Πανεπιστήμιο Μακεδονίας
ΔΠΜΣ Πληροφοριακά Συστήματα
Δίκτυα Υπολογιστών
Καθηγητής: Α.Α. Οικονομίδης

University of Macedonia
Master Information Systems
Computer Networks
Professor: A.A. Economides

Δίκτυα για την Επιτήρηση Κτιρίων: Ασφάλεια, Κλοπή, Φωτιά

Networks for Building Surveillance: Security, Theft, Fire

Κωνσταντίνος Κώτσιου
M.I.S 1012

Ιανουάριος 2013

Πίνακας Περιεχομένων

Περίληψη

Σε πολύ μεγάλο αριθμό κτιρίων σήμερα υπάρχουν συστήματα ασφαλείας που βασίζονται σε δίκτυα και δικτυακές εφαρμογές. Στην παρούσα εργασία θα μιλήσουμε για τα κτίρια στα οποία εγκαθίστανται αυτά τα συστήματα ασφαλείας. Θα γίνει μια αναφορά στα συστήματα CCTV την εξέλιξη τους και τις τεχνικές συμπίεσης video, στα συστήματα Access Control και τις τεχνικές ταυτοποίησης για παροχή πρόσβασης. Επίσης θα δούμε τα συστήματα Πυρανίχνευσης – πυρασφάλειας και πώς αυτά μπορούν να ενοποιηθούν μέσω δικτύου με άλλα συστήματα. Τέλος θα δούμε πώς τα συστήματα CCTV και Access Control μπορούν να ενοποιηθούν σε IP περιβάλλον και τα πλεονεκτήματα που προκύπτουν από μια τέτοια ενοποίηση.

Εισαγωγή

Στην εποχή μας γίνεται συνεχής λόγος για την ασφάλεια. Η ασφάλεια αφορά τόσο την προστασία των ανθρώπων, των υλικών και των εγκαταστάσεων όσο και των πληροφοριών. Στην πρώτη περίπτωση μιλάμε για φυσική ασφάλεια ενώ στην δεύτερη για λογική ασφάλεια. Στην παρούσα εργασία θα επικεντρωθούμε στα δίκτυα τα οποία μπορούν να προσφέρουν φυσική ασφάλεια σε κτίρια ως μέρος ενός συνολικού συστήματος ασφαλείας. Θα δούμε ποια είναι τα επιμέρους δίκτυα, πώς αυτά είναι δυνατόν αν αλληλεπιδράσουν μεταξύ τους και πώς είναι δυνατόν αυτά να ολοκληρωθούν σε ένα ολοκληρωμένο σύστημα.

1. Φυσική Ασφάλεια

Σύμφωνα με τον Εθνικό Κανονισμό Ασφαλείας «… Φυσική Ασφάλεια είναι το σύνολο των μέτρων που λαμβάνονται για την προστασία χώρων, υλικού και εγκαταστάσεων από απώλεια, κλοπή, κυρίευση, κατασκοπεία, δολιοφθορά, φυσικές καταστροφές ή αποκάλυψη αυτών με οποιονδήποτε τρόπο.» (ΕΚΑ, 2004).

Σύμφωνα με τον παραπάνω ορισμό οποιοδήποτε σύστημα ασφαλείας πρέπει να παρέχει μέτρα τα οποία θα προστατεύουν ένα κτίριο και τους ενοίκους του από φυσικές καταστροφές (φωτιά, πλημμύρα), μη εξουσιοδοτημένη πρόσβαση από άτομα τα οποία είναι ανεπιθύμητα, κλοπή ή άλλη ζημιά που συνιστά δολιοφθορά ή ζημία προς τον ένοικο. Το σύστημα ασφαλείας αποτελείται από δυο συνιστώσες, την ανθρώπινη και την τεχνολογική συνιστώσα, οι οποίες συνδυάζονται για να παρέχουν ένα ολοκληρωμένο σύστημα ασφαλείας. Η

ανθρώπινη συνιστώσα συνίσταται από φύλακες, οι οποίοι επιτηρούν τον χώρο είτε μέσω περιπολιών είτε μέσω των δικτύων επιτήρησης του κτιρίου, και οι οποίοι είναι υπεύθυνοι για την εφαρμογή της φυσικής ασφάλειας του κτιρίου.
Η τεχνολογική συνιστώσα του συστήματος ασφαλείας περιλαμβάνει ένα σύνολο δικτύων αισθητήρων που επιτρέπουν στο προσωπικό ασφαλείας την καλύτερη δυνατή απόδοση στο έργο του. Τα δίκτυα αυτά είναι:

1. Δίκτυα Τηλεόρασης Κλειστού Κυκλώματος (CCTV, Closed Circuit TV) για την επιτήρηση των χώρων του κτιρίου.
2. Δίκτυα Ελέγχου Πρόσβασης (Access Control Network) για τον έλεγχο της πρόσβασης στο εσωτερικό του κτιρίου.
3. Δίκτυα Πυρασφάλειας και Πυρανίχνευσης

2. Κτίρια

Στην εποχή μας τα κτίρια που κατασκευάζονται γίνονται συνεχώς όλο και μεγαλύτερα στεγάζοντας πλέον στον ολοένα και αυξανόμενο χώρο που διαθέτουν ένα πολύ μεγάλο αριθμό ανθρώπων. Για παράδειγμα το Willis Tower στο Chicago, Illinois των Ηνωμένων Πολιτειών με ύψος 443 μέτρα και 110 ορόφους παρέχει συνολικό καλυμμένο εμβαδό 418.064 τετραγωνικών μέτρων και αποτελεί το 8^{ο} υψηλότερο κτίριο του κόσμου και το ψηλότερο του δυτικού Ημισφαιρίου. Το συγκεκριμένο κτίριο έχει πάνω από 12000 κατοίκους ενώ το επισκέπτονται καθημερινά 25000 άνθρωποι. (Skydeck Chicago, 2009). Τα κτίρια μπορούν να χωριστούν ανάλογα με την χρήση που εξυπηρετούν σε τρεις κατηγορίες:

Εμπορικά Κτίρια. Χρησιμοποιούνται για εμπορικούς σκοπούς όπως για την στέγαση καταστημάτων ή γραφείων και ένοικοι συνήθως είναι υπάλληλοι των γραφείων, επισκέπτες και προσωπικό συντήρησης εγκαταστάσεων.

Κτίρια Κατοικιών. Οι γνωστές μας πολυκατοικίες με διαμερίσματα ή φοιτητικές εστίες αποτελούν παραδείγματα.

Κτίρια Ειδικού Σκοπού. Ξενοδοχεία, Νοσοκομεία, Κυβερνητικά Κτίρια, Σχολικές Εγκαταστάσεις αποτελούν κτίρια ειδικού σκοπού κα είναι συνήθως η κατηγορία των κτιρίων τα οποία αντιμετωπίζουν τις περισσότερες απειλές και έχουν τις μεγαλύτερες απαιτήσεις ασφαλείας.(ASIS Foundation, 2008)

Κτίρια του μεγέθους του Willis Tower που προαναφέρθηκε αλλά ακόμη και μικρότερα παρουσιάζουν λόγω ακριβώς των μεγεθών τους μια πολύ μεγάλη πρόκληση ασφαλείας. Οι κυριότερες απειλές ασφαλείας που αντιμετωπίζουν τα κτίρια μπορούν να χωριστούν σε τρεις κύριες κατηγορίες:

Εγκληματικές Ενέργειες

- Κλοπή και ειδικότερα διαρρήξεις σε προσωπικούς χώρους και χώρους στάθμευσης
- Καταστροφή περιουσιών με δολιοφθορά ή graffiti στους κοινόχρηστους χώρους και τους χώρους στάθμευσης
- Αδικήματα κατά προσώπων στους χώρους του κτιρίου τα οποία περιλαμβάνουν γενικά βία και ενδοοικογενειακή βία, προστριβές και διαφωνίες σε κοινόχρηστους χώρους μεταξύ των ενοίκων.

- Μη εξουσιοδοτημένη πρόσβαση σε υπηρεσίες που παρέχονται από το κτίριο όπως κλοπή τηλεπικοινωνιακών πόρων και ηλεκτρικού ρεύματος ακόμη και τον κίνδυνο βιομηχανικής ή άλλου είδους κατασκοπίας

Ενέργειες κατά της Τάξης και της κοινής ησυχίας

- Θέματα συμπεριφοράς όπως κακή συμπεριφορά υπό την επήρεια αλκοόλ ή ναρκωτικών ουσιών, διαμαρτυρίες, καταπάτηση και κατάληψη χώρων του κτιρίου.

