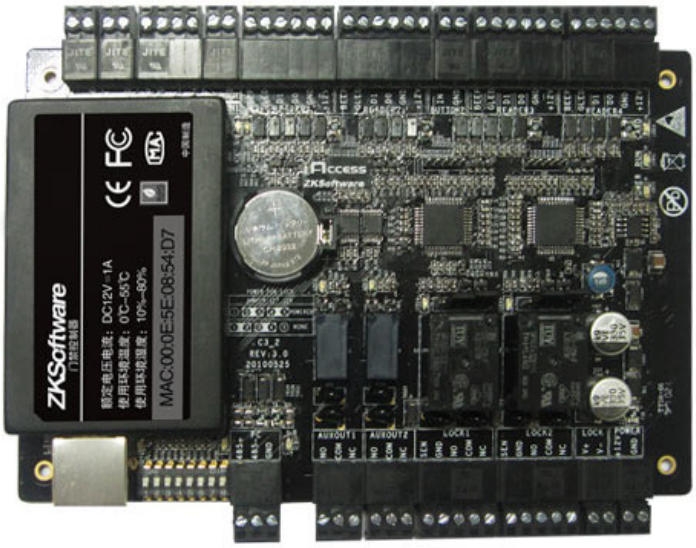
ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ Τ.Ε.

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ
Αριθμός 1204

ΑΝΑΠΤΥΞΗ ΚΑΙ ΕΓΚΑΤΑΣΤΑΣΗ ΣΥΣΤΗΜΑΤΟΣ ACCESS CONTROL ΕΡΓΑΣΤΗΡΙΟΥ ΜΙΚΡΟΫΠΟΛΟΓΙΣΤΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ



ΣΠΟΥΔΑΣΤΗΣ :
ΜΑΡΑΝΤΗΣ ΛΕΩΝΙΔΑΣ - ΠΑΝΑΓΙΩΤΗΣ

ΕΙΣΗΓΗΤΗΣ :
ΧΑΔΕΛΛΗΣ ΛΟΥΚΑΣ

ΠΑΤΡΑ ΝΟΕΜΒΡΙΟΣ 2013

ΠΡΟΛΟΓΟΣ

Σε ένα κοινόχρηστο χώρο, όπως το εργαστήριο μικροϋπολογιστικών συστημάτων για το οποίο απευθύνεται η εργασία, έχουν πρόσβαση αρκετοί φοιτητές καθώς και εργαζόμενοι. Επομένως, ο έλεγχος πρόσβασης αποτελεί παράγοντα ασφάλειας και ελέγχου για αυτόν, αλλά και για αυτούς που χρησιμοποιούν τον χώρο.

Για το λόγο αυτό υλοποιήθηκε, ένα σύστημα το οποίο επιτρέπει την είσοδο σε κάποιον μόνο εάν έχει στην κατοχή του το «κλειδί» για αυτό τον χώρο. Στην περίπτωση μας το κλειδί για την είσοδο δεν είναι ένα κοινό κλειδί πόρτας, αλλά μια κάρτα-κλειδί.

Βέβαια κάθε «κλειδί», επομένως κάθε εργαζόμενος, θα έχει πρόσβαση στο χώρο τις ώρες και τις ημέρες που του επιτρέπεται από τον υπεύθυνο-διαχειριστή του χώρου.

Στο εργαστήριο εγκαταστάθηκε ένα σύστημα ελέγχου πρόσβασης, το οποίο συνδέεται μέσω ethernet με ένα κεντρικό server. Το σύστημα διαβάζει το κλειδί εισόδου κάθε εργαζομένου και επικοινωνεί με τον πίνακα ελέγχου, ο οποίος θα εγκρίνει ή θα απορρίψει την πρόσβαση.

Επίσης κρατάει ένα αρχείο με τα άτομα που μπήκαν στον εργαστήριο καθώς και την ακριβή ώρα, ώστε ο διαχειριστής να έχει μια άποψη για την κίνηση του εργαστηρίου χωρίς να πρέπει να βρίσκεται ο ίδιος εκεί.

ΠΕΡΙΛΗΨΗ

Το αντικείμενο που διαπραγματεύεται η πτυχιακή εργασία είναι ένα σύστημα ελέγχου πρόσβασης το οποίο είναι σύμφωνο με τις πλέον σύγχρονες τεχνικές προδιαγραφές.
Ο έλεγχος πρόσβασης είναι ένα μέτρο ασφαλείας το οποίο ρυθμίζει την είσοδο ή έξοδο από ένα προστατευόμενο χώρο σύμφωνα με μια σχεδιασμένη πολιτική ασφαλείας και επιτρέπει την διέλευση μόνο σε άτομα με εξουσιοδοτημένες ιδιότητες και με βάση συγκεκριμένες συνθήκες.
Το σύστημα θα συνεργάζεται και θα λειτουργεί πάνω στις τεχνολογίες των συστημάτων ελέγχου και των δικτύων υπολογιστών.
Το σύστημα θα αποτελείται από ένα λογικό ελεγκτή που θα είναι συνδεδεμένος με ένα αναγνώστη καρτών proximity.
Κατά την είσοδο του χρήστη στο εργαστήριο θα απαιτείται η ανάγνωση της ειδικής κάρτας στον τοποθετημένο αναγνώστη τύπου weigand. Αμέσως το σύστημα θα ξεκινάει την διαδικασία αναγνώρισης της συγκεκριμένης κάρτας και θα ενεργοποιεί την ηλεκτρική κλειδαριά στην περίπτωση που έχει δικαίωμα πρόσβασης. Σε κάθε άλλη περίπτωση η πόρτα θα παραμένει κλειστή. Ο ελεγκτής θα είναι συνδεδεμένος επίσης με ένα κεντρικό server, μέσω ethernet, με τον οποίο θα γίνεται ο χειρισμός του καθώς και να μπορεί ο διαχειριστής να παρακολουθήσει σε πραγματικό χρόνο το ποιος εισέρχεται και εξέρχεται.
Στην πόρτα θα τοποθετηθεί επίσης μια μαγνητική επαφή που θα ελέγχει την κατάσταση της πόρτας (άμα είναι ανοιχτή ή κλειστή) και στην περίπτωση που θα είναι αδικαιολογήτως ανοιχτή ή γίνει παραβίαση θα σημαίνει συναγερμός.

Εις μνήμην του αγαπημένου θείου, Αθανάσιου Μαράντη

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 1

ΚΕΦΑΛΑΙΟ 2

ΚΕΦΑΛΑΙΟ 3

ΚΕΦΑΛΑΙΟ 1.

1.1 Έλεγχος πρόσβασης, βάση Ταυτοποίησης

Με τον όρο έλεγχος πρόσβασης (Access control) εννοούμε την παροχή έγκρισης ή απαγόρευσης πρόσβασης, μη εξουσιοδοτημένων χρηστών σε χώρο ή διαδικασία. Χαρακτηριστικό παράδειγμα ελέγχου χώρου είναι η ηλεκτρονική κλειδαριά, ενώ το πιο απλό παράδειγμα ελέγχου διαδικασίας είναι η ανάληψη χρημάτων από ATM.
Ο έλεγχος πρόσβασης βασίζεται σε δύο θεμελιώδεις διαδικασίες, της ταυτοποίησης και της πιστοποίησης (Identification&Authentication). Η ταυτοποίηση αφορά την διαδικασία δήλωσης της ταυτότητας από το χρήστη στο σύστημα, ενώ η πιστοποίηση αφορά την διαδικασία επιβεβαίωσης του ισχυρισμού της ταυτότητάς του χρήστη. Ανάλογα τώρα με τις τεχνικές ταυτοποίησης και πιστοποίησης μπορούμε να διαχωρίσουμε τα συστήματα ελέγχου πρόσβασης σε συστήματα που βασίζονται σε κωδικούς, σε συστήματα που βασίζονται στην κατοχή αντικειμένου και σε συστήματα που βασίζονται στη βιομετρία.

1.1.1 Συστήματα ταυτοποίησης βάση κωδικού (pin).

Τα συστήματα αυτά ουσιαστικά βασίζονται στο συσχετισμό του χρήστη με μία πληροφορία που κατέχει ο χρήστης (pin), χρησιμοποιούνται εδώ και πολλά χρόνια, οι χρήστες είναι αρκετά εξοικειωμένοι με αυτά, παρέχουν ικανοποιητικό επίπεδο ασφάλειας υπό την προϋπόθεση ότι οι κωδικοί διαχειρίζονται σωστά και φυλάσσονται επαρκώς.
Τα προβλήματα που οδηγούν στην αποκάλυψη των κωδικών σχετίζονται με την ταυτοποίηση της πληροφορίας όπως κωδικοί που εύκολα μαντεύονται ή δύσκολα απομνημονεύονται, καθώς και βιντεοσκόπηση της εισαγωγής του κωδικού που είναι και ο ποιο συνηθισμένος τρόπος.

