο πρόσβασης την Άμεση Διάδοση Ραδιοσυχνοτήτων Αλληλουχίας (DSSS). Τα πεδία πακέτου του Φυσικού Στρώματος είναι:

- Preamble (32 bits) – Συγχρονισμός
- Start of Packet Delimiter (8 bits)
- PHY Header (8 bits) – PSDU length
- PSDU (0 to 1016 bits) – Data field



Σχήμα 3.4.2.1.1: Δομή Πακέτου

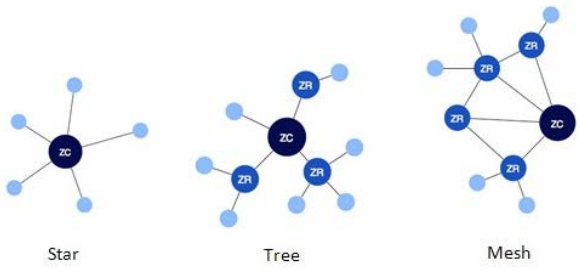
3.4.2.2 Στρώμα MAC

Αυτό το στρώμα παρέχει διασύνδεση μεταξύ του φυσικού στρώματος και του στρώματος δικτύου. Αυτό προσφέρει δύο υπηρεσίες: Υπηρεσίες δεδομένων MAC και υπηρεσίες διαχείρισης MAC. Η υπηρεσία δεδομένων MAC επιτρέπει την μετάδοση και λήψη μονάδων δεδομένων. Καθορίζει τέσσερις δομές πλαισίου : πλαίσιο Beacon, πλαίσιο δεδομένων, αναγνωριστικό πλαίσιο και πλαίσιο εντολής MAC. Βασικά υπάρχουν δύο είδη τοπολογίας , Αστέρας και peer-to-peer(P2P). Η τοπολογία peer-to-peer μπορεί να πάρει διάφορα σχήματα ανάλογα με τους περιορισμούς που έχει. Η peer-to-peer χωρίς περιορισμούς είναι γνωστή ως Mesh (πλέγμα).

Ακόμα μια μορφή είναι η τοπολογία δέντρου. Η διαλειτουργικότητα είναι ένα από τα πλεονεκτήματα της στοίβας πρωτοκόλλου ZigBee. Το ZigBee έχει ένα ευρύ φάσμα εφαρμογών, έτσι διαφορετικοί κατασκευαστές παρέχουν συσκευές ZigBee. Οι συσκευές ZigBee μπορούν να αλληλεπιδρούν μεταξύ τους ανεξάρτητα από τον κατασκευαστή (ακόμα και αν το μήνυμα είναι κρυπτογραφημένο).

3.4.2.3 Στρώμα δικτύου

Το στρώμα δικτύου αποτελεί την διεπαφή μεταξύ στρώματος εφαρμογής και του στρώματος MAC. Αυτό το στρώμα είναι υπεύθυνο για το σχηματισμό του δικτύου και της δρομολόγησης. Παρέχει την ασφάλεια του δικτύου και επιτρέπει σε συσκευές χαμηλής ισχύος να μεγιστοποιήσουν την διάρκεια ζωής της μπαταρίας τους. Από τις βασικές τοπολογίες, υπάρχουν τρεις τοπολογίες δικτύου (Σχήμα 3.4.2.3.1) που εξετάζονται στο IEEE802.15.4, η τοπολογία αστέρα, τοπολογία δέντρου και η τοπολογία Mesh (πλέγμα).



Σχήμα 3.4.2.3.1: τοπολογίες δικτύου

3.4.2.4 Στρώμα Εφαρμογής

Το επίπεδο εφαρμογών είναι το υψηλότερο στρώμα πρωτοκόλλου και φιλοξενεί τα αντικείμενα εφαρμογής. Οι προδιαγραφές του ZigBee χωρίζουν το στρώμα εφαρμογής σε τρία διαφορετικά υποστρώματα. Το υπόστρωμα υποστήριξης εφαρμογών, τα αντικείμενα συσκευών ZigBee και τον σκελετό των εφαρμογών που έχουν καθοριζόμενα από τον κατασκευαστή Αντικείμενα Εφαρμογής.

3.4.3 Συμπεράσματα

Η απόδοση του ZigBee όσον αφορά την ταχύτητα μεταφοράς δεδομένων είναι χαμηλή περίπου 250 kbps. Έτσι, αυτό το σύστημα είναι χρήσιμο για εφαρμογές που χρειάζονται χαμηλό ρυθμό δεδομένων. Μερικές από τις εφαρμογές του είναι :

- Σχεδιασμός Συστήματος Ελέγχου Παρακολούθησης θερμοκηπίου βασισμένο σε δίκτυο ασύρματων αισθητήρων ZigBee
- Σύστημα Παρακολούθησης κενής θέσης στάθμευσης Πολλαπλών Επιπέδων βασισμένο σε ZigBee
- Εφαρμογές ασύρματων δικτύων αισθητήρων στην παρακολούθηση του περιβάλλοντος

Επίσης, οι τυπικές εφαρμογές που υποστηρίζονται είναι Αυτοματισμού και Ελέγχου σπιτιών, αυτόματη ανάγνωση Μετρήσεων, Αυτοματισμοί Κτιρίων, Προσωπική φροντίδα υγείας, παρακολούθηση φυσικής κατάστασης στο σπίτι, στο γυμναστήριο και εν-κίνηση, έξυπνα δίκτυα ενέργειας, παρακολούθηση ασθενούς, Τηλεπικοινωνιακές Υπηρεσίες.

3.5 Z-Wave

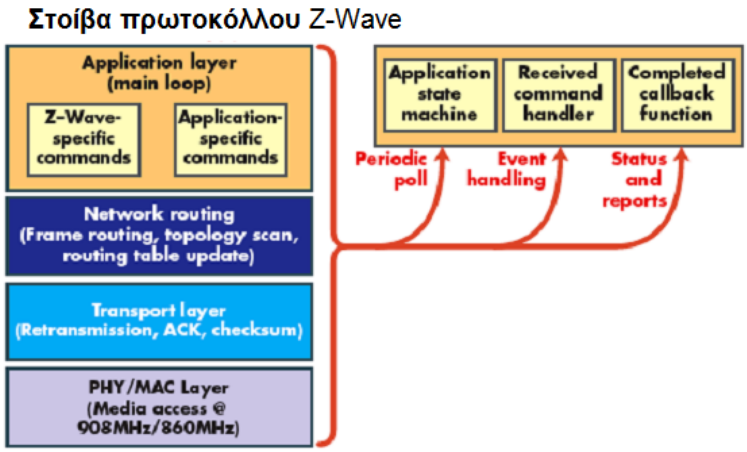
Το Z-Wave είναι ένα ασύρματο πρωτόκολλο που προσανατολίζεται στην αγορά του αυτοματισμού και έλεγχο κτιρίων. Από εννοιολογική άποψη, το Z-Wave έχει ως στόχο να παρέχει μια απλή αλλά αξιόπιστη μέθοδο για ασύρματο έλεγχο του φωτισμού και των συσκευών σε ένα σπίτι. Για να ανταποκριθεί σε αυτές τις παραμέτρους σχεδιασμού, το πακέτο Z-Wave περιλαμβάνει ένα τσιπ με χαμηλό ρυθμό μετάδοσης δεδομένων που προσφέρει αξιόπιστη παράδοση δεδομένων, μαζί με απλότητα και ευελιξία. Το Z-Wave λειτουργεί στην βιομηχανική, επιστημονική και ιατρική ζώνη (ISM) για την ενιαία συχνότητα χρησιμοποιώντας τη μέθοδο μετατόπισης συχνότητας (FSK). Η ρυθμαπόδοση είναι 40 kbps και είναι κατάλληλο για εφαρμογές ελέγχου και αισθητήρες. Κάθε δίκτυο Z-Wave μπορεί να περιλαμβάνει μέχρι 232 κόμβους και αποτελείται από δύο σύνολα κόμβων: ελεγκτών και συσκευών σκλάβων.

Οι κόμβοι μπορούν να ρυθμιστούν ώστε να αναμεταδίδουν το μήνυμα προκειμένου να διασφαλίζεται η συνδεσιμότητα. Η μέση απόσταση επικοινωνίας μεταξύ δύο κόμβων είναι 30 μέτρα και με την ικανότητά του μηνύματος να μεταπηδά μέχρι και τέσσερις φορές μεταξύ κόμβων, δίνει ικανοποιητική κάλυψη για τις περισσότερες κατοικίες. Η συμμαχία Z-Wave είναι μια κοινοπραξία κατασκευαστών που φτιάχνουν προϊόντα που βασίζονται στην πρωτόκολλο Z-Wave. Αρκετές γνωστές εταιρείες είναι ενταγμένες σε αυτή την συμμαχία όπως η Honeywell και η Leviton. Οι πρώτες συσκευές Z-Wave που παρουσιάστηκαν στην αγορά ήταν πακέτα ελέγχου φωτισμού κατοικιών και μπορούν τώρα να βρεθούν στο λιανικό εμπόριο ή στο Internet. Συνήθως, ένα πακέτο εκκίνησης περιλαμβάνει δύο dimmer φωτισμού και ένα κεντρικό ελεγκτή.

3.5.1 Επισκόπηση στοίβας πρωτοκόλλου

Ένας από τους στόχους του Z-Wave ήταν να προσφέρει ένα απλοποιημένο ασύρματο πρωτόκολλο που θα μεταφέρει αξιόπιστα μηνύματα σε μια κατοικία. Η στοίβα Z-Wave αποτελείται από (Σχήμα 3.5.1.1) :

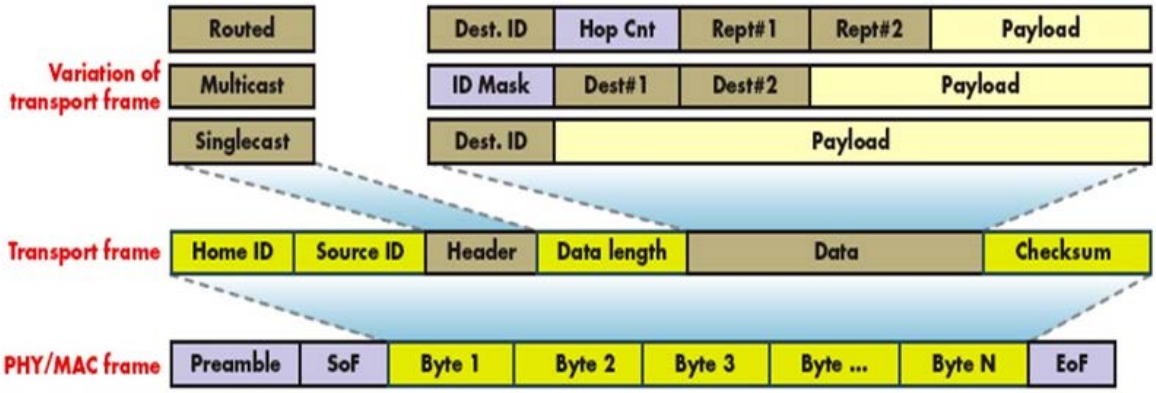
- Φυσικό στρώμα/στρώμα MAC για έλεγχο της πρόσβασης στο μέσο RF
- Στρώμα μεταφοράς που χειρίζεται ελέγχους ακεραιότητας πλαισίου, αναγνωρίσεις, και αναμεταδόσεις.
- Ένα στρώμα δικτύου που χειρίζεται την δρομολόγηση των πλαισίων και παρέχει διεπαφές εφαρμογών.