Επείγουσες Καταστάσεις

- Επείγουσες καταστάσεις προκαλούμενες ή σχετιζόμενες με ανθρώπους συμπεριλαμβανομένων πυρκαγιών, δομικών φθορών, βλαβών ανελκυστήρων, διακοπές ρεύματος και τρομοκρατικές επιθέσεις.
- Επείγουσες καταστάσεις προκαλούμενες ή σχετιζόμενες με φυσικές καταστροφές ή καιρικά φαινόμενα.

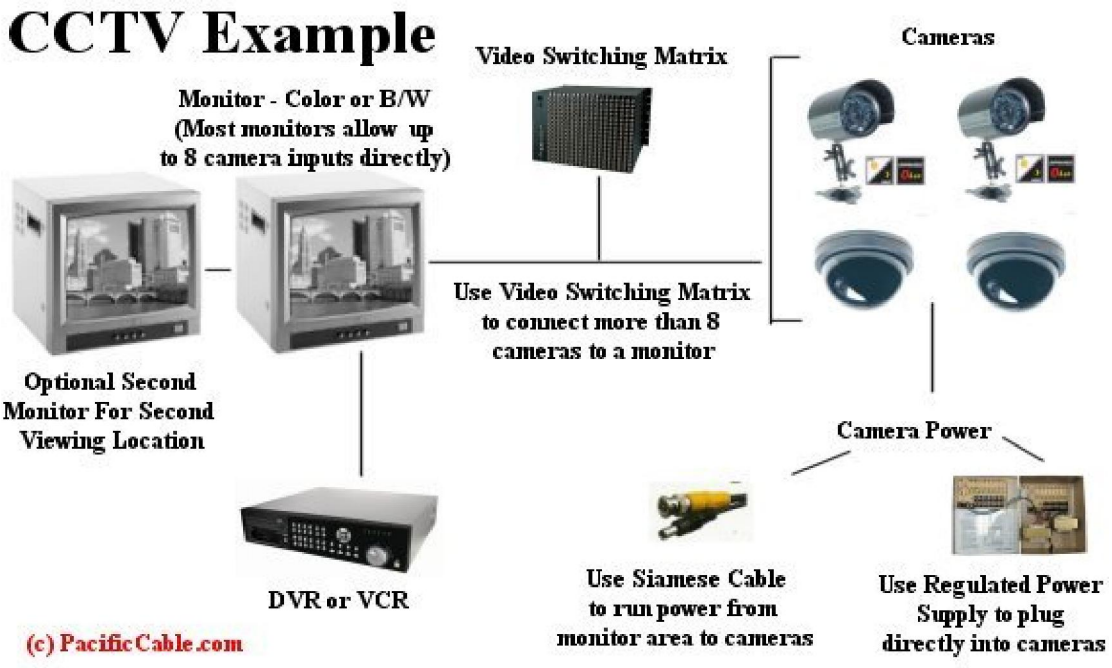
Σε καθεμία από τις παραπάνω περιπτώσεις απειλής ο ρόλος του συστήματος ασφαλείας είναι να προβλέψει και να προλάβει ή αν αυτό δεν καταστεί δυνατό, να εντοπίσει έγκαιρα την απειλή και να αντιδράσει προκειμένου να ελαχιστοποιήσει τα δυσάρεστα αποτελέσματα της στο κτίριο και τους ενοίκους του. Τέλος αν ούτε αυτό καταστεί δυνατό να προσφέρει στις αρχές τα απαραίτητα στοιχεία για τον εντοπισμό και την δίωξη των υπευθύνων. (ASIS Foundation, 2008)

3. Δίκτυα Ασφαλείας

Όπως προαναφέρθηκε τα δίκτυα ασφαλείας που υπάρχουν σε ένα κτίριο είναι δίκτυα επιτήρησης , Ελέγχου πρόσβασης, Πυρασφάλειας και πυρανίχνευσης. Τα δίκτυα αυτά μπορούν να είναι ανεξάρτητα μεταξύ τους (από πλευράς καλωδίωσης) ή να ολοκληρώνονται σε ένα συνολικό δίκτυο ακολουθώντας την τελευταία τάση για ενοποίηση των δικτύων ασφαλείας με λύσεις IP χρησιμοποιώντας την υπάρχουσα δομημένη καλωδίωση του κτιρίου. Στην συνέχεια θα δούμε τα συστήματα αυτά ξεχωριστά, τι προσφέρουν και πως ολοκληρώνονται χρησιμοποιώντας IP με τα όποια πλεονεκτήματα και μειονεκτήματα παρουσιάζει μια τέτοια λύση.

3.1 Δίκτυα Τηλεόρασης Κλειστού Κυκλώματος

Στο κομμάτι αυτό της εργασίας μας θα δούμε τα Δίκτυα Τηλεόρασης Κλειστού Κυκλώματος (CCTV). Πρόκειται για ένα δίκτυο καμερών το οποίο προσφέρει επιτήρηση πραγματικού χρόνου και καταγραφή των χώρων του κτιρίου σε 24-ωρη βάση. Στο σχήμα 1 φαίνεται ένα παράδειγμα δομής CCTV δικτύου.



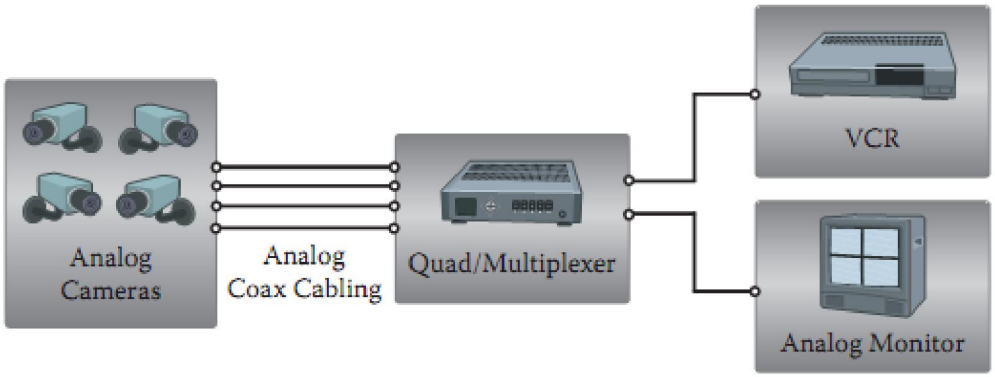
Σχήμα 1. Παράδειγμα δομής δικτύου CCTV

(Πηγή: http://www.pacificcable.com/LearningCenter/CCTV.html)

3.1.1 Εξέλιξη

Τα CCTV δίκτυα ακολούθησαν μια εξελικτική πορεία παράλληλη με την εξέλιξη της τεχνολογίας στους τομείς της καταγραφής και επεξεργασίας video και της μεταφοράς εικόνας.

Το αρχικό στάδιο ήταν τα VCR-Based αναλογικά CCTV συστήματα. Ένα παράδειγμα φαίνεται στο σχήμα 2.

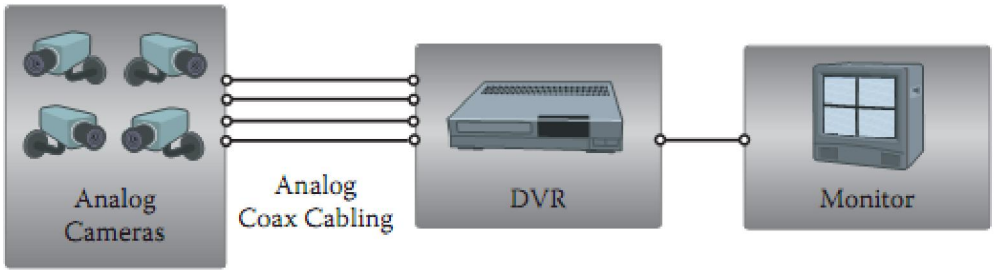


Σχήμα 2. Διάγραμμα κλασικού αναλογικού CCTV συστήματος (Πηγή: Intelligent Network Video; Understanding Modern Video Surveillance Systems)

Στα VCR-Based συστήματα αναλογικές κάμερες συνδεδεμένες με έναν πολυπλέκτη παρουσίαζαν σε μια οθόνη την εικόνα και από τις τέσσερις κάμερες και η εικόνα καταγράφονταν σε μαγνητικές ταινίες video. Αν και το σύστημα λειτουργούσε καλά υπήρχαν τα εξής μειονεκτήματα:

- Η ποιότητα της εικόνας ήταν τέτοια η οποία δεν δεχόταν ιδιαίτερη βελτίωση για την αποκάλυψη περισσότερων λεπτομερειών
- Υπήρχε ανάγκη περισσότερων της μιας καταγραφικών συσκευών ανάλογα με τον αριθμό των καμερών.
- Υπήρχε ανάγκη για αλλαγή των κασετών του συστήματος χειροκίνητα και η ποιότητα των εγγραφών μειωνόταν με τη πάροδο του χρόνου. (Nilsson, 2009)

Το επόμενο εξελικτικό βήμα ήταν τα DVR – Based αναλογικά CCTV συστήματα. Στο σχήμα 3 φαίνεται ένα παράδειγμα DVR – Based αναλογικού CCTV συστήματος.