1.1.2 Συστήματα που βασίζονται στην κατοχή αντικειμένου

Τα συστήματα αυτά βασίζονται στην κατοχή από την μεριά του χρήστη μιας κάρτας και χωρίζονται σε συστήματα μαγνητικών και ηλεκτρονικών καρτών (smart cards).
Οι μαγνητικές κάρτες έχουν συνήθως χωρητικότητα περίπου 250 Bytes, τα δεδομένα πιστοποίησης, καταγράφονται σε μια λωρίδα μαγνητικού υλικού, η οποία προσαρμόζεται στην επιφάνεια της κάρτας, χαρακτηριστικό αυτών των καρτών είναι ότι μόνο αποθηκεύουν και δεν είναι δυνατό να επεξεργάζονται την πληροφορία (π.χ. ATM κάρτες).
Οι Έξυπνες κάρτες (smart cards) διατίθενται με χωρητικότητες από bytes έως και mega bytes και χωρίζονται σε κάρτες μνήμες (memory cards), σε κάρτες με καλωδιωμένη λογική (π.χ. debit cards, phone cards) και σε κάρτες που διαθέτουν ενσωματωμένο μικροεπεξεργαστή. Προσπελαύνονται μέσω ειδικών συσκευών είτε ενσύρματα όπου οι επαφές τους ακουμπούν στις επαφές του chip που βρίσκονται στην επιφάνεια της κάρτας είτε ασύρματα (RF-IDs) όπου η επικοινωνία με τις επαφές του chip γίνεται με επαγωγικό τρόπο.
Ένα σημαντικό πλεονέκτημα των συστημάτων ελέγχου πρόσβασης χωρίς επαφές είναι ότι ο αναγνώστης δε χρειάζεται συντήρηση και δεν επηρεάζεται από σκόνες, βρομιά ή υγρασία.

1.1.3 Συστήματα που βασίζονται στη βιομετρία

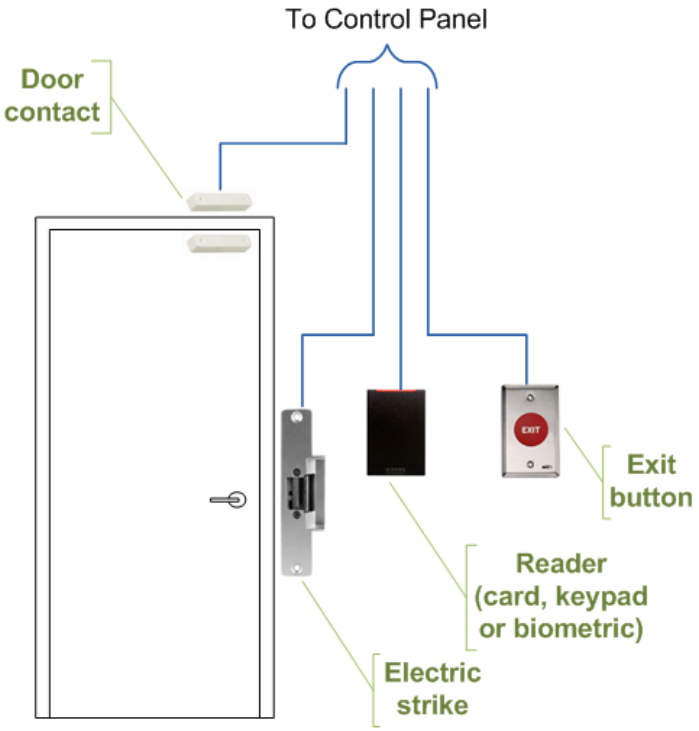
Στα συστήματα αυτά η πιστοποίηση γίνεται με βάση ατομικά χαρακτηριστικά του χρήστη με ποιο δημοφιλή τα δακτυλικά αποτυπώματα, χαρακτηριστικά ίριδας ματιού, γεωμετρία προσώπου ή παλάμης. Είναι κατάλληλα για περιβάλλοντα στα οποία απαιτείται πολύ υψηλός βαθμός ασφάλειας, τα μειονεκτήματα τους είναι το υψηλό κόστος, η τεχνική πολυπλοκότητα και το γεγονός ότι η τεχνολογία αυτή δεν είναι ακόμη σε φάση ωρίμανσης αλλά ανάπτυξης, χαρακτηριστικό παράδειγμα είναι η πιθανότητα αποτυχίας σε περίπτωση μεταβολής ατομικών χαρακτηριστικών (π.χ. χροιά φωνής). Το σίγουρο είναι ότι η τεχνολογία αυτή αποτελεί το μέλλον στον έλεγχο πρόσβασης.

1.2 Έλεγχος πρόσβασης, βάση δομής συστήματος

Κατά το σχεδιασμό συστημάτων ηλεκτρονικού ελέγχου πρόσβασης θα πρέπει πρώτα να διαχωρίσουμε δύο βασικά διαφορετικά συστήματα με τις αντίστοιχες ιδιότητες:
Τα online και τα standalone συστήματα.

1.2.1 Online συστήματα ελέγχου πρόσβασης

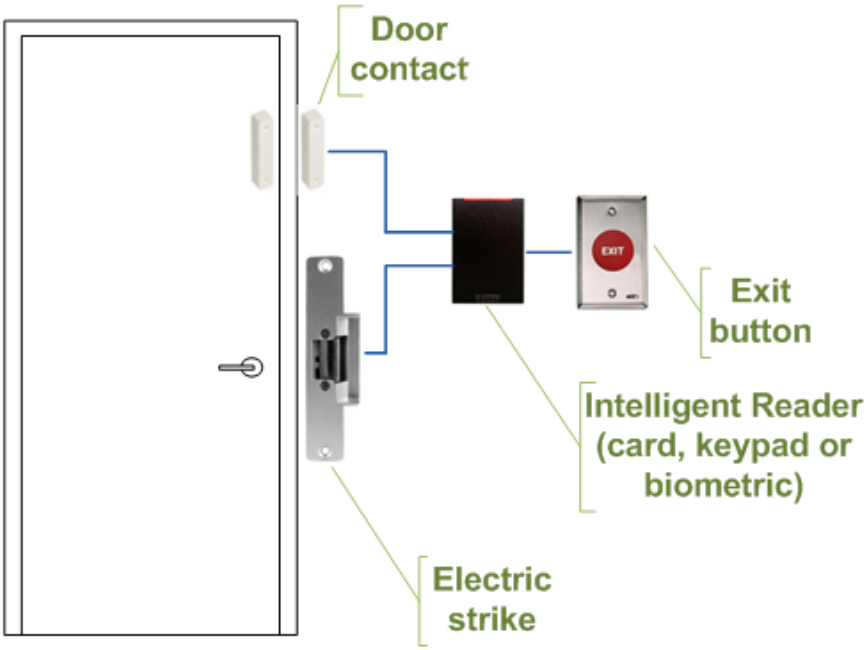
Τα online συστήματα τείνουν να χρησιμοποιούνται εκεί που η έγκριση πρόσβασης μεγάλου αριθμού ανθρώπων πρέπει να ελέγχεται σε λίγες εισόδους. Για παράδειγμα, τέτοια είναι η περίπτωση των κεντρικών εισόδων σε κτίρια γραφείων και στεγασμένους εμπορικούς χώρους. Σε αυτόν τον τύπο συστήματος, όλα οι ελεγκτές συνδέονται σε έναν κεντρικό υπολογιστή μέσω ενός δικτύου.



Ο κεντρικός υπολογιστής τρέχει μια βάση δεδομένων στην οποία στο κάθε τερματικό ανατίθενται συγκεκριμένες κάρτες που έχουν πρόσβαση σε αυτό. Τα δεδομένα πιστοποίησης που παράγονται από τη βάση δεδομένων φορτώνονται στους ελεγκτές.
Αλλαγές στην πιστοποίηση πρόσβασης ενός ατόμου μπορούν να γίνουν με μια μόνο καταχώρηση στον κεντρικό υπολογιστή του συστήματος ελέγχου πρόσβασης.
Αυτό είναι ένα πλεονέκτημα, μιας και ευαίσθητες περιοχές ασφαλείας μπορούν να προστατευτούν από μη εγκεκριμένες προσβάσεις ακόμα και στην περίπτωση που χαθεί μια κάρτα.
Οι κάρτες σε ένα online σύστημα χρειάζεται μόνο να αποθηκεύουν μια μικρή ποσότητα δεδομένων, για παράδειγμα έναν μοναδικό αριθμό εισόδου. Είναι δυνατή επίσης η χρήση καρτών που είναι μόνο για ανάγνωση.

1.2.2 Standalone συστήματα ελέγχου πρόσβασης

Τα standalone συστήματα έχουν γίνει διαδεδομένα πρωτίστως σε καταστάσεις όπου πολλά μεμονωμένα δωμάτια, στα οποία λίγοι άνθρωποι έχουν πρόσβαση, πρόκειται να εξοπλιστούν με ένα ηλεκτρονικό σύστημα ελέγχου πρόσβασης. Κάθε ελεγκτής έχει αποθηκευμένη μια λίστα όλων των καρτών που έχουν πρόσβαση σε αυτό. Δεν υπάρχει δίκτυο που το συνδέει με άλλους ελεγκτές ή με κεντρικό υπολογιστή.
Εφόσον η κάρτα είναι καταχωρημένη στον ελεγκτή, ο κάτοχος της έχει πρόσβαση στον χώρο.
Στην περίπτωση που χαθεί μια κάρτα θα πρέπει να διαγραφεί ένα αναγνωριστικό κλειδί από τον ελεγκτή που μας ενδιαφέρει με τη χρήση μιας κατάλληλης προγραμματιστικής συσκευής ή με την εισαγωγή στο μενού του διαχειριστή.



1.3 Αρχή λειτουργιάς Access control

Όταν μια κάρτα παρουσιάζεται σε έναν αναγνώστη, ο αναγνώστης στέλνει την πληροφορία της, συνήθως έναν αριθμό, στον πίνακα ελέγχου.
Ο πίνακας ελέγχου διαθέτει έναν επεξεργαστή ο οποίος συγκρίνει τον αριθμό της κάρτας με την λίστα με τους αριθμούς που έχουν πρόσβαση και ανάλογα χορηγεί ή αρνείται την αίτηση που παρουσιάζεται. Στέλνει επίσης ένα αρχείο καταγραφής κινήσεων στην βάση δεδομένων του κεντρικού server. Όταν η πρόσβαση δεν επιτρέπεται, βάση της λίστας, η πόρτα παραμένει κλειδωμένη.
Αν υπάρχει συσχέτιση του στοιχειού της κάρτας με την βάση, ο πίνακας ελέγχου δίνει εντολή σε ένα ρελέ και ξεκλειδώνει την πόρτα. Σε πολλά συστήματα ο αναγνώστης αναβοσβήνει σε περίπτωση άρνησης με ένα κόκκινο led και με πράσινο για να υποδείξει την χορήγηση πρόσβασης.

