ΜΑΡΤΙΟΣ 2016 ΤΜΗΜΑ ΑΥΤΟΜΑΤΙΣΜΟΥ

ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΠΕΙΡΑΙΑ

Α.Τ.Ε.Ι ΠΕΙΡΑΙΑ

Τίτλος : Σχεδιασμός και ανάπτυξη συστημάτων ελέγχου και επικοινωνίας συστημάτων ασφαλείας κτιρίων

Ον/μο Σπουδαστή:Λάμπρου Παναγιώτης

Ον/μο Επιβλέποντα Καθηγητή : Παπουτσιδάκης Μιχάλης

Νικολάου Γρηγόρης

Δρόσος Χρήστος

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ

ΤΜΗΜΑ ΑΥΤΟΜΑΤΙΣΜΟΥ

ΜΑΡΤΙΟΣ 2016

ΤΜΗΜΑ ΑΥΤΟΜΑΤΙΣΜΟΥ

Π.Ράλλη & Θηβών 250,12244 Αιγάλεω,Αθήνα -Ελλάδα

Τηλ:210-5381488

Περίληψη

Η παρούσα πτυχιακή εργασία αποτελεί μια ανασκόπηση των συστημάτων συναγερμού. Αρχικά, περιγράφεται η δομή και τα κύρια μέρη των συστημάτων αυτών. Παρουσιάζονται τα διάφορα είδη αισθητήρων που μπορούν να χρησιμοποιηθούν ανάλογα με την εφαρμογή, ο τρόπος διασύνδεσής τους, καθώς και η επικοινωνία του συστήματος με το κέντρο λήψης σημάτων. Τονίζεται η σημασία των πρωτοκόλλων επικοινωνίας μεταξύ του συστήματος και του κέντρου λήψης σημάτων και περιγράφεται το πιο διαδεδομένο από τα πρωτόκολλα αυτά, το Ademco Contact ID. Στη συνέχεια της εργασίας γίνεται αναφορά στα δίκτυα PSTN και GSM και στους αντίστοιχους κωδικοποιητές που μπορούν να χρησιμοποιηθούν. Ακόμη περιγράφονται οι πιο σύγχρονες τεχνολογίες που μπορούν να εφαρμοσθούν στα συστήματα συναγερμού, οι οποίες περιλαμβάνουν τη χρήση internet, με σκοπό τον απομακρυσμένο έλεγχο του συστήματος μέσω ηλεκτρονικού υπολογιστή ή μέσω εφαρμογής σε smartphone, παρουσιάζοντας συγκεκριμένα παραδείγματα από την ελληνική αγορά. Γίνεται αναφορά στα θέματα ασφάλειας που εγείρονται από τη χρήση συστημάτων απομακρυσμένου ελέγχου και στο τρόπο επίλυσής τους. Τέλος παρουσιάζονται τα συμπεράσματα και οι προεκτάσεις της συγκεκριμένης εργασίας ως προς τα συστήματα συναγερμού.

Λέξεις κλειδιά: Συστήματα συναγερμού, Πρωτόκολλα επικοινωνίας, Ademco Contact ID, Δίκτυα επικοινωνίας, Σύγχρονες τεχνολογίες.

Summary

This thesis is an overview of the alarm systems. Initially, describes the structure and the main parts of these systems. Shows the various types of sensors that can be used depending on the application, the manner of their interconnection and communication system with the monitoring station. The importance of communication protocols between the system and the alarm receiving center and described the most common of these protocols, the Ademco Contact ID. Then the project is reported in PSTN and GSM networks and to the respective encoders can be used. Even describing the latest technologies that can be applied to alarm systems, which include the use of internet, aiming the remote control system via computer or by application of a smartphone, presenting concrete examples from the Greek market. Reference is made to the security issues raised by the use of remote control systems and how to resolve them. Finally presents the findings and implications of this study with regard to alarm systems.

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος Λάμπρου Παναγιώτης του Δημητρίου, με αριθμό μητρώου 25041 φοιτητής του Τμήματος **Μηχανικών Αυτοματισμού Τ.Ε.** του Α.Ε.Ι. Πειραιά Τ.Τ. πριν αναλάβω την εκπόνηση της Πτυχιακής Εργασίας μου, δηλώνω ότι ενημερώθηκα για τα παρακάτω:

«Η Πτυχιακή Εργασία (Π.Ε.) αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο του συγγραφέα, όσο και του Ιδρύματος και θα πρέπει να έχει μοναδικό χαρακτήρα και πρωτότυπο περιεχόμενο.

Απαγορεύεται αυστηρά οποιοδήποτε κομμάτι κειμένου της να εμφανίζεται αυτούσιο ή μεταφρασμένο από κάποια άλλη δημοσιευμένη πηγή. Κάθε τέτοια πράξη αποτελεί προϊόν λογοκλοπής και εγείρει θέμα Ηθικής Τάξης για τα πνευματικά δικαιώματα του άλλου συγγραφέα. Αποκλειστικός υπεύθυνος είναι ο συγγραφέας της Π.Ε., ο οποίος φέρει και την ευθύνη των συνεπειών, ποινικών και άλλων, αυτής της πράξης.

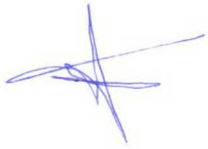
Πέραν των όποιων ποινικών ευθυνών του συγγραφέα σε περίπτωση που το Ίδρυμα του έχει απονείμει Πτυχίο, αυτό ανακαλείται με απόφαση της Συνέλευσης του Τμήματος. Η Συνέλευση του Τμήματος με νέα απόφασης της, μετά από αίτηση του ενδιαφερόμενου, του αναθέτει εκ νέου την εκπόνηση της Π.Ε. με άλλο θέμα και διαφορετικό επιβλέποντα καθηγητή. Η εκπόνηση της εν λόγω Π.Ε. πρέπει να ολοκληρωθεί εντός τουλάχιστον ενός ημερολογιακού 6μήνου από την ημερομηνία ανάθεσης της. Κατά τα λοιπά εφαρμόζονται τα προβλεπόμενα στο άρθρο 18, παρ. 5 του ισχύοντος Εσωτερικού Κανονισμού.»

Επίσης δηλώνω υπεύθυνα ότι έχω παρακολουθήσει το σεμινάριο συγγραφής και εκπόνησης πτυχιακής εργασίας που διοργανώνεται από το Τμήμα Μηχανικών Αυτοματισμού Τ.Ε. κατά το Εαρινό Εξάμηνο του Ακ. Έτους 2015/2016

Ο Δηλών

Ημερομηνία

21/04/2016



Λάμπρου Παναγιώτης

Περιεχόμενα

ΚΕΦΑΛΑΙΟ 1: Συστήματα Συναγερμού 9

1.1 Γενικά 9

1.2 Δομή συστήματος συναγερμού 9

1.3 Ανιχνευτές και αισθητήρες 10

1.3.1 Ανιχνευτές εξωτερικού χώρου 10

1.3.2 Ανιχνευτές εσωτερικού χώρου 13

1.4 Συσκευές συναγερμού ή σήμανσης 17

1.5 Κεντρική μονάδα συστήματος συναγερμού 18

1.5.1 Περιγραφή 18

1.6 Διασύνδεση συσκευών 20

1.6.1 Ασύρματη διασύνδεση 20

1.6.2 Ενσύρματη διασύνδεση 21

1.6.3 Συστήματα απομακρυσμένης πρόσβασης 22

1.7 Λειτουργικότητα εξοπλισμού και προδιαγραφές 23

1.8 Συσκευές επικοινωνίας με το κέντρο λήψης σημάτων 25

1.9 Συστήματα ελέγχου πρόσβασης 28

ΚΕΦΑΛΑΙΟ 2: Πρωτόκολλα επικοινωνίας 33

2.1 Εξέλιξη πρωτοκόλλου επικοινωνίας 33

2.2 Το πρωτόκολλο Ademco Contact ID 34

2.2.1 Περιγραφή 34

2.2.2 Βασικά πλεονεκτήματα του Contact ID 35

2.3 Απαιτήσεις για τη μετάδοση των σημάτων 35

2.3.1 Τόνοι Χειραψίας 36

2.3.2 Message Blocks 36

2.3.3 Τόνος αποδοχής kissoff 40

2.4 Κωδικοί γεγονότων 42

2.5 Βασική ορολογία συστημάτων συναγερμού 51

ΚΕΦΑΛΑΙΟ 3: Δίκτυα επικοινωνίας 54

3.1 Εισαγωγή 54

3.1.1 PSTN δίκτυο και κωδικοποιητής..... 54

3.1.2 Δικτυακός GSM κωδικοποιητής..... 56

3.2 Ενσωμάτωση GSM σε σύστημα συναγερμού 59

3.3 Δίκτυα νέας γενιάς 61

3.4 Συνδυασμένη μετάδοση 63

ΚΕΦΑΛΑΙΟ 4: Σύγχρονες τεχνολογίες 65

4.1 Δίκτυα επικοινωνιών 65

4.2 Επικοινωνία του συναγερμού 67

4.2.1 Πλακέτα Επικοινωνίας Universal..... 68

4.2.2 Συμβατικός χειρισμός και χειρισμός πλακέτας Universal..... 69

4.3 Δικτυακή κάμερα..... 70

4.3.1 Είδη δικτυακών καμερών 71

4.3.2 Διαφορές κάμερας δικτύου και κάμερας κλειστού κυκλώματος τηλεόρασης 71

4.4 Απομακρυσμένος έλεγχος μέσω smartphone 72

4.5 Ασφάλεια Συστήματος..... 77

Συμπεράσματα 78

Βιβλιογραφία 80

Ευρετήριο Εικόνων

Εικόνα 1.1: Ανιχνευτής δόνησης (www.boschsecurity.com) 12

Εικόνα 1.2: Φωτοηλεκτρικός ανιχνευτής δέσμης (www.boschsecurity.com) .. 13

Εικόνα 1.3: Λειτουργία παθητικού ανιχνευτή υπερύθρων (PIR) (www.securitymanager.gr) 15

Εικόνα 1.4: Κύκλωμα παθητικού αισθητήρα υπερύθρων (www.securitymanager.gr) 15

Εικόνα 1.5: Μαγνητικός διακόπτης πόρτας (Trimmer, 1999) 24

Εικόνα 1.6: Πίνακας ελέγχου συστήματος συναγερμού (www.szanwell.com) 25

Εικόνα 1.7: Απεικόνιση του συστήματος DualPath (www.dualpath.gr) 27

Εικόνα 1.8: Κωδικοποιητής και πλακέτα κωδικοποιητή (www.dualpath.gr) ... 28

Εικόνα 1.9: Κεντρική μονάδα συστήματος ελέγχου πρόσβασης (http://www.tdsi.co.uk/)..... 29

Εικόνα 1.10: Συσκευή ανάγνωσης καρτών (http://www.tdsi.co.uk/) 30

Εικόνα 1.11: Συσκευή ανάγνωσης μαγνητικής κάρτας (http://www.tdsi.co.uk/) 30

Εικόνα 1.12: Αριθμητικό πληκτρολόγιο ελέγχου εισόδου (http://www.tdsi.co.uk/)..... 31

Εικόνα 1.13: Βιομετρικές συσκευές ελέγχου πρόσβασης (http://www.tdsi.co.uk/)..... 32

Εικόνα 2.1: Επικοινωνία με το κέντρο λήψης σημάτων με το πρωτόκολλο Contact ID (www.eurogard.gr) 34

Εικόνα 2.2: Μπλοκ Διάγραμμα Μετάδοσης Δεδομένων (Digital Communication Standard, 1999) 41

Εικόνα 2.3: Κλάσεις κωδικών γεγονότων (Digital Communication Standard, 1999)..... 42

Εικόνα 3.1: Αντιστοίχιση πλήκτρων και συχνοτήτων σήματος DTMF (Ραγκούση, 2013) 55

Εικόνα 3.2: Αρχιτεκτονική δικτύου GSM (Shiller, 2002) 57

Εικόνα 3.3: Κυψελοειδές δίκτυο GSM (Shiller, 2002)..... 58

Εικόνα 3.4: Σύστημα συναγερμού με συσκευή GSM (http://www.noontech.gr) 60

Εικόνα 3.5: Σύστημα αμφίδρομης επικοινωνίας μέσω δικτύων GSM/GPRS (www.ilka.gr) 61

Εικόνα 4.1: Ενσύρματο δίκτυο (www.netacad.com)..... 65

Εικόνα 4.2: Ασύρματο δίκτυο http://www.primefocus.net/ 66

Εικόνα 4.3: Τοπολογία Δικτύου WLAN (Χαλκιώτης, 2005) 67

Εικόνα 4.4: Η πρώτη δικτυακή κάμερα Axis Neteye 200 (http://www.axis.com/) 70

Εικόνα 4.5: Δυνατότητα ξεχωριστού ελέγχου κάθε ζώνης του συστήματος (https://www.securityreport.gr) 73

Εικόνα 4.6: Ειδοποιήσεις για την κατάσταση του συστήματος συναγερμού (https://www.securityreport.gr) 74

Εικόνα 4.7: Διεπιφάνεια εφαρμογής απομακρυσμένης πρόσβασης i-Olympia alarm app (www.securitymanager.gr) 75

Εικόνα 4.8: Διεπιφάνεια εφαρμογής απομακρυσμένης πρόσβασης ECHO (www.securitymanager.gr) 76

Ευρετήριο Πινάκων

Πίνακας 2.1: Συχνότητες και αντιστοιχίες DTMF τόνων (Digital Communication Standard, 1999) 39

Πίνακας 2.2: Κωδικοί Γεγονότων Και Εμφανιζόμενο Μήνυμα (Digital Communication Standard, 1999) 42

ΚΕΦΑΛΑΙΟ 1: Συστήματα Συναγερμού

1.1 Γενικά

Τα συστήματα συναγερμού αποτελούν μια από τις πιο ασφαλείς και δοκιμασμένες λύσεις για την προστασία ενός κτιρίου από διάρρηξη ή άλλες κακόβουλες πράξεις. Τα συστήματα αυτά τοποθετούνται σε κατοικίες, σε χώρους γραφείων, αποθήκες, εργοστάσια, αλλά και σε δημόσια κτίρια, νοσοκομεία, αεροδρόμια, στρατόπεδα, και εν γένει όπου απαιτείται να ληφθούν μέτρα προστασίας.

Τόσο στα μεγάλα αστικά κέντρα, όσο και σε μικρότερους οικισμούς, στην επαρχία ή και στα περίχωρα των πόλεων, έχει αρχίσει να διεισδύει ανάμεσα στους κατοίκους, το αίσθημα της ανασφάλειας, τόσο για τη σωματική ακεραιότητά τους όσο και για τη διαφύλαξη της υλικής περιουσίας τους. Η Τα συστήματα ασφαλείας εφαρμόζονται τόσο για την προστασία των ανθρώπων, όσο και για την προστασία του κτιρίου, όπως π.χ. με την εγκατάσταση συστήματος ανίχνευσης καπνού για την αποφυγή της πυρκαγιάς.

Επιπλέον, η οικονομική κρίση και η αστάθεια του τραπεζικού συστήματος έχουν οδηγήσει πολλούς σε ανάληψη των χρημάτων τους από τις τράπεζες και της διατήρησής τους σε ασφαλές μέρος, πολλές φορές εντός της οικίας που διαμένουν. Η συγκέντρωση χρημάτων και πολύτιμων αντικειμένων στο σπίτι θέτει σε κίνδυνο τη ζωή των κατοίκων του σπιτιού.

Η αποτελεσματικότητα του συστήματος συναγερμού εξαρτάται από τη σημασία που έχει δοθεί κατά τη μελέτη της εγκατάστασης, ώστε το σύστημα που θα εφαρμοσθεί ναι είναι το καταλληλότερο για το συγκεκριμένο κτίριο. Είναι πάντως αναμφισβήτητο ότι και μόνο η ύπαρξη συστήματος συναγερμού σε ένα χώρο λειτουργεί αποτρεπτικά για έναν επίδοξο εισβολέα, σε σύγκριση με έναν αφύλακτο χώρο.

Οποιοσδήποτε ενδιαφέρεται να εγκαταστήσει σύστημα συναγερμού σε ένα χώρο που θέλει να προστατέψει πρέπει να φροντίσει ο εξοπλισμός που θα αγοράσει να είναι αξιόπιστος, να παρέχεται συνεχής τεχνική υποστήριξη και συντήρηση από την εταιρία και να παρακολουθείται από κέντρο λήψης σημάτων συναγερμού, σε εικοσιτετράωρη βάση.

1.2 Δομή συστήματος συναγερμού

Ο σχεδιασμός ενός συστήματος συναγερμού πρέπει να παρέχει προστασία σε όλους τους χώρους του σπιτιού, καθώς και σε ορισμένες περιπτώσεις οπτική ή ακουστική παρακολούθηση. Υπάρχουν συγκεκριμένα πρότυπα και

κανονισμοί την Ευρωπαϊκής Ένωσης (EN Standard) για τα συστήματα ασφαλείας. Το πρότυπο EN 50131-1 αφορά την παραγωγή και πιστοποίηση συστημάτων συναγερμού τα οποία κατατάσσονται σε 4 κατηγορίες (Grade 1-4), αναλόγως του βαθμού ασφαλείας και της επικινδυνότητας του χώρου. Υπάρχουν ακουστικοί αισθητήρες, οι οποίοι ανιχνεύουν τον ήχο, τη διάρρηξη μιας πόρτας ή ενός παραθύρου, την κίνηση του αέρα, τη θερμοκρασία του σώματος και άλλες καταστάσεις, οι οποίες υποδεικνύουν την ύπαρξη εισβολέα.

Ο καλός σχεδιασμός ενός συστήματος συναγερμού πρέπει να λαμβάνει υπόψη του τον τρόπο ζωής των κατοίκων του σπιτιού, να προστατεύει τους χώρους που περιέχουν αντικείμενα αξίας, τον τρόπο ελέγχου του συστήματος και τον τρόπο επικοινωνίας σε περίπτωση ενεργοποίησης του συναγερμού.

Ένα τυπικό σύστημα συναγερμού αποτελείται από τα εξής :

- Κεντρική Μονάδα Συστήματος
- Πληκτρολόγια για τον χειρισμό του συστήματος.
- Ανιχνευτές Κίνησης
- Ανιχνευτές Διαφόρων Τύπων
- Στοιχείο ηχητικής και οπτικής ένδειξης συναγερμού
- Κωδικοποιητής για την αποστολή των σημάτων σε κεντρικό σταθμό λήψεως σημάτων

1.3 Ανιχνευτές και αισθητήρες

1.3.1 Ανιχνευτές εξωτερικού χώρου

Αποτελούν πολύ σημαντικό στοιχείο ενός συστήματος συναγερμού καθώς οποιοδήποτε προσπάθεια εισβολής ξεκινά από τον εξωτερικό χώρο. Συνεπώς μπορεί να αναφερθεί ότι οι ανιχνευτές εξωτερικού χώρου αποτελούν την πρώτη γραμμή άμυνας έναντι της διάρρηξης.

Ανιχνευτές ηλεκτρικού πεδίου

Με τις διατάξεις αυτές παράγεται ένα ηλεκτροστατικό πεδίο μεταξύ ενσύρματων αγωγών και ηλεκτρικής γείωσης ή γύρω τους. Αν εντοπιστεί μια διείσδυση, ο ανιχνευτής ενεργοποιείται και παράγει σήμα συναγερμού. Για τη δημιουργία του ηλεκτροστατικού πεδίου απαιτείται μια γεννήτρια παραγωγής

εναλλασσόμενου ρεύματος, το οποίο όταν διέρχεται από τους αγωγούς παράγει ηλεκτροστατικό πεδίο. Απαιτείται επίσης ένας ενισχυτής σήματος, ο οποίος ενισχύει τις μεταβολές που προκαλούνται στην ένταση του ρεύματος. Οι αλλαγές αυτές ανιχνεύονται από τον επεξεργαστή και ενεργοποιείται ο συναγερμός. Όμως, για να μην ενεργοποιείται ο συναγερμός λόγω λανθασμένων μηνυμάτων, π.χ. λόγω της κίνησης του αέρα ή λόγω της διέλευσης κάποιου ζώου, πρέπει η ένταση του σήματος να υπερβαίνει μια προκαθορισμένη τιμή, το εύρος των συχνοτήτων που ανιχνεύεται να αντιστοιχεί σε άνθρωπο και η διάρκεια του σήματος να είναι πάνω από ένα ελάχιστο όριο. (www.securitymanager.gr)

Ανιχνευτές χωρητικότητας

Ο ανιχνευτής χωρητικότητας λειτουργεί με βάση τη μεταβολή της χωρητικότητας ενός πεδίου. Στις περισσότερες περιπτώσεις τοποθετούνται τρία σύρματα που διαρρέονται από ρεύμα χαμηλής τάσης πάνω από ένα φράκτη με αποτέλεσμα την παραγωγή ηλεκτρικού πεδίου, με το φράκτη να λειτουργεί στη γείωση. Ο συναγερμός τίθεται σε λειτουργία όταν υπάρχει επαφή με το σύρμα, αλλά σε πιο ευαίσθητα συστήματα η ανίχνευση της παρουσίας μπορεί να γίνει και από μεγαλύτερη απόσταση. . (www.securitymanager.gr)

Ανιχνευτές δόνησης

Οι συγκεκριμένοι ανιχνευτές βασίζεται στην αναγνώριση των κραδασμών που μπορεί να προκληθούν π.χ. από την προσπάθεια αναρρίχησης σε ένα φράκτη. Πρόκειται για ηλεκτρομηχανικούς ή πιεζοηλεκτρικούς μετατροπείς, οι οποίοι στέλνουν τα σήματα που λαμβάνουν σε έναν επεξεργαστή για να αναλυθούν. Ο συναγερμός ενεργοποιείται αν το σήμα έχει την κατάλληλη συχνότητα. (www.ilka.gr)

Εικόνα 1.1: Ανιχνευτής δόνησης (www.boschsecurity.com)

Φωτοηλεκτρικοί ανιχνευτές

Οι φωτοηλεκτρικοί ανιχνευτές δημιουργούν έναν ηλεκτρονικό φράκτη, εκπέμποντας δέσμες υπέρυθρου φωτός σε ένα δέκτη που βρίσκεται σε απόσταση. Όταν αυτή η νοητή δέσμη διακοπεί, προκαλείται ενεργοποίηση του συναγερμού. Αποτελούνται από έναν πομπό, ο οποίος είναι μια δίοδος εκπομπής φωτός (LED) που μεταδίδει μια συνεχόμενη υπέρυθρη ακτίνα φωτός και ένα δέκτη, ο οποίος είναι μια φωτοηλεκτρική κυψέλη, που λαμβάνει τη δέσμη και ανιχνεύει ή όχι την παρουσία της. Ο συναγερμός ενεργοποιείται όταν ο δέκτης δε λαμβάνει τουλάχιστον το 90% του φωτός που εκπέμπει ο πομπός για διάστημα τουλάχιστον ίσο με 75 ms, όσο δηλαδή απαιτείται για να διασχίσει ένας άνθρωπος τη νοητή δέσμη. Στα συστήματα αυτά η απόσταση μεταξύ πομπού και δέκτη μπορεί να είναι εκατοντάδες μέτρα, ενώ δεν επηρεάζονται από τυχόν εκπομπές θερμότητας, από λαμπτήρες φθορισμού ή από διάφορες ηλεκτρονικές παρεμβολές.

Στην Εικόνα 1.2 παρουσιάζεται φωτοηλεκτρικός ανιχνευτής διπλής δέσμης, ο οποίος παρέχει καλύτερη προστασία έναντι ψευδών συναγερμών. Η εμβέλειά του σε εξωτερικό χώρο είναι 90 m και τοποθετείται σε στύλο ή επιφάνεια. (www.ilka.gr) (www.securitymanager.gr)

Εικόνα 1.2: Φωτοηλεκτρικός ανιχνευτής δέσμης (www.boschsecurity.com)

Συστήματα επιτήρησης εξωτερικών χώρων

Υπάρχουν πολλά συστήματα που μπορούν να χρησιμοποιηθούν. Οι ενταφιασμένοι κάτω από το έδαφος ανιχνευτές, ανάλογα με τον τρόπο λειτουργίας τους έχουν ως υποκατηγορίες τους γραμμικούς ομοαξονικούς ανιχνευτές, τους ανιχνευτές πίεσης και τους ανιχνευτές με γαιόφωνα. Οι ανιχνευτές οπτικών ινών, οι ενταφιασμένοι ανιχνευτές. Άλλη κατηγορία αποτελούν οι ανιχνευτές επαφής, οι οποίοι ενεργοποιούνται με τη διακοπή της φυσικής επαφής, π.χ. σε μια πόρτα. . (www.securitymanager.gr)

1.3.2 Ανιχνευτές εσωτερικού χώρου

Και για τους εσωτερικούς χώρους, υπάρχει πληθώρα κατηγοριών που μπορούν να χρησιμοποιηθούν. Οι βασικότεροι τύποι είναι οι παθητικοί και οι ενεργοί ανιχνευτές υπερύθρων, οι ανιχνευτές μικροκυμάτων και οι διπλής τεχνολογίας. Άλλες δυο κατηγορίες με μικρότερη όμως διάδοση είναι οι ανιχνευτές υπερύθρων και οι ακουστικοί ανιχνευτές.