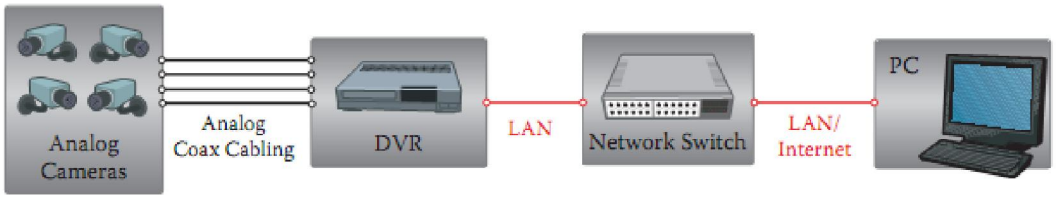
Σχήμα 3. Διάγραμμα DVR – Based αναλογικού CCTV συστήματος (Πηγή: Intelligent Network Video; Understanding Modern Video Surveillance Systems)

Στα DVR – Based συστήματα η καταγραφή του video γινόταν πάλι από αναλογικές κάμερες αλλά η εικόνα ψηφιοποιούνταν και καταγράφονταν ψηφιακά στο σκληρό δίσκο του DVR το οποίο έπαιζε επίσης και τον ρόλο του πολυπλέκτη. Στα αρχικά στάδια της εφαρμογής της τεχνολογίας και λόγω των περιορισμών στη χωρητικότητα των σκληρών δίσκων πολλές εταιρείες προχώρησαν στην ανάπτυξη αλγορίθμων συμπίεσης του video. Η υιοθέτηση των DVR – Based CCTV συστημάτων προσέφερε τα παρακάτω πλεονεκτήματα:

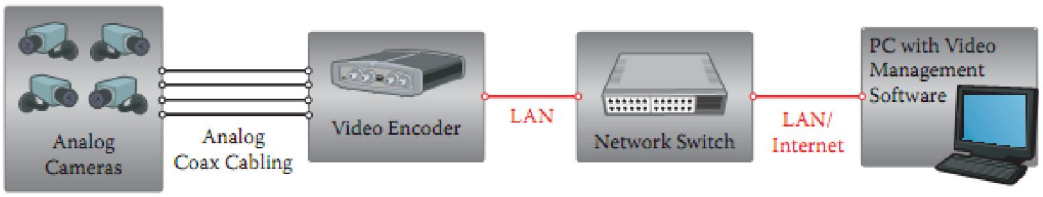
- Δεν ήταν απαραίτητη η χρήση κασετών και η συνεχής αλλαγή τους στο καταγραφικό
- Σταθερή ποιότητα εγγραφής video.
- Δυνατότητα γρήγορης αναζήτησης στα περιεχόμενα της καταγραφής. (Nilsson, 2009)

Η ψηφιοποίηση του video έδωσε την δυνατότητα στα συστήματα CCTV να συνδεθούν σε δίκτυα ηλεκτρονικών υπολογιστών είτε μέσω του DVR όπως φαίνεται στο σχήμα 4 είτε μέσω ενός κωδικοποιητή video όπως φαίνεται στο

σχήμα 5 παρέχοντας στον χρήστη απομακρυσμένη πρόσβαση και έλεγχο του συστήματος.



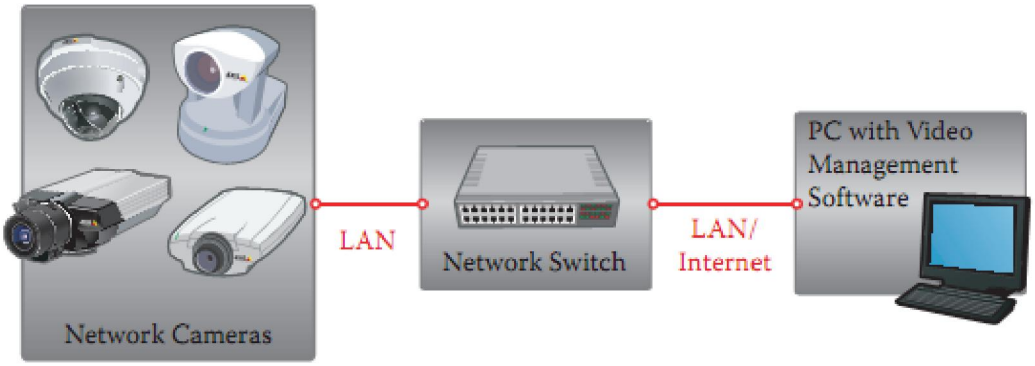
Σχήμα 4. Διάγραμμα DVR – Based αναλογικού CCTV συστήματος σε δίκτυο LAN (Πηγή: Intelligent Network Video; Understanding Modern Video Surveillance Systems)



Σχήμα 5. Διάγραμμα Video Encoder – Based αναλογικού CCTV συστήματος σε δίκτυο LAN (Πηγή: Intelligent Network Video; Understanding Modern Video Surveillance Systems)

Σήμερα τα συστήματα CCTV αξιοποιούν πλήρως την ψηφιακή τεχνολογία χρησιμοποιώντας δικτυακές κάμερες οι οποίες λειτουργούν εντός ενός δικτύου IP. Στην περίπτωση των δικτυακών καμερών η σύλληψη της εικόνας γίνεται με ψηφιακό τρόπο και παραμένει ψηφιακή καθ' όλη την διάρκεια της μεταφοράς του video εντός του δικτύου. Στο σχήμα 6 φαίνεται η δομή ενός δικτύου CCTV βασισμένο σε IP κάμερες. Η χρήση IP καμερών παρέχει κάποια πλεονεκτήματα σε σχέση με τις αναλογικές. Τα IP δίκτυα δίνουν την δυνατότητα σε πολλές κάμερες να χρησιμοποιήσουν ένα κοινό καλώδιο για την μεταφορά της εικόνας ενώ υπάρχει και η δυνατότητα για αμφίδρομη μεταφορά ήχου εάν η κάμερα

παρέχει την δυνατότητα. Επιπρόσθετα μέσω της δυνατότητας Power over Ethernet που προσφέρουν πολλές IP κάμερες είναι δυνατή ακόμη και η τροφοδοσία τους μέσω της δομημένης καλωδίωσης. Τέλος μέσω του δικτύου είναι δυνατή η χρήση λειτουργιών περιστροφής, ανύψωσης – καταβίβασης και μεγέθυνσης (pan/tilt/zoom) εφόσον οι κάμερες προσφέρουν αυτή την λειτουργία μέσω του λογισμικού ελέγχου χωρίς να είναι απαραίτητα άλλα χειριστήρια η επιπρόσθετη καλωδίωση.



Σχήμα 6. Διάγραμμα Network Camera – Based Network CCTV system (Πηγή: Intelligent Network Video; Understanding Modern Video Surveillance Systems)

Συνολικά ένα CCTV σύστημα βασισμένο σε δικτυακές κάμερες παρέχει τα παρακάτω πλεονεκτήματα:

- Δυνατότητα χρήση καμερών υψηλής ανάλυσης (high resolution – megapixel)
- Σταθερή ποιότητα εικόνας ανεξαρτήτως απόστασης
- Δυνατότητα χρήσης ασύρματών και Power over Ethernet λειτουργιών
- Πλήρης πρόσβαση σε pan/ tilt/ zoom δυνατότητες και αμφίδρομη μεταφορά ήχου.

- Απομακρυσμένη ρύθμιση της κάμερας και του συστήματος μέσω IP.
- Πλήρης ελαστικότητα και επεκτασιμότητα του συστήματος
- Μείωση του κόστους και της πολυπλοκότητας της καλωδίωσης. (Nilsson, 2009)

3.1.2 Τεχνολογίες Συμπίεσης Video

Όπως προαναφέρθηκε στα αρχικά στάδια της υιοθέτησης της τεχνολογίας ψηφιακής καταγραφής video λόγω περιορισμών στην χωρητικότητα των σκληρών δίσκων αναπτύχθηκαν πρότυπα συμπίεσης video. Τα πρότυπα αυτά τυποποιήθηκαν από τον ISO και είναι τα JPEG (Joint Photographic Experts Group) και MPEG (Moving Pictures Experts Group). Τα πρότυπα αυτά προτείνονται από την ITU (International Telecommunications Union) ενώ από το VCEG (Video Coding Experts Group) που αποτελεί τμήμα της ITU προέκυψαν τα πρότυπα H.261 και H.263 που χρησιμοποιούνται κυρίως για την κωδικοποίηση video σε βιντεοδιασκέψεις.