1.4 Μέρη που απαρτίζουν ένα Access control

Ένα σημείο πρόσβασης μπορεί να είναι μια πόρτα, μια πύλη πάρκινγκ, ένα ασανσέρ ή μια αυτόματη μπάρα ή καθώς και άλλα φυσικά εμπόδια που μπορούν να ελεγχθούν ηλεκτρονικά.
Τυπικά το σημείο πρόσβασης είναι μια πόρτα.
Μια ηλεκτρονική πόρτα ελέγχου πρόσβασης μπορεί να περιέχει διαφορά στοιχειά. Στην πιο απλή της μορφή αποτελείται από μια ηλεκτρική κλειδαριά και έναν διακόπτη που ενεργοποιεί την πόρτα. Τον διακόπτη αυτόν τον χειρίζεται κάποιος φύλακας και ανάλογα δίνει πρόσβαση. Εφόσον θέλουμε να αυτοματοποιήσουμε την κατάσταση αυτή ο διακόπτης αντικαθίσταται με έναν αναγνώστη.
Ο αναγνώστης αυτός θα μπορούσε να είναι ένα πληκτρολόγιο ο οποίος δέχεται ένα pin, μια συσκευή ανάγνωσης καρτών, η ένας βιομετρικός αναγνώστης.
Οι αναγνώστες συνήθως δεν παίρνουν την απόφαση πρόσβασης, άλλα στέλνουν τον αριθμό της κάρτας σε ένα πίνακα ελέγχου ο οποίο ταυτοποιεί και πιστοποιεί τον χρήστη.
Για την παρακολούθηση της θέσης της πόρτας ένας μαγνητικός διακόπτης επαφής μπορεί να χρησιμοποιηθεί. Έτσι το σύστημα γνωρίζει εάν η πόρτα παραμένει ανοιχτή η όχι.
Συνήθως αυτό που μας ενδιαφέρει είναι ο έλεγχος εισόδου. Στην περίπτωση όμως που μας ενδιαφέρει και ο έλεγχος εξόδου τοποθετείται ένας δεύτερος αναγνώστης στην μέσα πλευρά της πόρτας.
Στις περιπτώσεις που δεν απαιτείται έλεγχος εξόδου ο δεύτερος αναγνώστης αντικαθίσταται με μια REX (request to exit) συσκευή.
Η συσκευή αυτή μπορεί να είναι ένα μπουτόν εξόδου ή ένας ανίχνευτης κίνησης. Όταν το κουμπί ωθείται ή ο ανίχνευτης εντοπίσει κίνηση στην πόρτα, ο συναγερμός πόρτας αγνοείται προσωρινά και η πόρτα ανοίγει.
Στην περίπτωση που ο χρήστης προσπαθήσει να ανοίξει την πόρτα χωρίς το πάτημα του μπουτόν εξόδου ή προσπαθήσει να παραβιάσει την πόρτα ο πίνακας ελέγχου μέσω της μαγνητικής επαφής καταλαβαίνει την παραβίαση και δίνει εντολή στην σειρήνα να ηχήσει.
Το πρόγραμμα που διαχειρίζεται τον πινάκα ελέγχου μπορεί να ορίσει πάμπολλες συνθήκες για το ποτέ θα ηχεί ο συναγερμός ανάλογα με τις ανάγκες του χώρου και του διαχειριστή.

1.4.1 Αναγνώστες ελέγχου πρόσβασης

Ένας αναγνώστης καρτών είναι μια ηλεκτρονική συσκευή που η λειτουργία του είναι να διαβάζει μία κάρτα και να στέλνει τα δεδομένα σε μία κεντρική συσκευή ελέγχου, η οποία και καθορίζει αν ο κάτοχος της κάρτας έχει δικαίωμα πρόσβασης στο συγκεκριμένο χώρο.

1.4.1.1 Κατηγορίες αναγνωστών ανάλογα με τις λειτουργίες

Οι αναγνώστες των συστημάτων ελέγχου πρόσβασης μπορούν να χωριστούν σε κατηγορίες ανάλογα με τις λειτουργιές που είναι σε θέση να εκτελέσουν

Απλοί αναγνώστες
Διαβάζουν τον αριθμό της κάρτας ή ένα κωδικό εφόσον διαθέτουν πληκτρολόγιο και το διαβιβάζουν στον πινάκα ελέγχου. Στην περίπτωση που έχουμε βιομετρικό αναγνώστη διαβιβάζουν την ταυτότητα του χρήστη. Είναι η πιο διαδεδομένη κατηγορία αναγνωστών

Ημι-ευφυείς αναγνώστες
Διαθέτουν όλες τις εισόδους και εξόδους που απαιτούνται για τον έλεγχο της πόρτας άλλα δεν παίρνουν την απόφαση πρόσβασης. Διαβιβάζουν την πληροφορία της κάρτας στον πίνακα ελέγχου και περιμένουν απάντηση.

Έξυπνοι αναγνώστες
Διαθέτουν όλες τις εισόδους και εξόδους που απαιτούνται για τον έλεγχο της πόρτας Έχουν επίσης μνήμη και επεξεργαστή ώστε να παίρνουν αποφάσεις ανεξάρτητα. Όπως και οι ημι-ευφυείς αναγνώστες συνδέονται με τον κεντρικό πινάκα ελέγχου, ο οποίος στέλνει ενημερώσεις και άνακτα τα γεγονότα από τους αναγνώστες.

1.4.2 Μαγνητική επαφή

Κάθε προηγμένο σύστημα ελέγχου πρόσβασης διαθέτει ένα μαγνητικό αισθητήρα για να μπορεί να γνωρίζει εάν η πόρτα παραμένει ανοιχτή ή όχι. Αυτός ονομάζεται μαγνητική επαφή και έχει δυο ακροδέκτες. Οι ακροδέκτες του συνδέονται στα I/O του πίνακα ελέγχου. Ο διακόπτης ελέγχεται από ένα εφαρμοσμένο μαγνητικό πεδίο, με τη βοήθεια μαγνητικής επαγωγής από το ένα άκρο του αισθητήρα στο άλλο.
Όσο τα δυο άκρα δεν βρίσκονται πολύ κοντά (2-3 cm) το ένα στο άλλο τότε το κύκλωμα παραμένει ανοιχτό και έτσι δεν περνάει ρεύμα. Στην περίπτωση που τα δύο άκρα βρίσκονται σε επαφή ή τουλάχιστον πολύ κοντά τότε το κύκλωμα κλείνει και με αυτό τον τρόπο περνάει ρεύμα, το οποίο εντοπίζει ο πίνακας ελέγχου και έτσι αντιλαμβάνεται ότι η πόρτα παραμένει κλειστή.

1.4.3 Διακόπτης εξόδου

Σε ένα σύστημα ελέγχου πρόσβασης, πρέπει να υπάρχει η δυνατότητα να ανοίγει η πόρτα από μέσα, για να εξέλθει κάποιος που βρίσκεται μέσα. Το RFID reader μαζί με την κεραία για τον εντοπισμό της RFID κάρτας βρίσκεται έξω από την πόρτα, άρα δεν υπάρχει η δυνατότητα σε

κάποιον που βρίσκεται εντός του χώρου να περάσει την κάρτα του για να ανοίξει η πόρτα. Για τον λόγο αυτό πρέπει να υπάρχει ένας διακόπτης για έξοδο από την αίθουσα.
Ο διακόπτης έχει δυο ακροδέκτες, οι οποίοι συνδέονται στα I/O του πίνακα ελέγχου. Όταν ο διακόπτης πατηθεί κλείνει το κύκλωμα και περνάει ρεύμα στο δεύτερο ακροδέκτη. Αυτό έχει σαν αποτέλεσμα ο πίνακας να εντοπίζει την ύπαρξη ρεύματος, άρα να δίνει εντολή για να ανοίξει η πόρτα. Όσο ο διακόπτης δεν είναι πατημένος, το κύκλωμα παραμένει ανοιχτό, άρα δεν δίνεται εντολή για άνοιγμα της πόρτας.