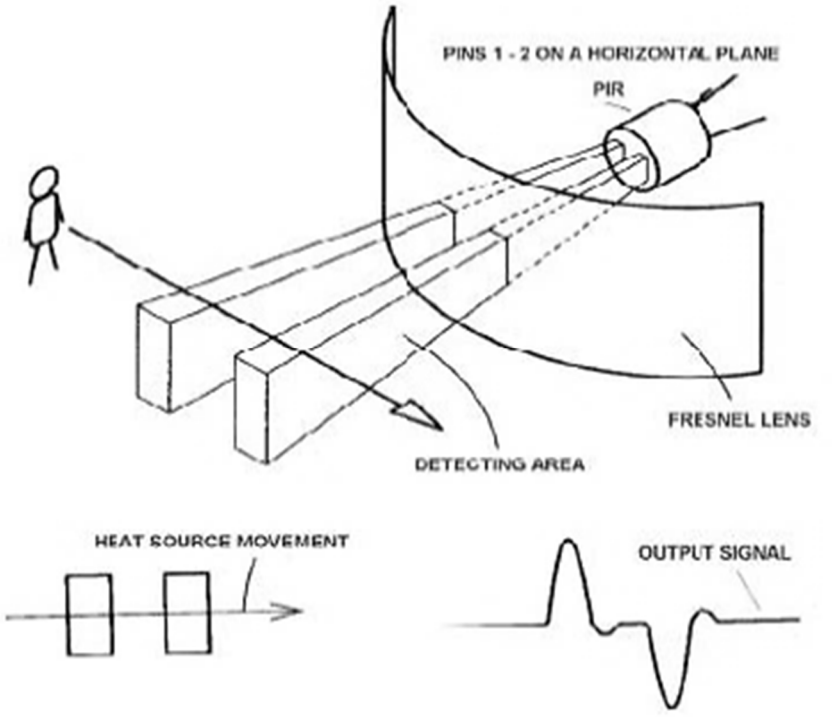
Παθητικοί και ενεργητικοί ανιχνευτές υπερύθρων

Όλα τα σώματα με θερμοκρασία πάνω από το απόλυτο μηδέν εκπέμπουν υπέρυθρη ακτινοβολία, η οποία προφανώς δε βρίσκεται στο ορατό φάσμα. Οι παθητικοί ανιχνευτές υπερύθρων (PIR) είναι ένας συνήθης

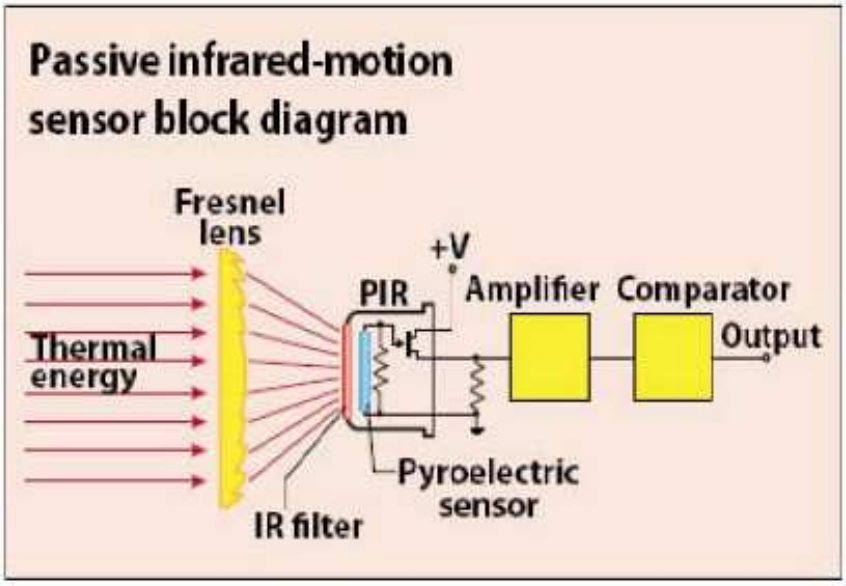
χρησιμοποιούμενος τύπος για την ανίχνευση αυτής της ακτινοβολίας, λόγω του πυροηλεκτρικού υλικού που περιέχουν στον πυρήνα τους. Το πυροηλεκτρικό υλικό μπορεί να είναι νιτρικό γάλλιο, νιτρικό καίσιο και τανταλικό λίθιο. Ο όρος παθητικοί αναφέρεται στο ότι δεν εκπέμπουν αλλά δέχονται σήματα, ως απόκριση στην υπέρυθρη ακτινοβολία που εκπέμπει ένα αντικείμενο. Όταν η υπέρυθρη ακτινοβολία πέσει στο πυροηλεκτρικό υλικό, δημιουργείται ένα μικρό ηλεκτρικό φορτίο. Όσο μεγαλύτερη η ποσότητα της ακτινοβολίας, τόσο μεγαλύτερο και το παραγόμενο φορτίο.

Συνήθως χρησιμοποιούνται για την ανίχνευση της ακτινοβολίας του ανθρώπινου σώματος και για το λόγο αυτό βρίσκουν εφαρμογή σε διακόπτες φωτισμού, ελεγκτές ανοίγματος πόρτας κ.λπ. Μετρούν τις μεταβολές της υπέρυθρης ακτινοβολίας και εντοπίζουν ένα θερμότερο στοιχείο σε σχέση με το ψυχρότερο περιβάλλον. Αυτό γίνεται διότι η μεγαλύτερη θερμοκρασία του ανθρώπινου σώματος σε σχέση με το περιβάλλον, δημιουργεί μεγαλύτερο ηλεκτρικό φορτίο. Το σήμα που παράγεται οδηγείται σε ένα κύκλωμα σύγκρισης. Όταν η μεταβολή που θα ανιχνευτεί είναι πάνω από μια ορισμένη τιμή, προκαλείται ενεργοποίηση του συναγερμού. (Trimmer, 1999)

Για να αποφεύγονται όμως οι ενεργοποιήσεις του συναγερμού που οφείλονται σε τυχαίους λόγους ταχείας μεταβολής της φωτεινότητας ή της θερμότητας, που δε συνιστούν απειλή, όπως π.χ. η λάμψη από έντονα φώτα, τοποθετούνται ειδικά φίλτρα που αποκόπτουν τα μήκη κύματος ακτινοβολίας που δεν αφορούν σε ανθρώπινη παρουσία. Η υπέρυθρη ακτινοβολία που εκπέμπει το ανθρώπινο σώμα έχει μήκος κύματος 9-10 μm. Τοποθετείται επίσης μπροστά από τον αισθητήρα φακός Fresnel, ο οποίος συγκεντρώνει την υπέρυθρη ενέργεια από διάφορες πηγές και χωρίζει την περιοχή σε θερμές και ψυχρές ζώνες ευαισθησίας, ώστε να παράγεται ένα μεταβαλλόμενο σήμα εξόδου σε περίπτωση κίνησης ανθρώπου. (www.ilka.gr)



Εικόνα 1.3: Λειτουργία παθητικού ανιχνευτή υπερύθρων (PIR) (www.securitymanager.gr)



Εικόνα 1.4: Κύκλωμα παθητικού αισθητήρα υπερύθρων (www.securitymanager.gr)

Οι ενεργοί ανιχνευτές υπερύθρων δημιουργούν μια διάταξη προσαρμοζόμενης υπέρυθρης ακτινοβολίας και ενεργοποιούνται σε κάθε αλλαγή συχνότητας ή διακοπή της εκπεμπόμενης ενέργειας, φαινόμενα τα

οποία υποδεικνύουν την κίνηση εισβολέα. Ο μεταδότης του ανιχνευτή καθορίζει τη ζώνη επιτήρησης, χρησιμοποιώντας μια ακτίνα laser, η οποία προσπίπτει σε μια αντανακλαστική ταινία που αποτελεί και το όριο της ζώνης επιτήρησης. Η ενέργεια που εκπέμπεται από το μεταδότη μέσω της ακτίνας, επιστρέφει σε αυτόν, λόγω της ανάκλασης στην ταινία. Όταν η ακτίνα πλησιάζει το δέκτη, περνά από ειδικούς φακούς που συγκεντρώνουν την ενέργεια που εκπέμπεται και από ειδική κυψέλη που μετατρέπει την υπέρυθρη ενέργεια σε ηλεκτρικό σήμα. Όταν η τιμή του σήματος βρίσκεται κάτω από ένα όριο, ενεργοποιείται ο συναγερμός. (www.ilka.gr)

Ανιχνευτές μικροκυμάτων

Αυτού του τύπου οι ανιχνευτές σαρώνουν μια περιοχή με ηλεκτρικό πεδίο και λειτουργούν με βάση το φαινόμενο Doppler. Τα μικροκύματα που εκπέμπουν δεν επηρεάζουν τις ανθρώπινες λειτουργίες ή σημαντικές συσκευές, όπως ο βηματοδότης. Η κίνηση του ανθρώπου παράγει συχνότητες μεταξύ 20 και 120 Hz. Όταν λοιπόν εμφανιστεί τέτοια συχνότητα, τίθεται σε λειτουργία ο συναγερμός.

Είναι επίσης εφικτός ο συνδυασμός των ανιχνευτών μικροκυμάτων με τους ανιχνευτές PIR, ώστε να προκύπτουν πιο αξιόπιστα αποτελέσματα από τη λειτουργία του συστήματος.

Εσωτερικοί ανιχνευτές υπερήχων

Οι ανιχνευτές υπερήχων διακρίνονται σε ενεργούς και παθητικούς. Οι παθητικοί ανιχνευτές υπερήχων εντοπίζουν τους υπερήχους μέσα σε μια επιτηρούμενη ζώνη και εμφανίζουν μεγάλες μεταβολές συχνοτήτων όταν εντοπίσουν κάποια κίνηση. Ο παραγόμενος ήχος μεταδίδεται μέσα από τον περιβάλλοντα αέρα και ταξιδεύει με τη μορφή κύματος. Όταν το ηχητικό κύμα προσεγγίσει τη συσκευή ανίχνευσης, αυτή διερευνά εάν η συχνότητα του κύματος ανήκει σε ενέργειες επικίνδυνες για την ασφάλεια του προστατευόμενου πεδίου, και σε αυτήν την περίπτωση δίνει ένα σήμα συναγερμού.

Οι ενεργοί ανιχνευτές υπερήχων και χρησιμοποιούν τις αλλαγές στην εκπεμπόμενη συχνότητα των υπερήχων για να αντιληφθούν τυχόν ενέργειες διείσδυσης. Οι υπέρηχοι εκπέμπονται από μια συσκευή και μεταδίδονται μέσω του αέρα, ταξιδεύοντας με τη μορφή ενεργειακών κυμάτων. Τα κύματα αντανακλώνται πίσω από τους περιβάλλοντες τοίχους του χώρου, με ένα χαρακτηριστικό βήμα. Όταν ένα πρόσωπο διεισδύει στο χώρο, τότε η αλληλουχία των κυμάτων μεταβάλλεται και αντανακλάται πίσω με γρηγορότερο ρυθμό, οπότε αυξάνεται το βήμα κύματος και ο ανιχνευτής δίνει σήμα συναγερμού. (www.ilka.gr)

Ακουστικοί ανιχνευτές

Μια άλλη κατηγορία ανιχνευτών εσωτερικού χώρου είναι οι ακουστικοί. Σαρώνουν το χώρο και αναζητούν ήχους προερχόμενους από την είσοδο ενός προσώπου στον επιτηρούμενο χώρο. Ο ανιχνευτής αποτελείται από δύο συσκευές. Από ένα μικρόφωνο που τοποθετείται σε τοίχους ή στην οροφή και έναν ενισχυτή που διαθέτει και ένα ηλεκτρονικό κύκλωμα επεξεργασίας. Τα μικρόφωνα αναζητούν ήχους και στη συνέχεια τους συλλέγουν και τους στέλνουν στον επεξεργαστή για ανάλυση και επεξεργασία. Ο επεξεργαστής συγκρίνει τους ήχους και διερευνά εάν πρόκειται για ύποπτους ήχους. Στην περίπτωση που διαπιστώνεται ότι κάποιος από τους συλλεγόμενους ήχους ανήκει στην κατηγορία των ήχων που είναι ταυτισμένοι με ενέργειες διάρρηξης και συνεχίζεται για ένα καθορισμένο χρονικό διάστημα, τότε ο ανιχνευτής δίνει σήμα συναγερμού. (www.ilka.gr)

1.4 Συσκευές συναγερμού ή σήμανσης

Οι σειρήνες έχουν στόχο να πανικοβάλλουν το διαρρήκτη και να τον αποτρέψουν από το έργο του. Συνήθως χρησιμοποιούνται δύο σειρήνες, μία στον εξωτερικό χώρο και μία στον εσωτερικό. Η εξωτερική σειρήνα πρέπει να είναι εμφανής από απόσταση, ώστε η παρουσία της και μόνο να είναι αποτρεπτική για κάποιον επίδοξο διαρρήκτη, καθώς και να τοποθετείται σε σημείο που να είναι δύσκολα προσβάσιμο, ώστε να είναι δύσκολη η απενεργοποίησή της από κάποιον γνώστη. Σε ορισμένες περιπτώσεις τοποθετείται και μια ψεύτικη σειρήνα, με σκοπό να παραπλανήσει το διαρρήκτη και να τον απομακρύνει από την πραγματική.

Αντιθέτως, η εσωτερική σειρήνα, τοποθετείται σε σημείο που δε φαίνεται εύκολα για να μην είναι εύκολο να την εντοπίσει ο διαρρήκτης και να την απενεργοποιήσει. Υπάρχουν απλές σειρήνες, οι οποίες είναι οικονομικές στη λειτουργία τους, αλλά δε λειτουργούν σε περίπτωση διακοπής –σε κάποιες περιπτώσεις εσκεμμένης- του ρεύματος. Υπάρχουν επίσης και αυτόνομες σειρήνες, οι οποίες συνεχίζουν να λειτουργούν και σε περίπτωση διακοπής του ρεύματος, μέσω μπαταρίας. Για να δυσκολεύουν ακόμη περισσότερο το διαρρήκτη, είναι προτιμότερο να είναι μεταλλικές, διότι είναι δύσκολο να τις σπάσει. Επιπλέον, αντί για σειρήνα μπορεί να χρησιμοποιηθεί σε εξωτερικό χώρο ισχυρός προβολέας ιωδίου (500 W ή 1000 W)

1.5 Κεντρική μονάδα συστήματος συναγερμού

1.5.1 Περιγραφή

Αποτελεί το πιο νευραλγικό κομμάτι του συστήματος καθώς όλα τα περιφερειακά αισθητήρια του συστήματος συνδέονται πάνω σε αυτήν και αυτή είναι υπεύθυνη για την λειτουργία και την εποπτεία ολόκληρου του συστήματος. Λαμβάνει τα σήματα από όλους τους αισθητήρες, καταγράφει τα συμβάντα και μεταδίδει τα σήματα, συνήθως μέσω της τηλεφωνικής γραμμής. Υπάρχουν στην αγορά διάφοροι τύποι κεντρικών μονάδων με διαφορετικές δυνατότητες, αλλά η αρχή της κατασκευής τους παραμένει σε γενικές γραμμές κοινή. Μια κεντρική μονάδα αποτελείται από ένα μετασχηματιστή, ο οποίος τροφοδοτεί το σύστημα με 6 ή 12 V DC, μια μπαταρία για εφεδρική παροχή ρεύματος, ένα εξωτερικό κουτί μέσα στο οποίο τοποθετούνται και ένα πληκτρολόγιο ή συσκευή τηλεχειρισμού.

Για να ανταποκριθεί μια κεντρική μονάδα στις απαιτήσεις ενός συστήματος συναγερμού πρέπει να διαθέτει τα ακόλουθα χαρακτηριστικά:

Το τροφοδοτικό της πρέπει να μπορεί να διαχειριστεί όλα τα φορτία του συστήματος και να αντέχει ένταση ρεύματος μεγαλύτερη των 2 Α. Πρέπει να υπάρχουν ενδείξεις για όλες τις μπαταρίες του συστήματος, ώστε να γίνεται έγκαιρα η φόρτιση ή η αντικατάστασή τους. Είναι σημαντικό να υπάρχουν αρκετές ζώνες στο σύστημα, όπως περιγράφεται ακολούθως ενώ είναι απαραίτητο να υπάρχει χρονοκαθυστέρηση, ώστε να είναι εύκολη η είσοδος και η έξοδος των χρηστών από τον προστατευόμενο χώρο. Απαιτείται επίσης ανεξάρτητη γραμμή τροφοδοσίας της κεντρικής μονάδας, στην οποία δεν θα είναι συνδεδεμένα άλλα φορτία.

Βασικά Χαρακτηριστικά Κεντρικής Μονάδας Συναγερμού :

- Αριθμός Ζωνών (Αριθμός Εισόδων)
- Αριθμός Υποσυστημάτων
- Αριθμός Χρηστών
- Αριθμός Εξόδων
- Τύπος Κωδικοποιητή (PSTN, TCP/IP, GSM/GPRS).
- Τρόποι Διαχείρισης της Κεντρικής Μονάδας .

Τα παραπάνω χαρακτηριστικά είναι τα σημαντικότερα, καθώς με βάση αυτά γίνεται η παραμετροποίηση για την ορθή λειτουργία του συστήματος με βάση τις ανάγκες του χώρου. Η κεντρική μονάδα του συστήματος συναγερμού είναι

επίσης απαραίτητη για την αποστολή σημάτων και τη σωστή απομακρυσμένη εποπτεία του συστήματος, και κατ' επέκταση του χώρου.

Αριθμός Ζωνών Κεντρικής Μονάδας

Ανάλογα με τον χώρο τον οποίο θέλουμε να ασφαλίσουμε πρέπει η εκάστοτε μονάδα να υποστηρίζει και τον απαραίτητο αριθμό ζωνών, τόσο για τον έλεγχο του χώρου, την απομακρυσμένη ειδοποίηση και τον έλεγχο του συστήματος, όσο και για την ευκολότερη επίλυση μια βλάβης που μπορεί να προκύψει στο σύστημα. Όταν για παράδειγμα ενεργοποιηθεί ο συναγερμός, θέλουμε να ξέρουμε ποιος ανιχνευτής και κατ' επέκταση ποια ζώνη ενεργοποίησε την κεντρική μονάδα.

Αριθμός Υποσυστημάτων

Ένα επιπλέον χαρακτηριστικό της Κεντρικής Μονάδας είναι ο διαχωρισμός της σε υποσυστήματα. Κάθε υποσύστημα μπορεί να λειτουργεί σαν ένα ανεξάρτητο σύστημα. Για παράδειγμα εάν έχουμε ένα πενταόροφο κτίριο είναι σημαντικό να ξέρουμε σε ποιον όροφο ενεργοποιήθηκε ο συναγερμός .

Αριθμός Χρηστών

Κάθε κεντρική μονάδα μπορεί να υποστηρίξει ένα συγκεκριμένο αριθμό χρηστών ο οποίος θα ενεργοποιεί / απενεργοποιεί το σύστημα. Κάθε φορά που κάποιος χρήστης ενεργοποιεί / απενεργοποιεί το σύστημα καταγράφεται στο ιστορικό του συστήματος και η πληροφορία αυτή αποστέλλεται στο κέντρο λήψεως σημάτων .

Αριθμός Εξόδων

Οι περισσότερες κεντρικές μονάδες συστημάτων συναγερμού εκτός από ζώνες εισόδου διαθέτουν και προγραμματιζόμενες εξόδους, οι οποίες μπορούν να ενεργοποιηθούν είτε μετά από την ενεργοποίηση ενός σήματος συναγερμού, είτε απομακρυσμένα από το χρήστη.

Τύπος Κωδικοποιητή

Σε κάθε κεντρική μονάδα ενσωματώνεται ένας κωδικοποιητής για την αποστολή των σημάτων στο κέντρο λήψεως. Συνήθως οι περισσότερες κεντρικές μονάδες ενσωματώνουν κωδικοποιητή PSTN γραμμής, ο οποίος μέσω συγκεκριμένου πρωτοκόλλου και συγκεκριμένης κωδικοποίησης αποστέλλει τα σήματα. Το συνηθέστερο πρωτόκολλο επικοινωνίας για τέτοιους κωδικοποιητές είναι το CONTACT ID της ADEMCO και είναι κοινό για

όλες της κατασκευάστριες εταιρείες συστημάτων συναγερμού, ενώ η αποστολή γίνεται μέσω DTMF κωδικοποίησης.

Εκτός από τους PSTN κωδικοποιητές μπορεί να χρησιμοποιείται και ένας GSM/GPRS κωδικοποιητής με χρήση κάρτας SIM είτε ως πρωτεύουσας επικοινωνίας είτε ως BACK UP σε περιπτώσεις όπου υπάρχει αυξημένη ανάγκη ασφάλειας. Τέλος οι κεντρικές μονάδες συναγερμού διαθέτουν TCP/IP κωδικοποιητές για την άμεση αποστολή σημάτων μέσω δικτύου. Οι κατασκευάστριες εταιρείες που χρησιμοποιούν TCP/IP κωδικοποιητές δεν έχουν κοινό πρωτόκολλο επικοινωνίας, αλλά κατασκευάζει η καθεμία το δικό της.

Τρόποι Διαχείρισης της Κεντρικής Μονάδας

Ένα άλλο σημαντικό στοιχείο του συστήματος έχει να κάνει με τον τρόπο διαχείρισης. Οι περισσότερες κεντρικές μονάδες που κυκλοφορούν στην ελληνική αγορά μέχρι στιγμής επιτρέπουν την διαχείριση του συστήματος τοπικά και μόνο μέσω του πληκτρολογίου. Απομακρυσμένα το μόνο που μπορούμε να κάνουμε είναι οπλισμό ή αφοπλισμό του συστήματος μέσω DTMF, χωρίς να μπορούμε να λάβουμε οποιαδήποτε πληροφορία για την κατάσταση του συστήματος. Οι νέες κεντρικές μονάδες και ειδικότερα αυτές που χρησιμοποιούν TCP/IP κωδικοποιητές έχουν τις εξής δυνατότητες διαχείρισης :

1. τοπικά μέσω πληκτρολογίου
2. τοπικά μέσω τοπικού δικτύου από SMARTPHONE,TABLET,PC
3. απομακρυσμένα μέσω Internet από SMARTPHONE,TABLET,PC

1.6 Διασύνδεση συσκευών

1.6.1 Ασύρματη διασύνδεση

Τα ασύρματα συστήματα συναγερμού χρησιμοποιούν πομπούς ραδιοκυμάτων, οι οποίοι λειτουργούν με μπαταρία και δέκτες στους οποίους συνδέονται διάφορες συσκευές, όπως κάμερες, αισθητήρες, ανιχνευτές κίνησης, σειρήνες, κεντρικοί ελεγκτές κ.λπ. Τα ασύρματα συστήματα αποτελούν την πιο απλή και οικονομική μέθοδο για τη διασύνδεση των διαφόρων μερών ενός συστήματος συναγερμού. Όταν ένας αισθητήρας ανιχνεύσει μια εισβολή, μεταφέρει την πληροφορία σε έναν πίνακα ελέγχου μέσω εκπομπής ραδιοκυμάτων και σημαίνει την κατάσταση συναγερμού σε έναν κεντρικό ελεγκτή.

Τα βασικά πλεονεκτήματα ενός ασύρματου συστήματος συναγερμού είναι τα ακόλουθα:

- ευκολία εγκατάστασης, καθώς παρακάμπτεται η δαπανηρή και χρονοβόρα διαδικασία της εγκατάστασης
- δυνατότητα μεταφοράς των τμημάτων του συστήματος συναγερμού σε περίπτωση μετακόμισης σε άλλο σπίτι
- Οι ασύρματοι αισθητήρες είναι σχεδιασμένοι να μεταδίδουν ένα μοναδικό κώδικα αναγνώρισης σε έναν ελεγκτή, και έτσι ο ελεγκτής μαθαίνει την ταυτότητα του κάθε αισθητήρα και τον συνδέει στην κατάλληλη ζώνη. Κάθε αισθητήρας μεταδίδει επίσης πληροφορίες σχετικά με τη στάθμη της μπαταρίας και άλλα διαγνωστικά μηνύματα.
- Οι ασύρματοι αισθητήρες, οι ανιχνευτές κίνησης και οι κάμερες παρακολούθησης μπορούν να εγκατασταθούν σε περιοχές οι οποίες δεν είναι προσβάσιμες σε ενσύρματο εξοπλισμό. (Trimmer, 1999)

Τα βασικά μειονεκτήματα των ασύρματων συστημάτων συναγερμού είναι:

- Οι προδιαγραφές σχεδιασμού ενός ασύρματου συστήματος περιορίζουν την απόσταση μεταξύ των αισθητήρων, των καμερών και του κεντρικού πίνακα ελέγχου.
- Σε ορισμένες περιοχές τα ασύρματα συστήματα είναι ευάλωτα σε ηλεκτρομαγνητικές παρεμβολές.
- Απαιτείται περιοδική αντικατάσταση των μπαταριών.
- Οι περισσότεροι εγκαταστάτες προτείνουν τα ασύρματα συστήματα ως την τελευταία επιλογή. (Trimmer, 1999)

1.6.2 Ενσύρματη διασύνδεση

Τα ενσύρματα συστήματα συναγερμού χρησιμοποιούν καλώδια τα οποία περνούν μέσα οπές στους τοίχους ή από κενούς σημεία, ώστε να συνδεθούν όλοι οι αισθητήρες σε ένα κεντρικό πίνακα ελέγχου. Οι κάμερες επιτήρησης ή τα μικρόφωνα συνδέονται επίσης σε μεγάφωνα ή οθόνες παρακολούθησης. Συνήθως η πηγή ισχύος ενός ενσύρματου συστήματος συναγερμού είναι το εναλλασσόμενο ρεύμα του δικτύου. Ο κεντρικός πίνακας ελέγχου διαθέτει επίσης επαναφορτιζόμενη μπαταρία, η οποία έχει εφεδρική χρήση για τις περιπτώσεις διακοπής ρεύματος. Τα ενσύρματα συστήματα απαρτίζονται από τις ίδιες συσκευές με τα ασύρματα, με τη διαφορά ότι δεν περιλαμβάνουν πομπό και δέκτη ραδιοκυμάτων. (Traister, 2001)

Η καλωδίωση των συστημάτων συναγερμού είναι χαμηλής τάσης και μπορεί να χρησιμοποιηθούν διάφορες διαστάσεις καλωδίων για τη σύνδεση των

αισθητήρων στον κεντρικό πίνακα ελέγχου. Από πολλούς εγκαταστάτες επιλέγεται το τετραπολικό καλώδιο, το οποίο εμπεριέχει τέσσερα καλώδια σε πλαστικό περίβλημα. Το ομοαξονικό καλώδιο χρησιμοποιείται για τη μεταφορά σημάτων βίντεο μεταξύ των συσκευών παρακολούθησης και των οθονών σε ένα οικιακό σύστημα παρακολούθησης. Η ποιότητα του σήματος επηρεάζεται από την ποιότητα ή τη λανθασμένη επιλογή του καλωδίου.