Σχήμα 3.5.1.1: Στοίβα πρωτοκόλλου Z-Wave

Το Z-Wave λειτουργεί στα 908 MHz (ΗΠΑ) και 860MHz (Ευρώπη). Χρησιμοποιεί διαμόρφωση FSK με κωδικοποίηση καναλιού Μάντσεστερ. Αρχικά το πρωτόκολλο εισήχθη με ταχύτητα δεδομένων 9.600 bits ανά δευτερόλεπτο αλλά επεκτάθηκε αργότερα σε 40 Kbps. Τα δεδομένα μεταφέρονται σε μπλοκ των 8 bit, και το πιο σημαντικό bit στέλνεται πρώτο. Κάθε Φυσικό πλαίσιο/πλαίσιο MAC αρχίζει με ένα προοίμιο συγχρονισμού, μετά ακολουθεί ένα διαχωριστικό Έναρξης Πλαισίου (SoF Start of Frame), ακολούθως τα δεδομένα ωφέλιμου φορτίου, και τελειώνει με ένα διαχωριστικό λήξης πλαισίου (EoF End of Frame) όπως φαίνεται στο σχήμα 2. Το μέγιστο μέγεθος των δεδομένων ωφέλιμου φορτίου είναι 64 bytes. Το πρωτόκολλο Z-Wave χρησιμοποιεί συνήθεις μεθόδους αποφυγής σύγκρουσης, όπου η μετάδοση αναβάλλεται για έναν τυχαίο αριθμό χιλιοστών του δευτερολέπτου, όταν το μέσο μετάδοσης είναι απασχολημένο.

Το στρώμα μεταφοράς του Z-Wave ελέγχει τη μεταφορά δεδομένων μεταξύ δύο κόμβων, συμπεριλαμβανομένου της αναμετάδοσης, του ελέγχου αθροίσματος, και της βεβαίωσης παραλαβής. Χρησιμοποιεί τέσσερις τύπους πλαισίων που μοιράζονται την ίδια δομή διάταξης. Μια επικεφαλίδα πλαισίου προηγείται των δεδομένων ωφέλιμου φορτίου και περιέχει πληροφορίες σχετικά με αναγνωριστικό του δικτύου, το αναγνωριστικό του κόμβου προέλευσης, το μέγεθος του ωφέλιμου φορτίου και τον τύπο του πλαισίου (πλαίσιο δεδομένων, πλαίσιο βεβαίωσης παραλαβής ACK, και πλαίσιο δρομολόγησης). Για την επαλήθευση της ακεραιότητας των δεδομένων, ένα byte αθροίσματος ελέγχου μεταδίδεται στο τέλος του πλαισίου. Εάν το μήνυμα ληφθεί επιτυχώς, ένα πλαίσιο ACK στέλνεται πίσω στον κόμβο προέλευσης. Το πλαίσιο ACK έχει την ίδια μορφή με το κανονικό πλαίσιο, αλλά το μέγεθος του ωφέλιμου φορτίου είναι μηδέν.



Σχήμα 3.5.1.2: Πλαίσιο Z-Wave

Εάν η διεύθυνση προορισμού έχει οριστεί σε 0xFF, το πλαίσιο αντιμετωπίζεται ως εκπομπή και όλοι οι κόμβοι στο δίκτυο λαμβάνουν το ωφέλιμο φορτίο. Παράλληλα, το πλαίσιο μπορεί να φέρει περισσότερες από μία διευθύνσεις προορισμού, γεγονός που το καθιστά πλαίσιο πολλαπλής διανομής (multicast). Σε αυτή την περίπτωση, το ίδιο ωφέλιμο φορτίο θα παραδοθεί μόνο στους επιλεγμένους κόμβους. Το στρώμα δρομολόγησης Z-Wave ελέγχει τη δρομολόγηση των πλαισίων από τον ένα κόμβο στον άλλο. Το στρώμα είναι υπεύθυνο τόσο για την αποστολή ενός πλαισίου με μια σωστή λίστα αναμεταδοτών όσο και στη διασφάλιση ότι το πλαίσιο επαναλαμβάνεται από κόμβο σε κόμβο.

Στην περίπτωση της συσκευής ελέγχου, το στρώμα δρομολόγησης είναι επίσης υπεύθυνο για τη σάρωση εύρεση της τοπολογίας του δικτύου και τη διατήρηση ενός πίνακα δρομολόγησης. Το στρώμα εφαρμογής του Z-Wave είναι υπεύθυνο για την αποκωδικοποίηση και εκτέλεση των εντολών. Το πλαίσιο του στρώματος εφαρμογής περιλαμβάνει μια επικεφαλίδα που περιγράφει τον τύπο του πλαισίου, πληροφορίες εντολών και συναφείς παραμέτρους. Οι εντολές χωρίζονται σε δύο κατηγορίες: εντολές πρωτόκολλου Z-Wave και συγκεκριμένες εντολές για εφαρμογές.

Κάθε δίκτυο Z-Wave έχει ένα μοναδικό αναγνωριστικό 32bit που ονομάζεται Home ID. Οι ελεγκτικές συσκευές έχουν προκαθορισμένο αναγνωριστικό δικτύου (network ID), ενώ συσκευές σκλάβοι αποκτούν το Home ID από τον ελεγκτή κατά την ένταξή τους στο δίκτυο. Αν κάποια άλλη συσκευή ελέγχου ενταχθεί στο δίκτυο, κληρονομεί το Home ID από το κύριο ελεγκτή. Οι μεμονωμένοι κόμβοι στο δίκτυο παίρνουν διεύθυνση χρησιμοποιώντας ένα αναγνωριστικό κόμβου 8 bit (Node ID) το οποίο επίσης εκχωρείται από τον ελεγκτή.

3.5.2 Τύποι συσκευών

Υπάρχουν δύο κύριοι τύποι συσκευών που ορίζονται στο πρωτόκολλο Z-Wave: οι ελεγκτές και οι συσκευές σκλάβοι. Οι ελεγκτές είναι σε θέση να ξεκινήσουν μια μετάδοση καθώς να κρατήσουν όλα τα στοιχεία που σχετίζονται με τις δρομολογήσεις του δικτύου. Οι συσκευές σκλάβοι, από την άλλη πλευρά, είναι απλά συσκευές γενικού σκοπού με λειτουργικότητα τύπου εισόδου-εξόδου (GPIO) που εκτελούν τυφλά αιτήματα του ελεγκτή. Οι ελεγκτές διαφοροποιούνται περαιτέρω ανάλογα με τη λειτουργικότητά τους στο δίκτυο. Οι Κύριοι τύποι ελεγκτών είναι φορητοί και στατικοί.

Ο ορισμός των φορητών ελεγκτών προϋποθέτει ότι οι συσκευές αυτές μπορούν να αλλάζουν τη θέση τους στο δίκτυο ελεύθερα. Έχουν την ικανότητα να ανακαλύπτουν εκ νέου τη θέση τους στο δίκτυο κάνοντας πινγκ στους γύρω κόμβους. Συνήθως οι φορητοί ελεγκτές είναι συσκευές που λειτουργούν με μπαταρία και χρησιμοποιούνται από το χρήστη για να στείλει εντολές στο δίκτυο. Μια δευτερεύουσα αλλά σημαντική λειτουργία του φορητού ελεγκτή είναι να συμπεριλάβει ή να αποκλείει συσκευές στο δίκτυο. Οι στατικοί ελεγκτές έχουν σταθερή θέση στο δίκτυο και τροφοδοτούνται από το ηλεκτρικό δίκτυο. Είναι πάντα σε «κατάσταση ακρόασης», ως εκ τούτου άλλες συσκευές μπορούν να επικοινωνούν μαζί τους ανά πάσα στιγμή. Οι συσκευές σκλάβοι έχουν πολύ πιο απλή λειτουργικότητα από τους ελεγκτές. Δεν μπορούν να ξεκινήσουν μια μετάδοση, εκτός εάν ανταποκρίνονται σε αίτημα ενός ελεγκτή.

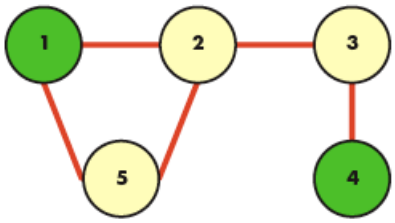
Η διαχείριση των κόμβων στο Z-Wave αποτελείται από δύο κύριες λειτουργίες, ένταξη/αποκλεισμός και συσχέτιση. Η ένταξη εγκαινιάζει ένα νέο κόμβο στο δίκτυο. Το αντίστροφο είναι ο αποκλεισμός, το οποίο περιγράφει τη διαδικασία για την απομάκρυνση ενός κόμβων. Μόνο πρωτοβάθμιοι ελεγκτές μπορούν να εντάξουν και να αποκλείουν κόμβους από και προς το δίκτυο. Η συσχέτιση είναι η δημιουργία της λογικής σύνδεσης μεταξύ των συσκευών. Με άλλα λόγια, η συσχέτιση χρησιμοποιείται για να αναθέσει τι ελέγχει τι. Τόσο οι πρωτοβάθμιοι όσο και οι δευτεροβάθμιοι ελεγκτές μπορούν να δημιουργήσουν συσχετίσεις.

3.5.3 Αρχές δρομολόγησης

Κατά τη διαδικασία ένταξης, ο πρωτεύων ελεγκτής "ρωτά" από την συσκευή σκλάβος να ερευνήσει για άλλες συσκευές Z-Wave προσβάσιμες από τη θέση του. Αυτές οι πληροφορίες αποθηκεύονται σε έναν πίνακα δρομολόγησης, όπως φαίνεται στο σχήμα 3 και

αντιπροσωπεύει τη στιγμιαία τοπολογία του δικτύου. Εάν η θέση των κόμβων αλλάξει, πρέπει να ανακαλυφθεί ξανά η τοπολογία του δικτύου και να ενημερωθεί ο πίνακας δρομολόγησης του ελεγκτή. Το Z-Wave χρησιμοποιεί ένα μηχανισμό δρομολόγησης προέλευσης κατά τον οποίο η συσκευή ελέγχου που εισάγει το μήνυμα δημιουργεί μια πλήρη διαδρομή προς τον τελικό προορισμό μέσω μιας σειράς κόμβων. Η διαδρομή τοποθετείται στο πλαίσιο, και κάθε κόμβος που λαμβάνει το πλαίσιο το προωθεί, ανάλογα με το περιεχόμενο του.