1.4.4 Ηλεκτρονικές κλειδαριές

Οι ηλεκτρονικές κλειδαριές διαχωρίζονται σε πολλούς τύπους και σε διαφορετικά επίπεδα πολυπλοκότητας: ηλεκτρομαγνητικές, με ηλεκτρικό κυπρί, με ηλεκτρονικό κύλινδρο και ηλεκτρομηχανικές (με ηλεκτρικό μοτέρ).
Ίσως ο πιο διαδεδομένος τύπος είναι οι επονομαζόμενες ηλεκτρομαγνητικές κλειδαριές, γνωστές και ως μαγνητικές. Αποτελούνται από έναν ισχυρό ηλεκτρομαγνήτη που τοποθετείται στο πλαίσιο της πόρτας, ενώ ένας μαγνήτης αντίθετης πολικότητας τοποθετείται στην πόρτα. Όταν ο ηλεκτρομαγνήτης τροφοδοτείται με ρεύμα και η πόρτα είναι κλειστή, τότε τα δύο σώματα έλκονται, με αποτέλεσμα η πόρτα να μη μπορεί να ανοίξει. Το πλεονέκτημα αυτού του τύπου κλειδαριών είναι η ευκολία στην εγκατάσταση και η ανθεκτικότητά τους. Ένα μειονέκτημα είναι ότι μια μικρή αστοχία στην εγκατάσταση ή αμέλεια κατά τη συντήρηση μπορεί να δημιουργήσει προβλήματα στη λειτουργία τους.
Επίσης υπάρχει ένα θέμα όσον αφορά στη λειτουργία τους υπό καταστάσεις έκτακτης ανάγκης, όπως παραδείγματος χάρη σε πυρκαγιά, καθώς οι οδηγίες της πυροσβεστικής είναι ξεκάθαρες και δίνουν έμφαση στη δυνατότητα άμεσης διέλευσης από μία πόρτα με την απλή ώθησή της. Υπάρχουν επίσης οι κλειδαριές με ηλεκτρικό κυπρί που αντικαθιστούν ουσιαστικά τις συμβατικές κλειδαριές με τη γλώσσα κλειδαριάς και την ανάλογη υποδοχή στην κάσα της πόρτας. Είναι απλές στην εγκατάσταση, αλλά ορισμένες φορές απαιτούν κάποιες μικρές προσαρμογές στην κάσα. Το κυπρί εγκαθίσταται στην κάσα και αποτελείται από μία γλώσσα που συγκρατεί την πόρτα στη θέση της μέσω ενός ηλεκτρικού μηχανισμού. Μόλις δοθεί η ανάλογη εντολή από το χειριστήριο και σταλεί ρεύμα στο μηχανισμό, τότε η γλώσσα αφήνεται ελεύθερη και η πόρτα ανοίγει. Πάντως οι ηλεκτρομαγνητικές κλειδαριές θεωρούνται ως πιο αξιόπιστη λύση από τα ηλεκτρικά κυπριά, καθώς στα δεύτερα υπάρχει συνήθως ένα κενό μεταξύ του κυπριού και της γλώσσας της κλειδαριάς, μέσω του οποίου μπορεί κάποιος να επέμβει και να ανοίξει την πόρτα.
Άλλη μία κατηγορία ηλεκτρονικών κλειδαριών είναι εκείνη των ηλεκτρονικών κυλίνδρων. Αποτελούν ουσιαστικά ηλεκτρονικές εκδόσεις των συμβατικών μηχανικών κλειδαριών και χρησιμοποιούνται συχνά για τη μετατροπή των υφιστάμενων κλειδαριών σε ηλεκτρονικές. Ο κάθε κύλινδρος είναι μοναδικά ταυτοποιημένος και προγραμματισμένος με κωδικούς πρόσβασης, βάσει των οποίων φαίνεται ότι ανήκει σε ένα σύστημα.
Οι ηλεκτρομηχανικές κλειδαριές διαθέτουν ένα μικρό κινητήρα στο εσωτερικό τους, γι΄ αυτό ονομάζονται και κλειδαριές με ηλεκτρικό μοτέρ - το οποίο όταν ενεργοποιηθεί από έναν ηλεκτρικό παλμό αναλαμβάνει να κινήσει το μηχανισμό της κλειδαριάς και να απελευθερώσει την πόρτα. Αυτού του τύπου οι κλειδαριές τοποθετούνται σε θύρες υψηλής ασφάλειας καθώς δεν έχουν εξωτερικό πόμολο, ενώ διακρίνονται και για την ανθεκτικότητά τους καθώς έχουν πολύ μεγάλη διάρκεια ζωής ακόμα και όταν χρησιμοποιούνται πολύ συχνά.

Μια ειδική κατηγορία ηλεκτρονικών κλειδαριών είναι αυτές που χρησιμοποιούνται σε θύρες εξόδου. Αυτές συνεργάζονται με τις μπάρες πανικού που τοποθετούνται στο εσωτερικό μέρος αυτών των θυρών και όταν κάποιος σπρώξει την πόρτα, ενεργοποιείται ο μηχανισμός της κλειδαριάς και αφήνει ελεύθερη την πόρτα. Το μειονέκτημά τους είναι η πολυπλοκότητά τους που απαιτεί ιδιαίτερη ικανότητα στην εγκατάστασή αλλά και στη συντήρηση τους, ώστε να διασφαλίζεται η σωστή λειτουργία τους.

1.4.5 Κάρτες πρόσβασης και τεχνολογίες

Η τυπική πιστοποίηση για την είσοδο σε ένα σύστημα ελέγχου πρόσβασης είναι η κάρτα.
Η χρήση καρτών pvc χρησιμοποιείται εδώ και πολύ καιρό.
Αρχικά χρησιμοποιούνταν διάτρητες κάρτες, οι οποίες μετά αντικαταστάθηκαν από υπέρυθρες κάρτες, κάρτες με μαγνητική λωρίδα, κάρτες Wiegand (με μεταλλική μαγνητική λωρίδα), και τελικά με έξυπνες κάρτες που περιλαμβάνουν microchip. Το πιο σοβαρό μειονέκτημα αυτών των καρτών ήταν η δυσκολία χρήσης, καθώς έπρεπε να εισαχθούν από τη σωστή πλευρά στον αναγνώστη.
Ο έλεγχος πρόσβασης με συστήματα χωρίς επαφές έχει καθιερωθεί ποια στον χώρο και επιτρέπει πολύ μεγαλύτερη ευελιξία, αφού η κάρτα αρκεί να περάσει σε μικρή απόσταση από την κεραία του αναγνώστη. Οι πιο διαδεδομένες κάρτες αυτή την στιγμή είναι οι RFID κάρτες και οι ασύρματες έξυπνες κάρτες .

1.4.5.1 Κάρτες RFID

Ο όρος **RFID** προέρχεται από τα αρχικά των λέξεων **R**adio **F**requency **Id**entification και σημαίνει αναγνώριση ταυτότητας με τη βοήθεια ραδιοσημάτων. Μπορείτε επίσης να το δείτε μεταφρασμένο και σαν «ραδιοαναγνώριση ταυτότητας» ή «ηλεκτρονικές κάρτες» ή «ηλεκτρονικός κώδικας προϊόντων».
Τα συστήματα RFID απαρτίζονται από δύο κύρια μέρη. Το πρώτο είναι οι πομποδέκτες (transponders), που συχνά αναφέρονται και ως κάρτες RFID. Οι κάρτες RFID είναι μικρά chips που αποτελούνται από ένα ολοκληρωμένο κύκλωμα, το οποίο περιλαμβάνει μνήμη ώστε να αποθηκεύει δεδομένα (πληροφορίες - σειριακό αριθμό αναγνώρισης) και μία κεραία. Το μέγεθός τους, μπορεί να είναι τόσο μικρό, όσο το μισό ενός κόκκου άμμου (1/3 του χιλιοστού), ανάλογα με το τύπο τις κάρτας.
Το δεύτερο μέρος, είναι οι αναγνώστες ή αισθητήρες (readers), οι οποίοι ανακτούν τα δεδομένα από τις κάρτες RFID. Οι αναγνώστες RFID, έχουν ενσωματωμένα μια κεραία και μια μονάδα ελέγχου.
Οι αναγνώστες παράγουν σήματα διπλής χρήσεως. Τροφοδοτούν την κάρτα με ενέργεια και δημιουργούν ένα σήμα αναγνώρισης. Το Transponder μπορεί να είναι είτε παθητικό (passive), ή ενεργό (active). «Αιχμαλωτίζει» την ενέργεια που λαμβάνει από τον αναγνώστη και στη συνέχεια εκτελεί τις εντολές που δέχεται, στέλνοντας πίσω ένα σήμα, που περιέχει ένα μοναδικό ψηφιακό ID 96 bit, το οποίο μπορεί να ελεγχθεί από μια βάση δεδομένων, που είναι διαθέσιμη στον αναγνώστη. Έτσι, προσδιορίζεται και πιστοποιείται η ταυτότητα της κάρτας. Τα παθητικά tags δέχονται όλη την ενέργεια που χρειάζονται, από το σήμα που στέλνει ο interrogator. Αυτό σημαίνει ότι από το ίδιο ραδιοκύμα που χρησιμοποιείται για μεταφορά δεδομένων, το tag είναι ικανό να απορροφήσει την ενέργεια που χρειάζεται για να

λειτουργήσει. Επομένως, το tag τροφοδοτείται μόνο όταν βρεθεί στο πεδίο δράσης του interrogator. Το tag, τότε, χρησιμοποιεί μία τεχνική που λέγεται backscatter για να απαντήσει στον interrogator. Αυτό δεν σημαίνει ότι υπάρχει πομπός στο tag, αλλά ότι «ανακλά» το φέρον κύμα, βάζοντας δεδομένα μέσα στο σήμα επανεκπομπής.
Το tag κατασκευάζεται από ένα chip και μια κεραία. Το chip περιλαμβάνει μνήμη και μικροεπεξεργαστή. Η μνήμη στα σύγχρονα tags είναι αναγνώσιμη και επανεγγράψιμη (γύρω στις 100.000 φορές), γεγονός που μας επιτρέπει χρήση σε πληθώρα εφαρμογών.
Το tag «μιλάει» στον interrogator, χρησιμοποιώντας αυτό που καλείται air-interface. Είναι μια προδιαγραφή για το πώς επικοινωνούν μεταξύ τους και περιλαμβάνει τη συχνότητα του φέροντος, το ρυθμό μετάδοσης των bits, τη μέθοδο της κωδικοποίησης και όποιες άλλες παραμέτρους χρειάζονται.
Οι κάρτες RFID, κατηγοριοποιούνται σε τρεις τύπους ανάλογα με τον τρόπο επικοινωνίας μεταξύ των καρτών και των αναγνωστών, στις ενεργές κάρτες, στις παθητικές κάρτες και στις ημι-παθητικές ή ημι-ενεργητικές.
Ένα ολοκληρωμένο κύκλωμα στις κάρτες RFID, μπορεί να περιέχει μνήμη μόνο για ανάγνωση (read only memory - ROM), επανεγγράψιμη μνήμη (Read – Write), μνήμη μιας εγγραφής και πολλών αναγνώσεων (Write Once and Read Many memory - WORM). Στο ολοκληρωμένο κύκλωμα με μνήμη ROM, η αναγνώριση της ταυτότητας κωδικοποιείται κατά τη διάρκεια της παραγωγής της και δεν επανεγράφεται. Συμβάλει στην αποθήκευση των δεδομένων ασφαλείας, με ένα μοναδικό σειριακό αριθμό.
Αντίθετα, τα ολοκληρωμένα κύκλωμα με επανεγγράψιμη μνήμη, χρησιμοποιούνται για να αποθηκεύουν δεδομένα – πληροφορίες, όταν η κάρτα βρίσκεται στην ακτίνα του αναγνώστη και παρουσιάζουν μεγαλύτερη ευελιξία, καθώς έχουν τη δυνατότητα τροποποίησης και προσθήκης πληροφοριών. Τέλος, τα ολοκληρωμένα κυκλώματα με μνήμη “WORM”, προγραμματίζονται από τον οργανισμό που τα χρησιμοποιεί, χωρίς όμως να έχουν τη δυνατότητα της επανεγγραφής.