JPEG, MJPEG

Το πρότυπο συμπίεσης JPEG χρησιμοποιείται για την συμπίεση φωτογραφιών. Το πρότυπο JPEG παρέχει στον χρήστη την δυνατότητα είτε για μια εικόνα υψηλής ποιότητας με σχετικά υψηλό λόγο συμπίεσης είτε για μια σχετικά χαμηλής ποιότητας εικόνα αλλά με πολύ υψηλό λόγω συμπίεσης που έχει ως αποτέλεσμα αρχεία εικόνας μικρού μεγέθους.

Τα αρχεία εικόνας JPEG μπορούν να χρησιμοποιηθούν σε ακολουθία σχηματίζοντας video οπότε πλέον έχουμε το Motion JPEG. Το motion JPEG

παρέχει τα ίδια πλεονεκτήματα με το απλό JPEG, σε ότι αφορά την συμπίεση. Επιπρόσθετα επειδή δεν υπάρχει άμεση σύνδεση μεταξύ των εικόνων αν χαθεί κάποια φωτογραφία από την ακολουθία δεν έχει επίπτωση στη συνολική ποιότητα του video. Το κυριότερο μειονέκτημα του MJPEG είναι ότι επειδή είναι μια ακολουθία από σταθερές εικόνες δεν χρησιμοποιεί καμιά τεχνική συμπίεσης video. Αυτό έχει ως αποτέλεσμα μικρότερο λόγο συμπίεσης για ακολουθίες video από ότι αν χρησιμοποιούνταν μια τεχνική συμπίεσης video όπως το MPEG. Το MJPEG είναι δημοφιλές σε εφαρμογές όπου απαιτούνται ξεχωριστά frames από μια ακολουθία video π.χ για ανάλυση της πληροφορίας. (Harwood, 2008)

MPEG

Το πρότυπο συμπίεσης video MPEG βασίζεται στην ίδια τεχνική συμπίεσης που βασίζεται και το πρότυπο JPEG περιλαμβάνοντας όμως και επιπλέον τεχνικές αποδοτικής κωδικοποίησης του video. Έχει παρουσιάσει πολλά στάδια εξέλιξης τα οποία βασίζονται στην ποιότητα του video που θέλουμε να επιτύχουμε, το μέσο εγγραφής του video και το εύρος ζώνης που χρησιμοποιούμε για την μεταφορά του video. Τα στάδια εξέλιξης του MPEG είναι τα MPEG – 1, MPEG – 2, MPEG – 4, MPEG – 4 AVC/H.264, MPEG – 7, MPEG – 21. Το πλέον χρησιμοποιούμενο σήμερα πρότυπο είναι το MPEG – 4 AVC/H.264. (Harwood, 2008)

3.1.3 Video Content Analysis

Με την εξάπλωση των συστημάτων CCTV και την αύξηση της υπολογιστικής ισχύος των ηλεκτρονικών υπολογιστών που χρησιμοποιούνται για την καταγραφή του video από τα συστήματα CCTV αναπτύχθηκαν εφαρμογές που αύξησαν την χρησιμότητα των συστημάτων CCTV. Οι εφαρμογές αυτές βασίζονται στην ιδέα του Έξυπνου video (Intelligent Video). Βασισμένο στο πρόγραμμα Video Surveillance and Monitoring της DARPA στόχος του ήταν η ανάπτυξη τεχνολογίας η οποία θα έδινε στον χειριστή την δυνατότητα να αντλήσει μεγάλο όγκο πληροφοριών από το video. (Nilsson, 2009)
Το σύστημα επιτήρησης με βάση παραμέτρους που θα είχε από τον χειριστή του θα μπορούσε να επιτελέσει από μόνο του διάφορες λειτουργίες όπως:

- Εντοπισμός και παρακολούθηση αντικειμένου
- Αναγνώριση γενικών κλάσεων αντικειμένων(π,χ ανθρώπων, φορτηγών, Ι.Χ αυτοκινήτων) αλλά κει ειδικών τύπων αντικειμένων (πχ περιπολικό, ταξί κλπ)
- Εκτίμηση θέσης αντικειμένου σε σχέση με γεωχωρικό μοντέλο θέσης
- Ενεργός έλεγχος καμερών και συνεργατική παρακολούθηση με πολλαπλές κάμερες
- Ανάλυση ανθρώπινου βαδίσματος
- Αναγνώριση απλών δραστηριοτήτων πολλαπλών πρακτόρων
- Αρχειοθέτηση Δεδομένων

Από τις λειτουργίες αυτές προέκυψαν εφαρμογές τριών κατηγοριών ανάλογα με τον τρόπο με το οποίο προκαλείται η εκκίνηση της εφαρμογής

1. Pixel based IV εφαρμογές. Αυτές οι εφαρμογές ενεργοποιούνται και στέλνουν ένα σήμα συναγερμού όταν διαπιστώνεται από το σύστημα απώλεια της ποιότητας του video σε κάποια από της κάμερες. Οι εφαρμογές που λειτουργούν με βάση αυτή την αρχή είναι :
    - Ανίχνευση Κίνησης. Αποτελεί τη πιο βασική εφαρμογή των τεχνικών έξυπνου video. Χρησιμοποιείται κυρίως για την ελάττωση του όγκου του video που καταγράφεται σε δεδομένο χώρο αποθήκευσης με την καταγραφή του video μόνο όταν υπάρχει κάποια αλλαγή στην εικόνα. Χρησιμοποιείται επίσης για την επισήμανση γεγονότων στους χειριστές του συστήματος (πχ είσοδος κάποιου ατόμου σε χώρου περιορισμένης πρόσβασης)(Βελντές, 2009)
    - Ανίχνευση μεταβολής της κατάστασης της κάμερας (Camera Tampering Detection). Αν για κάποιο λόγο η παρεχόμενη εικόνα από την κάμερα παρεμποδίζεται με αποτέλεσμα να υπάρχει κενό στην επιτήρηση το σύστημα ειδοποιεί τον χειριστή προκειμένου να ελεγχθεί για πιθανή βλάβη ή κακόβουλη ενέργεια.(Λυμπερόπουλος, 2010)

- Βελτίωση εικόνας. Σε πολλές περιπτώσεις οι καιρικές συνθήκες είναι πιθανό να διαστρεβλώσουν την εικόνα της κάμερας. Οι αλγόριθμοι IV μπορούν να αναλύσουν το διαστρεβλωμένο video και να εντοπίσουν τις διαστρεβλώσεις. Στην συνέχεια μπορούν να βελτιώσουν την εικόνα και να το επαναφέρουν στην κατάσταση στη οποία θα έπρεπε να μοιάζει σε κατάσταση με καλό καιρό. (Nilsson, 2009)

2. Object based IV Εφαρμογές. Στις εφαρμογές αυτές το σύστημα μπορεί να αναγνωρίσει αντικείμενα και να τα κατατάξει σε κλάσεις. Στην συνέχεια αυτή η κατάταξη μπορεί να χρησιμοποιηθεί στις παρακάτω εφαρμογές:
   - Μέτρηση αντικειμένων. Μπορεί να χρησιμοποιηθεί για την μέτρηση αντικειμένων ή ανθρώπων σε ένα συγκεκριμένο χώρο.
   - Ανίχνευση Αντικειμένων ή ανθρώπων. Το σύστημα έχει την ικανότητα να αναγνωρίσει ένα αντικείμενο ή άνθρωπο και στην συνέχεια να παρακολουθήσει την κίνηση του στο χώρο που επιτηρεί το σύστημα. Επίσης μπορεί να αναγνωρίσει αντικείμενα τα οποία έχουν αφεθεί σε θέσεις όπου δεν πρέπει να είναι ή ανθρώπους οι οποίοι παραμένουν σε περιοχές που δεν έχουν λογική να παραμένουν. Π.Χ ένα άτομο το οποίο παραμένει για πολύ ώρα σε ένα χώρο

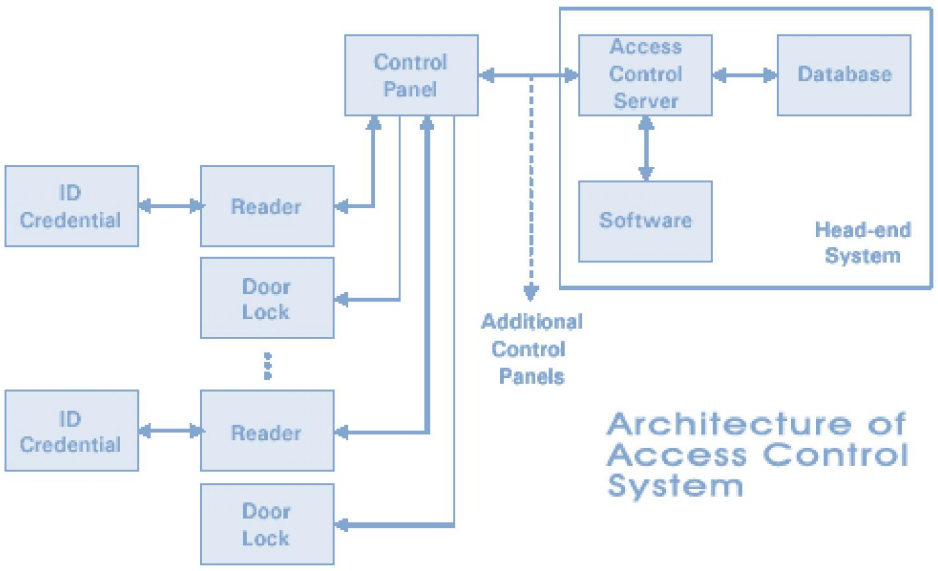
στάθμευσης ή κοντά σε ένα ATM μπορεί να υποδεικνύει πρόθεση για διάπραξη παράνομης πράξης. (Nilsson, 2009)