Η δρομολόγηση προέλευσης επιτρέπει την εφαρμογή ενός ελαφρού πρωτόκολλο χωρίς κατανεμημένες πληροφορίες δικτύου. Το μειονέκτημα της προσέγγισης αυτής είναι το αυξημένο μήκος πλαισίου, δεδομένου ότι η διαδρομή θα πρέπει να περιλαμβάνεται μέσα στο ωφέλιμο φορτίο.



	1	2	3	4	5	6
1	0	1	0	0	1	0
2	1	0	1	0	1	0
3	0	1	0	1	0	0
4	0	0	1	0	0	0
5	1	1	0	0	0	0
6	0	0	0	0	0	0

Source: courtesy of Zensys

Σχήμα 3.5.3.1: Πίνακας δρομολόγησης Z-Wave

4

Η Τεχνολογία openHAB

4.1 Εισαγωγή

Το openHAB είναι ένα λογισμικό για την ενοποίηση των διαφόρων συστημάτων και τεχνολογιών οικιακού αυτοματισμού σε μια ενιαία λύση που επιτρέπει την γεφύρωση ανάμεσα στα διάφορα πρωτόκολλα αυτοματισμού και προσφέρει μια ομοιόμορφη διεπαφή χρήστη.

Αυτό σημαίνει ότι το openHAB :

- έχει σχεδιαστεί για να είναι απολύτως ουδέτερο ως προς τον κατασκευαστή, καθώς και αδιάφορο ως προς το πρωτόκολλο και το υλικό που χρησιμοποιείται.
- μπορεί να τρέξει σε οποιαδήποτε συσκευή που είναι ικανή να εκτελεί JVM (Linux, Mac, Windows).
- μας επιτρέπει να ενσωματώνουμε μια πληθώρα διαφορετικών τεχνολογιών οικιακού αυτοματισμού σε ένα ενιαίο σύστημα.
- διαθέτει μια ισχυρή μηχανή κανόνων ώστε να εκπληρώσει όλες τις ανάγκες του αυτοματισμού που χρειαζόμαστε.
- έρχεται με διαφορετικά web-based περιβάλλοντα εργασίας χρήστη, καθώς και περιβάλλον εργασίας χρήστη για iOS και Android.
- είναι πλήρως ανοικτού κώδικα.

- είναι εύκολα επεκτάσιμο ώστε να ενσωματώνει νέα συστήματα και συσκευές.
- παρέχει APIs για να ενσωματωθεί σε άλλα συστήματα.

Υπάρχουν πολλές λύσεις οικιακού αυτοματισμού και Internet-of-Things (IoT) gadgets στην αγορά, τα οποία είναι όλα χρήσιμα από μόνα τους. Κάθε μία από αυτές τις συσκευές έχει τον δικό της τρόπο εγκατάστασης και διαμόρφωσης και είναι ιδανική για την προοριζόμενη χρήση της. Το openHAB δεν προσπαθεί να αντικαταστήσει τις υπάρχουσες λύσεις, αλλά θέλει να τις βελτιώσει - μπορεί έτσι να θεωρηθεί ως ένα σύστημα συστημάτων.

Μια κεντρική ιδέα για το openHAB είναι η έννοια του "στοιχείου". Ένα στοιχείο είναι ένα λειτουργικό δομικό μπλοκ δεδομένων – μπορούμε να το σκεφτούμε ως "ικανότητα". Το openHAB δεν νοιάζεται αν ένα στοιχείο (π.χ. μια τιμή θερμοκρασίας) σχετίζεται με μια φυσική συσκευή ή κάποια "εικονική" πηγή όπως μια υπηρεσία Web ή είναι αποτέλεσμα κάποιου υπολογισμού. Όλες οι δυνατότητες του openHAB προσφέρονται χρησιμοποιώντας αυτή την αφαίρεση του "αντικείμενου", πράγμα που σημαίνει ότι δεν θα βρούμε καμία αναφορά σε συγκεκριμένα χαρακτηριστικά της συσκευής (όπως διευθύνσεις IP, ταυτότητες κλπ) στους κανόνες της αυτοματοποίησης, στους ορισμούς διασύνδεσης χρήστη και ούτω καθεξής. Αυτό καθιστά απολύτως εύκολο να αντικατασταθεί μια τεχνολογία από μια άλλη χωρίς να γίνουν οποιεσδήποτε αλλαγές στους κανόνες και στο περιβάλλον εργασίας χρήστη. Μια πολύ σημαντική πτυχή της αρχιτεκτονικής του openHAB είναι η αρθρωτή σχεδίαση. Είναι πολύ εύκολο να προσθέσουμε νέα χαρακτηριστικά (όπως η ενσωμάτωση ενός ακόμα σύστηματος μέσω ενός " binding ") και μπορούμε να προσθέσουμε και να αφαιρέσουμε αυτά τα χαρακτηριστικά.

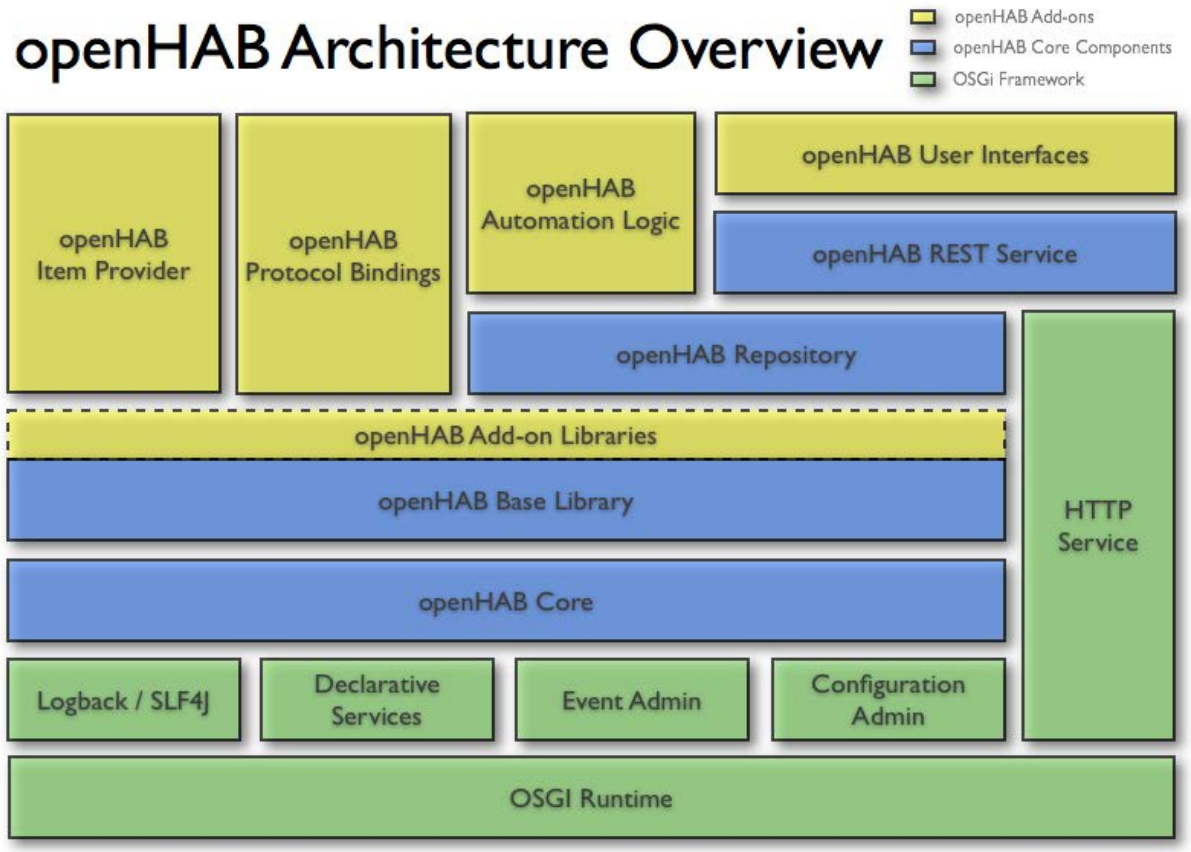
4.2 Αρχιτεκτονική.

Το πρόγραμμα openHAB χωρίζεται σε δύο μέρη: το openhab runtime το οποίο στην πραγματικότητα τρέχει σε έναν εξυπηρετητή και κάνει εκτελεί όλες τις βασικές διεργασίες του πρωτοκόλλου και το openhab designer το οποίο είναι ένα εργαλείο διαμόρφωσης του openhab runtime.

4.2.1 openHAB Runtime

Το runtime openHAB είναι ένα σύνολο από πακέτα OSGi (Open Services Gateway initiative) που έχει αναπτυχθεί σε ένα πλαίσιο OSGi (Equinox). Ως εκ τούτου, είναι μια λύση που

στηρίζεται στη Java και χρειάζεται JVM για να τρέξει. Στο Σχήμα 4.2.1.1 βλέπουμε μία αναφορά πάνω στις κύριες δέσμες (bundles) και πώς εξαρτώνται η μία από την άλλη:



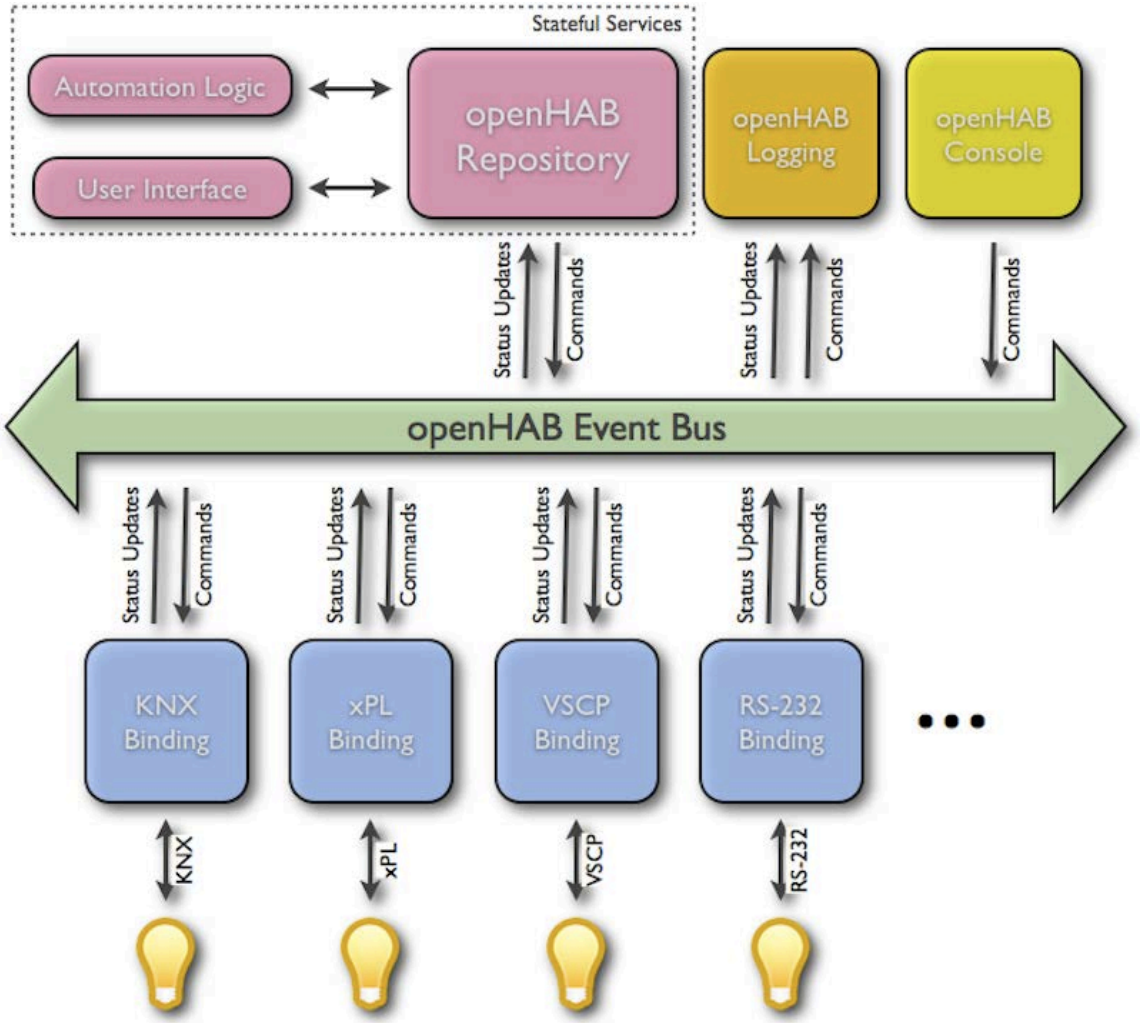
Σχήμα 4.2.1.1: Αρχιτεκτονική openHAB

Το openHAB έχει δύο διαφορετικά κανάλια εσωτερικής επικοινωνίας: ένα ασύγχρονο event bus και ένα σταθερό repository. Το event bus είναι η βασική υπηρεσία του openHAB. Όλες οι δέσμες (bundles) που δεν απαιτούν σταθερή συμπεριφορά πρέπει να το χρησιμοποιούν το event bus για να ενημερώνουν άλλες δέσμες για διάφορα γεγονότα και να ενημερώνονται από άλλες δέσμες για εξωτερικά γεγονότα. Υπάρχουν κυρίως δύο είδη γεγονότων: εντολές που ενεργοποιούν μια ενέργεια ή αλλαγή στην κατάσταση κάποιου στοιχείου/συσκευής και ενημερώσεις κατάστασης που ενημερώνουν για την αλλαγή της κατάστασης κάποιου στοιχείου/συσκευής (συχνά ως απάντηση σε μια εντολή). Όλα τα bindings πρωτόκολλου (που παρέχουν τη σύνδεση με τις πραγματικές συσκευές υλικού) θα πρέπει να επικοινωνούν μέσω του event bus. Αυτό εξασφαλίζει ότι υπάρχει μια πολύ χαλαρή σύνδεση ανάμεσα στις δέσμες, η οποία διευκολύνει τη δυναμική φύση του openHAB.

Το openHAB προσφέρει επίσης το Repository αντικειμένων, το οποίο είναι συνδεδεμένο με το Event bus και παρακολουθεί την τρέχουσα κατάσταση όλων των αντικειμένων. Το

Repository μπορεί να χρησιμοποιηθεί όποτε είναι απαραίτητο να υπάρξει πρόσβαση στην τρέχουσα κατάσταση των αντικειμένων. Π.χ. μια διεπαφή χρήστη θα πρέπει να εμφανίσει την τρέχουσα κατάσταση των αντικειμένων τη στιγμή της πρόσβασης των χρηστών. Επίσης, η λογική μηχανή εκτέλεσης του αυτοματισμού πρέπει πάντα να ενημερώνετε για την τρέχουσα κατάσταση των αντικειμένων.

Το παρακάτω διάγραμμα (Σχήμα 4.2.1.2) δείχνει πώς χρησιμοποιούνται αυτά τα κανάλια επικοινωνίας:



Σχήμα 4.2.1.2: Κανάλια Επικοινωνίας

Το openHAB έρχεται με μια γενική διαμόρφωση των προσφερόμενων προς τον χρήστη διεπαφών: Το λεγόμενο Sitemap. Το sitemap είναι μια δομή δέντρου από widgets, τα οποία καθορίζουν τις διάφορες σελίδες ενός UI και το περιεχόμενό τους. Τα Widgets μπορούν να συσχετιστούν με αντικείμενα, για τα οποία θα πρέπει να δείχνουν την κατάσταση ή/και τα στοιχεία ελέγχου τους. Ο ορισμός του Sitemap είναι αρκετά αφηρημένος από τον σχεδιασμό

του. Υποτίθεται ότι είναι ένα κατάλληλο μοντέλο UI για διαφορετικά είδη διεπαφών χρήστη, έτσι ώστε ο χρήστης δεν χρειάζεται να ρυθμίσει το καθένα από αυτά σε περίπτωση που δημιουργήσει πολλαπλά περιβάλλοντα εργασίας χρήστη. Εάν ένα UI έχει άλλες απαιτήσεις περισσότερες από αυτές του sitemap, είναι δυνατό να εισαχθούν πρόσθετες επιλογές διαμόρφωσης που θα είναι συγκεκριμένες για το εν λόγω UI.

Ως αντικείμενο καθορίζεται το σύνολο όλων των συσκευών ελέγχου, των αισθητήρων ή άλλων πληροφοριών που θέλετε να διατηρούνται στο σύστημά σας . Δεν χρειάζεται να είναι φυσική συσκευή , αλλά ο χρήστης μπορεί να ορίσει και μια πηγή πληροφοριών από το Διαδίκτυο όπως για παράδειγμα μία ιστοσελίδα για τον καιρό ή τις τιμές των μετοχών . Κάθε αντικείμενο μπορεί να ονομαστεί, να ενταχθεί σε πολλές ομάδες (ή καμιά) και να συνδεθεί με μια συγκεκριμένη συσκευή.

Τα Sitemaps ασχολούνται μόνο με τη διεπαφή που εμφανίζεται όταν ο χρήστης εισέρχετε στην εφαρμογή κινητού τηλεφώνου ή στην ιστοσελίδα του OpenHAB. Μέσω του sitemap, μπορεί να ελέγξει πώς ακριβώς θέλει να εμφανίζονται στην οθόνη τα διάφορα κουμπιά ελέγχου και πώς να παρουσιάζονται οι διάφορες πληροφορίες. Δίνει επίσης τη δυνατότητα να καθορίσει διάφορες ομάδες συσκευών ανά δωμάτιο του σπιτιού και επιλέγοντας την κάθε ομάδα να εμφανίζεται αναλυτικά μία λίστα με όλες τις συσκευές που είναι καταχωρημένες στο συγκεκριμένο δωμάτιο. Εναλλακτικά, ο χρήστης μπορεί να διαχωρίσει τις συσκευές ανά είδος, παραδείγματος χάριν να δημιουργήσει μία ομάδα για τον φωτισμό και μία άλλη για τις ηλεκτρικές πρίζες. Μπορεί να υπάρχουν κάποιες συσκευές που χρησιμοποιεί πολύ συχνά και να καθορίσει ένα κουμπί ελέγχου για αυτές στην αρχική οθόνη της εφαρμογής.

Ο οικιακός αυτοματισμός υλοποιείται με βάση τους κανόνες (rules) , όπου ενεργοποιώντας ένα κανόνα μπορείτε να ορίσετε χρονοδιαγράμματα ή προϋποθέσεις για να συμβεί μία δράση. Ένα απλό παράδειγμα θα ήταν το φως στην κρεβατοκάμαρα να αλλάζει σε κόκκινο χρώμα μετά τις 10 το βράδυ. Ένα πιο σύνθετο παράδειγμα κανόνα, θα ήταν να ενεργοποιείται το σύστημα θέρμανσης σε ένα χώρο εάν η θερμοκρασία κατέβει κάτω από 18°C και κάποιος είναι μέσα στο δωμάτιο. Θα βρείτε επίσης ένα φάκελο με προγράμματα (scripts) , το οποίο προσφέρει την ίδια λειτουργικότητα με τους κανόνες, αλλά σε ένα πιο σύνθετο επίπεδο προγραμματιζόμενης λογικής .

Με τον όρο Persistence καθορίζονται τα δεδομένα τα οποία ο χρήστης επιθυμεί να αποθηκεύσει σε αρχείο. Χωρίς πρόσθετη παραμετροποίηση το OpenHAB παρουσιάζει μόνο την τρέχουσα κατάστασης μίας συσκευής. Αν ο χρήστης επιθυμεί να κρατά ιστορικά στοιχεία για τη συγκεκριμένη συσκευή θα πρέπει να το προγραμματίσει ανάλογα το

OpenHAB. Ο χρήστης θα πρέπει να εισάγει παραμέτρους όπως τις συσκευές που επιθυμεί να παρακολουθεί, τα δεδομένα που θέλει να αποθηκεύει και για πόσο καιρό καθώς και το που θα αποθηκεύονται τα δεδομένα αυτά όπως για παράδειγμα σε μία βάση δεδομένων όπως η MySQL ή or σε ένα αρχείο.

Η μετατροπή δεδομένων (transform) χρησιμοποιείται για να αντιστοιχεί τις τιμές δεδομένων που συλλέγονται από τις συσκευές/αισθητήρες σε ετικέτες. Για παράδειγμα, το αρχείο humidex.scale ορίζει ένα εύρος τιμών του δείκτη υγρασίας και πώς θα πρέπει να εμφανίζονται στον χρήστη, για παράδειγμα 29-38 είναι θα μεταφράζεται στην ετικέτα « μερική δυσφορία » .

Το sitemap και τα αρχεία αντικειμένων είναι απαραίτητα για να τρέξει το OpenHAB. Ο χρήστης μπορεί να δημιουργήσει πολλαπλά sitemaps και αντικείμενα, έτσι ώστε να διατηρεί και το δοκιμαστικό sitemap ως σημείο αναφοράς για να επανέρχεται σε αυτό όταν έχει απορίες. Μπορεί επίσης να αλλάξει την διάταξη της διεπαφής ελέγχου και να προσθέσει τις παραμέτρους που επιθυμεί να ελέγχει ανάλογα με τις ανάγκες του.