Αναμεταδότες ή κάρτες διαφοροποιούνται βάση της περιοχής συχνοτήτων σε τέσσερις κατηγορίες:
- Χαμηλών Συχνοτήτων (Low Frequency) < 135 KHz
- Υψηλών Συχνοτήτων (High Frequency) 13,56 MHz
- Πολύ Υψηλών Συχνοτήτων (Ultra High Frequency) 860-930 MHz
- Συχνότητες Μικροκυμάτων (Microwaves) 2,45 GHz

Ένα σημαντικό κριτήριο για την επιλογή του συστήματος RFID, είναι η συχνότητα στην οποία επικοινωνούν ο αναγνώστης RFID με τις κάρτες. Πρέπει να δοθεί μεγάλη προσοχή για να αποφευχθούν «συγκρούσεις» συχνοτήτων, με άλλα ασύρματα συστήματα. Ο λόγος έγκειται στο γεγονός, ότι το RFID λειτουργεί στην ISM ζώνη συχνοτήτων, στην οποία λειτουργούν επίσης πολλές ιατρικές, βιομηχανικές και επιστημονικές εφαρμογές.

Ζώνη συχνοτήτων 100 – 135 KHz

Πλεονεκτήματα
- Χρήση χαμηλού κόστους παθητικών πομποδεκτών.
- Καλή διείσδυση στα μη μεταλλικά αντικείμενα, στο νερό και στους οργανικούς ιστούς.

- Τυποποίηση μέσω του ISO 11784/85.
- Σχετικά αδιαπέραστη σε μεταλλικές παρεμβολές.
- Ζώνη συχνοτήτων παγκοσμίως διαθέσιμη.
- Υψηλή επιτρεπόμενη ισχύς εκπομπής.

Μειονεκτήματα
- Ευρύ φάσμα των διαθέσιμων μορφών κατασκευής αναμεταδότη (υψηλή συνέλιξη της σπειροειδής κεραίας).
- Μικρή χωρητικότητα δεδομένων.
- Αργή μεταφορά δεδομένων.

Συχνότητα 13,56 MHz

Πλεονεκτήματα
- Χρήση χαμηλού κόστους παθητικών πομποδεκτών.
- Τυποποίηση μέσω του ISO 15693, Part 1-3.
- Υψηλή χωρητικότητα δεδομένων.
- Η μέση ταχύτητα μεταφοράς δεδομένων 26 kbit/sec.
- Ζώνη συχνοτήτων παγκοσμίως διαθέσιμη.
- Μειονεκτήματα
- Υψηλή εξασθένηση μέσα από μεταλλικά περιβάλλοντα.
- Η απόσταση ανάγνωσης περιορίζεται από τους νομικούς κανονισμούς.
- Μεγαλύτερες αποστάσεις ανάγνωσης, μπορούν να επιτευχθούν με μεγαλύτερες κεραίες.

Συχνότητες 896, 915 MHz

Πλεονεκτήματα
- Μεγάλες αποστάσεις ανάγνωσης.
- Απλός σχεδιασμός της κεραίας.
- Αποδοτικό από πλευράς κόστους.
- Τυποποίηση (EPC - electronic Product code).

Μειονεκτήματα
- Αδύναμη η διείσδυση στο νερό και τους οργανικούς ιστούς.

Συχνότητα 2,45 GHz

Πλεονεκτήματα
- Υψηλή ταχύτητα μεταφοράς δεδομένων.
- Μεγάλες αποστάσεις ανάγνωσης.

Μειονεκτήματα
- Μεγάλος μέγεθος.

- Υψηλό κόστος.
- Χρήση μπαταριών στους αναμεταδότες.
- Η διάρκεια ζωής περιορίζεται, λόγω των μπαταριών.
- Δεν υπάρχει τυποποίηση.

1.4.5.2 Ασύρματες έξυπνες κάρτες

Στον αντίποδα των καρτών RFID, βρίσκονται οι ασύρματες «έξυπνες» κάρτες που χρησιμοποιούνται βασικά σε εφαρμογές κατά τις οποίες η προστασία των δεδομένων που περιέχουν ή των συναλλαγών που επιτρέπουν είναι υψίστης σημασίας. Τις ίδιες υπηρεσίες, βέβαια, προσφέρουν και οι κοινές κάρτες που ενεργοποιούνται με επαφή χωρίς να περιλαμβάνουν την εύχρηστη τεχνολογία του RF interface, η οποία επιτρέπει την ανάγνωση των δεδομένων σε απόσταση κοντινή από το μηχανισμό σάρωσης.
Η ασύρματη συσκευή περιλαμβάνει ένα μικροεπεξεργαστή ασφαλείας και εσωτερική μνήμη, η οποία έχει τη μοναδική ικανότητα να διαχειρίζεται, να αποθηκεύει και να παρέχει πρόσβαση σε δεδομένα της κάρτας, καθώς και να εκτελεί πολύπλοκες διαδικασίες, όπως κρυπτογράφηση. Εφαρμογές που απαιτούν υψηλού βαθμού πληροφορίες και μεγάλη ασφάλεια επικοινωνιών, όπως είναι η μισθοδοσία, χρησιμοποιούν επίσης την τεχνολογία της ασύρματης «έξυπνης» κάρτας. Η τεχνολογία αυτή βασίζεται σε ένα διεθνές στάνταρ το οποίο περιορίζει την ικανότητα της ανάγνωσης από την ασύρματη συσκευή σε απόσταση 10 ςm. Στην περίπτωση που χρειαστεί μεγαλύτερη απόσταση ανάγνωσης, πρέπει να καταφύγουμε σε άλλες κατάλληλες φόρμες ασύρματης τεχνολογίας. Η τεχνολογία της ασύρματης «έξυπνης» κάρτας υποστηρίζει χαρακτηριστικά ασφαλείας τα οποία διασφαλίζουν την ακεραιότητα και την εχεμύθεια των πληροφοριών που αποθηκεύονται ή μεταδίδονται. Τέτοια είναι:

- Η αμοιβαία πιστοποίηση. Κατά την επεξεργασία των δεδομένων η συσκευή αναγνώρισης πιστοποιεί την αυθεντικότητα του χρήστη πριν ξεκινήσει τη διαδικασία της συναλλαγής.
- Η υψηλή ασφάλεια πληροφοριών. Οι πληροφορίες που είναι αποθηκευμένες σε κάρτες ή έγγραφα που χρησιμοποιούν την παραπάνω τεχνολογία μπορούν να κρυπτογραφηθούν. Το ίδιο μπορεί να συμβεί και στην επικοινωνία μεταξύ συσκευής και χρήστη, ώστε να αποφευχθεί η περίπτωση υποκλοπής.
- Η υψηλή ασφάλεια της ασύρματης μονάδας. Όπως συμβαίνει και στις υπόλοιπες κάρτες, έτσι και στις ασύρματες « έξυπνες» κάρτες, η τεχνολογία τους είναι πολύ δύσκολο να αντιγραφεί. Τα ολοκληρωμένα κυκλώματα τους περιλαμβάνουν μια ποικιλία λογισμικών τα οποία ανιχνεύουν οποιαδήποτε προσπάθεια αντιγραφής και αντιδρούν σε αυτήν.
- Η πιστοποιημένη πρόσβαση πληροφοριών. Η ικανότητα της ασύρματης «έξυπνης» κάρτας να επεξεργάζεται πληροφορίες και να αλληλεπιδρά με το περιβάλλον, της επιτρέπει την παροχή πιστοποιημένων μόνο πληροφοριών και την προστασία των προσωπικών δεδομένων. Οποιοσδήποτε ζητήσει πληροφορίες ελέγχεται και η πρόσβαση σε αυτές προστατεύεται από ένα προσωπικό αριθμό αναγνώρισης (PIN).
- Η μέγιστη ασφάλεια των προσωπικών δεδομένων. Η χρήση της τεχνολογίας της «έξυπνης» κάρτας ενδυναμώνει την ικανότητα του συστήματος να προστατεύει τα προσωπικά δεδομένα κάθε ατόμου σε αντίθεση με άλλες τεχνολογίες. Η «έξυπνη» κάρτα έχει ενσωματωμένο ένα προστατευτικό τείχος για κάθε χρήστη, που επιτρέπει την

- αποδέσμευση της πληροφορίας μόνο όταν αυτή ζητείται. Οι «έξυπνες» κάρτες γίνονται έτσι προστάτες του ιδιωτικού βίου των πολιτών.