3. Εξειδικευμένες εφαρμογές IV. Πρόκειται για εφαρμογές σχεδιασμένες να επιτελούν μια πολύ συγκεκριμένη λειτουργία βασισμένα σε στην εξαγωγή συγκεκριμένων στοιχείων από ένα video και αποτελούν συνδυασμό των τεχνικών που χρησιμοποιούνται στις παραπάνω μεθόδους. Οι πιο σημαντικές εφαρμογές είναι:
   - Αυτόματη αναγνώριση πινακίδων αυτοκινήτων (Automatic Number Plate Recognition – ANPR). Χρησιμοποιείται για τον έλεγχο πρόσβασης αυτοκινήτων σε χώρους στάθμευσης και τον εντοπισμό αυτοκινήτων στην κυκλοφορία μετά την διάπραξη αξιόποινων πράξεων
   - Αναγνώριση Προσώπου. Μπορεί να χρησιμοποιηθεί για τον εντοπισμό συγκεκριμένων ανθρώπων σε περιοχές ενδιαφέροντος, για τον εντοπισμό των κινήσεων συγκεκριμένων ατόμων σε προγενέστερο χρόνο σε αποθηκευμένα video κλπ.
   - Εντοπισμός Φωτιάς και Καπνού. Το έξυπνο video μπορεί να επεξεργαστεί ακολουθίες video ψάχνοντας για οπτικούς ενδείκτες φωτιάς ή/και καπνού. Επειδή οι φλόγες μπορεί να είναι ορατές πολύ πριν συγκεντρωθεί επαρκής ποσότητα καπνού ώστε να ενεργοποιηθούν οι παραδοσιακοί ανιχνευτές

καπνού το σύστημα μπορεί πιθανώς να εντοπίσει πολύ νωρίτερα μια πιθανή εστία φωτιάς δίνοντας έγκαιρη προειδοποίηση στο προσωπικό ασφαλείας. Ένα τέτοιο σύστημα μπορεί να δράσει συμπληρωματικά στο κυρίως σύστημα πυρασφάλειας. (Nilsson, 2009)

3.2 Συστήματα Ελέγχου Πρόσβασης.

Τα συστήματα ελέγχου πρόσβασης (Access Control Systems) είναι το πρώτο μέσο που χρησιμοποιείται προκειμένου να επιτευχθεί ασφάλεια σε ένα κτίριο. Μπορεί να είναι κάτι πολύ απλό, από μια απλή κλειδαριά στην πόρτα, μέχρι κάτι απολύτως εξειδικευμένο όπως ηλεκτρονικές κλειδαριές με βιομετρικά εργαλεία για την αναγνώριση του ατόμου το οποίο προσπαθεί να αποκτήσει πρόσβαση στον χώρο ο οποίος προστατεύεται από τα συστήματα Access Control.



Σχήμα 7. Βασικό διάγραμμα αρχιτεκτονικής ενός συστήματος Access Control

(Πηγή: http://www.infocrane.com)

Στο σχήμα 7 φαίνεται η βασική ιδέα πίσω από ένα σύστημα ελέγχου πρόσβασης. Τα συστήματα ελέγχου πρόσβαση ως τώρα αποτελούνταν όπως φαίνεται και στο σχήμα από το κύριο σύστημα ελέγχου με την βάση δεδομένων των πιστοποιημένων για είσοδο χρηστών, τον server και το λογισμικό ελέγχου. Από κει και πέρα υπάρχει ο πίνακας ελέγχου που συνδέει τις κλειδαριές και τους αναγνώστες των πιστοποιητικών ταυτότητας των χρηστών με το κεντρικό server.

3.2.1 Πρωτόκολλο Wiegand

Ακόμη και σήμερα στα περισσότερα συστήματα Access Control η καλωδίωση Wiegand και το αντίστοιχο πρωτόκολλο για την διασύνδεση των αναγνωστών των πιστοποιητικών ταυτότητας με το κεντρικό σύστημα. Η καλωδίωση αποτελείται από τρία καλώδια, ένα καλώδιο γείωσης και 2 καλώδια μετάδοσης δεδομένων. Τα καλώδια δουλεύουν σε τάσεις συνήθως +5VDC. Οι περισσότεροι κατασκευαστές συστημάτων Access Control δίνουν μέγιστη απόσταση από τον αναγνώστη μέχρι τον πίνακα ελέγχου περίπου στα 170 μέτρα.
Το πρωτόκολλο επικοινωνία που χρησιμοποιείται χρησιμοποιεί 26 bits. Από αυτά τα 26 bits το πρώτο είναι parity bit, τα επόμενα οκτώ είναι ο κωδικός της εγκατάστασης, τα επόμενα 16 είναι η ταυτότητα του χρήστη και το τελευταίο είναι επίσης parity bit. Το πρωτόκολλο Wiegand έχει παρουσιαστεί σε διάφορες παραλλαγές ανάλογα με τις εταιρείες κατασκευής. Σήμερα βρισκόμαστε σε μια περίοδο όπου τα συστήματα Access Control λόγω της εφαρμογής όλο και

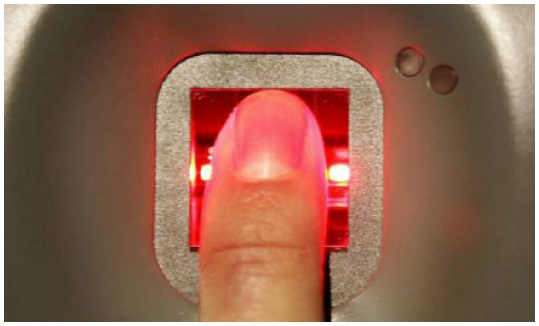
περισσότερων και πιο εξελιγμένων τεχνολογιών περνάνε από το πρωτόκολλο Wiegand σε ολοκληρωμένες IP λύσεις. (Mercury Security Corp, 2001)
Πιο κάτω θα δούμε τα κυριότερα συστήματα Access Control

3.2.2 Αναγνώστες Καρτών – Έξυπνες Κάρτες.

Η πλέον διαδεδομένη μορφή Access Control είναι οι αναγνώστες καρτών και οι αντίστοιχες κάρτες. Οι αναγνώστες καρτών μπορούν να περιλαμβάνουν πληκτρολόγιο για την εισαγωγή κάποιου κωδικού ή όχι. Σε κάθε περίπτωση η αρχή λειτουργίας είναι απλή. Ο χρήστης έχει στην διάθεση του μια κάρτα η οποία φέρει ένα μοναδικό κωδικό που πιστοποιεί ότι ο κάτοχος της έχει την δυνατότητα πρόσβασης στον συγκεκριμένο χώρο. Ο αναγνώστης καρτών δέχεται τον κωδικό και διαπιστώνει αν ο κάτοχος της κάρτας είναι πιστοποιημένος για την είσοδο. Επίσης αν ο αναγνώστης της κάρτας διαθέτει πληκτρολόγιο είναι δυνατόν πέρα α;πό την κάρτα για την διαπίστευση εισόδου να απαιτείται και η εισαγωγή κάποιου κωδικού. (Λυμπερόπουλος, 2010)
Οι κάρτες μπορούν χρησιμοποιούν αρκετές διαφορετικές τεχνολογίες. Οι κυριότερες από αυτές είναι οι:

- Ενεργητικές κάρτες στα 2,5 GHz.
- Παθητικές κάρτες στα UHF – 900
- Οι RFID Proximity κάρτες
- Οι Milfare κάρτες οι οποίες συνδυάζουν όλες τις παραπάνω τεχνολογίες. (Λυμπερόπουλος, 2010)

3.2.3 Biometrics



Σχήμα 8 Ανάγνωση αποτυπωμάτων (Πηγή: http://www.guardian.co.uk)