Τα βασικά πλεονεκτήματα ενός ενσύρματου συστήματος συναγερμού είναι:

- Θεωρούνται από πολλούς εγκαταστάτες πιο αξιόπιστα σε σχέση με τα ασύρματα συστήματα.
- Τα ενσύρματα συστήματα τοποθετούνται συνήθως από επαγγελματία εγκαταστάτη, ο οποίος αναλαμβάνει στη συνέχεια και την συντήρηση του συστήματος.
- Δεν αντιμετωπίζουν το πρόβλημα της ηλεκτρομαγνητικής παρεμβολής και τους περιορισμούς του εύρους των ραδιοκυμάτων, τα οποία είναι αναπόφευκτα στα ασύρματα συστήματα.
- Τα τμήματα ενός ενσύρματου συστήματος είναι συνήθως λιγότερο ορατά και λιγότερα αντιαισθητικά από τα μέρη ενός ασύρματου συστήματος.
- Τα ενσύρματα συστήματα δε χρειάζονται μπαταρία για να λειτουργήσουν, παρά μόνο ως εφεδρική πηγή ενέργειας σε περίπτωση διακοπής ρεύματος.

Τα μειονεκτήματα των ενσύρματων συστημάτων συναγερμού σε σχέση με τα ασύρματα είναι:

- Είναι πιο ακριβά σε σχέση με τα ασύρματα συστήματα.
- Σε αντίθεση με τα ασύρματα συστήματα, ένα ενσύρματο σύστημα γίνεται αναπόσπαστο τμήμα του χώρου στον οποίο εγκαθίσταται, καθώς τα μέρη του δεν είναι δυνατό να μεταφερθούν σε περίπτωση που οι κάτοικοι μετακομίσουν.
- Μπορεί να μην είναι εφικτή η εγκατάσταση αισθητήρων σε ορισμένες περιοχές του σπιτιού, λόγω μη προσβασιμότητας των καλωδίων. (Traister, 2001)

1.6.3 Συστήματα απομακρυσμένης πρόσβασης

Ένα σύστημα απομακρυσμένης πρόσβασης παρέχει τη δυνατότητα παρακολούθησης και ελέγχου ενός συστήματος συναγερμού από απόσταση. Μέσω μιας τηλεφωνικής κλήσης και ενός κωδικού μπορεί ο καλών να λάβει

πληροφορίες σχετικά με την κατάσταση του συστήματος συναγερμού. Τα απομακρυσμένα συστήματα μπορούν επίσης να είναι προγραμματισμένα να καλούν ένα συγκεκριμένο τηλεφωνικό νούμερο όταν παρουσιάζεται μια προκαθορισμένη κατάσταση. Ο καλών, μπορεί επίσης να εκτελέσει όλες τις λειτουργίες που θα εκτελούσε από το πληκτρολόγιο του συναγερμού από απόσταση, μέσω της εισαγωγής των κατάλληλων κωδικών. Ένα σύστημα απομακρυσμένης πρόσβασης μπορεί να δώσει πληροφορίες και για άλλα συστήματα, πέραν του συστήματος συναγερμού, όπως σύστημα πυρανίχνευσης, ελέγχου θερμοκρασίας κ.λπ.

Τα κυριότερα χαρακτηριστικά ενός συστήματος απομακρυσμένης πρόσβασης είναι τα ακόλουθα:

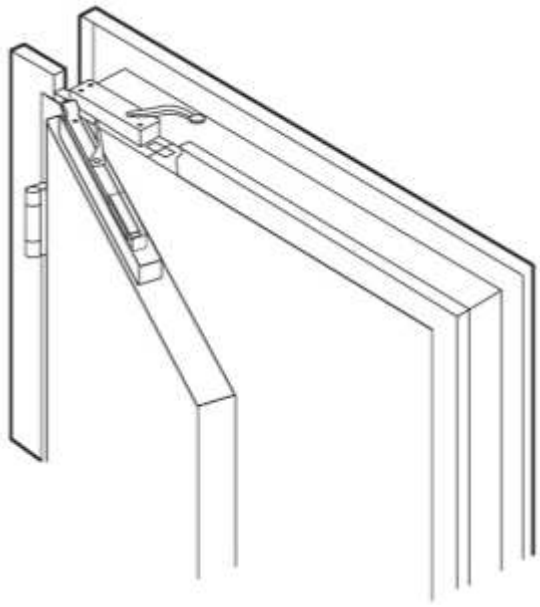
- Παρακολούθηση και αναφορά της θερμοκρασίας στο εσωτερικό και το εξωτερικό του σπιτιού
- Αναφορά αισθητήρων που έχουν υπερβεί ένα προκαθορισμένο κατώφλι τιμής
- Παρακολούθηση ισχυρών θορύβων που έχουν υπερβεί ένα καθορισμένο χρονικό διάστημα με χρήση μικροφώνου στο σύστημα συναγερμού
- Αναφορά της ημερομηνίας και της ώρας που παρουσιάστηκε η ενεργοποίηση του συναγερμού
- Αναφορά της κατάστασης των ανιχνευτών καπνού και των αισθητήρων θερμότητας (Traister, 2001)

1.7 Λειτουργικότητα εξοπλισμού και προδιαγραφές

Κάθε στοιχείο ενός συστήματος συναγερμού επιτελεί μια συγκεκριμένη λειτουργία.

Πόρτες

Οι πόρτες προστατεύονται μέσω της τοποθέτησης μικρών μαγνητικών διακοπτών στο πλαίσιό τους. Στην Εικόνα 1.5 παρουσιάζεται η θέση στην οποία τοποθετείται ο μαγνητικός διακόπτης. Τοποθετείται στο επάνω μέρος της πόρτας και οι επαφές του διακόπτη είναι ανοικτές όσο η πόρτα παραμένει κλειστή. Με το άνοιγμα της πόρτας, ο διακόπτης επηρεάζεται και ενεργοποιείται ο συναγερμός. Ο μαγνητικός διακόπτης κλείνει κύκλωμα, το οποίο συνδέεται με την κεντρική μονάδα. (Trimmer, 1999)



Εικόνα 1.5: Μαγνητικός διακόπτης πόρτας (Trimmer, 1999)

Παράθυρα

Οι μαγνητικοί διακόπτες δεν παρέχουν προστασία σε περίπτωση που κάποιος εισβάλλει στο σπίτι μέσω ενός σπασμένου παραθύρου. Υπάρχουν δύο κατηγορίες συστημάτων προστασίας έναντι θραύσης κρυστάλλων: δόνησης και ακουστικά. Το σύστημα δόνησης τοποθετείται επάνω στο τζάμι ή σε γειτονικό τοίχωμα και ανιχνεύει τυχόν κίνηση του γυαλιού. Τα ακουστικά συστήματα ανιχνεύουν τον ήχο από τη θραύση του γυαλιού. Η μονάδα ρυθμίζεται ώστε να ενεργοποιείται μόνο στη συχνότητα θραύσης του γυαλιού, συνήθως 4 kHz-6 kHz, ή να ενεργοποιείται σε οποιοδήποτε δυνατό ήχο. ήχο. Υπάρχουν κατασκευαστές οι οποίοι συνδυάζουν τις δύο αυτές τεχνολογίες, και η μονάδα δεν ενεργοποιείται αν δεν ανιχνευτούν και οι δύο. Μια τέτοια μονάδα χρησιμοποιείται όταν οι κανονικές συνθήκες είναι τέτοιες όπου η απλή ανίχνευση θα οδηγούσε σε ψευδή συναγερμό. (Trimmer, 1999)

Πίνακας ελέγχου

Ο πίνακας ελέγχου είναι ένα κουτί το οποίο περιλαμβάνει όλα τα ηλεκτρονικά μέρη, τα τερματικά σημεία των καλωδίων, τις εφεδρικές μπαταρίες και το τερματικό της τηλεφωνικής καλωδίωσης. Κάθε αισθητήρας λαμβάνει ισχύ και ελέγχεται από τον πίνακα ελέγχου. Παρακολουθεί την κατάσταση του συνολικού συστήματος και στέλνει σήμα στη σειρήνα, όταν εντοπιστεί κατάσταση συναγερμού. Ο πίνακας ελέγχου πρέπει να τοποθετείται σε σημείο που δεν είναι άμεσα ορατό και κοντά σε έξοδο εναλλασσόμενου ρεύματος, όπου μπορεί να χρησιμοποιηθεί μετασχηματιστής για την παροχή χαμηλής τάσης σε ολόκληρο το σύστημα. (Trimmer, 1999)

Εικόνα 1.6: Πίνακας ελέγχου συστήματος συναγερμού (www.szanwell.com)

1.8 Συσκευές επικοινωνίας με το κέντρο λήψης σημάτων

Σε περίπτωση ενεργοποίησης του συναγερμού, αποστέλλεται σήμα στο κέντρο λήψης σημάτων μέσω της τηλεφωνικής γραμμής, εφόσον φυσικά είναι σε λειτουργία. Από το σήμα που λαμβάνει το κέντρο, βλέπει ποια ζώνη έχει ενεργοποιηθεί και σε ποιο χώρο του σπιτιού. Το κέντρο λήψης σημάτων στη συνέχεια ενεργεί με βάση ό,τι έχει συμφωνηθεί με τους ιδιοκτήτες. Συνήθως καλεί στην τηλεφωνική γραμμή του σπιτιού, για να διαπιστωθεί αν πρόκειται όντως για διάρρηξη ή για λανθασμένη ενεργοποίηση από τους ιδιοκτήτες. Σε περίπτωση που απαντήσει ο ιδιοκτήτης και όντως πρόκειται για λάθος, ζητείται από το κέντρο να αναφέρει έναν προσυμφωνημένο κωδικό λάθους. Αν η κλήση δεν απαντηθεί, τότε το κέντρο συνήθως ειδοποιηθεί ορισμένα τηλέφωνα, όπως έχουν συμφωνηθεί στη σχετική σύμβαση, ή καλεί την αστυνομία. Το κέντρο επίσης ενημερώνει τον ιδιοκτήτη όταν η στάθμη της μπαταρίας του συστήματος είναι χαμηλή ή ύστερα από διακοπή ρεύματος.

Το κέντρο λήψης σημάτων μπορεί να ειδοποιηθεί όμως και με άλλους τρόπους, πέραν της σταθερής τηλεφωνικής γραμμής. Υπάρχει η δυνατότητα ενεργοποίησης του κέντρου από ανεξάρτητη τηλεφωνική γραμμή κινητής τηλεφωνίας, ώστε να υπάρχει μεγαλύτερη ασφάλεια σε περίπτωση καταστροφής της γραμμής σταθερής τηλεφωνίας από τους διαρρήκτες. Αξίζει βέβαια να αναφερθεί ότι κάτι τέτοιο δεν είναι τόσο σύνηθες φαινόμενο, ενώ παράλληλα το κόστος εγκατάστασης ανεξάρτητης γραμμής κινητής τηλεφωνίας είναι σημαντικό.

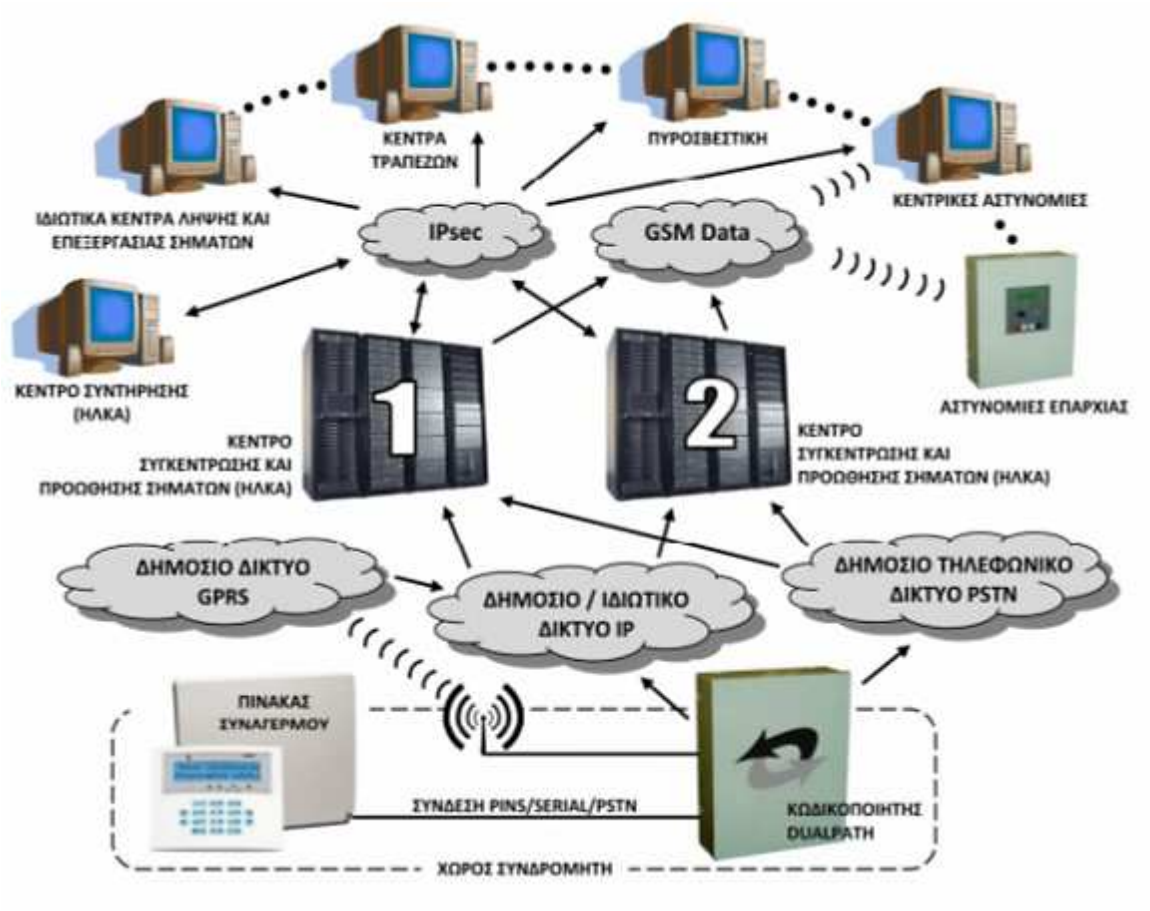
Αντί για γραμμή κινητής τηλεφωνίας, μπορεί να υπάρχει μισθωμένη αποκλειστική γραμμή επικοινωνίας με το κέντρο. Η γραμμή αυτή ενημερώνει

για την ενεργοποίηση του συναγερμού, ενώ όλα τα υπόλοιπα σήματα (ενεργοποιημένη ζώνη) λαμβάνονται από την τηλεφωνική γραμμή. Αποτελεί απλώς μια εφεδρική γραμμή επικοινωνίας, η οποία όμως λόγω του υψηλού κόστους της (1000 €/έτος) απαντάται σε τράπεζες και άλλες τέτοιου είδους υπηρεσίες με αυξημένο κίνδυνο διάρρηξης.

Επίσης είναι εφικτή η αποστολή εικόνας από τον εποπτευόμενο χώρο μέσω τηλεφωνικής γραμμής ISDN ή γραμμής κινητής τηλεφωνίας. Εφαρμόζεται επίσης το σύστημα αποστολής SMS στο κινητό τηλέφωνο του ιδιοκτήτη, ενώ υπάρχει και η περίπτωση της ύπαρξης χωριστού κωδικοποιητή ευθείας γραμμής για την αποστολή μόνο του βασικού σήματος. (www.dualpath.gr)

Επειδή κανένα από τα συστήματα αυτά δεν παρέχει πλήρη προστασία, ενώ επίσης είναι πολύ εύκολο να παραποιηθεί η λειτουργία τους από τον διαρρήκτη, χωρίς να φανεί κάποια ειδοποίηση στο κέντρο λήψης, πολλά συστήματα στέλνουν σήματα ελέγχου (test) μέσω τηλεφωνικής κλήσης ανά τακτά χρονικά διαστήματα, ώστε να επιβεβαιώνεται η σωστή λειτουργία τους. Η διαδικασία αυτή όμως αυξάνει σημαντικά το λειτουργικό κόστος του συστήματος, ενώ και πάλι, αν δε ληφθεί κάποιο σήμα, δεν είναι βέβαιο αν πρόκειται για κάποια απόπειρα παραβίασης του προστατευόμενου χώρου ή βλάβη. (www.dualpath.gr)

Ένας πιο εξελιγμένος τρόπος αποστολής σημάτων είναι μέσω του συστήματος DualPath. (Εικόνα 1.7) Τα συστήματα αυτά μπορούν να συνδεθούν με όλους τους πίνακες συναγερμού και αποστέλλουν τα σήματα σε δύο διαφορετικά κέντρα προώθησης και συγκέντρωσης σημάτων. Τα κέντρα αυτά είναι δύο, για λόγους εφεδρείας, και είναι εξοπλισμένα με σύγχρονους servers και ειδικά λογισμικά. Για την αποστολή των σημάτων χρησιμοποιούνται πολλαπλές διαδρομές επικοινωνίας, με πλήρη συγχρονισμό μεταξύ τους. Για τη διασφάλιση της σωστής επικοινωνίας τα κέντρα πρέπει να λαμβάνουν συνεχώς και σήματα ελέγχου (polling) από όλες τις πιθανές διαδρομές. Αν δε γίνει λήψη του σήματος ελέγχου από κάποιο κέντρο εντός ενός προκαθορισμένου χρονικού διαστήματος, αναφέρεται «πρόβλημα επικοινωνίας» με τη διαδρομή αυτή. Τα σήματα συναγερμού αποστέλλονται προς την αστυνομία, την πυροσβεστική κ.λπ. ανάλογα με το είδος του συναγερμού. Τα κέντρα αυτά ονομάζονται *κέντρα τελικής λήψης και επεξεργασίας σημάτων συναγερμού*. (www.dualpath.gr)



Εικόνα 1.7: Απεικόνιση του συστήματος DualPath (www.dualpath.gr)

Με τον τρόπο αυτό όλες οι επικοινωνίες, τόσο με τα κέντρα λήψης σήματος όσο και με την αστυνομία ή την πυροσβεστική γίνονται με ένα ενοποιημένο σύστημα. Η ύπαρξη πολλών διαδρομών διαφορετικής τεχνολογίας αυξάνει τη διαθεσιμότητα. Μέσα σε πολύ μικρό χρονικό διάστημα γίνεται αντιληπτό αν μια διαδρομή επικοινωνίας έχει πρόβλημα. Επιπρόσθετα, η επιβεβαίωση της λειτουργίας του συστήματος δε γίνεται με τηλεφωνικές κλήσεις, με αποτέλεσμα τη μείωση των λειτουργικών εξόδων. Επιπλέον μείωση προκύπτει και από το γεγονός ότι δεν απαιτείται γραμμή απευθείας σύνδεσης με την αστυνομία, όταν πρόκειται για χώρους υψηλού κινδύνου.

Για την αποστολή του σήματος στο κέντρο είναι απαραίτητο να υπάρχει αμφίδρομος κωδικοποιητής, ο οποίος επικοινωνεί με τον πίνακα συναγερμού του συνδρομητή. Η επικοινωνία μπορεί να γίνει μέσω ενσύρματου δικτύου Ethernet Broadband IP, ή και σε συνδυασμό με δευτερεύουσα επικοινωνία μέσω δικτύου κινητής τηλεφωνίας GPRS. Είναι επίσης εφικτό να υπάρχουν τρεις δίαυλοι επικοινωνίας, δηλαδή IP, GPRS και τηλεφωνική γραμμή. (www.dualpath.gr)

Εικόνα 1.8: Κωδικοποιητής και πλακέτα κωδικοποιητή (www.dualpath.gr)

1.9 Συστήματα ελέγχου πρόσβασης

Τα συστήματα ελέγχου πρόσβασης (access control) εφαρμόζονται με σκοπό να ελέγχουν την είσοδο σε έναν προστατευόμενο χώρο και να επιτρέπουν μόνο στα κατάλληλα άτομα την πρόσβαση. Όταν ένα τέτοιο σύστημα εφαρμόζεται σε χώρο εργασίας, μπορεί να λειτουργεί επίσης και ως σύστημα ελέγχου του ωραρίου των εργαζομένων.

Η εταιρία που έχει εγκαταστήσει ένα τέτοιο σύστημα έχει τη δυνατότητα να γνωρίζει πόσα άτομα βρίσκονται στο χώρο και την ώρα προσέλευσής τους. Επίσης μέσω των συστημάτων ελέγχου πρόσβασης δίνεται η δυνατότητα να μπορούν να εισέλθουν σε συγκεκριμένους χώρους της εταιρίας μόνο εξουσιοδοτημένα άτομα, αυξάνοντας με τον τρόπο αυτό την ασφάλειά της και έναντι εσωτερικών απειλών.

Η τυπική μορφή ενός συστήματος ελέγχου πρόσβασης αποτελείται από τα ακόλουθα τμήματα:

- *Κεντρική μονάδα ελέγχου με δυνατότητα σύνδεσης σε Η/Υ*

Η κεντρική μονάδα ελέγχου λαμβάνει όλα τα σήματα από τις περιφερειακές συσκευές και ενεργοποιεί την αντίστοιχη κατά περίπτωση έξοδο. Ο έλεγχος γίνεται μέσω ηλεκτρονικών ολοκληρωμένων μικροελεγκτών και του κατάλληλου λογισμικού ενός υπολογιστή.

Εικόνα 1.9: Κεντρική μονάδα συστήματος ελέγχου πρόσβασης (http://www.tdsi.co.uk/)

- *Τοπικό ελεγκτή (Controller)*

Τοποθετείται έξω από τον χώρο που απαιτεί αυξημένη ασφάλεια και εντοπίζει πότε προσεγγίζεται η είσοδος του συγκεκριμένου χώρου και επιτρέπει την πρόσβαση του ατόμου ή όχι. Υπάρχει ως υλικό ράγας και τοποθετείται σε κάποιο κεντρικό πίνακα ή ως συσκευή που τοποθετείται δίπλα στην προς έλεγχο είσοδο, η οποία διαθέτει ενσωματωμένο τον αναγνώστη της κάρτας.

Ο ελεγκτής στέλνει σήμα στην κεντρική μονάδα ελέγχου και αυτή αφού επεξεργαστεί το σήμα και διασταυρώσει τις πληροφορίες της κάρτας με τα αποθηκευμένα δεδομένα, δίνει εντολή στο ηλεκτρικό κυπρί να επιτρέψει την είσοδο στον χώρο.

Οι τοπικοί ελεγκτές, προγραμματίζονται, ώστε να αναγνωρίζουν ένα πλήθος κωδικών οι οποίοι αντιστοιχούν σε συγκεκριμένα άτομα. Με τον τρόπο αυτό έχουμε καταγραφή κινήσεων, των ατόμων που εισήλθαν στο φυλασσόμενο χώρο.

- *Συσκευές ανάγνωσης καρτών (Εγγύτητας, Βιομετρικοί, Smart κ.λπ.)*

Όσο αυξάνονται οι απαιτήσεις ασφαλείας του χώρου, τόσο πιο απροσπέλαστα συστήματα υιοθετούνται. Η πρόσβαση μέσω κάρτας έχει παρατηρηθεί ότι δεν αποτελεί αυξημένο μέτρο ασφάλειας. Συνεπώς, έχουν βρεθεί νέοι τρόποι ελέγχου της πρόσβασης που παρέχουν μεγαλύτερο βαθμό

ασφάλειας, όπως οι συσκευές ανάγνωσης μαγνητικών καρτών, οι βιομετρικοί αισθητήρες κ.λπ.