4.2.2 Σχεδιαστής openHAB

Ο σχεδιαστής openHAB είναι μια εφαρμογή Eclipse RCP (Rich Client Platform) για τη διαμόρφωση του περιβάλλοντος εκτέλεσης του openHAB. Έρχεται με συντάκτες για αρχεία ρυθμίσεων, όπως το sitemap. Το μεγάλο πλεονέκτημα έναντι των απλών επεξεργαστών κειμένου είναι η πλήρης υποστήριξη IDE (integrated development environment) όπως έλεγχος σύνταξης, αυτόματη συμπλήρωση, υπογράμμιση και βοήθεια περιεχόμενου.

4.3 Κανόνες

Το openHAB περιλαμβάνει μια ελαφριά αλλά ταυτόχρονα ισχυρή μηχανή κανόνων. Οι "κανόνες" χρησιμοποιούνται για την αυτοματοποίηση διαδικασιών. Κάθε κανόνας μπορεί να ενεργοποιηθεί, πράγμα το οποίο καλεί ένα σενάριο που εκτελεί κάθε είδους εργασίες, π.χ. άναψε τα φώτα, κάνε μαθηματικούς υπολογισμούς, ξεκίνα χρονόμετρα κτλ.

Οι κανόνες τοποθετούνται στο φάκελο ${openhab.home}/configurations/rules. Το runtime έρχεται με ένα αρχείο επίδειξης που ονομάζεται demo.rules, το οποίο έχει μερικά παραδείγματα τα οποία μπορεί να είναι ένα καλό σημείο εκκίνησης. Ένα αρχείο κανόνων μπορεί να περιέχει πολλαπλούς κανόνες. Όλοι οι κανόνες ενός αρχείου μοιράζονται ένα κοινό πλαίσιο εκτέλεσης, δηλαδή μπορούν ανταλλάσσουν και να έχουν πρόσβαση σε μεταβλητές

το ένα με το άλλο. Είναι επομένως λογικό να έχουμε διαφορετικά αρχεία κανόνων για διαφορετικές περιπτώσεις χρήσης ή κατηγορίες. Ο σχεδιαστής του openHAB προσφέρει πλήρη υποστήριξη IDE για τους κανόνες, η οποία περιλαμβάνει ελέγχους σύνταξης, επικύρωση με δείκτες σφάλματος, βοήθεια περιεχομένου , πρότυπα κ.λπ. Αυτό καθιστά τη δημιουργία κανόνων πολύ εύκολη. Ένα αρχείο κανόνας είναι ένα αρχείο κειμένου με την ακόλουθη δομή:

[Imports] [Εισαγωγή]

[Variable Declarations]

[Rules]

Το τμήμα εισαγωγής περιέχει δηλώσεις εισαγωγής ακριβώς όπως στην Java. Παράδειγμα: import org.openhab.core.library.types.* Το τμήμα δήλωσης μεταβλητών μπορεί να χρησιμοποιηθεί για να δηλώσει μεταβλητές που θα να είναι προσιτές σε όλους τους κανόνες σε αυτό το αρχείο. Μπορούμε να δηλώσουμε μεταβλητές με ή χωρίς αρχικές τιμές και τροποποιήσιμες ή read-only (π.χ var counter = 0). Η ενότητα “Κανόνες” περιέχει μια λίστα με κανόνες. Κάθε κανόνας έχει την ακόλουθη σύνταξη:

```
rule "rule name"
  when
    <TRIGGER CONDITION1> or
    <TRIGGER_CONDITION2> or
    <TRIGGER_CONDITION3>
    ...
  then
    <EXECUTION_BLOCK>
  End
```

Πριν να αρχίσει να δρα ένας κανόνας, θα πρέπει να ενεργοποιηθεί. Υπάρχουν διάφορες κατηγορίες ενεργοποίησης κανόνων:

- Ενεργοποίηση με βάση ένα αντικείμενο: Αντιδρούν σε γεγονότα που εκδηλώνονται στο event bus του openHAB, δηλαδή εντολές και ενημερώσεις κατάστασης για αντικείμενα.

- Ενεργοποίηση με βάση το χρόνο: Αντιδρούν σε ειδικές ώρες, π.χ. τα μεσάνυχτα, κάθε ώρα, κ.λπ.
- Ενεργοποιήσεις που βασίζονται στο σύστημα: Αντιδρούν σε ορισμένες καταστάσεις του συστήματος.

4.4 Υποστηριζόμενες πλατφόρμες και τεχνολογίες

Το openHAB είναι μια πλατφόρμα που βασίζεται καθαρά σε Javaι έτσι ώστε μπορεί να τρέξει οπουδήποτε συσκευή που υποστηρίζει Java. Τρέχει δηλαδή σε οποιοδήποτε πρότυπο Windows, Mac OS X ή Linux μηχάνημα με Java 1.7. Κάθε τεχνολογία ή συσκευή, κοινωνικό δίκτυο ή πλατφόρμα cloud ενσωματωθεί στο openHAB υποστηρίζεται από ένα συγκεκριμένο πακέτο (bundle). Αυτά τα πακέτα (bundles) είναι προαιρετικά και μπορούν να προστεθούν στο openHAB όποτε χρειαστεί. Τα Bindings παρέχουν ενοποίηση με διαφορετικές τεχνολογίες και συσκευές οικιακού αυτοματισμού ενώ υπάρχουν πάρα πολλά άλλα πακέτα που παρέχουν ενσωμάτωση και επικοινωνία με κοινωνικά δίκτυα, instant messaging, πλατφόρμες cloud IoT και πολλά άλλα.

Technology/Device	*Type*	*Tags*	*Status*	*Bundle*	*Since*
Zibase	Device	lighting, heating, shades, security, metering, locks	Production	zwave	1.7.0
Z-Wave	Device	lighting, heating, shades, security, metering, locks	Production	zwave	1.5.0
Yamaha AVR	Device	audio, video	Production	yamaha	1.5.0
xPL	Protocol	homeautomation	Production	xPL	1.5.0
Xively	Cloud	data, graphs	Production	xively	1.3.0
XBMC	MediaCenter	audio, video, pictures	Production	xbmc	1.5.0
X10 (through Insteon PLM)	Device	light, switch, heating	Production	x10	1.7.0
Withings	Device	fitness, quantified self	Production	withings	1.5.0
Waterkotte Ecotouch	Device	heating	Production	ecotouch	1.6.0
Wake on LAN	Protocol	network	Production	wol	0.6.0
WAGO	Device	lighting, heating	Production	wago	1.7.0
Vitotronic	Device	heating	Preview	vitotronic	2.0a2

Vellemann K8055	Device	gpio	Production	k8055	1.5.0
VDR	Device	video, tv	Production	vdr	0.9.0
UC Projects	Device	diy	Production	ucprojects	1.8.0
Twitter	Cloud	social	Production	twitter	1.2.0
Tivo	Device	video, multimedia	Production	tivo	1.4.0
Tinkerforge	Device	io, diy	Production	tinkerforge	1.3.0
Tesla Motors	Device	car	Preview	tesla	2.0a2
Tellstick	Wireless	lighting, sockets, devices	Production	tellstick	1.5.0
TCP/UDP	Protocol	network	Production	tcp	1.1.0
TA CMI	Device	automation	Production	tacmi	1.8.0
System Info	Device	system, network	Production	systeminfo	1.3.0
Swegon	Device	climate, ventilation	Production	swegon	1.1.0
Stiebel Heatpump	Device	heating	Production	stiebelheatpump	1.8.0
Squeezebox	Device	audio, music	Production	squeeze	1.3.0
Souliss	Device	arduino, devices	Production	souliss	1.7.0
Sonos	Device	audio, music	Production	sonos	1.1.0
Sonance	Device	audio, dsp	Production	sonance	1.8.0
Somfy URTSI	Device	shades	Production	urtsi	1.3.0
SNMP	Protocol	network	Production	snmp	0.9.0
SMA Energy Meter	Device	energy meter	Production	smaenergymeter	2.0.0
Serial	Protocol	serial	Production	serial	0.6.0
Sen.se	Cloud	data, graphs	Production	sense	1.3.0
Satel Integra Alarm System	Device	security	Production	satel	1.7.0
Samsung TV	Device	tv, video	Production	samsungtv	1.2.0
Sallegra	Device	lighting, automation	Production	sallegra	1.8.0
SagerWeatherCaster	Algorithm	weather	Production	sagerweathercaster	1.7.0
RWE Smarthome	Device	automation	Production	rwesmarthome	1.8.0
RME Rainmaster	Device	irrigation	Production	-	1.5.0
RFXCOM	Wireless	lighting, heating, security	Production	rfxcom	1.2.0
RCSwitch	Device	diy	Production	rcswitch	1.8.0

Pushover	Cloud	social, messaging	Production	-	1.5.0
Pulseaudio Server	Device	audio, music	Production	pulseaudio	1.2.0
Prowl	Cloud	social, messaging	Production	-	0.6.0
Primare	Device	audio, video	Production	primare	1.7.0
Plugwise	Wireless	lighting, metering	Production	plugwise	1.1.0
Plex	Software	audio, video	Production	plex	1.7.0
PLC Bus	Powerline		Production	plcbus	1.1.0
Pioneer AV Receiver	Device	audio, video	Production	pioneeravr	1.4.0
Pilight	Device		Production	pilight	1.6.0
Piface	Device		Production	piface	1.3.0
Picnet Sapp	Device	automation	Production	picnet	1.8.0
Philips Hue	Wireless	lighting	Production	hue	1.2.0
panSTAMP	Device	automation	Production	panstamp	1.8.0
Panasonic TV	Device	tv	Production	panasonictv	1.7.0
Openpaths	Protocol	geolocation	Production	openpaths	1.4.0
Open Sprinkler	Device	plants	Production	openSprinkler	1.3.0
Open Energy Monitor	Device	energy	Production	openenergymonitor	1.4.0
Onkyo AV Receiver	Device	audio, video	Production	onkyo	1.3.0
One Wire	Wired	lighting, heating, climate	Production	onewire	0.6.0
Octoller	Device	diy	Production	-	1.8.0
Oceanic Water Softener	Device	water	Production	-	1.5.0
NTP	Protocol	date, time	Production	ntp	0.8.0
Novelan/Luxtronic	Device	heating, heatpump	Production	novelanheatpump	1.0.0
Nikobus	Wired	lighting, shades, security	Production	nikobus	1.3.0
Nibe Heat Pump	Device	heating, heatpump	Production	nibeheatpump	1.3.0
Network UPS Tool	Device	network, infrastructure	Production	nut	1.7.0
Network Health	Protocol	network, ping	Production	nh	0.6.0
Netatmo	Device	weather, climate	Production	netatmo	1.4.0