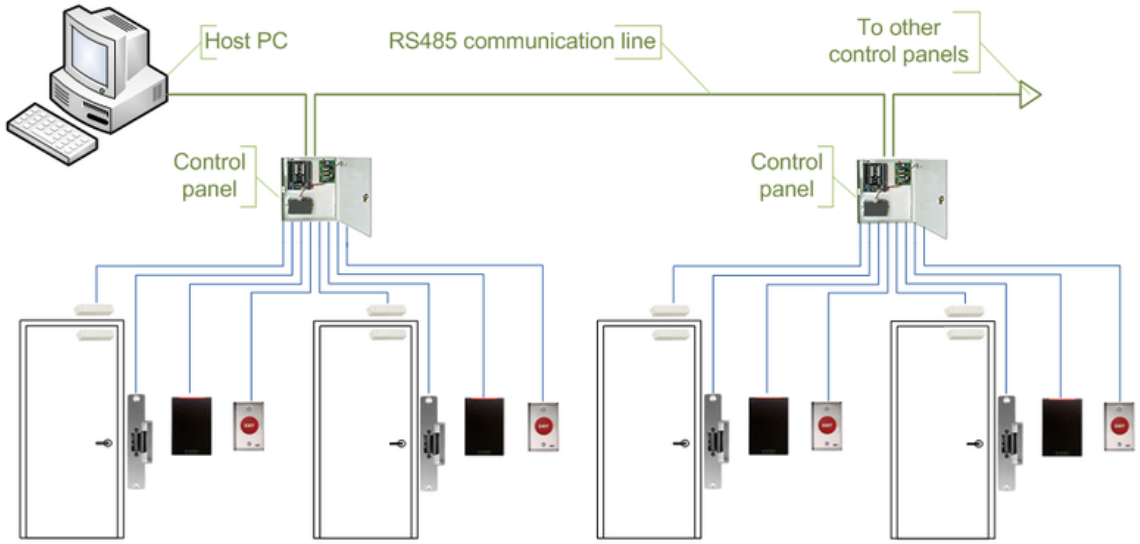
Είδη έξυπνων καρτών

Στις μέρες μας, οι έξυπνες κάρτες μπορούν να κατηγοριοποιηθούν με δύο βασικά κριτήρια: επεξεργαστική ικανότητα και δυνατότητες εισόδου-εξόδου.
Με βάση την επεξεργαστική ικανότητα:
Διακρίνουμε τις εξής κατηγορίες:

- Κάρτες μνήμης – κάρτες αποθήκευσης πληροφοριών (memory cards). Οι κάρτες αυτές περιέχουν κάποια μνήμη και λογική σε υλικό (hardware logic), η οποία μπορεί να θέσει ή να διαγράψει τιμές στη μνήμη. Οι κάρτες μνήμης αναφέρονται καταχρηστικά ως έξυπνες κάρτες, καθώς δεν έχουν δυνατότητα επεξεργασίας των δεδομένων.
- Έξυπνες κάρτες (smart cards, IC cards, microprocessor cards). Είναι οι «κλασικές» έξυπνες κάρτες ή κάρτες με μικροεπεξεργαστή,. Ο επεξεργαστής τους, πέρα από την αποθήκευση και ασφάλιση πληροφοριών, μπορεί να λαμβάνει αποφάσεις που ορίζονται στις προδιαγραφές του έργου για το οποίο θα χρησιμοποιηθούν.
- Έξυπνες κάρτες πολλαπλών εφαρμογών (multi-application smart cards). Οι έξυπνες κάρτες τελευταίας γενιάς έρχονται με ανοικτά λειτουργικά συστήματα (Java, MULTOS)και μπορούν να εκτελούν περισσότερες από μία εφαρμογές. Παρέχεται επίσης η δυνατότητα στο χρήστη να «φορτώνει» νέες εφαρμογές, ή να διαγράφει άλλες ανάλογα με τις ανάγκες του. Οι κάρτες με μικροεπεξεργαστή, εκτός από ςPU, διαθέτουν μνήμη ROM για την αποθήκευση του λειτουργικού συστήματος της κάρτας, μνήμη RAM για γρήγορη εκτέλεση υπολογισμών και μνήμη EE PROM για την αποθήκευση εφαρμογών και δεδομένων. Πρόκειται ουσιαστικά για ολοκληρωμένους μικροσκοπικούς Η/Υ, οι οποίοι στερούνται μόνο συσκευών εισόδου / εξόδου. Έτσι προκειμένου να επικοινωνήσουμε με τους υπολογιστές αυτούς χρησιμοποιούμε τις συσκευές αποδοχής έξυπνων καρτών (card readers).

1.5 Τοπολογία συστημάτων ελέγχου πρόσβασης και εξέλιξη

1.5.1 Σειριακοί πίνακες ελέγχου
Οι σειριακοί πίνακες ελέγχου είναι συνδεδεμένοι με τον κεντρικό server μέσω RS-485 γραμμή επικοινωνίας.
Για την επικοινωνία με τον κεντρικό υπολογιστή θα πρέπει να τοποθετηθούν ειδικοί μετατροπείς RS232/RS485 εφόσον οι στάνταρ υπολογιστές δεν διαθέτουν θύρα RS485.



Πλεονεκτήματα

Το πρότυπο RS-485 επιτρέπει μακριές διαδρομές καλωδίων από πάνελ σε πάνελ έως 1200 μέτρα.

- Υψηλή αξιοπιστία και ασφάλεια εφόσον δεν μοιράζεται η γραμμή με άλλα συστήματα.

Μειονεκτήματα

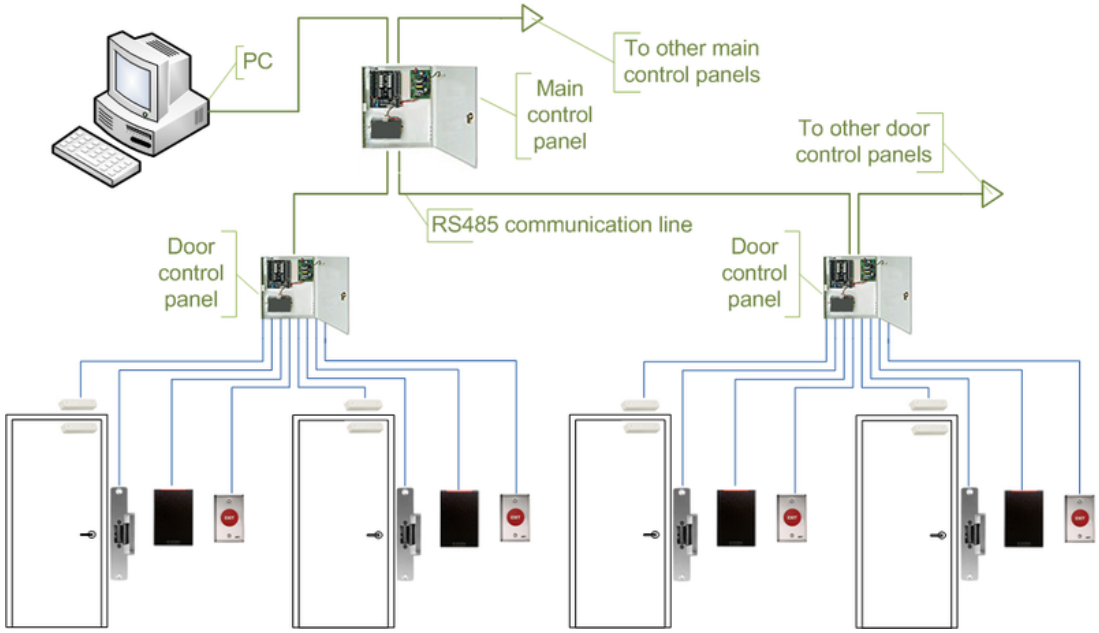
Δεν είναι κατάλληλη για τη μεταφορά μεγάλων ποσοτήτων δεδομένων. Η υψηλότερη δυνατή απόδοση είναι 115,2 kbit / ses , αλλά στις περισσότερες περιπτώσεις το σύστημα υποβαθμίζεται σε 56,2 kbit / ses ή λιγότερο , να αυξηθεί η σταθερότητα .

- Δεν επιτρέπει στον κεντρικό υπολογιστή να επικοινωνεί με όλους τους ελεγκτές που συνδέονται ταυτόχρονα . Συνεπώς, σε μεγάλα συστήματα το να μεταφέρουμε χρήστες, στους ελεγκτές ή για να κάνουμε διαφορές παραμετροποιήσεις μπορεί να διαρκέσει πολύ χρόνο .
- Το καλώδιο που χρησιμοποιείται για τα RS -485 πρότυπα είναι σημαντικά πιο ακριβό από τα UTP καλώδιο δικτύου Κατηγορίας 5.
- Η λειτουργία του συστήματος σε μεγάλο βαθμό εξαρτάται από τον κεντρικό υπολογιστή .Σε περίπτωση που ο κεντρικός υπολογιστής έχει πρόβλημα, τα γεγονότα από τους ελεγκτές δεν μπορούν να ανακτηθούν και οι λειτουργίες που απαιτούν αλληλεπίδραση μεταξύ των ελεγκτών (π.χ. anti passbaϲk) σταματούν.

1.5.2 Σειριακοί πίνακες ελέγχου και υποελεγκτές

Σε αυτή την περίπτωση όλα τα στοιχειά της πόρτας είναι συνδεδεμένα σε υποελεγκτές.

Οι υποελεγκτές με την σειρά τους συνδέονται με τους σειριακούς πινάκες ελέγχου που έχουν και τα στοιχεία πρόσβασης. Κάθε σειριακός πίνακας μπορεί να υποστηρίξει συνήθως από 16-32 υποελεγκτές. Οι σειριακοί πίνακες ελέγχου είναι συνδεδεμένοι με τον κεντρικό server μέσω RS-485 γραμμή επικοινωνίας.