Εικόνα 1.10: Συσκευή ανάγνωσης καρτών (http://www.tdsi.co.uk/)

- *Λογισμικό διαχείρισης κινήσεων και διαβάθμισης της προσβασιμότητας*

- *Κάρτες ελέγχου πρόσβασης απλές ή προτυπωμένες (μαγνητικές, εγγύτητας κ.λπ.)*

Η συσκευή ανάγνωσης μαγνητικών καρτών είναι είτε αυτόνομη είτε ενσωματωμένη στον τοπικό ελεγκτή. Η κάρτα τοποθετείται στη συσκευή ή είναι ενσωματωμένη στη κλειδαριά της πόρτας και παρέχει μέτριο βαθμό προστασίας. Έχει το βασικό μειονέκτημα της απαραίτητης και συνεχούς κατοχής της κάρτας, με αποτέλεσμα, όταν κάποιος εργαζόμενος δεν την έχει μαζί του για κάποιο λόγο, να γίνεται δύσκολη η κίνησή του στους χώρους.

Εικόνα 1.11: Συσκευή ανάγνωσης μαγνητικής κάρτας (http://www.tdsi.co.uk/)

Τα αριθμητικά πληκτρολόγια εισόδου δεν απαιτούν μαγνητική κάρτα, αλλά την πληκτρολόγηση ενός συγκεκριμένου κωδικού. Χρησιμοποιείται συχνά σε

εισόδους parking εταιρειών ή οργανισμών, και επίσης, το συναντάμε στις Μ.Ε.Θ, όπου ιατρικό και νοσηλευτικό προσωπικό εισέρχεται και εξέρχεται συχνά στον χώρο, ενώ απαγορεύεται η ελεύθερη πρόσβαση στους επισκέπτες.

Εικόνα 1.12: Αριθμητικό πληκτρολόγιο ελέγχου εισόδου (http://www.tdsi.co.uk/)

Σε χώρους που απαιτούν μεγάλο βαθμό ασφάλειας και ελεγχόμενης πρόσβασης μπορούν να τοποθετηθούν βιομετρικοί αναγνώστες δακτυλικών αποτυπωμάτων ή ακόμη και σύστημα ανάγνωσης της ίριδας. Και τα δύο αυτά χαρακτηριστικά είναι μοναδικά για κάθε άνθρωπο.

Ο βιομετρικός αναγνώστης δακτυλικών αποτυπωμάτων αναγνωρίζει έναν χρήστη χωρίς αυτός να χρειάζεται κάρτα ή κωδικό, με βάση κάποια πρότυπα που έχει αποθηκευμένα. Αποτελεί επιλογή με υψηλό δείκτη ασφάλειας μια και είναι δύσκολη έως αδύνατη η αντιγραφή των δακτυλικών αποτυπωμάτων.

Η ίριδα είναι η κυκλική επιφάνεια που περικλείει την κόρη του ματιού. Η ίριδα του ματιού περιέχει ένα πλούσιο και πολύπλοκο μωσαϊκό γραφών και σχημάτων (υπάρχουν περίπου 200 τέτοια σημεία), τα οποία είναι μοναδικά για κάθε υποκείμενο. Οι μέθοδοι αναγνώρισης που βασίζονται στην ίριδα θεωρούνται από τις πλέον ακριβείς (accurate) μεθόδους. Για να μπορεί να εφαρμοσθεί η μέθοδος αυτή πρέπει αρχικά να φωτογραφηθεί η ίριδα με υπέρυθρη ακτινοβολία.

Εικόνα 1.13: Βιομετρικές συσκευές ελέγχου πρόσβασης (http://www.tdsi.co.uk/)

Τα συγκεκριμένα συστήματα βρίσκουν εφαρμογή σε:

- γραφεία για τον έλεγχο πρόσβασης σε φυλασσόμενους χώρους, όπως αποθήκες, computer rooms, αίθουσες συνεδριάσεων, αλλά και για τη διευκόλυνση μετακίνησης του προσωπικού μεταξύ ορόφων ή τμημάτων της επιχείρησης.
- νοσοκομεία για τον έλεγχο πρόσβασης σε κλινικές, ΜΕΘ, ΜΑΦ, φαρμακεία, λογιστήρια, αποθήκες εξοπλισμού γα την αποτροπή ανεξέλεγκτης εισόδου επισκεπτών.
- σε κατοικίες και διαμερίσματα στην κεντρική είσοδο ή στις βοηθητικές εισόδους αποθηκών και γκαράζ για την ταχύτερη είσοδο των ενοίκων, χωρίς χρήση κλειδιού.
- βιομηχανικούς και αποθηκευτικούς χώρους για την αποτροπή πρόσβασης μη εξουσιοδοτημένων ατόμων σε αυτοματοποιημένες γραμμές παραγωγής, υγειονομικούς και αποθηκευτικούς χώρους.
- καταστήματα εξυπηρέτησης κοινού (Εστιατόρια – Καφετέριες – Καταστήματα λιανικής) για την προστασία υγειονομικών χώρων (τουαλέτες – κουζίνες – παρασκευαστήρια), για τον έλεγχο αποθηκών ή ταμείου, αλλά και για την προστασία εργαζομένων κατά τη διάρκεια νυκτερινής εργασίας.

ΚΕΦΑΛΑΙΟ 2: Πρωτόκολλα επικοινωνίας

2.1 Εξέλιξη πρωτοκόλλου επικοινωνίας

Η επικοινωνία μεταξύ του συστήματος συναγερμού και του κέντρου λήψης σημάτων απαιτεί την εφαρμογή συγκεκριμένου πρωτοκόλλου επικοινωνίας για την αποστολή και τη λήψη των δεδομένων. Με τον όρο πρωτόκολλο αναφερόμαστε σε ένα ή περισσότερους τρόπους ηλεκτρονικής μετάδοσης ενός σήματος και σε μια συγκεκριμένη κωδικοποίηση. Οι διαθέσιμες επιλογές επικοινωνίας είναι αρκετές, αλλά η πιο συνηθισμένη είναι το πρωτόκολλο επικοινωνίας Ademco Contact ID. Πρέπει όμως το κάθε σύστημα συναγερμού να αξιολογείται μεμονωμένα και να επιλέγεται το καταλληλότερο κατά περίπτωση σύστημα επικοινωνίας. Η γνώση των πρωτοκόλλων είναι απαραίτητη για τη σωστή επιλογή των μέσων μετάδοσης των σημάτων συναγερμού.

Σε περίπτωση ενεργοποίησης του συναγερμού λόγω κάποιου συμβάντος που εντοπίστηκε, το σύστημα συναγερμού πραγματοποιεί μια κλήση στον αριθμό του κέντρου λήψης σημάτων, ο οποίος έχει οριστεί από τον τεχνικό κατά την εγκατάσταση του συστήματος. Με τον τρόπο αυτό ο δίαυλος επικοινωνίας τίθεται σε λειτουργία και το μήνυμα μεταδίδεται βάσει του προκαθορισμένου πρωτοκόλλου.

Από τα πρώτα πρωτόκολλα που χρησιμοποιήθηκαν ήταν το *Ademco Express 4x2.* Πρόκειται για ένα διψήφιο πρωτόκολλο, απλό στον προγραμματισμό του, το οποίο όμως δεν έχει ενιαίο λεξικό και είναι ξεχωριστό για την κάθε εφαρμογή. Ο τεχνικός αντιστοιχίζει κάθε συμβάν σε ένα ψηφίο, αλλά πρέπει να ενημερώσει το κέντρο λήψης σημάτων για τις αντιστοιχίες αυτές, καθώς δεν υπάρχει ενιαίο λεξικό και το πρωτόκολλο πρέπει να διαβαστεί από τους χειριστές.

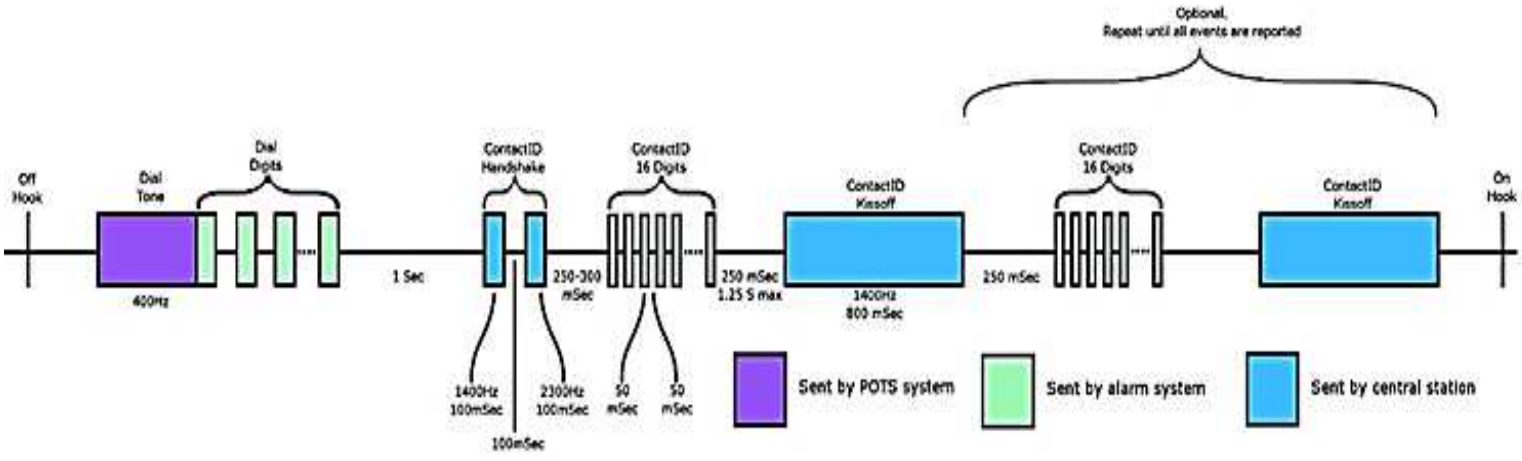
Το σήμα που λάμβανε το κέντρο αποτελούνταν από έναν τετραψήφιο κωδικό, ο οποίος προσδιόριζε τον πελάτη και ένα διψήφιο κωδικό που δήλωνε το συμβάν που ενεργοποίησε τον συναγερμό. Τα δύο αυτά ψηφία όμως δεν ήταν επαρκή για να περιγράψουν το συμβάν με μεγάλη λεπτομέρεια. Με την εξέλιξη των συστημάτων ήταν απαραίτητο να μεταδίδονται πληροφορίες σχετικά με την παρακολούθηση περισσότερων ζωνών, με την επίβλεψη της λειτουργίας των ανιχνευτών και του συνολικού συστήματος.

Για το λόγο αυτό το πρωτόκολλο αυτό αντικαταστάθηκε από το πρωτόκολλο *Contact ID*, η λειτουργία του οποίου βασίζεται σε νέα, διαφορετική φιλοσοφία. (Digital Communication Standard, 1999)

2.2 Το πρωτόκολλο Ademco Contact ID

2.2.1 Περιγραφή

Το Contact ID είναι ένα πρωτόκολλο επικοινωνίας το οποίο κατασκευάστηκε από την εταιρεία ADEMCO και χρησιμοποιεί τους DTMF τόνους για την μεταβίβαση των πληροφοριών από το πομπό στο δέκτη. Η λογική του πρωτοκόλλου βασίζεται στη δημιουργία ενός κοινού πρωτοκόλλου, με κοινή κωδικοποίηση για όλους. Ο σταθμός λήψης σημάτων λαμβάνει την κλήση και περιμένει για ένα δευτερόλεπτο, μετά το οποίο περιμένει τη χειραψία (handshake). Ύστερα από 250 ms, το σύστημα συναγερμού στέλνει το μήνυμα, το οποίο αποτελείται από 16 ψηφία DTMF (σήμα πολυσυχνότητας διπλού τόνου). Το τελευταίο ψηφίο είναι που επιτρέπει στον κεντρικό σταθμό να επαληθεύσει την ακεραιότητα του ληφθέντος μηνύματος. Το Contact ID είναι συμβατό με τις περισσότερες κεντρικές μονάδες των συστημάτων συναγερμού που κυκλοφορούν στην παγκόσμια αγορά ανεξαρτήτως κατασκευαστή. (www.eurogard.gr)



Εικόνα 2.1: Επικοινωνία με το κέντρο λήψης σημάτων με το πρωτόκολλο Contact ID (www.eurogard.gr)

Αναλυτικά, το μήνυμα Contact-ID περιέχει τα εξής 16 ψηφία :

Τα 4 πρώτα ψηφία προσδιορίζουν το συγκεκριμένο σύστημα συναγερμού ή πελάτη στον κεντρικό σταθμό. Με τα ψηφία αυτά το κέντρο λήψης σημάτων προσδιορίζει από ποιον πελάτη λαμβάνει το σήμα μεταξύ χιλιάδων πελατών.

Ο τριψήφιος κωδικός που ακολουθεί αναφέρει τι είδους συμβάν έχει προκύψει στο σύστημα συναγερμού (ενεργοποίηση ή επαναφορά/αποκατάσταση).

Ακολουθεί η μετάδοση του διψήφιου Group/ Αριθμός Partition και του τριψήφιου Αριθμού Ζώνης, ψηφία τα οποία διευκρινίζουν ποια περιοχή του συστήματος αφορά το συμβάν.

Αν η λήψη του μηνύματος είναι επιτυχής, ο σταθμός στέλνει ένα σήμα kissoff. Εάν το σύστημα συναγερμού δεν λάβει το kissoff, αναμεταδίδει το μήνυμα ενώ σε περίπτωση μη μετάδοσης του μηνύματος, το σύστημα εμφανίζει βλάβη/service.

Η χρήση λοιπόν του Contact ID επιτρέπει την αναλυτική μετάδοση συμβάντων με απεριόριστες δυνατότητες περιγραφής, π.χ. μια ζώνη έχει τη δυνατότητα να στείλει συναγερμό διάρρηξης, παρεμπόδισης οπλισμού κ.ά. Η σημαντική διαφορά είναι ότι τίποτα απ' όλα αυτά δεν προγραμματίζεται από τον τεχνικό, γεγονός που διευκολύνει ιδιαίτερα τον προγραμματισμό ενός συστήματος, την επικοινωνία του με το κέντρο λήψης σημάτων, την ανάγνωση των συμβάντων και συνεπώς καθιστά την παρακολούθηση ενός συστήματος πιο αξιόπιστη.

2.2.2 Βασικά πλεονεκτήματα του Contact ID

- Παροχή *απομακρυσμένων πληροφοριών* για την λειτουργία ενός συστήματος συναγερμού .Οι πληροφορίες αυτές θα πρέπει να είναι σε μια μορφή η οποία θα είναι *εύκολα διαχειρίσιμη από τον χειριστή ενός κέντρου λήψης σημάτων*.
- Ε*λάχιστος χρόνος μεταβίβασης* της πληροφορίας, με πλεονεκτήματα τη μείωση των δεκτών που απαιτούνται για την λήψη των πληροφοριών από τον κεντρικό σταθμό και μειωμένο κατά το ελάχιστο τον χρόνο δέσμευσης της τηλεφωνικής γραμμής.
- *Ελαχιστοποίηση του σφάλματος* κατά την μετάδοση των πληροφοριών
- *Ελαχιστοποίηση* του κοστολογίου των υλικών που απαιτούνται για την μετάδοση των πληροφοριών.

2.3 Απαιτήσεις για τη μετάδοση των σημάτων

Όπως αναφέρθηκε, για την επικοινωνία μεταξύ πομπού και δέκτη είναι απαραίτητα τρία στοιχεία:

1. Χειραψία (Handshake): Η χειραψία αποτελείται από ένα ζεύγος τόνων μονής συχνότητας με χρονική αλληλουχία
2. Message Block: Αποτελείται από μια σειρά DTMF τόνων χωρισμένων με κενά

3. Acknowledgement: Αποτελείται από έναν απλό τόνο. (Digital Communication Standard, 1999)

2.3.1 Τόνοι Χειραψίας

Οι τόνοι χειραψίας εκπέμπονται από το δέκτη. Ο στόχος είναι να δώσει σήμα στον πομπό ότι το κανάλι επικοινωνίας είναι έτοιμο για την μεταφορά των δεδομένων. Η ακολουθία τόνων χειραψίας εκπέμπεται από το δέκτη μόλις κλείσει η σύνδεση και με καθυστέρηση τουλάχιστον 0,5 sec, τυπικά όμως η καθυστέρηση αυτή δεν ξεπερνάει τα 2 sec. Στο χρονικό αυτό διάστημα εγκαθίσταται η σύνδεση του τηλεφωνικού δικτύου και ξεκινά η διαδικασία επικοινωνίας.

Σύνθεση Τόνων Χειραψίας

Η ακολουθία τόνων χειραψίας αποτελείται από:

- Τόνος 1400 Hz ±3% με διάρκεια 100 msec ±5%
- Παύση των 100 msec ±5%
- Τόνος 2300 Hz ±3% με διάρκεια 100 msec ±5%

Πρέπει να σημειωθεί ότι οι πομποί θα πρέπει να δέχονται ένα σφάλμα συχνότητας τουλάχιστον ± 5% για να εξασφαλιστεί η συμβατότητα με δέκτες παλαιότερου τύπου. (Digital Communication Standard, 1999)

2.3.2 Message Blocks

Ένα Message Block αποστέλλεται από τον πομπό για κάθε μήνυμα που βρίσκεται στην ουρά του πομπού. Κάθε Message Block περιέχει επαρκείς πληροφορίες, ώστε να αναφέρει ένα συμβάν στο σύστημα. Το πρώτο message block αποστέλλεται ξεκινώντας 250 msec (250 msec ελάχιστη τιμή και μέγιστη 300 msec) μετά το τέλος είτε της ακολουθίας τόνων χειραψίας είτε μετά τον τόνο αποδοχής (acknowledgement). Η χρονική καθυστέρηση μετράται από το τέλος του τόνου.

Σύνθεση μηνύματος

Η μορφή του μηνύματος είναι:

ACCT MT Q XYZ GG CCC

όπου:

ACCT: Είναι ο τετραψήφιος κωδικός αναγνώρισης του εκάστοτε συστήματος από το κέντρο λήψεως σημάτων (1-9, B-F).

MT: Είναι μια ακολουθία 2 ψηφίων η οποία υποδηλώνει ότι τα δεδομένα στέλνονται με πρωτόκολλο Contact ID. Μπορεί να είναι ο αριθμός 18 είτε ο αριθμός 98. Το 18 είναι προτιμότερο γιατί παλαιότερα μοντέλα δεκτών δεν δέχονται το 98.

Q: Τύπος γεγονότος, μας δίνει συγκεκριμένες πληροφορίες για το εκάστοτε γεγονός

- 1 = Νέο Γεγονός ή αφοπλισμός συστήματος
- 3 = Νέα Αποκατάσταση ή οπλισμός συστήματος
- 6 = Προηγούμενο γεγονός το οποίο έχει αποσταλεί αλλά παραμένει ακόμα.

XYZ: Κωδικός γεγονότος.

GG: Περιοχή ή Partition που αφορά το συγκεκριμένο γεγονός. Λαμβάνει την τιμή 00 αν το σύστημα δεν είναι χωρισμένο σε περιοχές.

CCC: Αριθμός ζώνης ή Χρήστη. Λαμβάνει την τιμή 000 σε περίπτωση που δεν αναφέρεται σε κάποια συγκεκριμένη ζώνη ή συγκεκριμένο χρήστη.

S: 1 ψηφίο Hex άθροισμα ελέγχου, το οποίο υπολογίζεται ως :

(Άθροισμα όλων των ψηφίων του μηνύματος + S) MOD 15 = 0.

Στη συνέχεια ακολουθούν δύο ενδεικτικά παραδείγματα, ώστε να γίνει κατανοητός ο τρόπος επικοινωνίας του πομπού με το δέκτη με βάση το πρωτόκολλο Contact ID. Πρέπει να σημειωθεί ότι το «0» πρέπει να μεταδοθεί ως 10 και να μετρηθεί ως 10 στο άθροισμα των ψηφίων για την επαλήθευση.

1ο Παράδειγμα

- *Σήμα περιμετρικού συναγερμού στην ζώνη 15 του 1ου υποσυστήματος από το χρήστη 1234*

Η ακολουθία είναι η εξής :

1234 18 1131 01 015 8

1234: Είναι ο αριθμός αναγνώρισης του πίνακα συναγερμού από το κέντρο λήψεως σήματος

18: Το σήμα είναι Contact ID

1: Είναι νέο γεγονός

131: Περιμετρικός Συναγερμός

01: Σήμα από το πρώτο υποσύστημα

015: Η ζώνη 15 είναι η ζώνη που έδωσε συναγερμό

8: Είναι το CheckSum και υπολογίζετε ως εξής :

- Προσθέτω όλα τα ψηφία του σήματος μηνύματος και όπου έχω ψηφίο «0» το μετράω για 10: (1+2+3+4)+(1+8)+(1+1+3+1)+(10+1)+(10+1+5) = 52
- Βρίσκω το επόμενο μεγαλύτερο πολλαπλάσιο του 15 και το αφαιρώ από το άθροισμα των ψηφίων 60-52=8

2ο Παράδειγμα

- *Ακύρωση σήματος συναγερμού της ζώνης 15 του 1ου υποσυστήματος από το χρήστη 1234*

Η ακολουθία είναι η εξής :

1234 18 3131 01 015 6

1234: Είναι ο αριθμός αναγνώρισης του πίνακα συναγερμού από το κέντρο λήψεως σήματος

18: Το σήμα είναι Contact ID

3: Ακύρωση συναγερμού

131: Περιμετρικός Συναγερμός

01: Σήμα από το πρώτο υποσύστημα

015: Η ζώνη 15 είναι η ζώνη που έδωσε συναγερμό

6: Είναι το CheckSum

Το μήνυμα αποστέλλεται με τυπικούς τόνους DTMF. Ο χρονισμός των τόνων πρέπει να είναι ο ακόλουθος:

Έναρξη- 50 msec (μέγιστο 60 msec)-Λήξη-50 msec (μέγιστο 60 msec)*
(Digital Communication Standard, 1999)

Πίνακας 2.1: Συχνότητες και αντιστοιχίες DTMF τόνων (Digital Communication Standard, 1999)

Digit	Low Tone (Hz.)	High Tone (Hz.)	Digit Value
0	941	1336	10
1	697	1209	1
2	697	1336	2
3	697	1477	3
4	770	1209	4
5	770	1336	5
6	770	1477	6
7	852	1209	7
8	852	1336	8
9	852	1477	9
B (*)	941	1209	11
C (#)	941	1477	12
D	697	1633	13
E	770	1633	14
F	852	1633	15

Παρατηρούμε ότι το ψηφίο «0» μεταφέρεται με την τιμή 10 και ως 10 πρέπει να προσμετράται στο άθροισμα των ψηφίων του μηνύματος. Το ζεύγος DTMF 941 Hz και 1633 Hz δε χρησιμοποιείται σε αυτό το format, ενώ η απόκλιση συχνότητας είναι κατά μέγιστο ±1,5%.

Μετά την αποστολή του μηνύματος, ο πομπός αναμένει για 1,25 sec για την έναρξη ενός τόνου kissoff από το δέκτη. Αν ανιχνευτεί η αρχή του τόνου, ο πομπός πρέπει να συνεχίσει να χρονομετρά τον τόνο. Ο πίνακας πρέπει να ανιχνεύσει τουλάχιστον 400 msec τον τόνο kissoff για να θεωρηθεί έγκυρος.

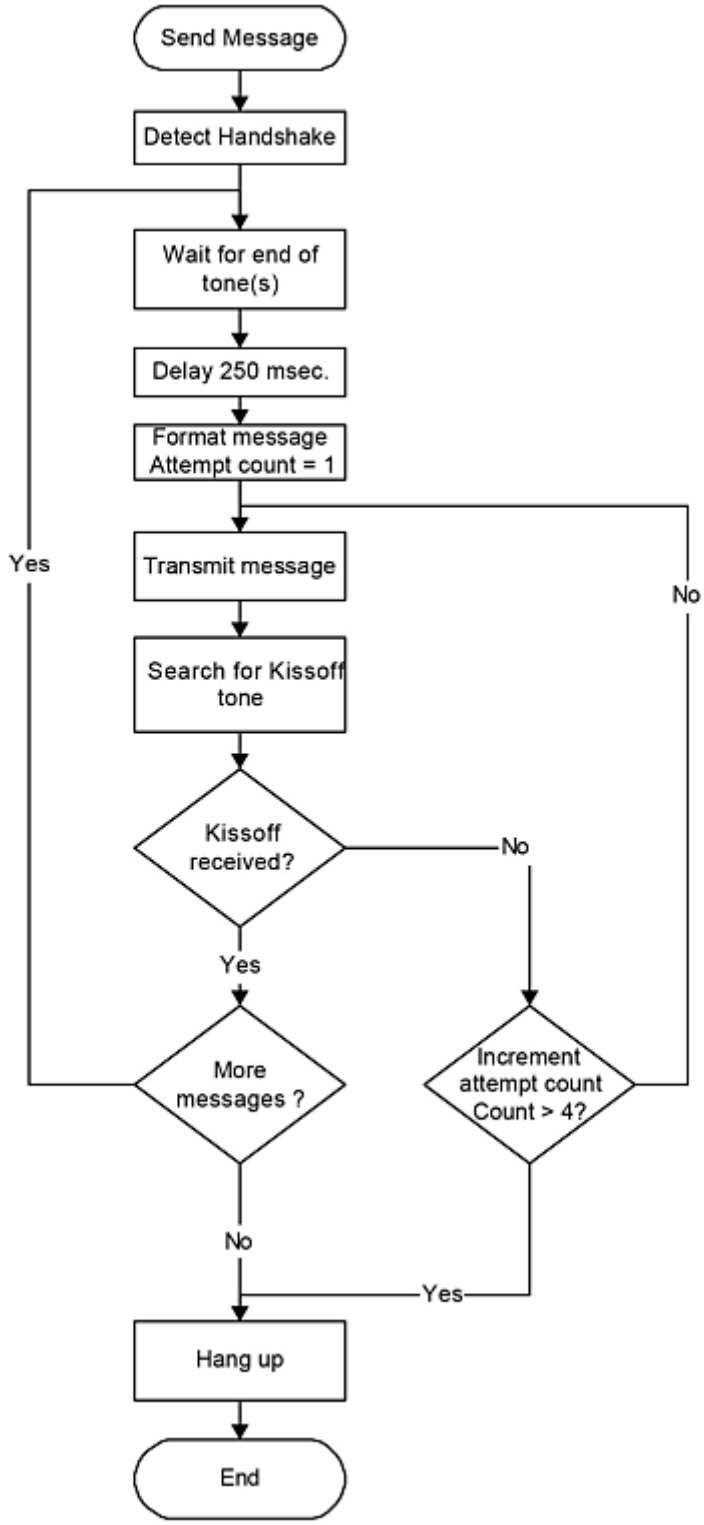
Αν ανιχνευτεί ένας τόνος kissoff, ο πομπός πρέπει να περιμένει να ολοκληρωθεί ο τόνος και ακόμη 250 msec (μέγιστο 300 msec) πριν την έναρξη του επόμενου μηνύματος. Αν δε ληφθεί τόνος kissoff, το μήνυμα πρέπει να επαναληφθεί μετά τη λήξη των 1,25 sec. (Digital Communication Standard, 1999)

2.3.3 Τόνος αποδοχής kissoff

Ο τόνος kissoff εκπέμπεται από το δέκτη και χρησιμοποιείται για να ενημερώσει τον πομπό ότι το μήνυμα έχει ληφθεί επιτυχώς. Η συχνότητα του τόνου πρέπει να είναι 1400 Hz ±3% και πρέπει να αποστέλλεται από το λήπτη για τουλάχιστον 750 msec και κατά μέγιστο για 1 sec. Ο πομπός πρέπει να ανιχνεύσει τον τόνο για 400 msec για να θεωρηθεί ο τόνος kissoff έγκυρος.