Nest	Device	heating, security	Production	nest	1.7.0
MyStrom	Device	energy	Production	mystrom	1.8.0
MQTTitude	Protocol	location	Production	mqttitude	1.4.0
MQTT	Protocol	message, bus	Production	mqtt	1.3.0
Mpd	Protocol	audio, music	Production	mpd	0.8.0
Modbus	Wired	lighting, heating, metering, ventilation, climate, industrial	Production	modbus	1.1.0
MiOS (Vera)	Device	lighting, heating, shades, security, metering, ventilation, climate	Production	mios	1.6.0
Milight	Wireless	lighting	Production	milight	1.3.0
MAX!Cube	Wireless	lighting, heating, shades, security, metering, ventilation, climate	Production	maxcube	1.4.0
Mailcontrol	Protocol	control	Production	-	1.7.0
Logitech Harmony	Device	remote control	Production	harmony	1.7.0
Lightwave RF	Device	remote control	Production	-	1.7.0
LIFX	Device	light	Preview	lifx	2.0a1
Libelium eHealth Kit	Device	health	Production	-	1.6.0
LG TV	Device	video	Production	lgtv	1.6.0
Leviton/HAI Omnilink	Protocol	home automation, security, lights, thermostats, audio, video	Production	omnilink	1.5.0
LCN	Device	automation	Production	lcn	1.8.0
Koubachi	Wireless	plants	Production	koubachi	1.2.0
KNX	Wired	lighting, heating, shades, security, metering, ventilation, climate	Production	knx	0.1.0
KEBA EV Charging Station	Device	ev, energy	Preview	lifx	2.0a2

Jointspace	Protocol	audio, video	Production	jointspace	1.5.0
IRTrans	Wireless	infrared, climate, audio, video	Production	irtrans	1.5.0
IPX800	Device	automation	Production	ipx800	1.8.0
Insteon PLM	Powerline	lighting, shades, security	Production	insteonplm	1.5.0
Insteon Hub	Powerline	lighting, shades, security	Production	insteonhub	1.4.0
IHC / ELKO	Wired	lighting, heating, shades, security, metering	Production	ihc	1.1.0
IEC 6205621	Device	metering	Production	iec6205621	1.6.0
HTTP	Protocol	http	Production	http	0.6.0
HomeMatic	Wireless	lighting, heating, shades, security, metering	Production	homematic	1.2.0
HMS FHZ 1x00	Device	temperature, humidity	Production	hms	1.7.0
Heatmiser	Wired	heating	Production	heatmiser	1.4.0
HDAnywhere	Device	audio, video	Production	hdanywhere	1.4.0
GPIO	Device	system, gpio	Production	gpio	1.5.0
Google Calendar	Cloud	automation, scheduling	Production	gcal	1.1.0
Frontier Silicon Radio	Device	audio	Production	frontiersilicon	1.7.0
Fritz Box	PBX	telephony, sip	Production	fritzbox	0.7.0
Fritz AHA	Wireless Powerline	lighting, metering	Production	fritzaha	1.3.0
FreeSWITCH	PBX	telephony, sip	Production	freeswitch	1.5.0
Exec	Protocol	cli	Production	exec	0.6.0
Epson Projector	Device	video, projector	Production	epsonprojector	1.3.0
Enphase Energy	Device	pv	Production	enphase	1.7.0
EnOcean	Wireless	lighting, heating, metering	Production	enocean	1.3.0
Enigma2	Device	av	Production	-	1.6.0
Energenie	Device	energy saving	Production	energenie	1.6.0
eKey	Device	fingerprint, security, access control	Production	eKey	1.5.0

ecobee	Device	heating	Production	ecobee	1.7.0
eBus	Protocol	hvac	Production	eBus	1.7.0
DSMR Smartmeter	Device	smart meter	Production	dsmr	1.7.0
DSC Alarm	Serial	security	Production	dscalarm	1.6.0
Dropbox	Cloud	storage	Production	dropbox	1.3.0
DMX	Wired	lighting	Production	dmx	1.2.0
digitalSTROM	Powerline	lighting, metering, shades	Production	digitalstrom	1.3.0
Denon	Device	audio, video	Production	denon	1.7.0
Davis	Device	weather	Production	davis	1.6.0
Daikin	Device	climate	Production	daikin	1.5.0
CUPS	Device	printer	Production	cups	1.1.0
ComfoAir Zehnder	Device	ventilation, climate	Production	comfoair	1.3.0
Chamberlain MyQ	Device	garage	Production	chamberlainmyq	1.8.0
Bticino/Legrand	Device	door communication	Production	bticino	1.7.0
Bluetooth	Wireless	presence, wearables	Production	bluetooth	0.3.0
BenQ Projector	Device	av	Production	benqprojector	1.6.0
Belkin Wemo	Wireless	light, switch	Production	wemo	1.6.0
Autelis	Device	pool	Production	autelis	1.7.0
Astro	System	astronomical time	Production	astro	1.5.0
Asterisk	PBX	telephony, sip	Production	asterisk	0.9.0
Anel NET-PwrCtrl	Device	light, io	Production	anel	1.6.0
AlarmDecoder	Device	security	Production	alarmdecoder	1.6.0
AKM868	Device	presence	Production	akm868	1.8.0

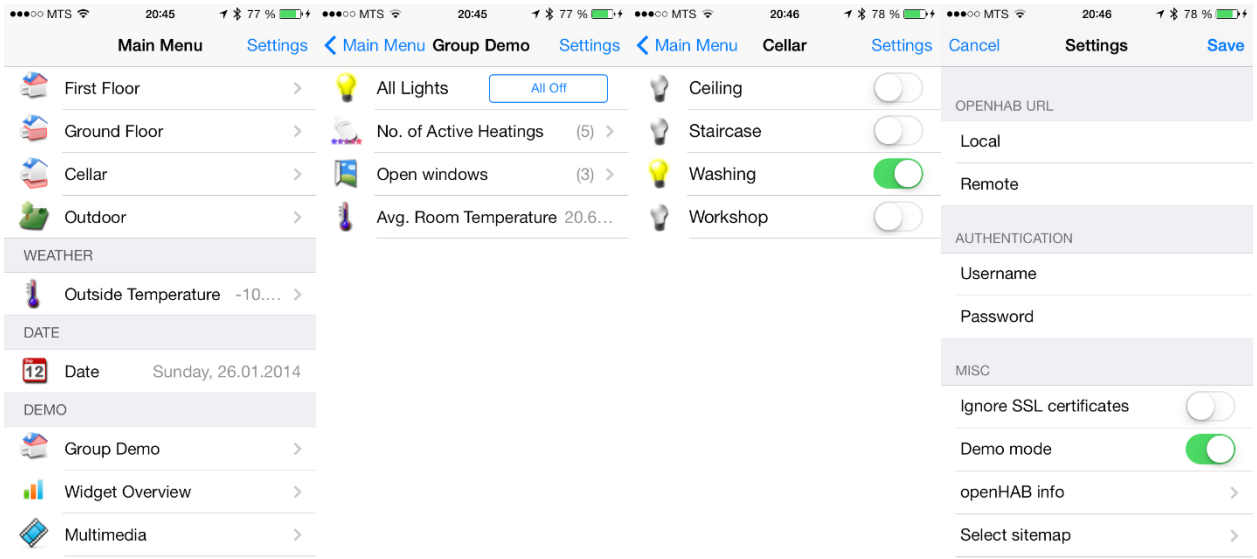
4.5. Διασύνδεση χρήστη

Ένα από τα μοναδικά χαρακτηριστικά τoy openHAB είναι η ενιαία εμπειρία του χρήστη όταν αλληλοεπιδρά με διαφορετικές τεχνολογίες και συσκευές που συνδέονται στο openHAB. Δεν εξαρτάται από κάποιο συγκεκριμένο σύστημα αυτοματισμού. Μπορείς πάντα να έχεις μια απλή ενιαία άποψη από το σπίτι σας ανεξάρτητα από το είδος τις τεχνολογίας που χρησιμοποιείς.

Το Android UI (Σχήμα 4.5.1) υλοποιείται ως μια εγγενής εφαρμογή του Android και είναι διαθέσιμη στο Google Play δωρεάν. Και τα τηλέφωνα και οι ταμπλέτες υποστηρίζονται από την παρούσα εφαρμογή.

Σχήμα 4.5.1 : Android UI

Το iOS UI (Σχήμα 4.5.2) υλοποιείται ως εγγενής iOS 7 εφαρμογή η οποία είναι διαθέσιμη στο AppStore δωρεάν. Και τα τηλέφωνα και οι ταμπλέτες υποστηρίζονται στην παρούσα εφαρμογή.



Σχήμα 4.5.2: iOS UI

Το Classic UI (Σχήμα 4.5.3) είναι η πρώτη γενιά διεπαφής χρήστη του openHAB. Είναι μια διεπαφή web-based στο πλαίσιο WebApp.Net και μπορεί να προσπελαστεί μέσω οποιουδήποτε web browser. Παρά το γεγονός ότι το WebApp.Net είναι μια καθαρή HTML JS

λύση, μιμείται τις εφαρμογές iPhone και έχει βελτιστοποιηθεί για λειτουργία αφής. Δεν λειτουργεί μόνο στο iPhone / iPod touch, αλλά λειτουργεί τέλεια και στο Android. Ακόμη υποστηρίζονται Symbian και Blackberrys και φυσικά όλοι οι web browsers. Έτσι, όπου κι αν βρισκόμαστε και ό, τι συσκευή έχουμε στη διάθεσή μας θα πρέπει να είμαστε σε θέση να έχουμε πρόσβαση στο UI για να λειτουργούμε το σπίτι μας.

Σχήμα 4.5.3: Classic UI

5

Παραδείγματα Εφαρμογής

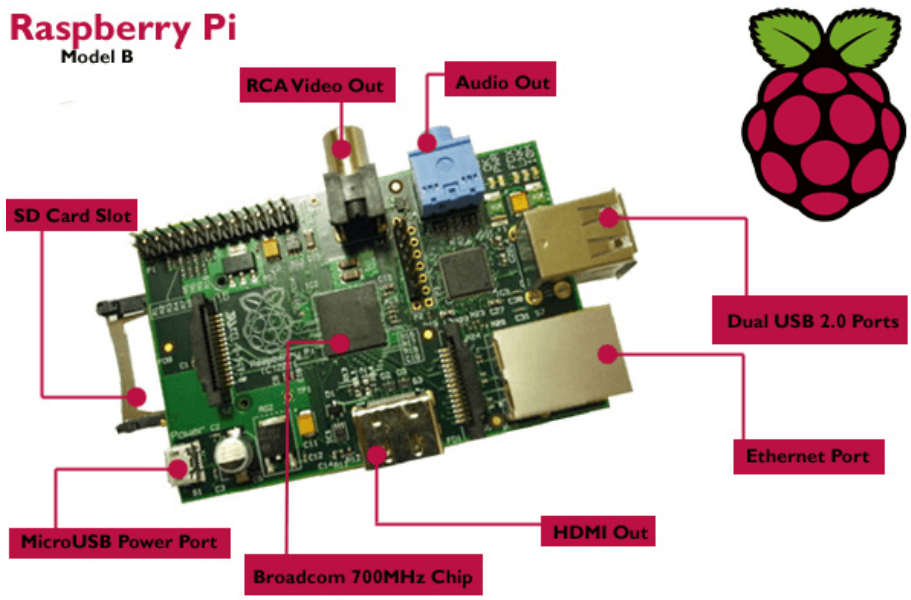
5.1 Εισαγωγή

Στο κεφάλαιο αυτό θα δούμε μια πρακτική εφαρμογή του openHAB. Θα εγκαταστήσουμε το λογισμικό σε μια πλατφόρμα Raspberry Pi η οποία θα παίξει τον ρόλο του κεντρικού επεξεργαστή του όλου συστήματος από όπου θα ελέγχονται οι διάφορες άλλες συσκευές. Ακολούθως θα προσθέσουμε κάποια bindings και προφίλ για διάφορες συσκευές και συγκεκριμένα για το έξυπνο σύστημα λαμπτήρων της Philips το Philips HUE.