Η δεύτερη κυριότερη μέθοδος που χρησιμοποιείται είναι η βιομετρική αναγνώριση του ατόμου από κάποιο ιδιαίτερο χαρακτηριστικό του. Η πλέον συνήθης μέθοδος είναι η αναγνώριση των δακτυλικών αποτυπωμάτων σε ειδικούς αναγνώστες. Ο χρήστης τοποθετεί το δάκτυλο του στον αναγνώστη των αποτυπωμάτων. Το αποτύπωμα ψηφιοποιείται και αντιπαραβάλλεται με τα υπάρχοντα δακτυλικά αποτυπώματα στην βάση δεδομένων του συστήματος Access Control. Επειδή η διαδικασία της αντιπαραβολής μπορεί να διαρκέσει αρκετό διάστημα η ανάγνωση αποτυπωμάτων συνήθως συνδυάζεται με την χρήση κάποιας κάρτας που υποδεικνύει στο σύστημα ποιο αποτύπωμα να ελέγξει από την βάση δεδομένων. (Navavati, Thieme & Nanavati, 2002)

Άλλες τεχνικές που χρησιμοποιούνται είναι η αναγνώριση προσώπου, η αναγνώριση της ίριδας και τώρα τελευταία και η ανάγνωση της φλέβας με υπέρυθρο φως. (Wilson, 2010)

Τα biometrics θεωρούνται μια πολύ ασφαλής μέθοδος Access Control καθώς είναι πολύ δύσκολο να πλαστογραφηθούν και να χρησιμοποιηθούν ιδιαίτερα σωματικά χαρακτηριστικά του ατόμου.

Τα περισσότερα συστήματα Access Control όπως προαναφέρθηκε χρησιμοποιούν ακόμη και σήμερα το πρότυπο Wiegand. Η στροφή που

παρατηρείται προς τα IP συστήματα οφείλεται στα παρακάτω πλεονεκτήματα που επιτυγχάνονται με την χρήση τους:

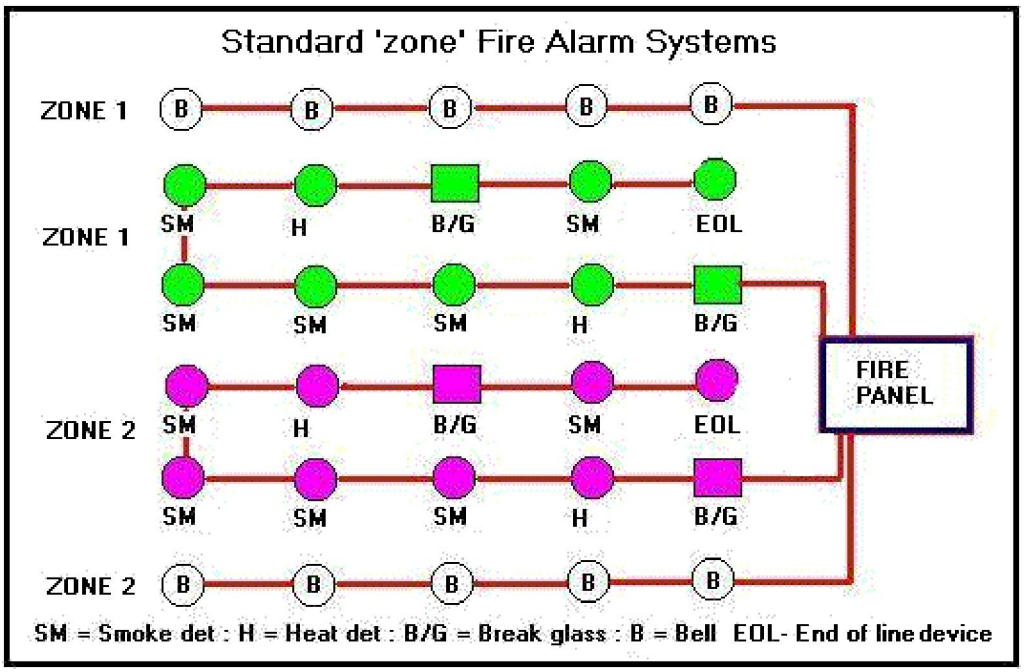
- Μείωση του κόστους κατασκευής. Πλέον όλες οι εταιρείες λειτουργούν εσωτερικά πληροφοριακά δίκτυα τα οποία χρησιμοποιούν δομημένη καλωδίωση. Η χρήση IP συστημάτων Access Control συνεπάγεται μείωση του κόστους καθώς δεν είναι απαραίτητη η εγκατάσταση ξεχωριστή καλωδίωσης αλλά χρησιμοποιείται η δομημένη καλωδίωση η οποία ούτως η άλλως θα εγκατασταθεί.
- Μείωση του κόστους λειτουργίας – συντήρησης. Ένα σύστημα IP Access Control μπορεί να χρησιμοποιήσει τους servers του IP CCTV συστήματος μειώνοντας το κόστος λειτουργίας και ξεχωριστών υπολογιστικών συστημάτων. Επίσης επειδή η τεχνολογία των δικτύων IP είναι πολύ πιο διαδεδομένη την συντήρηση του συστήματος μπορεί να την αναλάβει το IT τμήμα της επιχείρησης ή να δοθεί ως συνολικό έργο μαζί με την συντήρηση του δικτύου επιτήρησης σε εξωτερικό εργολάβο επιτυγχάνοντας καλύτερες τιμές και υποστήριξη απ’ ότι αν το έργο δινόταν τμηματικά.
- Διευκόλυνση της εκπαίδευσης στον συνδυασμό των συστημάτων CCTV – Access Control. Αν και τα δυο συστήματα είναι βασισμένα σε τεχνολογία ΙΠ είναι δυνατή η πολύ πιο εύκολη εκπαίδευση των χειριστών σε δύο όμοια συστήματα ή ακόμη καλύτερα σε ένα συνδυασμένο σύστημα παρά σε δυο τελείως διαφορετικά μεταξύ τους συστήματα.

- Αξιοπιστία. Όλες οι εταιρείες που χρησιμοποιούν πληροφορικά δίκτυα παρουσιάζουν άμεσο και μεγάλο ενδιαφέρον στην εύρυθμη και αξιόπιστη λειτουργία των δικτύων αυτών. Από τη στιγμή που το δίκτυο Access Control λειτουργεί ως μέρος του πληροφορικού δικτύου η αξιοπιστία του είναι ίδια με του υπολοίπου συστήματος. (Λυμπερόπουλος, 2009)

3.3 Δίκτυα Πυρασφάλειας – Πυρανίχνευσης

Τα δίκτυα πυρασφάλειας – πυρανίχνευσης υπάρχουν στα κτίρια προκειμένου να υπάρξει έγκαιρος εντοπισμός και αντιμετώπιση της φωτιάς. Τα δίκτυα αυτά αποτελούνται από τους αισθητήρες καπνού και φωτιάς και τις κονσόλες ελέγχου του συστήματος. Τα συστήματα πυρανίχνευσης χωρίζονται σε δυο μεγάλες κατηγορίες:

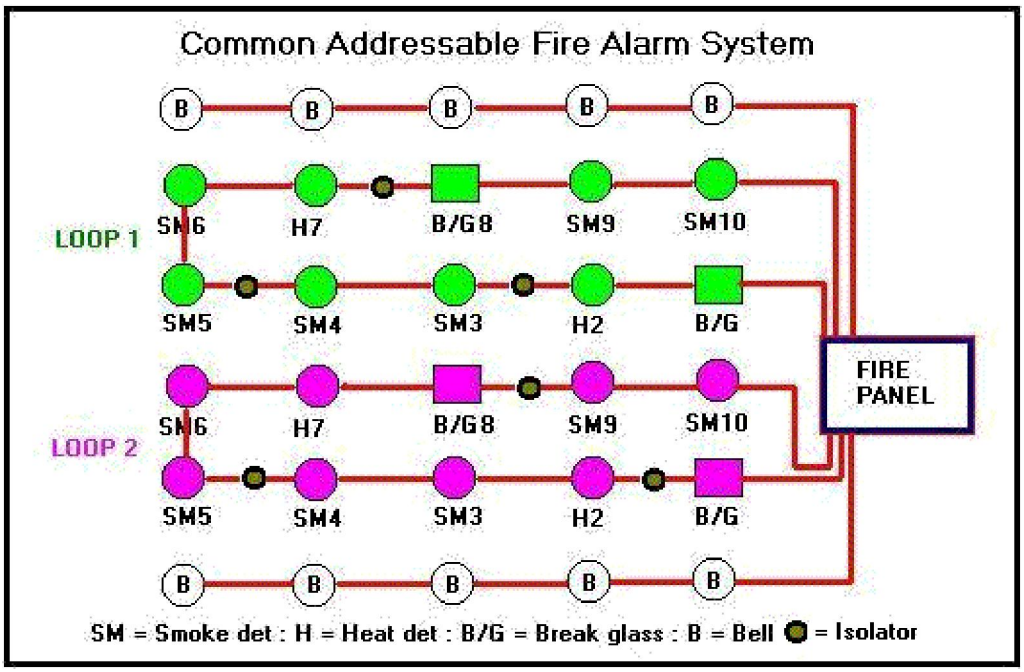
- Συμβατικά που αφορούν μικρές εγκαταστάσεις. Η εγκατάσταση χωρίζεται σε ζώνες οι οποίες περιλαμβάνουν έναν οι περισσότερους αισθητήρες καπνού – φωτιάς. Σε περίπτωση πυρκαγιάς στην κεντρική κονσόλα του συστήματος σημαίνει συναγερμός και ο χειριστής του συστήματος γνωρίζει απλά την ζώνη στην οποία έχει ξεσπάσει πυρκαγιά.