Ο πομπός επιτρέπεται να εκτελέσει ως 4 προσπάθειες για να μεταδώσει το μήνυμα, προτού τερματιστεί η κλήση και επαναληφθεί. Ο μετρητής μηδενίζεται κάθε φορά που λαμβάνεται ένα έγκυρο σήμα kissoff.

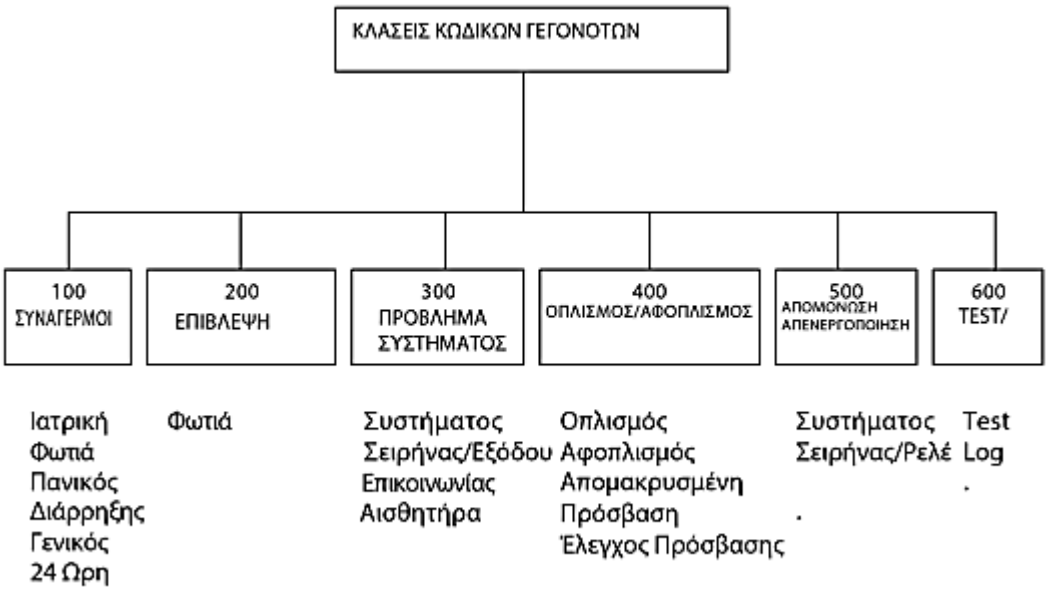
Η προηγούμενη διαδικασία περιγράφεται σχηματικά στην Εικόνα 2.2.



Εικόνα 2.2: Μπλοκ Διάγραμμα Μετάδοσης Δεδομένων (Digital Communication Standard, 1999)

2.4 Κωδικοί γεγονότων

Στην Εικόνα 2.3 παρουσιάζονται οι κωδικοί των γεγονότων σύμφωνα με το πρωτόκολλο Ademco Contact ID.



Εικόνα 2.3: Κλάσεις κωδικών γεγονότων (Digital Communication Standard, 1999)

Οι επεξηγήσεις των κωδικών του πρωτοκόλλου παρουσιάζονται ακολούθως (Πίνακας 2.2).

Πίνακας 2.2: Κωδικοί Γεγονότων Και Εμφανιζόμενο Μήνυμα (Digital Communication Standard, 1999)

Κωδικός	Μήνυμα Στην Οθόνη
Συναγερμοί Ιατρικής Βοήθειας	
100	Επείγον - Ιατρική Βοήθεια
101	Επείγον - Ιατρική Βοήθεια
102	Αποτυχία Ελέγχου
Συναγερμοί Φωτιάς	
110	Φωτιά – Συναγερμός Φωτιάς
111	Φωτιά - Ανίχνευση Καπνού
112	Φωτιά - Καύση
113	Φωτιά - Κατάσβεση

114	Φωτιά - Ενεργοποίηση Θερμοδιαφορικού Ανιχνευτή
115	Φωτιά - Ενεργοποίηση Μπουτόν Πυρανίχνευσης
116	Φωτιά - Ενεργοποίηση Ανιχνευτή Αγωγού
117	Φωτιά - Ενεργοποίηση Ανιχνευτή Φλόγας
118	
Συναγερμοί Πανικού	
120	Πανικός – Συναγερμός Πανικού
121	Πανικός – Αφοπλισμός Υπό Απειλή
122	Πανικός - Σιωπηλός Πανικός
123	Πανικός - Ηχητικός Συναγερμός
Συναγερμοί Διάρρηξης	
130	Διάρρηξη – Συναγερμός Διάρρηξης
131	Διάρρηξη – Περιμετρικός Συναγερμός
132	Διάρρηξη – Εσωτερικού Χώρου Συναγερμός
133	Διάρρηξη – 24ωρος Συναγερμός
134	Διάρρηξη – Συναγερμός Εισόδου/Εξόδου
135	Διάρρηξη – Συναγερμός Ημέρας/Νύχτας
136	Διάρρηξη – Συναγερμός Εξωτερικού Χώρου
137	Διάρρηξη – Συναγερμός από Tamper
Γενικοί Συναγερμοί	
140	Συναγερμός – Γενικός Συναγερμός
141	Συναγερμός – Έλεγχος ανοιχτού Βρόγχου
142	Συναγερμός – Έλεγχος μήκος βρόγχου
143	Συναγερμός – Αποτυχία πλακέτας επέκτασης
144	Συναγερμός – Tamper ανιχνευτή
145	Συναγερμός – Tamper πλακέτας επέκτασης
146	Συναγερμός – Σιωπηλός Συναγερμός
147	Συναγερμός - Εποπτεία Αισθητήρα
24ωρο Συναγερμός όχι από διάρρηξη	
150	Συναγερμός - 24ωρη όχι διάρρηξης
151	Συναγερμός - Ανίχνευση αερίου
152	Συναγερμός - Χαμηλή Θερμοκρασία

153	Συναγερμός - Απώλεια Θερμότητας
154	Συναγερμός - Πλημμύρα
156	Συναγερμός - Ζώνη Ημέρας
157	Συναγερμός - Χαμηλό επίπεδο στάθμης αερίου
158	Συναγερμός - Υψηλή θερμοκρασία
159	Συναγερμός - Χαμηλή Θερμοκρασία
161	Συναγερμός – Απώλεια ροής αέρα
162	Συναγερμός – Μονοξείδιο του Άνθρακα
163	Πρόβλημα – Στάθμη δεξαμενής
168	Πρόβλημα – Υψηλή υγρασία
Εποπτεία Φωτιάς	
200	Εποπτεία – Φωτιά
201	Εποπτεία - Χαμηλή πίεση του νερού
202	Εποπτεία - Χαμηλό διοξείδιο του άνθρακα
203	Εποπτεία – Αισθητήρας βαλβίδας
204	Εποπτεία – Χαμηλή στάθμη νερού
205	Εποπτεία – Ενεργοποίηση Αντλίας
206	Εποπτεία – Αποτυχία αντλίας

Προβλήματα Συστήματος	
300	Πρόβλημα - Συστήματος
301	Πρόβλημα – Απώλεια AC
302	Πρόβλημα – Πτώση Μπαταρίας
303	Πρόβλημα – Πρόβλημα RAM
304	Πρόβλημα - Πρόβλημα ROM
305	Πρόβλημα – Reset Συστήματος
306	Πρόβλημα – Αλλαγή Προγραμματισμού
307	Πρόβλημα - Αποτυχία Test
308	Πρόβλημα – Κλείσιμο Συστήματος
309	Πρόβλημα - Αποτυχία Test Μπαταρίας
310	Πρόβλημα - Πρόβλημα Γείωσης
311	Πρόβλημα - Απώλεια Μπαταρίας

312	Πρόβλημα - Υπερτροφοδότηση
313	Πρόβλημα - Reset Εγκαταστάτη
Προβλήματα Σειρήνων/Ρελέ	
320	Πρόβλημα - Σειρήνα/Ρελέ
321	Πρόβλημα - Σειρήνα 1
322	Πρόβλημα - Σειρήνα 2
323	Πρόβλημα - Ειδοποίηση Ρελέ
324	Πρόβλημα - Πρόβλημα Ρελέ
325	Πρόβλημα - Αναστροφή Ρελέ
326	Πρόβλημα - Αναστροφή Ρελέ
327	Πρόβλημα - Κοινοποίηση Συσκευών 4
Προβλήματα Περιφερειακών Συστήματος	
R330	Πρόβλημα - Περιφερειακά Συστήματος
331	Πρόβλημα - Πρόβλημα Ανοιχτού Βρόγχου
332	Πρόβλημα - Πρόβλημα Βρόγχου
333	Πρόβλημα - Αποτυχία Πλακέτας Επέκτασης
334	Πρόβλημα - Αποτυχία Επαναλήπτη
335	Πρόβλημα - Έλλειψη χαρτιού στο τοπικό εκτυπωτή
336	Πρόβλημα - Αποτυχία τοπικού εκτυπωτή
337	Πρόβλημα - Έλλειψη Τάσης Στην Πλακέτα Επέκτασης
338	Πρόβλημα - Χαμηλή Μπαταρία Στην Πλακέτα Επέκτασης
339	Πρόβλημα - Reset Πλακέτας Επέκτασης
341	Πρόβλημα - Tamper Πλακέτας Επέκτασης
342	Πρόβλημα - Απώλεια Τάσης Πλακέτας Επέκτασης
343	Πρόβλημα - Αποτυχία Test Πλακέτας Επέκτασης
344	Πρόβλημα - Ανίχνευση Jam στον Ασύρματο Δέκτη
Προβλήματα Επικοινωνίας	
350	Πρόβλημα - Επικοινωνία
351	Πρόβλημα - Σφάλμα Δέκτη 1
352	Πρόβλημα - Σφάλμα Δέκτη 2
353	Πρόβλημα - Σφάλμα Ασύρματου Στοιχείου Μακρινής Δέσμης
354	Πρόβλημα - Αποτυχία Επικοινωνίας

355	Πρόβλημα - Απώλεια Εποπτείας Ασύρματων Συσκευών
356	Πρόβλημα - Απώλεια Ασύρματου Δέκτη
357	Πρόβλημα - Πρόβλημα Ασύρματου Στοιχείου Μακρινής Δέσμης
Προστασία Βρόγχου	
370	Πρόβλημα - Προστασία Βρόγχου
371	Πρόβλημα - Προστασία Ανοιχτού Βρόγχου
372	Πρόβλημα - Προστασία Βρόγχου
373	Πρόβλημα - Πρόβλημα Φωτιάς
374	Πρόβλημα - Λανθασμένη Έξοδος
375	Πρόβλημα - Πρόβλημα στη ζώνη πανικού
376	Πρόβλημα - Πρόβλημα στη ζώνη ομηρίας
377	Πρόβλημα - Πρόβλημα Ταλαντωτή
378	Πρόβλημα - Πρόβλημα Διασταυρωμένης ζώνης
Αισθητήρες	
380	Πρόβλημα - Πρόβλημα ανιχνευτή
381	Πρόβλημα - Απώλεια Εποπτείας RF
382	Πρόβλημα - Απώλεια Εποπτείας RPM
383	Πρόβλημα - Tamper αισθητήρα
384	Πρόβλημα - Χαμηλή Μπαταρία RF
385	Πρόβλημα - Υψηλή ευαισθησία καπνού
386	Πρόβλημα - Χαμηλή ευαισθησία καπνού
387	Πρόβλημα - Υψηλή ευαισθησία διάρρηξης
388	Πρόβλημα - Χαμηλή ευαισθησία διάρρηξης
389	Πρόβλημα - Αποτυχία Test ανιχνευτή
391	Πρόβλημα - Σφάλμα στο ρολοι του αισθητήρα
393	Πρόβλημα - Ειδοποίηση Συντήρησης
Άνοιγμα/Κλείσιμο Συστήματος	
400	Οπλισμός/Αφοπλισμός συστήματος
401	Οπλισμός/Αφοπλισμός από χρήστη
402	Οπλισμός/Αφοπλισμός από ομάδα
403	Αυτόματος οπλισμός/αφοπλισμός
404	Αργοπορημένος Οπλισμός/Αφοπλισμός

405	Αναβαλλόμενος Οπλισμός/Αφοπλισμός
406	Ακύρωση από χρήστη
407	Απομακρυσμένος οπλισμός/αφοπλισμός
408	Γρήγορος οπλισμός
409	Οπλισμός/Αφοπλισμός μέσω κλειδοδιακόπτη
435	Πρόσβαση δεύτερου χρήστη
436	Ακανόνιστη πρόσβαση
441	Οπλισμός STAY
442	Οπλισμός STAY από κλειδοδιακόπτη
451	Άνοιγμα/Κλείσιμο Νωρίς από χρήστη
452	Άνοιγμα/Κλείσιμο Αργά από χρήστη
453	Αποτυχία Ανοίγματος
454	Αποτυχία Κλεισίματος
455	Αποτυχία αυτόματου οπλισμού
456	Μερικός Οπλισμός
457	Λάθος έξοδος από χρήστη
459	Πρόσφατο κλείσιμο
461	Εισαγωγή λάθος κωδικού
462	Εισαγωγή σωστού κωδικός
463	Επανόπλιση μετά από συναγερμό
464	Αυτόματος οπλισμός με την λήξη του χρόνου
465	Reset Συναγερμού Πανικού
466	Service
Απομακρυσμένη Πρόσβαση	
411	Απομακρυσμένα - Απαιτείται επανάκληση
412	Απομακρυσμένα - Επιτυχημένη πρόσβαση
413	Απομακρυσμένα – Αποτυχημένη Πρόσβαση
414	Απομακρυσμένα - Κλείσιμο συστήματος
415	Απομακρυσμένα - Κλείσιμο Τηλεφωνητή
416	Απομακρυσμένα - Επιτυχημένο Upload
Έλεγχος Πρόσβασης	
421	Πρόσβαση – Απαγόρευση Πρόσβασης

422	Πρόσβαση – Πρόσβαση Χρήστη
423	Πανικός - Βίαιη Πρόσβαση
424	Πρόσβαση –Απαγόρευση εξόδου
425	Πρόσβαση – Έξοδος
426	Πρόσβαση –Πόρτα Ανοιχτή
427	Πρόσβαση –Πρόβλημα στην κατάσταση της πόρτας
428	Πρόσβαση – Έξοδος της ζώνης με πρόβλημα
429	Πρόσβαση – Είσοδος στον προγραμματισμό
430	Πρόσβαση – Έξοδος από προγραμματισμό
431	Πρόσβαση – Αλλαγή επιπέδου απειλής
432	Πρόσβαση – Σφάλμα στην έξοδο του καρταναγνώστη
433	Πρόσβαση –Αποκλεισμός ζώνης με σφάλμα
434	Πρόσβαση –Αποκλεισμός καρταναγνώστη με πρόβλημα κατάστασης
435	Πρόσβαση – Πρόσβαση 2 χρήστη
436	Πρόσβαση – Ακανόνιστη πρόσβαση
Απενεργοποίηση Συστήματος	
501	Απενεργοποίηση – Απενεργοποίηση Καρταναγνώστη

Απενεργοποίηση Σειρήνων/Ρελέ	
520	Απενεργοποίηση - Σειρήνων/Ρελέ
521	Απενεργοποίηση – Σειρήνα 1
522	Απενεργοποίηση – Σειρήνα 2
523	Απενεργοποίηση – Ρελέ Συναγερμού
524	Απενεργοποίηση – Ρελέ Προβλήματος
525	Απενεργοποίηση - Αναστροφή Ρελέ
526	Απενεργοποίηση - Σειρήνα 3
527	Απενεργοποίηση –Σειρήνα 4
Απενεργοποίηση Περιφερειακών	
531	Πρόσθεση Στοιχείου
532	Αφαίρεση Στοιχείου
Απενεργοποιήσεις Επικοινωνίας	

551	Απενεργοποίηση Τηλεφωνητή
552	Απενεργοποίηση Ασύρματου
553	Απενεργοποίηση Απομακρυσμένου Upload/Download
Απομονώσεις	
570	Απομόνωση Ζώνης
571	Απομόνωση Ζώνης Φωτιάς
572	Απομόνωση 24ωρης ζώνης
573	Απομόνωση ζώνης διάρρηξης
574	Απομόνωση ομάδας χρηστών
575	Απομόνωση ταλαντευτή
576	Παρέκκλιση ζώνης Πρόσβασης
577	Απομόνωση σημείου πρόσβασης
578	Παράκαμψη ζώνης
579	Παράκαμψη ζώνης διεξόδου
Test	
601	Χειροκίνητο Test
602	Περιοδικό Test
603	Περιοδικό Test Ασύρματων
604	Test Φωτιάς
605	Κατάσταση Ακολουθίας
606	Ενεργητικό Άκουσμα
607	Βηματικό Τεστ
608	Πρόβλημα Συστήματος
609	Βίντεο αναμεταδότη ενεργό
611	Τεστ σημείου
612	Μη τεστ σημείου
613	Τεστ ζώνης διάρρηξης
614	Τεστ ζώνης Φωτιάς
615	Τεστ ζώνης πανικού
616	Αίτημα για Service

Ιστορικό Γεγονότων

621	Reset ιστορικού γεγονότων
622	Μνήμη Ιστορικού γεγονότων 50%
623	Μνήμη Ιστορικού γεγονότων 90%
624	Υπερχείλιση Μνήμης Ιστορικού
625	Reset Ημερομηνίας και ώρας
626	Λάθος Ημερομηνία και ώρα
627	Είσοδος στο προγραμματισμό
628	Έξοδος από προγραμματισμό
Προγραμματισμός	
630	Αλλαγή Προγράμματος
631	Αλλαγή εξαιρέσεων προγράμματος
632	Αλλαγή προγράμματος πρόσβασης
Προσωπική Εποπτεία	
641	Μη αποστολή σημάτων για αρκετό χρόνο
642	Αφοπλισμός συστήματος
Διάφορα	
654	Απενεργοποίηση Συστήματος
900	Ματαίωση Απομακρυσμένου Download
901	Ξεκίνημα Απομακρυσμένου Download
	Τέλος Απομακρυσμένου Download
902	Διακοπή Απομακρυσμένου Download
910	Αυτόματο κλείσιμο με απομόνωση
911	Κλείσιμο Απομόνωσης
912	Σιωπηλός Συναγερμός Πυρκαγιάς
913	Εποπτεία Test Σημείου Αρχή/Τέλος
914	Κράτημα Τεστ Αρχή/Τέλος
915	Εκτύπωση τεστ διάρρηξης
916	Εκτύπωση Τεστ εποπτείας
917	Διαγνωστικά Διάρρηξης
918	Διαγνωστικά Φωτιάς
919	Μη δακτυλογραφούμενα διαγνωστικά
920	Προβληματικό Κλείσιμο

921	Αρνηση πρόσβασης λάθος κωδικός
922	Εποπτεία σημείου συναγερμού
923	Εποπτεία σημείου απομόνωσης
924	Εποπτεία σημείου με πρόβλημα
925	Κράτημα απομονωμένου σημείου
926	Διακοπή Ac τροφοδοσίας για 4 ώρες
927	Πρόβλημα εξόδου
928	Κωδικός χρήστη
929	Αποσύνδεση

2.5 Βασική ορολογία συστημάτων συναγερμού

Abort: Χειροκίνητη παρέμβαση κατά την διάρκεια μιας διαδικασίας η οποία ακυρώνει την συγκεκριμένη διαδικασία

Access Code: Είναι ο κωδικός πρόσβασης και αποτελείται από μια σειρά ψηφίων που πρέπει να εισάγει ο χρήστης στο πληκτρολόγιο του συστήματος για να αποκτήσει πρόσβαση στην λειτουργία του συστήματος

Account: Κωδικός αναγνώρισης του εκάστοτε συστήματος συναγερμού από το Κέντρο Λήψεως Σημάτων

Acknowledgement ή ACK: Σήμα το οποίο στέλνει το κέντρο λήψεως σημάτων όταν έχει πραγματοποιηθεί σωστή λήψη των σημάτων.

Alarm: Ένδειξη σήματος εκτάκτου ανάγκης, το οποίο μπορεί να προέρχεται από μια ζώνη παραβίασης ή μια ζώνη πυρανίχνευσης είτε από κάποια άλλη αιτία. Τοπικά μπορεί το συγκεκριμένο σήμα να γίνεται αντιληπτό από μια οπτικό-ακουστική ένδειξη και απομακρυσμένα ο κεντρικός σταθμός λαμβάνει το συγκεκριμένο σήμα, αλλά και την αιτία που προκάλεσε το σήμα αυτό.

Alarm Cancel: Χειροκίνητη επαναφορά του συστήματος σε κατάσταση ηρεμίας μετά από σήμα συναγερμού. Ο κεντρικός σταθμός λαμβάνει και τις δύο καταστάσεις του συστήματος.

Alarm Verification: Γενική ονομασία για τις διάφορες τεχνικές που χρησιμοποιούνται για την επαλήθευση ή μη ενός σήματος συναγερμού, το οποίο στάλθηκε στο κέντρο.

Arm: Οπλισμός του συστήματος από τον χρήστη

Area: Προκαθορισμένο τμήμα της συνολικής περιοχής που καλύπτει το σύστημα το οποίο μπορεί να οπλιστεί/αφοπλιστεί ανεξάρτητα από το υπόλοιπο. Συνήθως το συναντάμε με την ορολογία **“PARTITION”**.

Bypass: Απομόνωση κάποιας ζώνης ή ενός ανιχνευτή. Όταν μια ζώνη ή ένας ανιχνευτής απομονωθεί δεν δίνει σήματα συναγερμού όταν αλλάζει η κατάστασή του κατά τη διάρκεια που το σύστημα είναι οπλισμένο.

Close: Χειροκίνητος ή αυτόματος οπλισμός ενός συστήματος ασφαλείας.

Control/Control Panel: Το μέρος ενός συστήματος ασφαλείας που χειρίζεται τον έλεγχο και την επικοινωνία είτε σαν συνδυασμό είτε ως ξεχωριστές φυσικές μονάδες.

Disarm: Αφοπλισμός του συστήματος.

DTMF: Τυποποιημένη μέθοδος σήματος για την κλήση και τη μεταφορά των δεδομένων, χρησιμοποιώντας ένα συνδυασμό δύο ημιτονοειδών κυμάτων με διαφορετική συχνότητα.

Duress: Κωδικός αφοπλισμού του συστήματος σε περιπτώσεις που ο χρήστης βρεθεί υπό απειλή.

Entry Delay: Ο χρόνος που δίνει το σύστημα για να μπορέσει ο χρήστης να αφοπλίσει το συναγερμό κατά την είσοδο του στο χώρο.

Exit Error: Σήμα που στέλνει η κεντρική μονάδα όταν γίνει ολικός οπλισμός του συστήματος με ανοιχτές ζώνες.

Exit Delay: Είναι ο χρόνος που μας δίνει το σύστημα για να αποχωρήσουμε από τον χώρο πριν τεθεί σε λειτουργία ο συναγερμός.

Fail to Close: Ένα γεγονός που δημιουργείται από το σύστημα σε προκαθορισμένο χρόνο εφόσον αυτό παραμένει σε κατάσταση αφοπλισμού.