Το επόμενο βήμα είναι να ενεργοποιήσουμε την απομακρυσμένη πρόσβαση στο όλο σύστημα ώστε ο χρήστης να μπορεί να ελέγχει το σπίτι του από οπουδήποτε με πρόσβαση στο διαδίκτυο. Ακόμη θα εγκαταστήσουμε στο κινητό μας την εφαρμογή openHAB mobile app ώστε να έχουμε ένα γραφικό περιβάλλον πρόσβασης στο σύστημα από το κινητό μας. Τέλος στην τελευταία ενότητα θα αναδείξουμε την χρησιμότητα του openHAB παρουσιάζοντας κάποια σενάρια αυτοματισμού σπιτιών τα οποία δεν θα ήταν δυνατο να πραγματοποιηθούν χωρίς το openHAB το οποίο αποτελεί τον συνδετικό κρίκο ανάμεσα στις διάφορες τεχνολογίες και πρωτόκολλα αυτοματισμού που κυκλοφορούν στην αγορά.

5.2 *Εγκατάσταση openHAB σε Ruspberry-pi*

Στο παράδειγμα μας θα χρησιμοποιήσουμε το Raspberry Pi model B (Σχήμα 5.2.1) στο οποίο αρχικά έχουμε εγκαταστήσει το Raspbian το επίσημο υποστηριζόμενο λειτουργικό σύστημα της πλατφόρμας Raspberry Pi.



Σχήμα 5.2.1: Raspberry Pi model B

Συνδέουμε το Raspberry Pi με τον υπολογιστή μας μέσω ενός καλωδίου δικτύου. Η περιήγηση γίνεται μέσω SSH και η εγκατάσταση του openHAB γίνεται από την γραμμή εντολής με τις ακόλουθες εντολές:

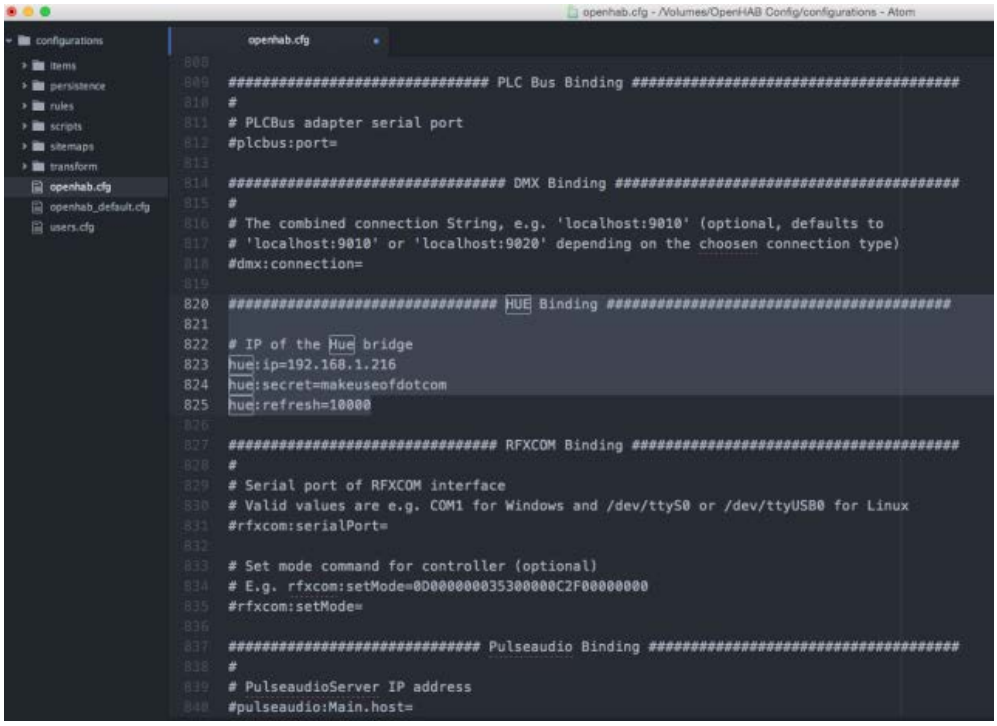
- sudo raspi-config

5.3 *Προσθήκη Philips-Hue*

Η αλληλεπίδραση του openHAB με άλλες συσκευές και αντικείμενα γίνεται μέσω των bindings (μπορούμε να σκεφτούμε τα bindings σαν ένα πρόγραμμα οδήγησης συσκευής).Για να γίνει η εγκατάσταση ενός Binding στο Raspberry Pi πρέπει πρώτα να γίνει λήψη από την ιστοσελίδα του openHAB όπου υπάρχουν πέρα των 160 bindings για διάφορες συσκευές. Ο ευκολότερος τρόπος για να γίνει αυτό είναι χρησιμοποιώντας την εντολή apt-get :

```
sudo apt-get install openhab-addon-binding-hue
sudo chown -hR openhab:openhab /usr/share/openhab
```

Στη συνέχεια θα πρέπει να πούμε στο OpenHAB να φορτώσει αυτό το binding και να ρυθμίσει όποιες μεταβλητές απαιτούνται. Το μόνο πράγμα που πρέπει να αλλάξει στην προκειμένη περίπτωση είναι η τιμή IP της γέφυρας HUE.



Στη συνέχεια, ανοίγουμε το αρχείο home.items, στο οποίο θα προσθέσουμε την λαμπτήρα Hue. Ακολούθως ορίζουμε το στοιχείο:

```
Color Bedroom_Hue "Bedroom Hue" <hue> (Bedroom) {hue="1"}
```

- Η λέξη Color διευκρινίζει τι είδους έλεγχο έχουμε πάνω σε αυτό το αντικείμενο. Οι λαμπτήρες RGB Hue είναι "Color", δεδομένου ότι έχουμε πλήρη έλεγχο ως προς το χρώμα τους. Άλλα φώτα μπορεί απλά να είναι ένας διακόπτη ON/OFF.
- Επόμενη είναι η κωδική ονομασία του αντικειμένου: Επέλεξα Bedroom_Hue, - επειδή είναι κάτι περιγραφικό , γιατί θα πρέπει να το θυμόμαστε αργότερα, όταν κάνουμε το sitemap. Η κωδική ονομασία δεν πρέπει να έχει κενά.
- Ανάμεσα στα εισαγωγικά είναι η ετικέτα. Η δική μας είναι απλή σε αυτή την περίπτωση, αλλά για ορισμένα στοιχεία όπως η θερμοκρασία ή κάτι που αναφέρει μια τιμή, θα πρέπει να προσθέσουμε κάποιο ειδικό κωδικό που να λέει πώς να εμφανίζετε αυτήν η τιμή. Η ετικέτα είναι για τη διασύνδεση, και μπορεί να έχει κενά.
- Μεταξύ των αγκύλων είναι το όνομα του εικονιδίου. Μπορούμε να βρούμε όλα τα διαθέσιμα εικονίδια του OpenHAB, κάτω από τον κατάλογο webapps/εικόνες. Υπάρχει στην πραγματικότητα μια ολόκληρη σειρά από εικονίδια που αντιπροσωπεύουν διαφορετικές αποχρώσεις, λαμπρότητες ή λειτουργίες on / off.

- Στις παρενθέσεις δηλώνουμε σε ποιες ομάδες θα λαμβάνει μέρος - σε αυτή την περίπτωση, μόνο στη ομάδα υπνοδωμάτιο.
- Τέλος, συνδέουμε το αντικείμενο με το κατάλληλο binding και τις μεταβλητές που απαιτούνται. Σε αυτήν την περίπτωση, έχουμε το hue binding και αριθμό λαμπτήρων 1.

Έχουμε προσθέσει συνολικά δύο λαμπτήρες, καθώς και μια απλή δήλωση των ομάδων που ανήκουν. Εδώ είναι το πλήρης home.items μου :

```
Group Bedroom
Group Office
Group Lights

* Lights */
Color Bedroom_Hue "Bedroom Hue" <hue> (Bedroom,Lights) {hue="1"}
Color Office_Hue "Office Hue" <hue> (Office, Lights) {hue="2"}
```

Τώρα που έχουμε προσθέσει τις συσκευές θα δημιουργήσουμε τα στοιχεία διεπαφής στο sitemap:

```
sitemap home label="My Home"
{
 Frame {
  Group item=Lights label="All lighting" icon="hue"
  Group item=Bedroom label="Bedroom" icon="bedroom"
  Group item=Office label="Office" icon="desk"
 }
}
```

Στο πρόγραμμα περιήγησης εμφανίζεται το εξής :

5.4 Απομακρυσμένη πρόσβαση με την διαδικτυακή υπηρεσία MyOpenHAB.

Μέχρι τώρα, θα πρέπει να βρισκόμαστε στο ίδιο τοπικό δίκτυο για να έχουμε πρόσβαση στο openHAB. Για να ελέγξουμε τις συσκευές και τους αισθητήρες του αυτοματισμού μας, όταν είμαστε εκτός της εμβέλειας του Wi-Fi μας, θα πρέπει να ρυθμίσουμε την απομακρυσμένη πρόσβαση με την υπηρεσία web My.OpenHAB, η οποία παρακάμπτει την ανάγκη για ασχοληθούμε με την προώθηση θυρών (port forwarding) και τις ρυθμίσεις του δρομολογητή. Πρώτα κάνουμε εγκατάσταση του αντίστοιχου binding:

```
sudo apt-get install openhab-addon-io-myopenhab
sudo chown -hR openhab:openhab /usr/share/openhab
```

Για να μπορέσουμε να εγγραφούμε στην ιστοσελίδα My.OpenHAB, θα χρειαστεί να δημιουργήσουμε ένα μυστικό κλειδί, και να βρούμε το UUID μας, το οποίο προσδιορίζει μοναδικά την εγκατάσταση μας. Ελέγχουμε κάτω από το OpenHAB Home share -> webapps -> static όπου βρίσκουμε ένα αρχείο UUID που περιέχει το μοναδικό αναγνωριστικό μας. Ακολούθως πρέπει επίσης να βρούμε ένα αρχείο στο φάκελο webapps/static με την ονομασία secret. Ανοίγουμε και τα δύο αρχεία secret and uuid, και αντιγράφουμε τα στοιχεία που υπάρχουν σε αυτά τα αρχεία για να δημιουργήσουμε λογαριασμό στο My.OpenHAB .