Πλεονεκτήματα

- Το φόρτος εργασίας για τον κεντρικό υπολογιστή έχει μειωθεί σημαντικά , επειδή χρειάζεται να επικοινωνεί με λιγότερους πινάκες ελέγχου
- Το συνολικό κόστος του συστήματος είναι μικρότερο , επειδή οι υποελεγκτές είναι φθηνότερες συσκευές.

Μειονεκτήματα

- Η λειτουργία του συστήματος εξαρτάται σε μεγάλο βαθμό από τους πινάκες ελέγχου. Σε περίπτωση που ένας από τους πινάκες ελέγχου αποτύχει, τα γεγονότα από τους υποελεγκτές δεν θα ανακτηθούν, και λειτουργίες που απαιτούν αλληλεπίδραση μεταξύ των υποελεγκτών σταματούν.
- Οι κεντρικοί πινάκες ελέγχου έχουν μεγάλο κόστος και ως εκ τούτου, μια τέτοια τοπολογία δεν είναι πολύ κατάλληλη για συστήματα με πολλαπλές απομακρυσμένες περιοχές που έχουν μικρό αριθμό πορτών.

1.5.3 Σειριακοί πίνακες ελέγχου με τερματικοί διακομιστές

Τερματικός διακομιστής (Terminal server) είναι ένας μετατροπέας που επιτρέπει να συνδεθούν συσκευές με σειριακές θύρες σε τοπικό δίκτυο Lan.
Ο κεντρικός υπολογιστής συνδέεται με ένα ή περισσότερα switch τα οποία συνδέονται με τερματικούς διακομιστές και αυτοί με την σειρά τους με τους πίνακες ελέγχου

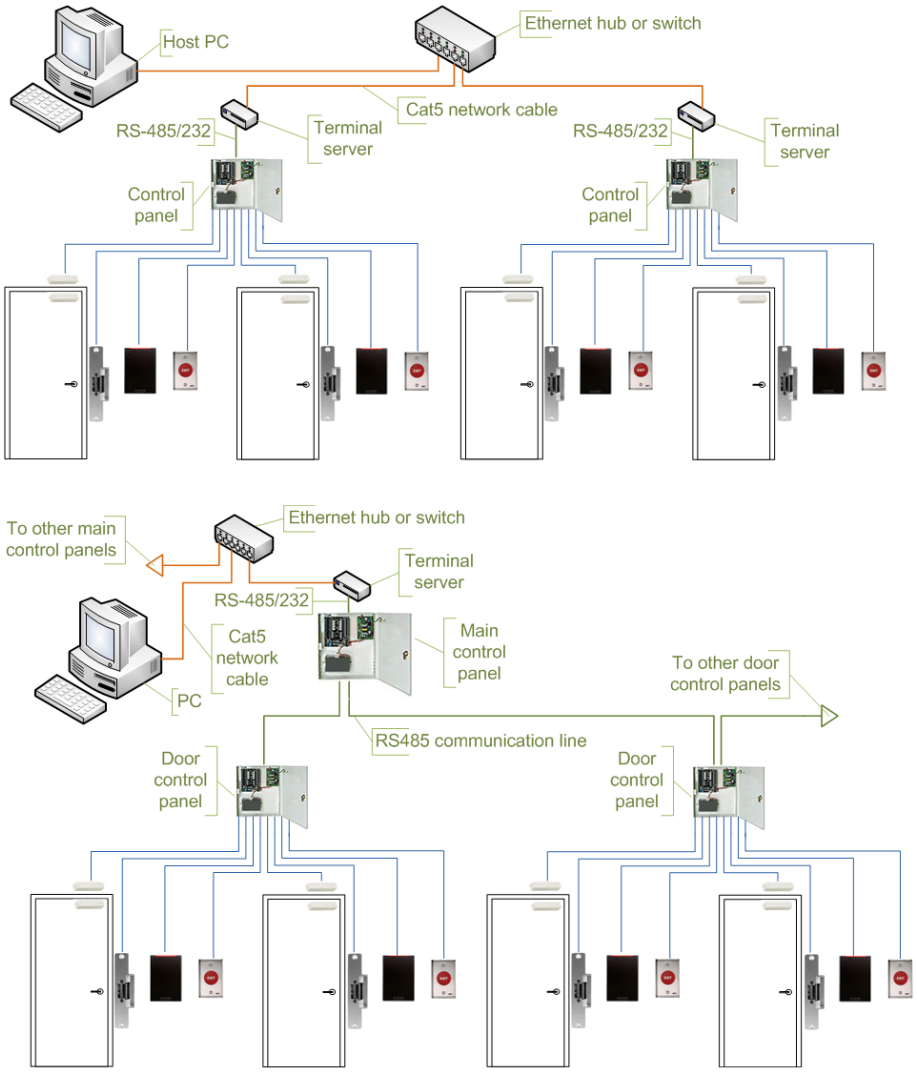
Πλεονεκτήματα

- Επιτρέπει τη χρήση της υπάρχουσας υποδομής δικτύου για τη σύνδεση διαφορετικών τμημάτων του συστήματος .

- Παρέχει μια βολική λύση σε περιπτώσεις όπου η εγκατάσταση μιας γραμμής RS -485 είναι δύσκολη ή αδύνατη.

Μειονεκτήματα

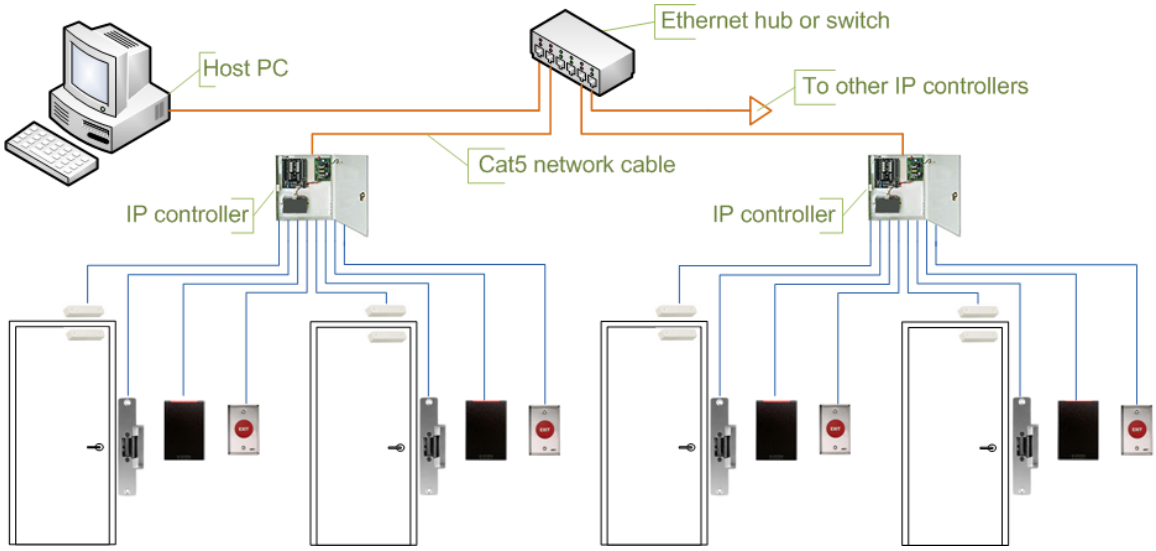
- Αυξάνει την πολυπλοκότητα του συστήματος .
- Δημιουργεί πρόσθετη εργασία για τους εγκαταστάτες. Οι τερματικοί διακομιστές πρέπει να ρυθμιστούν ανεξάρτητα από το υπόλοιπο σύστημα ελέγχου πρόσβασης.
- Η σειριακή σύνδεση επικοινωνίας μεταξύ των πινάκων ελέγχου και των τερματικών διακομιστών επιβραδύνει το σύστημα ακόμη και αν τα δεδομένα μεταξύ του Pς και του terminal server ταξιδεύει με την ταχύτητα του δικτύου 10/100/1000Mbit/seς. Θα πρέπει να επιβραδύνει στην ταχύτητα της σειριακής 112,5 kbit / seς ή λιγότερο. Υπάρχουν, επίσης, πρόσθετες καθυστερήσεις στην διαδικασία της μετατροπής μεταξύ σειριακού και ethernet δικτύου.



1.5.4 Δικτυακοί πίνακες ελέγχου (IP controllers)

Οι δικτυακοί πινάκες ελέγχου συνδέονται με τον κεντρικό υπολογιστή μέσω Ethernet Lan ή Wan. Είναι η εξέλιξη όσον άφορα τα συστήματα ελέγχου πρόσβασης.

Ένας τυπικός ip πίνακας ελέγχου πρόσβασης υποστηρίζει από έναν έως 4 αναγνώστες και συνήθως διαθέτει ενσωματωμένο web server ώστε να διαχειρίζεται ευέλικτα μέσω browser.