Fail to Open: Ένα γεγονός που δημιουργείται από το σύστημα σε προκαθορισμένο χρόνο εφόσον αυτό παραμένει σε κατάσταση οπλισμού.

Handshake: Σήμα που στέλνει το κέντρο λήψεως στο κέντρο συναγερμού και δηλώνει ότι έχει επιτευχτεί η ζεύξη για την αποστολή των σημάτων.

Keypad: Το πληκτρολόγιο του συστήματος μέσω του οποίου ο χρήστης μπορεί να οπλίσει/αφοπλίσει το σύστημα και να έχει πρόσβαση σε όλες τις λειτουργίες του συστήματος.

Open: Χειροκίνητος ή αυτόματος αφοπλισμός ενός συστήματος ασφαλείας.

Panic: Σήμα εκτάκτου ανάγκης. Αποστέλλεται από το σύστημα όταν ο χρήστης κινδυνεύει να βρεθεί σε κατάσταση απειλής.

Receiver: Ο εξοπλισμός που βρίσκεται σε ένα κεντρικό σταθμό λήψεως σημάτων και επικοινωνεί με έναν πίνακα έλεγχου.

Recent Closing: Σήμα που μας δείχνει ότι ο συναγερμός έχει οπλιστεί πρόσφατα.

Report: Σήμα που αποστέλλεται από τον πίνακα έλεγχου προς τον κεντρικό σταθμό και περιέχει λεπτομερείς πληροφορίες σχετικά με ένα γεγονός που έχει ανιχνευθεί ή πληροφορίες για την κατάσταση του συστήματος ασφαλείας.

Supervisory Signal: Σήμα για περιπτώσεις κατάσβεσης πυρκαγιάς, συστήματα περιπολιών κ.λπ.

Transmitter: Το μέρος του συστήματος που στέλνει τα δεδομένα στο κέντρο λήψεως σημάτων.

Trip: Σήμα συναγερμού που παράγεται ως αποτέλεσμα από την ανίχνευση ενός αισθητήρα.

Trouble: Σήμα που αποστέλλεται στο κέντρο λήψεως σημάτων όταν υπάρχει κάποιο πρόβλημα στο σύστημα, όπως για παράδειγμα πρόβλημα στην παροχή ή την τηλεφωνική γραμμή.

Unbypass: Επανενεργοποίηση των απομονωμένων ζωνών.

Verified Alarm: Σήμα συναγερμού το οποίο έχει επιβεβαιωθεί από το κέντρο λήψεως σημάτων. (Digital Communication Standard, 1999)

ΚΕΦΑΛΑΙΟ 3: Δίκτυα επικοινωνίας

3.1 Εισαγωγή

Ένας από τους πιο βασικούς τομείς για τη λειτουργία και την αποτελεσματικότητα ενός συστήματος συναγερμού είναι η δυνατότητα επικοινωνίας του συστήματος είτε με τον τελικό χρήστη, είτε με κεντρικό σταθμό λήψεως σημάτων ή ακόμα και με τον εγκαταστάτη του συστήματος. Ο τρόπος επικοινωνίας διαφέρει ανάλογα με τον κωδικοποιητή που χρησιμοποιεί η κάθε μονάδα. Μια κεντρική μονάδα μπορεί να χρησιμοποιεί παραπάνω από έναν κωδικοποιητές εάν χρειάζεται να έχει εναλλακτικό τρόπο επικοινωνίας σε περιπτώσεις δολιοφθοράς του δικτύου ή βλάβης.

Οι κωδικοποιητές χωρίζονται ανάλογα με τον τρόπο αποστολής των σημάτων (ασύρματη/ενσύρματη αποστολή) αλλά και τον τύπο αυτών (δικτυακά σήματα ή σήματα DTMF).

Η αποστολή των δεδομένων προς το κέντρο λήψης σημάτων μπορεί να γίνει:

- μέσω σταθερής τηλεφωνικής γραμμής (PSTN, ISDN, ADSL)
- μέσω κινητής τηλεφωνίας (GSM, GPRS)
- ασύρματα VHF/UHF

Από τη δεκαετία του ’80 ως σήμερα, ο τρόπος επικοινωνίας με το κέντρο λήψης σημάτων έχει εξελιχθεί και για το λόγο αυτό είναι διαθέσιμες πολλές εναλλακτικές επιλογές, όπως η μετάδοση του σήματος μέσω της τηλεφωνικής γραμμής (PSTN), η μετάδοση του σήματος μέσω κινητής τηλεφωνίας (GSM), τα ασύρματα δίκτυα και οι συσκευές μεταφοράς σήματος μέσω internet. Η εξέλιξη αυτή είναι απαραίτητη, ώστε να μπορεί να σταλεί μεγαλύτερος όγκος πληροφοριών προς το ΚΛΣ. (**www.securitymanager.gr**)

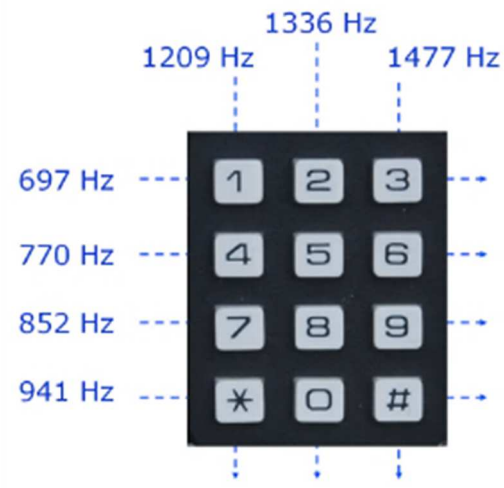
3.1.1 PSTN δίκτυο και κωδικοποιητής

Το δημόσιο τηλεφωνικό δίκτυο μεταγωγής (public switched telephone network- PSTN) είναι το παγκόσμιο τηλεφωνικό δίκτυο. Αποτελείται από τηλεφωνικές γραμμές, οπτικές ίνες, συνδέσμους μέσω μικροκυμάτων, κυψελωτά δίκτυα, τηλεπικοινωνιακούς δορυφόρους, και υποθαλάσσια καλώδια, όλα διασυνδεδεμένα μεταξύ τους μέσω κέντρων μεταγωγής (switching), τα οποία επιτρέπουν σε οποιοδήποτε τηλέφωνο στον κόσμο να επικοινωνήσει με οποιοδήποτε άλλο.

Το PSTN περιγράφεται από τεχνικά πρότυπα που δημιουργεί κυρίως ο διεθνής οργανισμός ITU-T, τα οποία επιτρέπουν την απρόσκοπτη διασύνδεση μεταξύ τηλεφωνικών δικτύων διεθνώς. Για τη διευθυνσιοδότηση (τα κοινά τηλεφωνικά νούμερα) χρησιμοποιούνται τα πρότυπα E.163/ E.164. Ο συνδυασμός των διασυνδεδεμένων δικτύων και του μοναδικού σχήματος αριθμοδοσίας κάνουν δυνατή την επικοινωνία μεταξύ δύο τηλεφωνικών συσκευών. (www.internetsociety.org)

Ο Pstn Κωδικοποιητής είναι ο συνηθέστερος κωδικοποιητής στα συστήματα συναγερμού. Το δίκτυο της σταθερής τηλεφωνίας ήταν το πρώτο μέσο για τη μεταφορά σημάτων, μέσω της χρήσης συσκευών modem. Για να κάνει αποστολή των σημάτων χρησιμοποιεί τη σταθερή τηλεφωνία του εκάστοτε παρόχου και τα σήματα που στέλνει είναι κωδικοποιημένα Dtmf σήματα. Αρκετά είναι και τα πρωτόκολλα τα οποία χρησιμοποιεί ο κωδικοποιητής για την αποστολή σημάτων, με επικρατέστερο τα τελευταία χρόνια το Ademco Contact Id. Άλλα πρωτόκολλα είναι το 4+2,SIA κ.ά.

Για την αποστολή ενός σήματος DTMF απαιτείται η εσωτερική σύνδεση ενός ζεύγους ηχητικών τόνων για κάθε αριθμητικό ψηφίο που πατιέται. Κάθε πλήκτρο της συσκευής αντιστοιχίζεται με ένα ζεύγος συχνοτήτων, το οποίο στην ουσία είναι οι συντεταγμένες του πλήκτρου πάνω στο πληκτρολόγιο. Έτσι, όλα τα πλήκτρα στην ίδια γραμμή έχουν κοινή την 1η συχνότητα ζεύγους, ενώ όλα τα πλήκτρα στην ίδια στήλη έχουν κοινή τη 2η συχνότητα ζεύγους (Ραγκούση, 2013).



Εικόνα 3.1: Αντιστοίχιση πλήκτρων και συχνοτήτων σήματος DTMF (Ραγκούση, 2013)

Πλεονεκτήματα

- Το μεγαλύτερο μέρος των συστημάτων συναγερμού χρησιμοποιούν PSTN κωδικοποιητές.
- Χρήση του πρωτοκόλλου Contact Id το οποίο μπορούν να λαμβάνουν όλοι οι κεντρικοί σταθμοί λήψεως σημάτων από τις περισσότερες κεντρικές μονάδες συναγερμού που κυκλοφορούν στην αγορά.

Μειονεκτήματα

- Χαμηλή ταχύτητα μετάδοσης σημάτων
- Δεν έχει τη δυνατότητα επιτήρησης της τηλεφωνικής γραμμής (www.internetsociety.org)

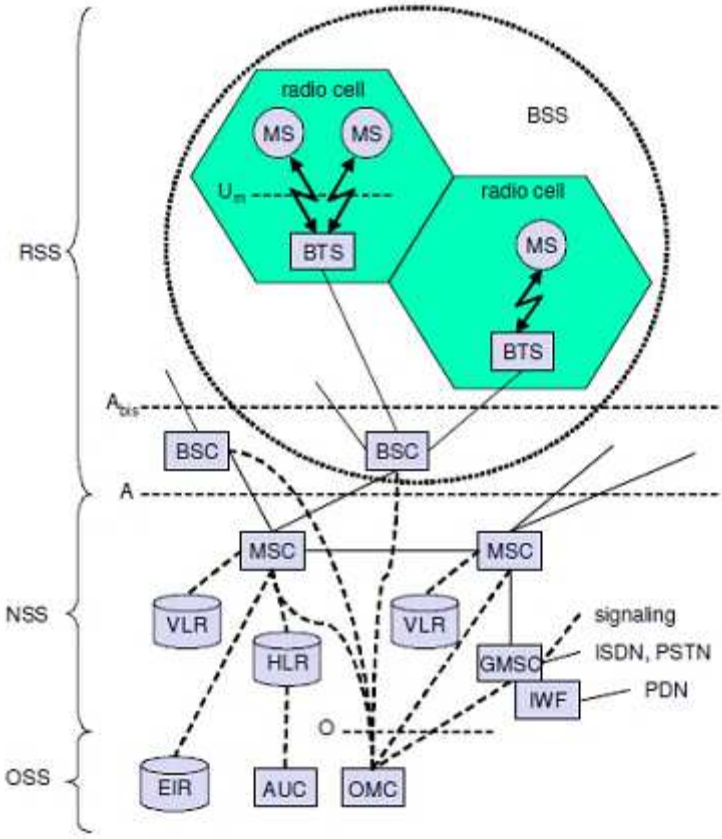
3.1.2 Δικτυακός GSM κωδικοποιητής

Το Παγκόσμιο Σύστημα Κινητών Επικοινωνιών (Global System for Mobile communications-GSM) αποτελεί ένα κοινό ευρωπαϊκό ψηφιακό σύστημα κινητής τηλεφωνίας. Τα πρώτα δίκτυα GSM άρχισαν να λειτουργούν το 1990 για να προσφέρουν υπηρεσίες φωνής και χαμηλού ρυθμού μετάδοσης δεδομένων σε συχνότητες 900 MHz με βάση τη λογική μεταγωγής κυκλώματος (circuit switching).

Το εύρος 890- 915 MHz χρησιμοποιήθηκε για την επικοινωνία με το σταθμό βάσης, ενώ το εύρος 935- 960 MHz είναι για την επικοινωνία του σταθμού βάσης με το κινητό τηλέφωνο. Το 1991 παρουσιάστηκε το σύστημα DCS 1800, στο οποίο τα ζεύγη επικοινωνίας του κινητού με το σταθμό βάσης και του σταθμού βάσης με το κινητό είναι 1710-1785 MHz και 1805-1880 MHz, αντίστοιχα. Το δίκτυο αυτό στη συνέχεια μετονομάστηκε σε GSM 1800, για να γίνει αισθητή η δυναμικότητά του. Τα μεταγενέστερα δίκτυα κινητών επικοινωνιών 2,5 G-GPRS/3G βασίζονται στη δομή του GSM.

Το δίκτυο είναι δομημένο σε διάφορα επιμέρους τμήματα:

- Ασύρματο υποσύστημα (RSS) - το τμήμα το οποίο υποστηρίζει την ασύρματη συνδρομητική πρόσβαση
- Υποσύστημα δικτύου και μεταγωγής (NSS) - το τμήμα του δικτύου που μοιάζει περισσότερο με ένα σταθερό δίκτυο, μερικές φορές απλά ονομάζεται «κεντρικό δίκτυο»
- GPRS Δίκτυο - το προαιρετικό μέρος που επιτρέπει συνδέσεις «πακέτων» που βασίζονται στο Internet.
- Υποσύστημα διαχείρισης υποστήριξης (OSS) - συντήρηση του δικτύου.

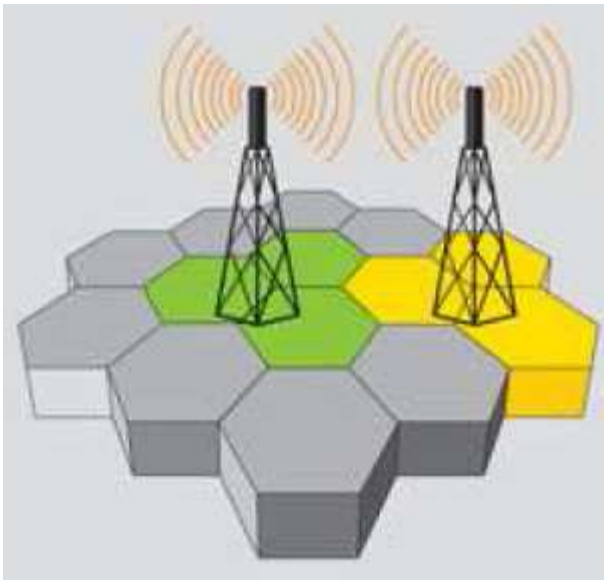


Εικόνα 3.2: Αρχιτεκτονική δικτύου GSM (Shiller, 2002)

Το GSM είναι ένα κυψελοειδές δίκτυο, πράγμα που σημαίνει ότι για να συνδεθούν τα κινητά τηλέφωνα σε αυτό ψάχνουν για κελιά που βρίσκονται σε άμεση γειτνίαση. Αυτό το κυψελοειδές δίκτυο αποτελεί στην ουσία και την περιοχή κάλυψης του δικτύου. Μέσα στα κελιά αυτά κινούνται οι χρήστες του συστήματος, οι οποίοι επικοινωνούν με τον σταθμό βάσης. Η σύνδεση γίνεται με τον σταθμό βάσης που εμφανίζει το «καλύτερο» σήμα. Ο σταθμός βάσης αναλαμβάνει την ασύρματη διασύνδεση.

Σε ένα δίκτυο GSM υπάρχουν πέντε διαφορετικά μεγέθη κελιών: -μακρο-, μικρο-, πικο-, φεμτο- και κελιά ομπρέλες. Η κάλυψη του κάθε κελιού διαφέρει ανάλογα με το περιβάλλον χρήσης. Τα μακροκελιά μπορούν να θεωρηθούν ως κελιά όπου η κεραία του σταθμού βάσης βρίσκεται σε ιστό ή κτίριο πάνω από το μέσο επίπεδο της οροφής. Τα μικροκελιά είναι κελιά στα οποία το ύψος της κεραίας είναι κάτω από το μέσο επίπεδο της οροφής και χρησιμοποιούνται συνήθως σε αστικές περιοχές. Τα πικοκελιά είναι μικρά κελιά, τον οποίων η ακτίνα κάλυψης είναι μερικές δεκάδες μέτρα και χρησιμοποιούνται κυρίως σε εσωτερικούς χώρους. Τα φεμτοκελιά σχεδιάζονται για χρήση σε οικιακά περιβάλλοντα ή μικρές επιχειρήσεις και συνδέονται στο δίκτυο του παρόχου μέσω ευρυζωνικής σύνδεσης. Τα κελιά ομπρέλες χρησιμοποιούνται για την κάλυψη σκιασμένων περιοχών και κενών μεταξύ των κελιών. (www.internetsociety.org)

Επειδή το φάσμα συχνοτήτων που είναι διαθέσιμο για την κινητή τηλεφωνία είναι πολύ περιορισμένο, μέσα στις πόλεις είναι αναγκαία η τοποθέτηση σταθμών βάσης πολύ χαμηλής ισχύος μέσα στις πόλεις και πολύ κοντά ο ένας στον άλλο, ώστε να καλύψει ο καθένας μία κυψέλη. Οι συχνότητες πρέπει να επαναχρησιμοποιούνται, για να μπορούν πολλοί συνδρομητές να μιλούν ταυτόχρονα. (www.internetsociety.org)



Εικόνα 3.3: Κυψελοειδές δίκτυο GSM (Shiller, 2002)

Οι συγκεκριμένοι κωδικοποιητές περιλαμβάνονται στις κεντρικές μονάδες συστημάτων συναγερμού τελευταίας γενιάς και τα σήματα αποστέλλονται μέσω δικτύου.

Πλεονεκτήματα

- Ταχύτητα στη μετάδοση των σημάτων
- On-Line στον Server του κεντρικού σταθμού

Μειονεκτήματα

Αποτελεί νέα τεχνολογία και κάθε κεντρική μονάδα χρησιμοποιεί δικό της πρωτόκολλο για την αποστολή σημάτων. Συνεπώς για να μπορεί ο κεντρικός σταθμός να δέχεται τα σήματα από τις διάφορες κεντρικές μονάδες, πρέπει να χρησιμοποιεί πλήθος δεκτών και αποκωδικοποιητών.

Οι κωδικοποιητές χωρίζονται σε 2 βασικές κατηγορίες:

- Αυτόνομοι Κωδικοποιητές, οι οποίοι μπορούν να λειτουργούν ανεξάρτητα από την κεντρική μονάδα
- Εξαρτώμενοι Κωδικοποιητές, οι οποίοι κουμπώνουν στην κεντρική μονάδα και δουλεύουν μόνο σε συνεργασία με αυτήν.

Οι αυτόνομοι κωδικοποιητές μπορούν να συνεργαστούν με οποιοδήποτε κέντρο συναγερμού και το μοναδικό τους μειονέκτημα είναι ότι σε περίπτωση που λειτουργούν ως GPRS, αν υπάρξει κάποια βλάβη στην μονάδα του συστήματος, συνεχίζουν να στέλνουν PING στον κεντρικό σταθμό με αποτέλεσμα ο χειριστής του κεντρικού σταθμού να βλέπει On-Line το σύστημα και να μην έχει δυνατότητα ανάγνωσης της βλάβης.

Οι GSM/GPRS κωδικοποιητές μπορεί να δουλεύουν ως πρωτεύουσα μονάδα επικοινωνίας σε περιπτώσεις όπου δεν υπάρχει δυνατότητα ενσύρματης σύνδεσης, είτε ως εναλλακτική μορφή επικοινωνίας σε περιπτώσεις όπου υπάρχει αυξημένη ανάγκη ασφάλειας ενός συγκεκριμένου χώρου.

Μια κεντρική μονάδα ενός συστήματος συναγερμού μπορεί λοιπόν να χρησιμοποιεί είτε ένα τύπο κωδικοποιητή, είτε οποιονδήποτε συνδυασμό των προαναφερόμενων κωδικοποιητών, σε περιπτώσεις όπου οι συνθήκες το απαιτούν. (www.internetsociety.org)(www.ilka.gr)

3.2 Ενσωμάτωση GSM σε σύστημα συναγερμού

Η αλματώδης εξέλιξη της τεχνολογίας στα συστήματα συναγερμών έχει οδηγήσει σε μείωση των τιμών τους, προς όφελος του καταναλωτή. Μια από τις πιο σύγχρονες εξελίξεις είναι οι συναγερμοί GSM, οι οποίοι βρίσκουν εφαρμογή σε οικιακές και επαγγελματικές εφαρμογές. Η διαφοροποίηση τους σε σχέση με το συνηθισμένο τύπο συναγερμού είναι ότι οι συναγερμοί GSM χρησιμοποιούνται για την φύλαξη ενός χώρου που διαθέτει τεχνολογία κινητής τηλεφωνίας.

Αυτό σημαίνει ότι οι συναγερμοί GSM αποτελούν ιδανική λύση για χώρους που δε διαθέτουν σταθερή τηλεφωνική γραμμή. Το μόνο που χρειάζεται είναι η αγορά μιας κάρτας SIM, η οποία θα επιτρέπει να χρησιμοποιούμε την υπηρεσία GSM. Ακόμη όμως και σε χώρους που διαθέτουν σταθερή τηλεφωνία, ένα τέτοιο σύστημα αποτελεί εφεδρική λύση στην περίπτωση όπου ο ληστής επιχειρήσει να κόψει το καλώδιο του τηλεφώνου. Μέσω της κάρτας SIM της κινητής τηλεφωνίας, πραγματοποιούν τηλεφωνική κλήση σε

σταθερό ή κινητό, στο οποίο μπορούν να αποστέλλουν και μήνυμα σε περίπτωση ληστείας ή άλλου κινδύνου.

Η κεντρική μονάδα του συναγερμού είναι εξοπλισμένη με GSM module Στους συναγερμούς GSM μπορούμε να συνδέσουμε ασύρματους και ενσύρματους αισθητήρες, εξωτερικούς και εσωτερικούς, όπως μαγνητικές παγίδες, ανιχνευτές κίνησης, σειρήνες και άλλες συσκευές.

Όταν ένας αισθητήρας ενεργοποιήσει το συναγερμό, η πληροφορία αυτή διαβιβάζεται μέσω της ραδιοφωνικής συχνότητας στο GSM module. Αυτό με τη σειρά του διαβιβάζει το σήμα κινδύνου με τη μορφή μηνύματος ή κλήσης στο κέντρο λήψης σημάτων που έχει μισθωθεί γι' αυτό το σκοπό ή σε κινητό τηλέφωνο που έχει προγραμματιστεί να καλείται σε επείγον περιστατικό.

Με το σύστημα αυτό δίνεται επίσης η δυνατότητα στο χρήστη να οπλίζει η να αφοπλίζει το συναγερμό, μέσω σύντομου μηνύματος SMS από το κινητό του τηλέφωνο.

Εικόνα 3.4: Σύστημα συναγερμού με συσκευή GSM (http://www.noontech.gr)

Παράδειγμα ενός τέτοιου συστήματος αμφίδρομης επικοινωνίας μέσω δικτύων GSM/GPRS παρουσιάζεται στην Εικόνα 3.5. Μπορεί να χρησιμοποιηθεί σε βιομηχανικές και οικιακές εφαρμογές, και κυρίως σε σημαντικές εφαρμογές όπου πρέπει να υπάρχει εναλλακτική λύση σε περίπτωση διακοπής της απλής τηλεφωνικής γραμμής.