Σχήμα 9 Συμβατικό σύστημα Πυρανίχνευσης

(Πηγή: http://www.claydons.org)

- Διευθυνσιοδοτούμενα που αφορούν μεγάλες εγκαταστάσεις. Στην περίπτωση αυτή αριθμοί αισθητήρων συνδέονται μεταξύ τους σε βρόχους δίνοντας την δυνατότητα για το ακριβή εντοπισμό του σημείου στο οποίο έχει πιάσει φωτιά σε σχέση με τον αισθητήρα ο οποίος εντόπισε την φωτιά.



Σχήμα 10 Διευθυνσιοδοτούμενο σύστημα Πυρανίχνευσης
(Πηγή: http://www.claydons.org)

Οι αισθητήρες καπνού και φωτιάς είναι αρκετών διαφορετικών ειδών. Τα κυριότερα είδη των αισθητήρων είναι :

- Καπνού – Ιονισμού. Ενεργοποιείται όταν ανιχνεύσει στην ατμόσφαιρα σωματίδια καύσης, με την είσοδο τους στον θάλαμο ιονισμού του.
- Θερμοκρασίας. Ενεργοποιείται όταν η θερμοκρασία στον χώρο υπερβεί μια συγκεκριμένη τιμή για ένα συγκεκριμένο χρονικό διάστημα.
- Θερμοδιαφορικός. Ενεργοποιείται όταν η θερμοκρασία στον χώρο μεταβληθεί κατά μια συγκεκριμένη τιμή.
- Φωτοηλεκτρικός. Ενεργοποιείται όταν ανιχνεύσει προϊόντα καύσης τα οποία μεταβάλλουν το μαγνητικό του πεδίο.

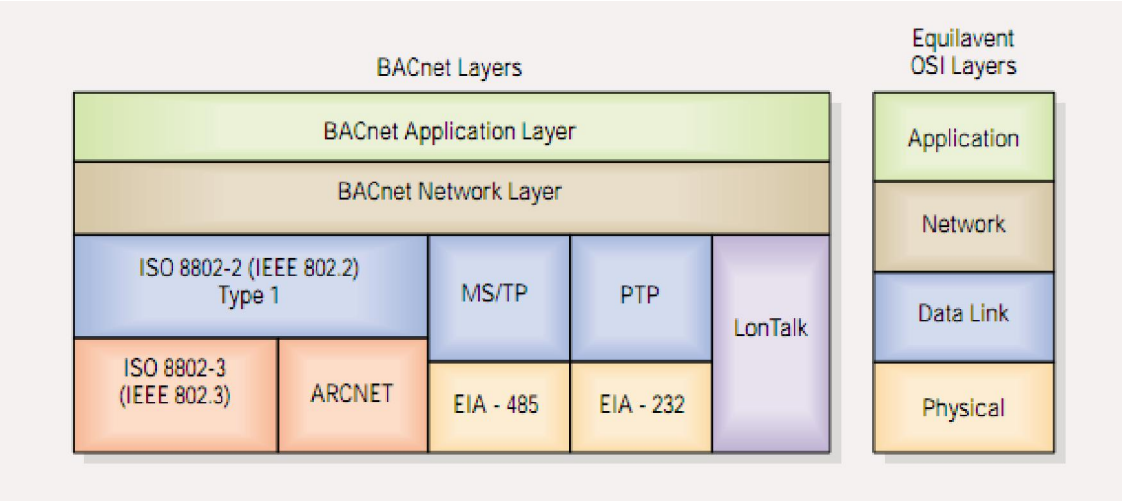
- Ορατού καπνού. Ενεργοποιείται όταν το ποσοστό σκίασης που προκαλείται από τον καπνό ξεπεράσει ένα προκαθορισμένο ποσοστό
- Εκρηκτικών αερίων. Ενεργοποιείται μόλις ανιχνεύσει στην ατμόσφαιρα ποσότητα αερίων
- Αλκοόλης – Μεθανίου. Ενεργοποιείται όταν το ποσοστό περιεκτικότητας στην ατμόσφαιρα φτάσει σε όρια επικινδυνότητας
- Μονοξειδίου και Διοξειδίου του άνθρακα. Είναι κατάλληλος για ανίχνευση φωτιάς αργής εξάπλωσης.

Τα παραπάνω είδη αισθητήρων συνήθως χρησιμοποιούνται σε συνδυασμό μεταξύ τους.(Beez Technology, 2013)

3.3.1 Ολοκλήρωση (Integration) των συστημάτων πυρανίχνευσης με άλλα συστήματα.

Τα συστήματα πυρασφαλείας εδώ και χρόνια έχουν ολοκληρωθεί με διάφορα άλλα συστήματα αυτοματισμού κτιρίων όπως τα συστήματα θέρμανσης – εξαερισμού (HVAC), συστήματα πυρόσβεσης και συστήματα Access Control. Η ολοκλήρωση αυτή όμως γινόταν με καθαρά αναλογικό τρόπο μέσω ρελέ τα οποία έλεγχαν την παροχή ρεύματος στα συστήματα αυτά. Πλέον χρησιμοποιώντας ψηφιακή τεχνολογία και διασύνδεση Ethernet με βάση το πρωτόκολλο BACnet. Το BACnet είναι ένα πρότυπο πρωτόκολλο επικοινωνιών που έχει αναπτυχθεί από την Αμερικανική Εταιρεία Μηχανικών Θέρμανσης, Ψύξης και κλιματισμού (ASHRAE). Έχει υιοθετηθεί από την Ευρωπαϊκή Ένωση ως προ – πρότυπο (prestandard) και έχει προταθεί και ως πρότυπο ISO.

Πρόκειται για ένα πρότυπο που προσφέρει επικοινωνία μεταξύ συσκευών σε διάφορα επίπεδα κατ' αναλογία με τα επίπεδα OSI. Στο σχήμα 11 φαίνεται η συσχέτιση των επιπέδων του BACnet με τα αντίστοιχα επίπεδα OSI.



Σχήμα 11 Συσχέτιση των επιπέδων του BACnet με τα αντίστοιχα επίπεδα OSI (Πηγή: http://www.claydons.org)

Η ολοκλήρωση των συστημάτων γίνεται μέσω της διασύνδεσης τους με κάποιο πρότυπο LAN.

Η ολοκλήρωση των συστημάτων πυρανίχνευσης με άλλα συστήματα του κτιρίου μπορεί να είναι επωφελής για πολλούς λόγους. Τα παραδείγματα περιλαμβάνουν διαχείριση του καπνού διαμέσου των συστημάτων HVAC, εντοπισμός ατόμων που κινδυνεύουν άμεσα από τις συνέπειες της φωτιάς μέσω του συστήματος Access Control και ενημέρωση του προσωπικού διάσωσης κ.α. (Bushby, 2001)

4. Ολοκλήρωση – Ενοποίηση Συστημάτων

Όλα τα συστήματα που είδαμε πιο πάνω στις περισσότερες περιπτώσεις ως τώρα λειτουργούν ως ανεξάρτητα συστήματα. Το καθένα παρείχε συγκεκριμένες δυνατότητες και παρείχε στους χειριστές έναν όγκο πληροφοριών που αυτοί θα έπρεπε να επεξεργαστούν σε πολύ μεγαλύτερο χρονικό διάστημα απ' ότι ίσως ήταν επιθυμητό. Τα συστήματα ασφαλείας με δικτύωση IP προσφέρουν στον χρήστη σημαντική ευελιξία και μεγαλύτερο εύρος δυνατοτήτων απ' ότι τα συστήματα που δουλεύουν ανεξάρτητα μεταξύ τους.