5.5 Προγραμματισμός Σεναρίων.

Χρησιμοποιώντας τα κατάλληλα bindings μπορούμε να προσθέσουμε όσες έξυπνες συσκευές θέλουμε στο σύστημά μας. Μετά από αυτό μπορούμε να χρησιμοποιήσουμε όλες αυτές τις συσκευές σαν ένα ενιαίο σύστημα και να δημιουργήσουμε διάφορα σενάρια τα οποία θα μας προσφέρουν περισσότερη άνεση στο σπίτι, εξοικονόμηση ενέργειας και ασφάλεια. Παρακάτω περιγράφουμε μερικά από αυτά τα σενάρια σαν παραδείγματα. Πάντως οι επιλογές μας στην διαμόρφωση σεναρίων είναι ανεξάντλητες και περιορίζονται μόνο από την φαντασία μας.

6

Επίλογος – Συμπεράσματα

6.1 Εισαγωγή

Στην παρούσα διπλωματική εργασία αρχικά παρουσιάστηκαν τα κύρια πρωτόκολλα (KNX, c-bus, Zigbee, zwave) που χρησιμοποιούνται στα συστήματα αυτοματισμού κτιρίων καθώς και την νέα τάση της τεχνολογίας που ονομάζεται διαδίκτυο των πραγμάτων. Στη συνέχεια παρουσιάστηκε μια πλατφόρμα που συνδυάζει όλες αυτές τις τεχνολογίες σε ένα ενιαίο σύστημα μέσω του ανοιχτού λογισμικού openHAB. Το κεφάλαιο αυτό αποτελεί τον επίλογο της διπλωματικής εργασίας όπου παρατίθενται τα κυριότερα συμπεράσματα που εξήχθησαν καθ' όλη τη διάρκεια εκπόνησης της διπλωματικής και παρουσιάζονται οι προοπτικές που αναπτύσσονται από την χρήση του ανοιχτού λογισμικού openHAB.

6.2 Συμπεράσματα και αξιολόγηση openHAB

Το επόμενο κύμα στην εποχή των υπολογιστών θα είναι έξω από τη σφαίρα του παραδοσιακού desktop. Στο Ίντερνετ των πραγμάτων (IoT), πολλά από τα αντικείμενα που μας περιβάλλουν θα είναι στο δίκτυο με τη μία μορφή ή την άλλη. Μέχρι το τέλος της δεκαετίας, αναμένεται να υπάρχουν δεκάδες συνδεδεμένες συσκευές ανά ανθρώπινο ον στον πλανήτη με την ετήσια αύξηση να εκτιμάται σε 20%. Στο δρόμο προς την «Πλατφόρμα για Συνδεδεμένα Έξυπνα αντικείμενα" η μεγαλύτερη πρόκληση θα είναι να ξεπεραστεί ο

κατακερματισμός σε κλειστά συστήματα και αρχιτεκτονικές προς τα ανοικτά συστήματα και ολοκληρωμένα περιβάλλοντα και πλατφόρμες.

Μέσω της μελέτης που έχει διεξαχθεί γίνετε αντιληπτό ότι υπάρχει μια πληθώρα κατασκευαστών αυτοματισμών κτιρίων καθώς και έξυπνων συσκευών οι οποίοι χρησιμοποιούν ένα φάσμα διαφορετικών πρωτοκόλλων. Το openHAB μέσω του κατάλληλου προγραμματισμού αποτελεί ένα δυνατό εργαλείο για ενοποίηση όλων αυτών των τεχνολογιών και συσκευών σε μια πλατφόρμα και την δημιουργία ενός ενιαίου συστήματος. Το ενιαίο αυτό σύστημα οδηγεί όχι μόνο στην αξιοποίηση των δυνατοτήτων κάθε συσκευής χωριστά αλλά στην δημιουργία ενός ολοκληρωμένου συστήματος αυτοματισμού στο οποίο γίνετε δυνατή η επικοινωνία μεταξύ όλων αυτών των συσκευών. Με τον τρόπο αυτό μπορούμε να πετύχουμε μεγαλύτερο βαθμό άνεσης, σωστότερη διαχείριση ενέργειας και προγραμματισμό διαφόρων σεναρίων.

Σκοπός λοιπόν της διπλωματικής εργασίας ήταν η δημιουργία αυτής της πλατφόρμας μέσω του openHAB. Η υλοποίηση έγινε σε δύο στάδια. Αρχικά έγινε η εγκατάσταση του λογισμικού του openHAB σε μια συσκευή Raspberry Pi για να προσδώσουμε στο Raspberry Pi την δυνατότητα ελέγχου του συστήματος κτιριακού αυτοματισμού. Στο επόμενο στάδιο έγινε η εγκατάσταση μιας "έξυπνης" συσκευής λαμπτήρα από την κατασκευάστρια εταιρία Philips μέσω του κατάλληλου binding. Προγραμματίζοντας το openHAB πετύχαμε τον έλεγχο του λαμπτήρα μέσω του γραφικού περιβάλλοντος του openHAB πετυχαίνοντας έτσι την ενσωμάτωση του Philips hue. Από εκεί και πέρα με τον σωστό προγραμματισμό υλοποιήσαμε κάποια σενάρια αυτοματισμού.

6.3 Προοπτικές

Στην παρούσα διπλωματική επιτεύχθηκε η εγκατάσταση και η λειτουργία του λαμπτήρα Philips Hue στην πλατφόρμα ανοικτού κώδικα λογισμικού openHAB. Αυτό ήταν το πρώτο βήμα για την υλοποίηση ενός ολοκληρωμένου συστήματος αυτοματισμού κτιρίου. Ακολουθώντας την ίδια διαδικασία με πιο πάνω μπορούμε να προσθέσουμε όσες έξυπνες συσκευές θέλουμε από διάφορους κατασκευαστές και να φτιάξουμε ένα ολοκληρωμένο σύστημα για τις δικές μας ανάγκες χωρίς περιορισμούς ως προς τον κατασκευαστή και ως προς τις δυνατότητες του συστήματος.

7

Βιβλιογραφία

[MOP16] Morgan J., A Simple Explanation of the Internet of Things, Forbes, May 2016, http://www.forbes.com/sites/jacobmorgan/#38233f418e4a

[BRI16] Britton K., Handling Privacy and Security in the Internet of Things, Journal of Internet Law, April 2016.

[SFB16] Scuotto V., Ferraris A., Bresciani S., Internet of Things, Business Process Management Journal, Vol.22 Issue2 pp.357–367, May 2016, http://dx.doi.org/10.1108/BPMJ-05-2015-0074

[ASH16] Ashour H., Energy Saving Through Smart Home, The Online Journal on Power and Energy Engineering, Vol.2, No.3, June 2016, http://www.infomesr.org/attachments/053.pdf

[CLO16] Cloudrail, The difference between IoE and IoT, June 2016, http://cloudrail.com/internet-of-everything-vs-internet-of-things

[WIL16] Williams J.L., Privacy in the age of the Internet of Things, Human Rights, 00468185, Vol. 41, Issue 4, 2016.

[BOJ15] Bojanova I., What makes up the Internet of Things, March 2015, https://www.computer.org/web/sensing-iot/content?g=53926943&type=article&urlTitle=what-are-the-components-of-iot-

[NEW14] Newman L.H., Pretty much every smart home device you can think of has been hacked, December 2016.
http://www.slate.com/blogs/future_tense/2014/12/30/the_internet_of_things_is_a_long_way_from_being_secure.html

[HP015] Hewlett Packard, Internet of Things – Research Study, 2015 http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf

[ZET15] Zetter K., Medical Devices that are Vulnerable to life threading hacks, November 2015, http://www.wired.com/2014/04hospital-equipment-vulnerable.

[MAC15] MacGullivray, Worldwide Internet of things forecast 2015 – 2020, May 2015.

[MEH15] Mehta Y., 5 Great Internet of Things examples with their applications, December 2015.
http://www.business2community.com/business-innovation/5-great-internet-things-iot-examples-applications-01406647#IyHrkk2xLkqTlAUc.99

[CIC15] Cisco Publications, AT&T Digital Life - Home Security and Automation Service, March 2015.
http://www.cisco.com/c/en/us/solutions/collateral/service-provider/vni-service-adoption-forecast/Cisco_ATT_DigitalLife_CS.html

[EUR09] EUR-Lex, European Union Law, Internet of Things, September 2009, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Asi0009

[EUR13] European Commission, Conclusions of the Internet of Things public consultation, February 2013. https://ec.europa.eu/digital-single-market/news/conclusions-internet-things-public-consultation j

[CLI08] Clipsal Integrated Systems, Serial Interface User Guide – C-Bus Serial Interface & C-Bus Devalopment kid, December 2008. http://training.clipsal.com/downloads/OpenCBus/Serial%20Interface%20User%20Guide.pdf

[KNX16] KNX, The KNX standard basics, 2016, https://www.knx.org/knx-en/knx/association/introduction/index.php

[GBM+] Gubbia J., Buyyab R., Marusic S., Palaniswami M., Internet of Things (IoT): A vision, architectural elements, and future directions, Future Generation Computer Systems, 2013.
http://www.buyya.com/papers/Internet-of-Things-Vision-Future2013.pdf

[CZE11] Department of Control Engineering Faculty of Electrical Engineering Czech Technical University, Buses, Protocols and Systems for Home and Building Automation, 2011. http://www.tecnolab.ws/pdf/Buses,%20Protocols%20and%20Systems%20for%20Home%20and%20Building%20Automation.pdf

[TOM11] Tomar A., Introduction to Zibgbee Technology", Global Technology Centre, Volume 1, July 2011

[GAL06] Galeev M., Catching the Z-Wave, Electronic Engineering Times India, October 2006. http://www.drdobbs.com/embedded-systems/catching-the-z-wave/193104353

[SOY12] Somani N. A., Patel Y., ZIGBEE: A LOW POWER WIRELESS TECHNOLOGY FOR INDUSTRIAL APPLICATIONS, International Journal of Control Theory and Computer Modelling (IJCTCM) Vol.2, No.3, May 2012. http://airccse.org/journal/ijctcm/papers/2312ijctcm03.pdf