Η μονάδα ελέγχει σταθερά την κατάσταση της τηλεφωνικής γραμμής και σε περίπτωση απώλειας, όλες οι συνδεδεμένες συσκευές χρησιμοποιούν τον προσομοιωτή τηλεφωνικής γραμμής που παρέχεται από την μονάδα, για να πραγματοποιήσουν ή να λάβουν κλήσεις, μέσω δικτύου GSM, χάρη στην ψηφιακή έξοδο ήχου που διαθέτει η συσκευή. Υπάρχει επίσης η δυνατότητα χρήσης δύο καρτών SIM, από διαφορετικούς παρόχους κινητής τηλεφωνίας,

για μέγιστη δυνατή κάλυψη από το δίκτυο. Το σύστημα ελέγχει την κατάσταση του δικτύου GSM, μετρώντας το επίπεδο του σήματος και την ποιότητά του, επαληθεύοντας την ορθή καταχώρηση στο δίκτυο και ανιχνεύοντας την παρουσία παρεμβολών. Επιπλέον ελέγχεται το πιστωτικό υπόλοιπο όλων των προπληρωμένων καρτών SIM, και ενημερώνεται αυτόματα ο χρήστης όταν χρειάζεται ανανέωση και όταν πλησιάζει η ημερομηνία λήξης της κάθε κάρτας. . (www.ilka.gr)

Η συσκευή έχει τη δυνατότητα να αποκωδικοποιεί τα σήματα του πρωτοκόλλου Contact ID και να αποστέλλει φωνητικά μηνύματα, SMS ή emails, προσαρμοσμένα για κάθε κέντρο ελέγχου και για κάθε ζώνη Τα μηνύματα ,τα SMS και τα emails μπορούν να έχουν περισσότερους από 128 χαρακτήρες, για ένα σύνολο 200 μηνυμάτων, τα οποία μπορούν να αντιστοιχηθούν σε αντίστοιχα συμβάντα του πρωτοκόλλου Contact ID. Η συσκευή απαιτεί τροφοδοσία 13,8 V συνεχούς ρεύματος. (www.ilka.gr)

Εικόνα 3.5: Σύστημα αμφίδρομης επικοινωνίας μέσω δικτύων GSM/GPRS (www.ilka.gr)

3.3 Δίκτυα νέας γενιάς

Παγκόσμιο σύστημα κινητών τηλεπικοινωνιών UMTS (Universal Mobile Telecommunications System)

Το παγκόσμιο σύστημα κινητών τηλεπικοινωνιών UMTS είναι ένα από τα συστήματα τεχνολογιών κινητής τηλεφωνίας τρίτης γενιάς (3G), το οποίο έχει

όμως και τη δυνατότητα για χρήση και στην τεχνολογία τέταρτης γενιάς (4G). Όμως το UMTS απαιτεί νέα υποδομή σταθμών βάσης και νέα κατανομή συχνοτήτων. Παρ' όλα αυτά, σχετίζεται άμεσα με το GSM/EDGE αφού δανείζεται και κτίζεται πάνω σε σχέδια του GSM. Οι περισσότερες φορητές συσκευές που υποστηρίζουν το δίκτυο UMTS, υποστηρίζουν επίσης και το GSM, επιτρέποντας άρρηκτη διπλή λειτουργία. Η διακριτική ονομασία UMTS, χρησιμοποιείται κυρίως στην Ευρώπη. Εκτός Ευρώπης, το συγκεκριμένο σύστημα είναι γνωστό με άλλα ονόματα, όπως FOMA ή W-CDMA. Στην αγορά, προβάλλεται ως 3G ή 3G+. (http://broadband.cti.gr/el/evrizonikotita/umts.php)

Πρόσβαση υψηλής ταχύτητας λήψης πακέτων HSDPA (High-Speed Downlink Packet Access)

Το συγκεκριμένο πρωτόκολλο τηλεπικοινωνιών κινητής τηλεφωνίας, επιπέδου εξελιγμένου 3G (τρίτης γενιάς), ανήκει στα πρωτόκολλα High Speed Packet Access (HSPA). Με το πρωτόκολλο αυτό είναι εφικτές υψηλότερες ταχύτητες και χωρητικότητες μετάδοσης δεδομένων σε δίκτυα βασισμένα στο UMTS. Οι υπάρχουσες διαμορφώσεις HSDPA, υποστηρίζουν ταχύτητες λήψης 1,8 Mbits/s, 3,6 Mbits/s, 7,2 Mbits/s και 14,4 Mbits/s. Περαιτέρω αύξηση ταχύτητας είναι διαθέσιμη με τη χρήση HSPA+, που υποστηρίζει ταχύτητες λήψης έως και 42 Mbits/sec.

Βελτιωμένοι ρυθμοί μετάδοσης Δεδομένων για την Εξέλιξη του GSM EDGE (Enhanced Data rates for GSM Evolution)

Πρόκειται για ψηφιακή τεχνολογία κινητής τηλεφωνίας, που επιτρέπει βελτιωμένους ρυθμούς μετάδοσης δεδομένων ως επέκταση του GSM. Είναι επίσης γνωστό ως βελτιωμένο GPRS. Θεωρείται ράδιο-τεχνολογία επιπέδου προ-3G. Αναπτύχθηκε στα 30 δίκτυα GSM από το 2003. Η τεχνολογία EDGE συνεισφέρει στην επίτευξη βελτιωμένων ρυθμών μετάδοσης ανά ράδιο-κανάλι, αυξάνοντας σημαντικά τη χωρητικότητα και την απόδοση σε σύγκριση με μια κοινή σύνδεση GSM/GPRS. Αυτό είναι εφικτό λόγω της χρήσης ιδιαίτερα προηγμένων μεθόδων κωδικοποίησης και μετάδοσης δεδομένων. Με την εξέλιξή του (evolved EDGE) παρέχει μειωμένες λανθάνουσες καταστάσεις και υπερδιπλασιασμένη απόδοση, ικανοποιώντας τις απαιτήσεις High-Speed Packet Access (HSPA). Οι τυπικοί ρυθμοί μετάδοσης που επιτυγχάνονται είναι 400 Kbits/s και οι μέγιστοι ρυθμοί έως 1 Mbit/s. (http://broadband.cti.gr/el/evrizonikotita/umts.php)

Γενικό Πακέτο Ράδιο-Υπηρεσιών GPRS (General Packet Radio Service)

Πρόκειται για υπηρεσία μετάδοσης δεδομένων σε δομή πακέτων, η οποία παρέχεται με χρέωση από τα δίκτυα κινητής τηλεφωνίας 2G και 3G GSM.Είναι διαθέσιμη σε περισσότερες από 200 χώρες σε παγκόσμιο επίπεδο. Σε συστήματα 2G, το GPRS παρέχει ρυθμούς μετάδοσης δεδομένων 56-114 kbits/s. Η τεχνολογία 2G, συνδυασμένη με το GPRS, μερικές φορές χαρακτηρίζεται ως 2,5G, ανάμεσα δηλαδή στις τεχνολογίες κινητής τηλεφωνίας δεύτερης και τρίτης γενιάς. Από το 1997 και μετά, οι τεχνολογίες GSM ενσωματώνουν και την τεχνολογία GPRS. Η χρέωση χρήσης της υπηρεσίας βασίζεται είτε στη λογική του προπληρωμένου πακέτου όγκου δεδομένων, είτε στη μέθοδο «πληρωμή σύμφωνα με τη χρήση». Πρωτοτυποποιήθηκε από το Ευρωπαϊκό Ινστιτούτο Προτύπων Τηλεπικοινωνίας (European Telecommunications Standards Institute ETSI) με σκοπό τη βελτίωση των παλαιοτέρων τεχνολογιών CDPD και i-mode. Σήμερα, συντηρείται από το 3rd Generation Partnership Project (3GPP).

3GPP: 3rd Generation Partnership Project

Πρόκειται για μια συνεργασία των οργανισμών τηλεπικοινωνιών παγκοσμίως, με σκοπό την δημιουργία παγκόσμιου συστήματος κινητής τηλεφωνίας 3ης γενιάς με τυποποιημένα τεχνικά χαρακτηριστικά. Οι προδιαγραφές του 3GPP, βασίζονται σε μια εξέλιξη των προδιαγραφών του συστήματος GSM. Οι ομάδες που συνθέτουν τον οργανισμό είναι :

- European Telecommunications Standards Institute,
- Association of Radio Industries and Businesses/Telecommunication Technology Committee (ARIB/TTC) (Ιαπωνία)
- China Communications Standards Association,
- Alliance for Telecommunications Industry (Βόρεια Αμερική)
- Telecommunications Technology Association (Νότια Κορέα).

Η συνεργασία ξεκίνησε τον Δεκέμβριο του 1998. (http://www.3gpp.org/)

3.4 Συνδυασμένη μετάδοση

Πολλά συστήματα συναγερμού έχουν τη δυνατότητα μετάδοσης δεδομένων με δύο τουλάχιστον μέσα μεταφοράς, με σκοπό να επιτευχθεί μεγαλύτερη ασφάλεια του συστήματος συναγερμού. Ο βασικός τρόπος είναι συνήθως η τηλεφωνική γραμμή και ο συμπληρωματικός η κινητή τηλεφωνία. Σε άλλο συστήματα, ο βασικός τρόπος μετάδοσης είναι μέσω internet και ο

δευτερεύων η κινητή τηλεφωνία. Όταν χρησιμοποιείται η κινητή τηλεφωνία για την επικοινωνία, είναι δυνατή και η αποστολή μηνύματος SMS.

Η μετάδοση σήματος μέσω internet έχει δώσει νέες δυνατότητες στα συστήματα ασφαλείας, καθώς επιτυγχάνεται η αμφίδρομη και άμεση επικοινωνία μεταξύ του συστήματος συναγερμού και του ΚΛΣ. Ένα σύστημα που μεταδίδει σήματα μέσω internet μπορεί να ελέγχεται κάθε λεπτό ή και λιγότερο, ώστε να διασφαλίζεται η σωστή λειτουργία του.

Η μετάδοση σημάτων από χιλιάδες συνδρομητές με χρήση διαφορετικών τεχνολογιών δυσκολεύει συχνά την ανίχνευση προβλημάτων που μπορεί να οφείλονται σε βλάβες των συστημάτων συναγερμού ή προβληματικού μέσου μεταφοράς ή και βλάβες των δεκτών. Στην περίπτωση αυτή, ο τεχνικός πρέπει να γνωρίζει επαρκώς τις φάσεις μεταφοράς ενός σήματος για την ανίχνευση του προβληματικού συστήματος ή της αιτίας που το προκάλεσε. Σήμερα, ο εγκαταστάτης συστημάτων ασφαλείας διαθέτει στο οπλοστάσιό του εξελιγμένα συστήματα με αυξημένων δυνατοτήτων κεντρικές μονάδες ελέγχου πολλαπλών ζωνών, πλήθος αισθητηρίων για την παγίδευση του χώρου ελέγχου και πολλαπλούς τρόπους μετάδοσης των σημάτων συναγερμού προς το ΚΛΣ, προσφέροντας στον πελάτη τη μεγαλύτερη δυνατή ασφάλεια, με ταχύτητα και αξιοπιστία.

http://www.securitymanager.gr/sub_site/arxeio/contents_article/alarm_4

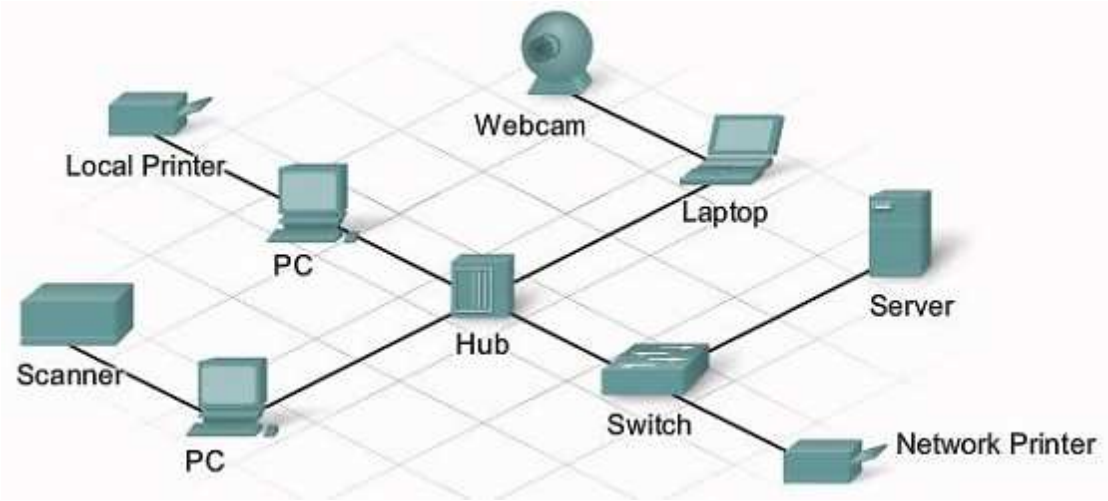
ΚΕΦΑΛΑΙΟ 4: Σύγχρονες τεχνολογίες

4.1 Δίκτυα επικοινωνιών

Τα δίκτυα μπορούν να χωριστούν σε διάφορες κατηγορίες, ανάλογα με το κριτήριο με το οποίο εξετάζονται:

- ανάλογα με το φυσικό μέσο διασύνδεσης, χαρακτηρίζονται ως ενσύρματα ή ασύρματα

Η ενσύρματη επικοινωνία περιλαμβάνει όλων των ειδών τις εναέριες, τις επίγειες και τις υπόγειες συνδέσεις αυτού του είδους. Παραδείγματα τέτοιων δικτύων αποτελούν όλα τα χάλκινα καλωδιακά δίκτυα, όπως επίσης και τα οπτικά δίκτυα.



Εικόνα 4.1: Ενσύρματο δίκτυο (www.netacad.com)

Η λειτουργία ενός ασύρματου δικτύου βασίζεται στο ραδιοκύματα για τη μεταφορά της πληροφορίας. Ραδιοκύματα ονομάζονται οι χαμηλές συχνότητες του ηλεκτρομαγνητικού φάσματος, που εκτείνονται περίπου από τα 3 KHz ως τα 300 GHz. Οι ασύρματες τηλεπικοινωνίες γίνονται συνήθως με ραδιοκύματα ευρείας εκπομπής (από τα 30 MHz ως το 1 GHz), ή μικροκύματα (από τα 2 GHz ως τα 40 GHz). Ασύρματα είναι συνήθως τα τηλεφωνικά δίκτυα και τα δίκτυα υπολογιστών. Σε αντίθεση με την ενσύρματη μετάδοση, δε χρησιμοποιείται καλώδιο για τη μεταφορά. Σήμερα όλα τα ασύρματα δίκτυα είναι ψηφιακά.

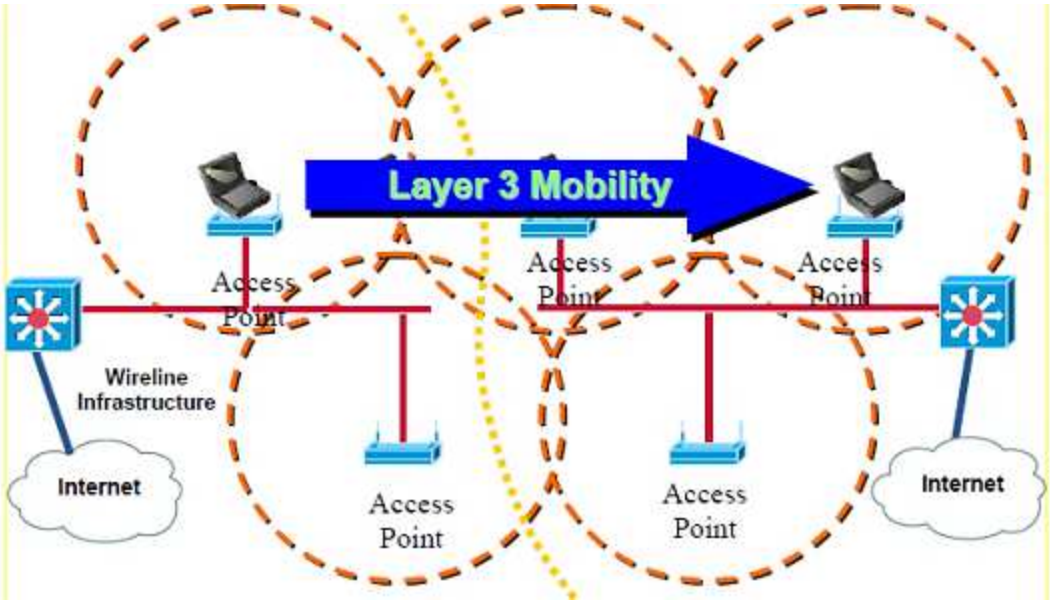
Εικόνα 4.2: Ασύρματο δίκτυο http://www.primefocus.net/

- ανάλογα με τον τρόπο πρόσβασης σε αυτά, χαρακτηρίζονται ως δημόσια ή ιδιωτικά δίκτυα
- ανάλογα με την γεωγραφική κάλυψη του δικτύου χαρακτηρίζονται ως τοπικά (**LAN και WLAN**), μητροπολιτικά **(MAN και WMAN)** , ευρείας κάλυψης **(WAN και WWAN)**, και προσωπικά **(PAN και WPAN)**

Οι χαρακτηρισμοί με το πρόσθετο W ανταποκρίνονται στον ασύρματο (Wireless) τρόπο σύνδεσης.

Ένα τοπικό δίκτυο (LAN) είναι ένα δίκτυο που συνδέει υπολογιστές σε κοντινές αποστάσεις, π.χ. σε ένα δωμάτιο ή που απέχουν μέχρι μερικά χιλιόμετρα, π.χ. σε γραφεία εταιριών, πανεπιστήμια κ,λπ. Λίγο μεγαλύτερες αποστάσεις καλύπτονται από τα μητροπολιτικά δίκτυα (MAN). Όταν οι αποστάσεις που πρέπει να καλυφθούν από το δίκτυο αφορούν μεγάλες γεωγραφικές περιοχές, π.χ. διαφορετικές πόλεις ή ολόκληρη ήπειρος, απαιτούνται δίκτυα ευρείας περιοχής (WAN). Τα δίκτυα ευρείας περιοχής συνδέουν τοπικά δίκτυα και χρησιμοποιούν τηλεφωνικά δίκτυα ή τηλεπικοινωνιακούς δορυφόρους. Τα διαδίκτυα μπορούν να καλύψουν

περισσότερες ηπείρους, μέσω της σύνδεσης επιμέρους δικτύων. Το μεγαλύτερο δίκτυο τέτοιου είδους είναι το Internet.



Εικόνα 4.3: Τοπολογία Δικτύου WLAN (Χαλκιώτης, 2005)

4.2 Επικοινωνία του συναγερμού

Οικιακή αναφορά ονομάζεται η επικοινωνία μεταξύ της κεντρικής μονάδας και του χρήστη. Κάθε κεντρική μονάδα συναγερμού μπορεί να δεχθεί ένα πλήθος τηλεφωνικών αριθμών, οι οποίοι ειδοποιούνται σε περιπτώσεις συναγερμού ή σφάλματος. Το βασικό μειονέκτημα σε αυτό το είδος επικοινωνίας είναι ότι επειδή ένα σταθερό τηλέφωνο ή ένα κινητό δε διαθέτει αποκωδικοποιητή, το σήμα που λαμβάνουμε είναι απλά μια κλήση από το τηλέφωνο με το οποίο είναι συνδεδεμένη η κεντρική μονάδα.

Κάποια συστήματα συναγερμού ενσωματώνουν ειδικές μονάδες, οι οποίες ονομάζονται κάρτες φωνής, στις οποίες ο χρήστης μπορεί να ηχογραφήσει διάφορα μηνύματα, όπως για παράδειγμα «Συναγερμός στη ζώνη 1» ή «Πτώση Μπαταρίας», έτσι ώστε σε περίπτωση που ο συναγερμός καλεί, να μπορεί ο χρήστης να αντιληφθεί την κατάσταση του συστήματος. Ένας άλλος τρόπος, ειδικά σε καινούρια συστήματα συναγερμού, είναι με τη χρήση GSM κωδικοποιητή, με τον οποίο η κεντρική μονάδα στέλνει SMS στον χρήστη.

Υπάρχει επίσης η επικοινωνία του συστήματος με έναν κεντρικό Server, ο οποίος λαμβάνει όλα τα σήματα του συστήματος. Τα σήματα αυτά, εκτός από την ειδοποίηση σε περιπτώσεις συναγερμού, μπορεί να είναι και τα σήματα βλαβών του συστήματος αλλά και του χειρισμού.

Τα βασικά μειονεκτήματα στους δύο προαναφερθέντες τρόπους επικοινωνίας είναι:

- Πολλά συστήματα δε μπορούν να ενσωματώσουν και τους 2 τρόπους επικοινωνίας.
- Στην περίπτωση της οικιακής αναφοράς δεν είναι συμβατές όλες οι μονάδες με κάρτες φωνής, έτσι ώστε να μπορεί ο χρήστης να λάβει σήματα και για τυχόν προβλήματα του συστήματος.
- Μια κεντρική μονάδα παρόλο που μπορεί να υποστηρίζει κάρτα φωνής δεν είναι συμβατή με όλες τις κάρτες του εμπορίου.
- Στο κέντρο λήψεως σημάτων απαιτείται ετήσια συνδρομή.

Στόχος μας λοιπόν είναι να βρούμε μια λύση με βάση την οποία θα μπορούσαμε από οποιοδήποτε ήδη εγκατεστημένο σύστημα συναγερμού το οποίο έχει σαν πρωτόκολλο επικοινωνίας το Contact ID να μπορεί τις πληροφορίες που στέλνει στο κέντρο λήψεως σημάτων να τις λάβει ο χρήστης χωρίς να πληρώνει ετήσια συνδρομή στο κέντρο. Αυτό μπορεί να επιτευχθεί με την κατασκευή και τη χρήση μιας universal πλακέτας, η οποία θα μπορεί να ενσωματώνεται σε οποιοδήποτε σύστημα συναγερμού και με βάση το πρωτόκολλο να μπορεί να στέλνει μια ειδοποίηση στον τελικό χρήστη.

4.2.1 Πλακέτα Επικοινωνίας Universal

Η πλακέτα επικοινωνίας Universal θα τοποθετείται στην έξοδο του κωδικοποιητή και θα μπορεί να «υποκλέπτει» τα σήματα που στέλνει η μονάδα στο κέντρο λήψεως σημάτων. Με την βοήθεια ενός αποκωδικοποιητή τα σήματα αυτά θα μπορούν να διαβαστούν σε έναν υπολογιστή. Με τη χρήση της πλακέτας αυτής και ενός απλού προγράμματος στον υπολογιστή, το οποίο το μόνο που θα έχει να κάνει είναι να διαβάσει το πρωτόκολλο Contact ID, θα εμφανίζεται στην οθόνη του υπολογιστή το αντίστοιχο μήνυμα, το οποίο θα το έχουμε εγγράψει εμείς στην μνήμη του προγράμματος.

Αν θέλαμε να κάνουμε κάτι πιο πολύπλοκο θα μπορούσαμε να κατασκευάσουμε μια πλακέτα η οποία θα κουμπώνει στο bus της κεντρικής μονάδας, εκεί δηλαδή που κουμπώνει και το πληκτρολόγιο του συστήματος. Στο πληκτρολόγιο του συστήματος εμφανίζονται όλες οι ενδείξεις της κατάστασης του συστήματος και των προβλημάτων αυτού. Θα μπορούσαμε να μελετήσουμε τα πληκτρολόγια των κυριότερων και των μεγαλύτερων κατασκευαστών των συστημάτων συναγερμού και κάθε φορά να ορίζουμε ποιον τύπο πληκτρολογίου θα ακολουθεί η πλακέτα.

Οπότε, οτιδήποτε στέλνει η κεντρική μονάδα προς το πληκτρολόγιο του συναγερμού μπορούμε με την πλακέτα αυτή να το αποκωδικοποιήσουμε και εν συνεχεία μπορούμε να το στείλουμε προς τον υπολογιστή. Χρησιμοποιώντας τη δεύτερη περίπτωση μπορούμε με την βοήθεια και την κατασκευή ειδικής εφαρμογής να χειριζόμαστε και τον συναγερμό απομακρυσμένα. Η πιο εύκολη περίπτωση σαφώς είναι η πρώτη γιατί δεν χρειάζεται να μελετήσουμε την λειτουργία των περισσοτέρων συστημάτων συναγερμού, καθώς όλες τις πληροφορίες τις αντλούμε από το κοινό πρωτόκολλο που όλοι οι συναγερμοί χρησιμοποιούν.

4.2.2 Συμβατικός χειρισμός και χειρισμός πλακέτας Universal

Ο χειρισμός των περισσότερων συστημάτων γίνεται τοπικά μέσω του πληκτρολογίου του συστήματος. Ο απομακρυσμένος χειρισμός σε συστήματα τα οποία δεν είναι δικτυακά γίνεται μέσω DTMF σημάτων. Ο χειρισμός που μπορεί να γίνει σε ένα τέτοιο σύστημα είναι ο απολύτως απαραίτητος, ενώ ο χρήστης δε μπορεί να λάβει πληροφορίες, για παράδειγμα, για την κατάσταση του συστήματος τη συγκεκριμένη χρονική στιγμή. Ο χειρισμός αυτός πραγματοποιείται με την κλήση από οποιαδήποτε τηλεφωνική συσκευή προς τη γραμμή που είναι συνδεδεμένο το σύστημα συναγερμού και μετά από ένα συγκεκριμένων αριθμό κουδουνισμάτων, τον οποίο εμείς έχουμε καθορίσει, ανοίγει ο κωδικοποιητής του κέντρου και εμείς μέσω των DTMF τόνων πραγματοποιούμε οποιονδήποτε χειρισμό.

Και σε αυτή την περίπτωση κάποιες κεντρικές μονάδες χρησιμοποιούν κάρτες φωνής με ηχογραφημένα μηνύματα, έτσι ώστε να έχουμε μια στοιχειώδη ενημέρωση. Οι τελευταίας τεχνολογίας μονάδες συναγερμού είναι δικτυακές και, πέραν του πλεονεκτήματος της άμεσης ενημέρωσης καθώς είναι μόνιμα συνδεδεμένες στο Server του κεντρικού σταθμού, διαθέτουν και ειδική εφαρμογή για τον χειρισμό του συστήματος μέσω ηλεκτρονικού υπολογιστή ή κινητού τηλεφώνου. Ο χειρισμός μέσω της εφαρμογής είναι πλήρης, μπορεί δηλαδή ο χρήστης να πραγματοποιήσει οποιοδήποτε χειρισμό μπορεί να κάνει και τοπικά μέσω πληκτρολογίου. Επίσης η κεντρική μονάδα έχει τη δυνατότητα να στέλνει και ειδοποιήσεις τις οποίες μπορεί να βλέπει ο χρήστης μέσω της εφαρμογής.