Το σημαντικότερο πλεονέκτημα που παρέχουν στον χρήστη τα συστήματα ασφαλείας με δικτύωση IP είναι η δυνατότητα άμεσης μεταφοράς πληροφορίας ανάμεσα στα διάφορα συστήματα. Σήμερα η πλήρης ενοποίηση των συστημάτων ασφαλείας όπου όλα τα συστήματα συνεργάζονται μεταξύ τους σαν ένα μέσω μίας μόνο εφαρμογής δεν είναι δυνατή. Είναι όμως δυνατή η διασύνδεση των συστημάτων με την διαβίβαση πληροφοριών από τα διάφορα συστήματα προς ένα το οποίο έχει επιλεγεί ως κύριο. Το σύστημα το οποίο επιλέγεται ως κύριο συνήθως είναι το CCTV καθώς είναι αυτό το οποίο χρησιμοποιείται συχνότερα. Η διαδικασία μεταφοράς πληροφορίας από τα υπόλοιπα συστήματα δημιουργεί πρακτικά μια αλληλουχία ενεργειών τύπου «αίτιο και αποτέλεσμα» (cause and effect). Οποιαδήποτε πληροφορία από κάποιο σύστημα φτάνει στο κύριο σύστημα λειτουργεί ως αίτιο για την εκκίνηση μιας λειτουργίας από το κύριο σύστημα. Αυτό είναι και το κυριότερο πλεονέκτημα

που παρέχουν τα ενοποιημένα συστήματα ειδικά αν συνδεθούν και με τα συστήματα διαχείρισης του κτιρίου (BMS – Building Management Systems). Πρακτικά όμως τι σημαίνει αυτή η αλληλουχία ενεργειών «cause and effect»; Ας δούμε τα παρακάτω παραδείγματα.

Πόρτα που ανοίγει με κάρτα

Αίτιο:

Κάποιος χρησιμοποιώντας μια κάρτα που δεν ισχύει σε κάποια πόρτα προσπαθεί να αποκτήσει πρόσβαση σε κάποιο χώρο του κτιρίου.

Αποτέλεσμα:

Το σύστημα CCTV στρέφει την κάμερα που βρίσκεται σε εκείνο τον χώρο προς το άτομο αυτό, ξεκινά καταγραφή της δραστηριότητας και παρακολουθεί τις κινήσεις του ατόμου.

Πόρτα που ανοίγει με κωδικό

Αίτιο:

Κάποιος προσπαθεί να ανοίξει την πόρτα με λανθασμένο κωδικό.

Αποτέλεσμα:

Το σύστημα CCTV στρέφει προς το πρόσωπο που προσπαθεί να ανοίξει την πόρτα εστιάζει στο πρόσωπο του ανθρώπου και προχωρεί σε αναγνώριση προσώπου ενώ γίνεται και επικοινωνία μεταξύ του χειριστή στο Control Room και του προσώπου μέσω της μεγαφωνικής εγκατάστασης.

Βιομηχανικός χώρος

Αίτιο:

Ένδειξη μεταβολής των συνθηκών του περιβάλλοντος.

Αποτέλεσμα:

Στην κεντρική οθόνη του Control Room θα εμφανιστεί η περιοχή ενδιαφέροντος και ο χειριστής μπορεί να ελέγξει οπτικά την κατάσταση στον χώρο πριν την αποστολή προσωπικού για επιτόπιο έλεγχο.

Από τα παραπάνω παραδείγματα προκύπτει ότι η ενοποίηση των συστημάτων αυτοματοποιεί τις διαδικασίες, επιταχύνει την επεξεργασία των πληροφοριών και δίνει στους χειριστές των συστημάτων καλύτερη επίγνωση κατάστασης σε μικρότερο χρόνο. (Λυμπερόπουλος, 2009)

4.1 Διαχείριση του συστήματος

Το καθένα από τα συστήματα ασφαλείας του κτιρίου κατά την διάρκεια λειτουργίας του συγκεντρώνει έναν αρκετά μεγάλο όγκο πληροφοριών. Οι πληροφορίες αυτές αποθηκεύονται σε βάσεις δεδομένων. Κάθε σύστημα μπορεί να παράγει τις δικές του αναφορές. Όταν όμως ο χρήστης θέλει μια συνολική αναφορά από όλα τα συστήματα υπάρχει πρόβλημα καθώς ο μηχανισμός αναφορών του κάθε συστήματος δεν είναι πάντα εφικτό να ενοποιηθεί ή να συνεργαστεί με τους αντίστοιχους μηχανισμούς των υπολοίπων συστημάτων. Το πρόβλημα επιλύεται με την χρήση ενός ενιαίου προτύπου επικοινωνίας μεταξύ των βάσεων δεδομένων γνωστού και ως ODBC. Με τη χρήση αυτού του προτύπου είναι δυνατή η πρόσβαση στο σύνολο των βάσεων δεδομένων και η δημιουργία συνολικών αναφορών από όλα τα συστήματα.

Ένα άλλο σοβαρό θέμα που αφορά στην διαχείριση των συστημάτων είναι η πρόσβαση των χειριστών στα διάφορα συστήματα. Είναι προφανές ότι δεν είναι

δυνατόν ο κάθε χειριστής να κάνει login σε όλα τα συστήματα χρησιμοποιώντας διαφορετικά στοιχεία εισόδου. Για τον λόγο αυτό δημιουργούνται λογαριασμοί χρηστών με συγκεκριμένα δικαιώματα πρόσβασης κοινοί για όλα τα συστήματα. (Λυμπερόπουλος, 2009)

Συμπεράσματα

Από τα όσα αναφέρθηκαν παραπάνω μπορούμε να συμπεράνουμε ότι η εξέλιξη της τεχνολογίας είχε ευεργετικά αποτελέσματα στα συστήματα ασφαλείας των κτιρίων. Τα συστήματα ασφαλείας πλέον ακόμη και όταν δουλεύουν ανεξάρτητα μεταξύ τους μπορούν να δώσουν πάρα πολλές λύσεις στον χρήστη τους παρέχοντας του μια πληθώρα πληροφοριών και δυνατοτήτων άντλησης πληροφοριών. Η ενοποίηση των συστημάτων όμως είναι αυτή που πραγματικά εκτοξεύει τις δυνατότητες το συστημάτων ασφαλείας σε απίστευτα επίπεδα. Σε κάθε περίπτωση οι αυξημένες δυνατότητες των ενοποιημένων συστημάτων παρέχουν στον χειριστή τους αυξημένη επίγνωση κατάστασης που μεταφράζεται σε αυξημένη δυνατότητα πρόληψης ή έγκαιρης αντιμετώπισης απειλών ασφαλείας.

Σε μια εποχή που οι απειλές ασφαλείας αυξάνονται καθημερινά η τεχνολογία των συστημάτων ασφαλείας χρησιμοποιώντας εξελιγμένες τεχνικές δίνει την δυνατότητα για αντιμετώπιση των απειλών με τον καλύτερο δυνατό τρόπο.

Βιβλιογραφία

Εθνικός Κανονισμός Ασφαλείας, ΓΕΕΘΑ. ΔΙΠΟΠΛΗ (2004).

Skydeck Chicago (2009). *Fun Facts For kids*. Retrieved 2013, from http://www.theskydeck.com

ASIS Foundation. (2008). *From the Ground Up: Security for Tall Bildings*. Alexandria, VA: ASIS Foundation.

Fredrik Nilsson (2009). *Intelligent Network Video; Understading Modern Video Surveillance Systems*. New York: CRC Press

Emily Harwood (2008). *Digital CCTV; A security Professional's Guide*. Burlington, MA : Elsevier Academic Press.

Mercury Security Corp. (2001). *Wiegand Technology: An Overview*. Retrieved 2013, from http://www.mercury-security.com/technology/whenyou.htm

Αριστοτέλης Λυμπερόπουλος (2010). Καρταναγνώστης. Τα μυστικά της σωστής επιλογής και εγκατάστασης. *Security manager*, 26, 86.

Αριστοτέλης Λυμπερόπουλος (2010). Ελέγχοντας τους επισκέπτες. *Security manager*, 28, 93.

Samir Nanavati, Michael Thieme, Raj Nanavati (2002). *Biometrics Identity Verification in a Networked* World. New York: John Wiley & Sons, Inc.

Chuck Wilson (2010). *Vein Pattern A Privacy-Enhancing* Biometric. Boca Raton, FL: CRC Press.

Αριστοτέλης Λυμπερόπουλος (2009). Συστήματα Access Control μέσω IP. Ουσιαστική Λύση ή Ουτοπία;. *Security manager,* 24, 88-93.

Γιώργος Βελντές (2009). Η εφαρμογή των Video Analytics ως ανιχνευτές κίνησης. *Security Manager*, 23, 78-80.

Αριστοτέλης Λυμπερόπουλος (2010). VCA Τα CCTV αποκτούν ευφυία. *Security manager,* 24, 88-93.

Συστήματα Πυρανίχνευσης. Retrieved 2013, from http://www.beeztech.gr/yphresies/asfaleia/systhmata-pyranixneushs.html

Steven T. Bushby (2001). Integrating Fire Alarm Systems with Building Automation and Control Systems. *Fire Protection Engineering*, 11, 5-11.

Αριστοτέλης Λυμπερόπουλος (2009). *Σύγκλιση CCTV και ACCESS σε IP περιβάλλον.* Security manager, 19, 84-87.