Χειρισμός πλακέτας επικοινωνίας Universal

Μπορούμε μελετώντας τη χρήση και τα δεδομένα αποστολής και λήψης των πληκτρολογίων των συνηθέστερων κεντρικών μονάδων να κατασκευάσουμε μια πλακέτα η οποία θα συνδέεται στο Bus του συστήματος και θα έχει τη

λειτουργία ενός πληκτρολογίου. Η πλακέτα αυτή θα προγραμματίζεται μέσω υπολογιστή και θα μπορούμε να επιλέγουμε τον κατάλληλο τύπο κεντρικής μονάδας, έτσι ώστε μέσω της εφαρμογής που θα κατασκευαστεί να μπορεί να χειριστεί το σύστημα πλήρως. Εκτός από τον απομακρυσμένο χειρισμό της κεντρικής μονάδας, ο χρήστης θα μπορεί να λαμβάνει επίσης ειδοποιήσεις από το σύστημα σε περιπτώσεις συναγερμού, αλλά και για περιπτώσεις βλάβης του συστήματος. Ο χρήστης θα μπορεί να λαμβάνει όλα τα σήματα και να χειρίζεται το σύστημα του σαν να είναι στο χώρο, χωρίς ο συναγερμός του να είναι συνδεδεμένος με 24ωρο κέντρο λήψεως σημάτων.

Η πλακέτα θα περιλαμβάνει ένα μικροελεγκτή στο οποίο θα προγραμματίσουμε τις κεντρικές μονάδες και στον οποίο θα ορίζουμε ποια κεντρική μονάδα θα ελέγχει και μια κάρτα δικτύου, με βάση την οποία ο συναγερμός θα μπορεί να στέλνει και να λαμβάνει τα δεδομένα. Με τη χρήση λοιπόν της πλακέτας χειρισμού, ο χρήστης θα μπορεί να χειρίζεται το σύστημα του τόσο τοπικά μέσω πληκτρολογίου ή τοπικού δικτύου μέσω υπολογιστή tablet και κινητού τηλεφώνου όσο και απομακρυσμένα.

4.3 Δικτυακή κάμερα

Οι δικτυακές κάμερες ή IP (Internet Protocol) κάμερες είναι βιντεοκάμερες ψηφιακού σήματος που χρησιμοποιούνται για την επιτήρηση και την παρακολούθηση χώρων. Μπορούν να αποστέλλουν ή να λαμβάνουν δεδομένα, μέσω δικτύου υπολογιστή ή διαδικτύου, κάτι το οποίο δεν είναι εφικτό με τις αναλογικές κάμερες κλειστού κυκλώματος τηλεόρασης (CCTV). Η πρώτη δικτυακή κάμερα κυκλοφόρησε στην αγορά το 1996 με την ονομασία Ο όρος «IP κάμερα" ή "netcam" εφαρμόζεται συνήθως μόνο σε περιπτώσεις Axis Neteye 200.

Εικόνα 4.4: Η πρώτη δικτυακή κάμερα Axis Neteye 200 (http://www.axis.com/)

4.3.1 Είδη δικτυακών καμερών

Υπάρχουν δύο είδη δικτυακών καμερών:

- Κεντρική δικτυακή κάμερα, η οποία απαιτεί μια κεντρική δικτυακή συσκευή εγγραφής βίντεο για να χειριστεί την καταγραφή και τη διαχείριση του συναγερμού.

- Αποκεντρωμένη δικτυακή κάμερα, η οποία δεν απαιτεί μια κεντρική δικτυακή συσκευή εγγραφής βίντεο, έχει ενσωματωμένη λειτουργία καταγραφής και μπορεί έτσι να καταγράψει άμεσα σε κάθε πρότυπο μέσο αποθήκευσης, όπως οι φωτογραφικές μηχανές. (www.electrologos.gr/news/17)

4.3.2 Διαφορές κάμερας δικτύου και κάμερας κλειστού κυκλώματος τηλεόρασης

Για να γίνει η αναμετάδοση της πληροφορίας από κάμερα κλειστού κυκλώματος τηλεόρασης CCTV, το σήμα μετατρέπεται από αναλογικό σε ψηφιακό και γίνεται η καταγραφή. Σε πολλές περιπτώσεις δε γίνεται η μετατροπή αυτή και το σήμα παραμένει αναλογικό. Το σήμα των δικτυακών καμερών είναι απευθείας ψηφιακό, συνεπώς δεν απαιτείται μετατροπή, και άρα η εικόνα που παράγεται έχει πολύ καλύτερη εικόνα διότι δεν υπάρχουν απώλειες.

Οι κάμερες κλειστού κυκλώματος δε δίνουν τη δυνατότητα απομακρυσμένης πρόσβασης. Από την άλλη, οι δικτυακές κάμερες παρέχουν πρόσβαση στο χώρο που παρακολουθείται από οπουδήποτε σε πραγματικό χρόνο. Με τον τρόπο αυτό μπορεί κάποιος να παρακολουθεί σε πραγματικό χρόνο τι καταγράφει μια δικτυακή κάμερα που είναι εγκατεστημένη στο εξοχικό του, από την κύρια κατοικία του. Πέραν του ότι μπορεί ο χρήστης να λάβει την πληροφορία αυτή από τη δικτυακή κάμερα, έχει και τη δυνατότητα να στείλει ο ίδιος πληροφορία στην κάμερα. Ο χρήστης έχει για παράδειγμα τη δυνατότητα να δώσει εντολή στην κάμερα να εστιάσει σε ένα συγκεκριμένο σημείο ή να αλλάξει γωνία λήψης κ.λπ.

Λόγω του ότι οι δικτυακές κάμερες διαθέτουν δικό τους επεξεργαστή, αποτελούν έξυπνες συσκευές οι οποίες έχουν τη δυνατότητα να διαχειρίζονται από μόνες τους διάφορες καταστάσεις και να μας ενημερώνουν απευθείας για ύποπτες κινήσεις που καταγράφουν. Οι δικτυακές κάμερες είναι απλές στη χρήση τους για κάποιον χρήστη που έχει βασικές γνώσεις χειρισμού ηλεκτρονικού υπολογιστή.

Σημαντική διαφορά που παρουσιάζουν οι δικτυακές από τις κάμερες κλειστού κυκλώματος τηλεόρασης είναι στο θέμα της καλωδίωσης. Συγκεκριμένα, οι CCTV κάμερες απαιτούν ξεχωριστό καλώδιο για κάθε τύπο παροχής, δηλαδή ένα για τη μεταφορά του ήχου, ένα για τη μεταφορά της εικόνας και ένα για την παροχή του ρεύματος. Από την άλλη, οι δικτυακές κάμερες με ένα μόνο καλώδιο μπορούν να μεταφέρουν όλα τα παραπάνω.

Οι δικτυακές κάμερες μεταφέρουν το σήμα με ασφάλεια, λόγω της κωδικοποίησης, αποτρέποντας με τον τρόπο αυτό την υποκλοπή προσωπικών δεδομένων. Στις απλές cctv κάμερες αυτό επιτυγχάνεται μόνο με τη χρήση ακριβών οπτικών ινών. Επιπλέον, οι δικτυακές κάμερες λόγω του ότι βασίζονται σε πρότυπα, μπορούν να συνεργαστούν εύκολα και να ενσωματωθούν σε διάφορα συστήματα ασφαλείας χωρίς να προκύπτουν προβλήματα συμβατότητας, τα οποία είναι συνηθισμένα σε κάμερες κλειστού κυκλώματος τηλεόρασης CCTV.

Οι δικτυακές κάμερες έχουν εξαιρετική ποιότητα καταγραφής, λόγω της ψηφιακής μετάδοσης της πληροφορίας, ακόμα και όταν τα αντικείμενα ή οι άνθρωποι που καταγράφονται κινούνται με μεγάλη ταχύτητα. Όταν σταματήσουμε το βίντεο από μια δικτυακή κάμερα για να απομονώσουμε κάποιο καρέ, η εικόνα είναι πολύ καθαρή και μπορεί να χρησιμοποιηθεί για τη διερεύνηση κάποιου συμβάντος. Αντιθέτως, μια κάμερα CCTV δε μπορεί να καταγράψει καθαρά και με ακρίβεια αντικείμενα που κινούνται με ταχύτητα, και όταν απομονωθεί κάποιου καρέ του βίντεο η εικόνα που προκύπτει είναι θολή.

Στις δικτυακές κάμερες, η ψηφιακή μετάδοση του σήματος επιτρέπει τη μεταφορά του σε οποιαδήποτε απόσταση, ενώ σε μια κάμερα CCTV η απόσταση είναι πολύ περιορισμένη διότι εμφανίζονται σημαντικές απώλειες λόγω της αναλογικής μετάδοσης.

Τέλος η επιλογή μιας δικτυακής κάμερας εξασφαλίζει τη συμβατότητα του καταγραφικού συστήματος με μελλοντικές αναβαθμίσεις, ενώ αντιθέτως οι κάμερες CCTV θεωρούνται ήδη αρκετά ξεπερασμένες από τεχνολιγκής άποψης. Προς το παρόν όμως έχουν τη δυνατότητα να εκαλύπτουν συγκεκριμένες απαιτήσεις. (www.electrologos.gr/news/17)

4.4 Απομακρυσμένος έλεγχος μέσω smartphone

Για την πλειοψηφία των ανθρώπων τα έξυπνα τηλέφωνα (smartphone) έχουν μεγάλη σημασία και χρησιμότητα στην καθημερινότητά τους. Η συσκευή αυτή έχει μετατραπεί, από μια συσκευή επικοινωνίας σε μέσο για την πραγματοποίηση πολλών προσωπικών και επαγγελματικών ενεργειών. Μερικές από τις ενέργειες αυτές είναι η βιντεοκλήση, η διαχείριση του

ηλεκτρονικού ταχυδρομείου καθώς και πολλές εφαρμογές ψυχαγωγίας. Στο πλαίσιο αυτό, έχει δημιουργηθεί πληθώρα εφαρμογών που παρέχουν στο χρήστη τη δυνατότητα ελέγχου ενός συστήματος συναγερμού μέσω του smartphone του.

Τα σύγχρονα συστήματα συναγερμού δίνουν τη δυνατότητα στον ιδιοκτήτη, καταρχάς να ενημερωθεί για ενδεχόμενη παραβίαση του χώρου του, αλλά και να ελέγξει το χώρο από απόσταση, δηλαδή να οπλίσει ή να αφοπλίσει το συναγερμό μέσω εφαρμογής στη συσκευή smartphone που διαθέτει. Τέτοιου είδους εφαρμογές υποστηρίζουν διάφορα λειτουργικά συστήματα (apple, iOS, Android κ.λπ.) και μπορούν να έχουν ποικίλα επίπεδα πολυπλοκότητας. Για παράδειγμα, μια απλή εφαρμογή απομακρυσμένου ελέγχου δίνει στο χρήστη τη δυνατότητα να οπλίσει ή να αφοπλίσει το συναγερμό, ενώ πιο πολύπλοκες εφαρμογές προσφέρουν και άλλες λειτουργίες, όπως ξεχωριστός έλεγχος κάθε ζώνης ή παρακολούθηση του χώρου μέσω κάμερας. Ο χρήστης έχει τη δυνατότητα να παρακολουθεί την κατάσταση του συστήματος συναγερμού σε πραγματικό χρόνο. http://www.electrologos.gr/news/246

SMobile

Εικόνα 4.5: Δυνατότητα ξεχωριστού ελέγχου κάθε ζώνης του συστήματος (https://www.securityreport.gr)

Για τη χρήση της εφαρμογής, απαιτείται η εισαγωγή προσωπικού κωδικού, ίδιου ή διαφορετικού από τον κωδικό του συστήματος συναγερμού, ώστε να εξασφαλίζεται η χρήση της εφαρμογής μόνο από το κατάλληλο εξουσιοδοτημένο άτομο. Ένα ακόμη εξαιρετικά σημαντικό χαρακτηριστικό είναι η άμεση ενημέρωση του χρήστη μέσω push notifications, με τα οποία ο χρήστης ενημερώνεται για όλες τις ενέργειας με ειδοποίηση στο smartphone. Τα σήματα εμφανίζονται ανά κατηγορία και κρατείται ιστορικό, ώστε να έχει ο χρήστης τη δυνατότητα να αναζητήσει τις ειδοποιήσεις μιας συγκεκριμένης ημερομηνίας. https://www.securityreport.gr/articles/reviews/item/77-

Εικόνα 4.6: Ειδοποιήσεις για την κατάσταση του συστήματος συναγερμού (https://www.securityreport.gr)

Το σύστημα αυτό μπορεί να χρησιμοποιηθεί επίσης για τον έλεγχο των αυτοματισμών του χώρου, καθώς και την ενεργοποίηση ή την απενεργοποίηση οικιακών συσκευών, όπως π.χ. ο θερμοσίφωνας. https://www.securityreport.gr/articles/reviews/item/77-

i-Olympia alarm app

Μια άλλη διαθέσιμη εφαρμογή που έχει αναπτύξει η OLYMPIA ELECTRONICS A.E. παρέχει άμεση πρόσβαση στο αντικλεπτικό σύστημα του χρήστη, με τη χρήση sms. Σε περίπτωση που κάποιος, για παράδειγμα, οπλίσει το σύστημα, πατώντας το κατάλληλο πλήκτρο, η εφαρμογή στέλνει sms στον πίνακα συναγερμού, αναμένει την απάντηση και μόλις τη λάβει ενημερώνει τον χρήστη ότι εκτελέστηκε η ενέργεια. Η εφαρμογή αυτή είναι διαθέσιμη για android και για iOS.

Ο χρήστης έχει τη δυνατότητα να ενημερωθεί για το υπόλοιπο της κάρτας SIM, να έχει πρόσβαση στις εξόδους (πχ για ενεργοποίηση-απενεργοποίηση οικιακών συσκευών, ή φωτιστικών μέσων, δεύτερης σειρήνας κ.τ.λ.) ή να στείλει συναγερμό πανικού και σιωπηλό συναγερμό. Η εφαρμογή διατηρεί επίσης ιστορικό με όλα τα sms, καθώς και των αναφορών παράδοσης.

Τα καλοσχεδιασμένα εικονίδια καταδεικνύουν ξεκάθαρα στον χρήστη τι πρέπει να πατήσει, ανάλογα με την περίπτωση. Η έκδοση του android μάλιστα, δίνει μία ξεχωριστή ηχητική ειδοποίηση σε περίπτωση συναγερμού, παράγοντας έναν ήχο σειρήνας, ώστε να καταλάβει άμεσα ο χρήστης ότι κάτι τρέχει με το σύστημά του. Επίσης δημιουργεί στην περίπτωση αυτή ένα κόκκινο εικονίδιο συναγερμού στην μπάρα, ώστε σε περίπτωση που δεν ακούσει ο χρήστης τον ήχο της σειρήνας, να καταλάβει με το που ανοίξει το κινητό του και βλέποντας την μπάρα, ότι κάτι συνέβη στον φυλασσόμενο χώρο του. Η έκδοση του android λειτουργεί και σε tablet που έχουν τη δυνατότητα να δεχτούν κάρτα SIM. (*www.securitymanager.gr*)

Εικόνα 4.7: Διεπιφάνεια εφαρμογής απομακρυσμένης πρόσβασης i-Olympia alarm app (www.securitymanager.gr)

ECHO

Η απόλυτη ανάγκη για 24ωρη ασφάλεια και on-line ειδοποίηση κάθε αρμόδιας αρχής σε περίπτωση έκτακτης ανάγκης, σε συνδυασμό με την τεράστια αύξηση των «έξυπνων» κινητών τηλεφώνων διεθνώς, ώθησε στο σχεδιασμό και στη διάθεση σε όλους τους χρήστες κινητών νέας τεχνολογίας (κι όχι μόνο για τους συνδεδεμένους συνδρομητές), της εφαρμογής με την ονομασία ECHO.

Η εφαρμογή ECHO διατίθεται δωρεάν για όλα τα smsrtphone και τα tablet με κάρτα SIM. Χρέωση υπάρχει μόνο σε περίπτωση κλήσης βοήθειας. Σε περίπτωση προσωπικής απειλής και ανάγκης για άμεση βοήθεια, υπάρχει η δυνατότητα αποστολής σήματος alert, καθώς και στις περιπτώσεις όπου υπάρχει κίνδυνος πυρκαγιάς ή απαιτείται ιατρική βοήθεια. Το σήμα alert αποστέλλεται σε 24ωρο κέντρο λήψης σημάτων, το οποίο τηλεφωνεί στο τηλέφωνο του χρήστη για επιπλέον διευκρινήσεις. Αν η συσκευή διαθέτει GPS ή είναι συνδεδεμένη στο internet τη στιγμή του συμβάντος, αποστέλλεται η ακριβής τοποθεσία του χρήστη.

http://www.securitymanager.gr/newsite/contents_article.php?id=871&catid=6

Εικόνα 4.8: Διεπιφάνεια εφαρμογής απομακρυσμένης πρόσβασης ECHO (www.securitymanager.gr)

4.5 Ασφάλεια Συστήματος

Το μεγαλύτερο πρόβλημα ενός συστήματος το οποίο δέχεται απομακρυσμένο χειρισμό είναι η ασφάλεια που μπορεί να παρέχει. Είναι λοιπόν σημαντικό να διασφαλίσουμε τον τρόπο με τον οποίο θα μπορεί ο χρήστης να χειρίζεται απομακρυσμένα το σύστημα, χωρίς να επιτρέπεται η πρόσβαση σε οποιονδήποτε άλλον.

Μια λύση θα ήταν η δημιουργία ενός Server από τον οποίο θα γινόταν η επικοινωνία του χρήστη με την κεντρική μονάδα του συναγερμού. Θα μπορούσαμε να αντιστοιχούμε την Mac-Address του τηλεφώνου ή του tablet του χρήστη και μόνο αν είναι αντιστοιχισμένα να μπορεί ο χρήστης να στείλει και να λάβει δεδομένα από την κεντρική μονάδα. Επίσης για να μπορεί ο χρήστης να κάνει οποιοδήποτε χειρισμό στο σύστημα, θα πρέπει να πληκτρολογεί τον κωδικό λειτουργίας του συστήματος.

Τα παραπάνω θα πρέπει να ισχύουν για όλους τους χρήστες του συστήματος. Ο κύριος χρήστης όμως θα πρέπει να είναι αυτός που θα επιλέγει τι ακριβώς δυνατότητες θα έχει ο καθένας από τους υπόλοιπους χρήστες και θα είναι αυτός που θα μπορεί να διαγράφει όταν το θελήσει οποιονδήποτε από τους χρήστες. Τέλος στον Server θα πρέπει επίσης να αποθηκεύεται και ένα ιστορικό του συστήματος, από το οποίο θα μπορεί ο διαχειριστής να λάβει όλες τις απαραίτητες πληροφορίες σχετικά με την κίνηση του συστήματος.

Συμπεράσματα

Η εγκατάσταση συστήματος συναγερμού στοχεύει στην προστασία της περιουσίας και τα τελευταία χρόνια γίνεται συνεχώς όλο και πιο απαραίτητη. Σε κάθε περίπτωση πρέπει να γίνεται η επιλογή του κατάλληλου συστήματος ασφαλείας, λαμβάνοντας υπόψη όλες τις προσφερόμενες εναλλακτικές επιλογές. Η επιλογή του κατάλληλου συστήματος πρέπει να γίνεται από εξειδικευμένο τεχνικό, ο οποίος θα εγκαταστήσει ένα αξιόπιστο σύστημα συναγερμού βάσει των αναγκών και των απαιτήσεων ασφαλείας του κάθε χώρου, ενώ αν χρειάζεται θα μεριμνά για την ύπαρξη δικλείδων προστασίας στην περίπτωση που αποτύχει κάποιο από τα συστήματα.

Πλέον οι διαθέσιμες επιλογές, τόσο για τον έλεγχο του συστήματος συναγερμού όσο και για την επιλογή των κατάλληλων αισθητήρων, είναι πάρα πολλές και απαιτείται η συνεχής ενημέρωση των τεχνικών ώστε να προτείνουν κάθε φορά στον πελάτη το σύστημα που καλύπτει τις ανάγκες του με το βέλτιστο τρόπο. Οι εγκαταστάτες των συστημάτων πρέπει να γνωρίζουν τους διαθέσιμους τύπους αισθητήρων και τα χαρακτηριστικά τους, ώστε να επιτυγχάνεται η μέγιστη δυνατότητα ανίχνευσης αλλά και να ελαχιστοποιούνται παράλληλα οι ψευδείς συναγερμοί. Σε πολλούς τύπους αισθητήρων οι περιβαλλοντικές συνθήκες που επικρατούν στο χώρο εγκατάστασης, κυρίως όταν πρόκειται για αισθητήρες εξωτερικού χώρου, π.χ. άνεμοι, παρουσία θορύβου, ηλεκτρομαγνητικές παρεμβολές, επηρεάζουν τη λειτουργία του. Το γεγονός αυτό πρέπει να έχει ληφθεί υπόψη από τον εγκαταστάτη, τόσο για τη σωστή επιλογή όσο και για τη σωστή ρύθμιση του αισθητήρα.

Παράλληλα έχει εξελιχθεί και η πρόσβαση στα συστήματα συναγερμού, μέσω της χρήσης της βιομετρίας. Αντί για το απλό πληκτρολόγιο, στο οποίο πληκτρολογείται ένας κωδικός ασφαλείας, μπορούν να χρησιμοποιηθούν τεχνικές αναγνώρισης για τον προσδιορισμό της ταυτότητας των χρηστών μέσα από χαρακτηριστικά που είναι εγγενή στον καθένα μας, όπως η ίριδα του ματιού, η εικόνα του προσώπου, το δακτυλικό αποτύπωμα κ.λπ. Με τον τρόπο αυτό παρέχεται ασφάλεια υψηλών προδιαγραφών.

Η επικοινωνία με ένα σύστημα συναγερμού μπορεί να γίνει με διάφορους τρόπους. Η παλαιότερη τεχνολογία αφορούσε τον έλεγχο μέσω της σταθερής τηλεφωνικής γραμμής, ενώ στη συνέχεια δόθηκε και η δυνατότητα ελέγχου μέσω της κινητής τηλεφωνίας. Τα τελευταία χρόνια, οι εταιρίες εξέλιξαν ακόμη περισσότερο τα συστήματά τους, εντάσσοντας σε αυτά την τεχνολογία του internet. Με την εξέλιξη αυτή γίνεται εφικτός ο απομακρυσμένος έλεγχος των συστημάτων από διάφορα μέσα, όπως οι ηλεκτρονικοί υπολογιστές, τα tablet ή τα smartphone. Με τη διάδοση της τεχνολογίας του απομακρυσμένου ελέγχου, τίθενται ορισμένα θέματα ασφάλειας, τα οποία όμως επιλύονται μέσω της πιστοποίησης του κάθε χρήστη που έχει πρόσβαση στην εφαρμογή.

Ο απομακρυσμένος έλεγχος ενός συστήματος συναγερμού μπορεί να προσφέρει υπηρεσίες και να χρησιμοποιηθεί σε σημαντικές εφαρμογές, πέραν του τομέα της φύλαξης του χώρου. Μια τέτοια εφαρμογή είναι ο απομακρυσμένος έλεγχος διαφόρων συστημάτων του σπιτιού, όπως το σύστημα θέρμανση ή ο απομακρυσμένος χειρισμός διαφόρων ηλεκτρικών συσκευών. Μια διαφορετική χρήση είναι επίσης η σύνδεση του συστήματος με βιομετρικούς αισθητήρες, οι οποίοι θα ειδοποιούν τον κάτοχο του συστήματος σε περίπτωση που π.χ. κάποιος ηλικιωμένος ή κάποιος που πάσχει από κάποια χρόνια ασθένεια βρίσκεται σε κίνδυνο. Με τον τρόπο αυτό γίνεται εμφανές ότι ο απομακρυσμένος έλεγχος μπορεί να βρει εφαρμογή σε πολλές περιπτώσεις, για τις οποίες πρέπει να είναι ενημερωμένος ο εγκαταστάτης του συστήματος συναγερμού.

Βιβλιογραφία

Digital Communication Standard, Ademco Contact ID Protocol for Alarm System Communications, 1999.

http://broadband.cti.gr/el/evrizonikotita/umts.php

http://www.3gpp.org/

http://www.electrologos.gr/news/246

http://www.noontech.gr

http://www.primefocus.net/

http://www.securitymanager.gr/sub_site/arxeio/contents_article/alarm_42_3.php

http://www.tdsi.co.uk/

https://www.securityreport.gr

Schiller J., Mobile Communications, Addison-Wesley, 2002.

Traister, John E. and Terry Kennedy. Low Voltage Wiring: Security/Fire Alarm Systems, Third Edition. New York: McGraw-Hill Professional, 2001.

Trimmer, William H. Understanding and Servicing Alarm Systems, Third Edition. St. Louis: Butterworth-Heinemann, 1999.

www.boschsecurity.com

www.dualpath.gr

www.electrologos.gr/news/17

www.eurogard.gr

www.ilka.gr

www.internetsociety.org

www.securitymanager.gr

www.szanwell.com

Κωνσταντινίδης Συμεών, Τεχνολογικές Εξελίξεις & Προκλήσεις στον τομέα της Ασφάλειας, Space Hellas S.A.

Ραγκούση Μαρία, Ψηφιακή Επεξεργασία Σήματος- Σύνθεση τόνων για τηλεφωνικές συσκευές Dual Tone Multiple Frequency DTMF, Ανώτατο Εκπαιδευτικό Ίδρυμα Πειραιά Τεχνολογικού Τομέα, 2013.

Χαλκιώτης Κ., Βασικές αρχές λειτουργίας των δικτύων κινητών επικοινωνιών (GSM/GPRS-UMTS), των κινητών τηλεφώνων και άλλων ασύρματων διατάξεων μικρής εμβέλειας (Bluetooth, WLAN), Εθνικό Ίδρυμα Ερευνών, 2005.