Πλεονεκτήματα

- Η υπάρχουσα υποδομή του δικτύου μπορεί να χρησιμοποιηθεί πλήρως
- Δεν υπάρχουν περιορισμοί όσον αφορά τον αριθμό των ελεγκτών (ως 32 ανά γραμμή σε περιπτώσεις RS - 485) .
- Η επικοινωνία με τους ελεγκτές μπορεί να γίνει με την πλήρη ταχύτητα του δικτύου , το οποίο είναι σημαντικό, αν μεταφέρονται πολλά δεδομένα (βάσεις δεδομένων με χιλιάδες χρήστες καθώς και βιομετρικά στοιχειά) .
- Απλοποιείται η εγκατάσταση των συστημάτων που αποτελούνται από πολλαπλές θέσεις και χωρίζονται από μεγάλες αποστάσεις.
- Ευρεία γκάμα στάνταρ δικτυακού εξοπλισμού είναι διαθέσιμη για την παροχή πρόσβασης ανάλογα με την περίπτωση (οπτικές ίνες , ασύρματη σύνδεση , VPN , PoE)

Μειονεκτήματα

- Το σύστημα γίνεται επιρρεπές σε προβλήματα που σχετίζονται με το δίκτυο, όπως καθυστερήσεις στην περίπτωση traffic και προβλήματα στον εξοπλισμό δικτύου .
- Οι ελεγκτές πρόσβασης μπορούν να γίνουν προσβάσιμοι σε hackers εάν το δίκτυο δεν είναι καλά προστατευμένα. Αυτή η απειλή μπορεί να εξαλειφθεί με φυσικό διαχωρισμό του δικτύου ελέγχου πρόσβασης από το κεντρικό δίκτυο. Επίσης θα πρέπει να σημειωθεί ότι οι περισσότεροι ελεγκτές IP χρησιμοποιούν πλατφόρμα Linux γεγονός που τους καθιστά πιο δύσκολο να χακαριστούν. Χρησιμοποιείται επίσης πρωτόκολλο κρυπτογράφησης δεδομένων.
- Η μέγιστη απόσταση από switch σε ελεγκτή (αν χρησιμοποιείτε καλώδιο χαλκού) δεν μπορεί να ξεπερνάει τα 100 μέτρα.

ΚΕΦΑΛΑΙΟ 2.

2.1 Υλικά εγκατάστασης

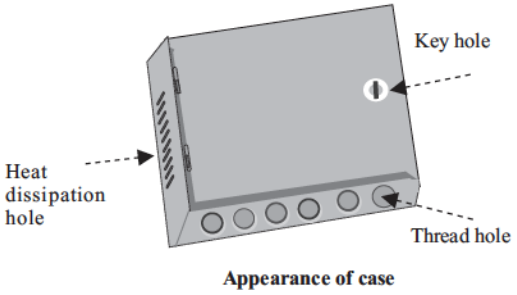
Η υλοποίηση του συστήματος ελέγχου πρόσβασης βασίστηκε στον πίνακα ελέγχου ZKSoftware C3-100 και στήθηκε γύρω από αυτό. Η αρχιτεκτονική του πίνακα επιτρέπει τη σύνδεση διαφόρων εξαρτημάτων (αισθητήρων, συσκευών) τα οποία με τον κατάλληλο προγραμματισμό επιτελούν έναν στόχο.
Ο πίνακας ελέγχει και διαχειρίζεται ένα σύνολο υλικών-εξαρτημάτων το οποία είναι τα εξής :

ΥΛΙΚΑ	ΤΕΜΑΧΙΑ
KR201 Wiegand Reader	1
Μαγνητικός αισθητήρας επαφής	1
Ηλεκτρικό κυπρί	1
Button για άνοιγμα πόρτας	2

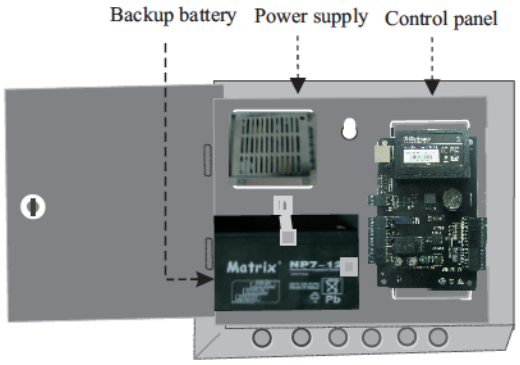
Ουσιαστικά αυτό που υλοποιεί ο ZKSoftware είναι να μαζεύει πληροφορίες και γεγονότα, αλληλεπιδρώντας με το περιβάλλον, μέσω των υλικών και των εξαρτημάτων που είναι συνδεδεμένα σε αυτό. Στη συνέχεια στέλνει αυτά τα δεδομένα στον server μέσω δικτύου.

2.2 Πίνακας ελέγχου ZKSoftware C3-100

Η καρδιά του συστήματος είναι ο έξυπνος ελεγκτής πρόσβασης μιας θύρας C3-100.
Ο ελεγκτής βρίσκεται μέσα σε ένα μεταλλικό κουτί που τον προστατεύει, το όποιο περιλαμβάνει επίσης ένα τροφοδοτικό 220VAC - 12VDC καθώς και backup μπαταρία στην περίπτωση διακοπής ρεύματος.



Appearance of case



Η σειρά προϊόντων ελέγχου πρόσβασης iAccess της ZKSoftware σχεδιάστηκε με γνώμονα την ευελιξία προσφέροντας διαχείριση, επιτήρηση σε πραγματικό χρόνο και παραμετροποίηση του συστήματος ελέγχου πρόσβασης απλά με την χρήση ενός Browser (Internet Explorer, Firefox, chrome κ.α.) χωρίς να χρειάζεται εγκατάσταση έξτρα λογισμικού. Ιδιαίτερη έμφαση έχει δοθεί στην επεκτασιμότητα του συστήματος.

Ο ελεγκτής C3-100 διαθέτει θύρες I/O για διασύνδεση με συστήματα κλειστού κυκλώματος τηλεόρασης, πυρασφάλειας και BMS και αποτελεί μια αξιόπιστη και αποδοτική λύση χωρίς περιορισμό σε μελλοντικές αναβαθμίσεις.
Ο ελεγκτής C3-100 διαθέτει 2 τύπους επικοινωνίας, RS-485 38.4 Kbps ή TCP/IP Ethernet και τεράστια μνήμη (30.000 χρήστες – 100.000 συμβάντα) καλύπτοντας πλήρως τις ανάγκες κάθε μικρής ή μεγάλης εγκατάστασης.
Παράλληλα προσφέρεται το SDK (Software Development Kit) για την προσαρμογή και διασύνδεση του συστήματος ελέγχου πρόσβασης με αλλά υποσυστήματα.

2.2.1 Χαρακτηριστικά και λειτουργιές πίνακα ελέγχου

- Υποδοχή κάρτας SD για Backup δεδομένων.
- Σε περίπτωση οποιασδήποτε δυσλειτουργίας του συστήματος, ο διαχειριστής έχει την δυνατότητα να επαναφέρει το σύστημα σε πλήρη λειτουργικότητα χωρίς την παραμικρή απώλεια δεδομένων χρησιμοποιώντας το αρχείο Backup που αποθηκεύεται στην κάρτα SD.
- Πολλαπλό κύκλωμα προστασίας.
- Ο ελεγκτής C3 διαθέτει προστασία υπέρτασης και αναστροφής πολικότητας στα υποσυστήματα τροφοδοσίας και I/O
- Υποστήριξη διαφορετικών αναγνωστών Wiegand.
- Ο ελεγκτής C3 υποστηρίζει πολλαπλά πρωτόκολλα Wiegand και διαφορετικού τύπου αναγνώστες όπως κάρτας ID, Mifare, HID κ.α.
- Θύρες I/O.
- Δυνατότητα σύνδεσης ποικιλίας αισθητήρων, σειρήνων, μπουτόν εξόδου, ηλεκτρονικών κλειδαριών και άλλων συσκευών.
- Επιτήρηση σε πραγματικό χρόνο.
- Με την χρήση απλώς ενός Browser δίνεται η δυνατότητα της επιτήρησης και διαχείρισης της κατάσταση κάθε θύρας του συστήματος.
- Εύκολη παραμετροποίηση Ελέγχου πρόσβασης
- Λειτουργία Multi-card.
- Με την λειτουργία Multi-card μπορούμε να ορίσουμε να επιτρέπεται η πρόσβασή μόνο αν αναγνωσθούν 2 ή περισσότερες κάρτες την ιδία στιγμή για χώρους με υψηλό βαθμό ασφάλειας.
- Λειτουργία Anti-Passback.
- Λειτουργία Duress.
- Αναλυτική αναφορά για την κίνηση στον χώρο : χρόνος, υπάλληλος και καταγραφή σε αρχείο
- Δημιουργία χρονικών ζωνών πρόσβασης
- Δημιουργία τμημάτων και έλεγχος της πρόσβασης τους
- Απομακρυσμένο άνοιγμα και κλείσιμο πορτών
- Electro-map
- First Card Normal Open
- Interlock

2.2.2 Τεχνικές προδιαγραφές πίνακα ελέγχου

ZKSoftware C3-100	
Επεξεργαστής	32bit MIPS CPU 400MHz
Μνήμη RAM	32 M
Μνήμη Flash	256 M
Αριθμός Χρηστών	30.000
Μνήμη συμβάντων	100.000
Τροφοδοσία	DC 9.6V ~ 14.4V, 1A max
Θύρες Αναγνωστών	2 (26/23bit Wiegand, 8bit Burst for PIN)
Επικοινωνία	RS-485, TCP/IP Ethernet
Baud Rate	9.600bps, 19.200bps, 57.600bps
Ψηφιακές είσοδοι	2 (μπουτόν εξόδου 1#, αισθητήρας θύρας 1#)
Θερμοκρασία Λειτουργίας	0 ~ +55° C
Έξοδοι ρελέ	1(FORM-C 2A@30VDC 1#)
Ενδεικτικά LED	3 (Επικοινωνίας, κατάστασης, ανάγνωσης κάρτας)
Διαστάσεις	345(Μ) x 275(Π) x 70(Β) Μεταλλικό κουτί με τροφοδοτικό
Λειτουργικό	LINUX
Λογισμικό	ZKSoftware

2.2.3 Ενδεικτικά Leds πίνακα ελέγχου

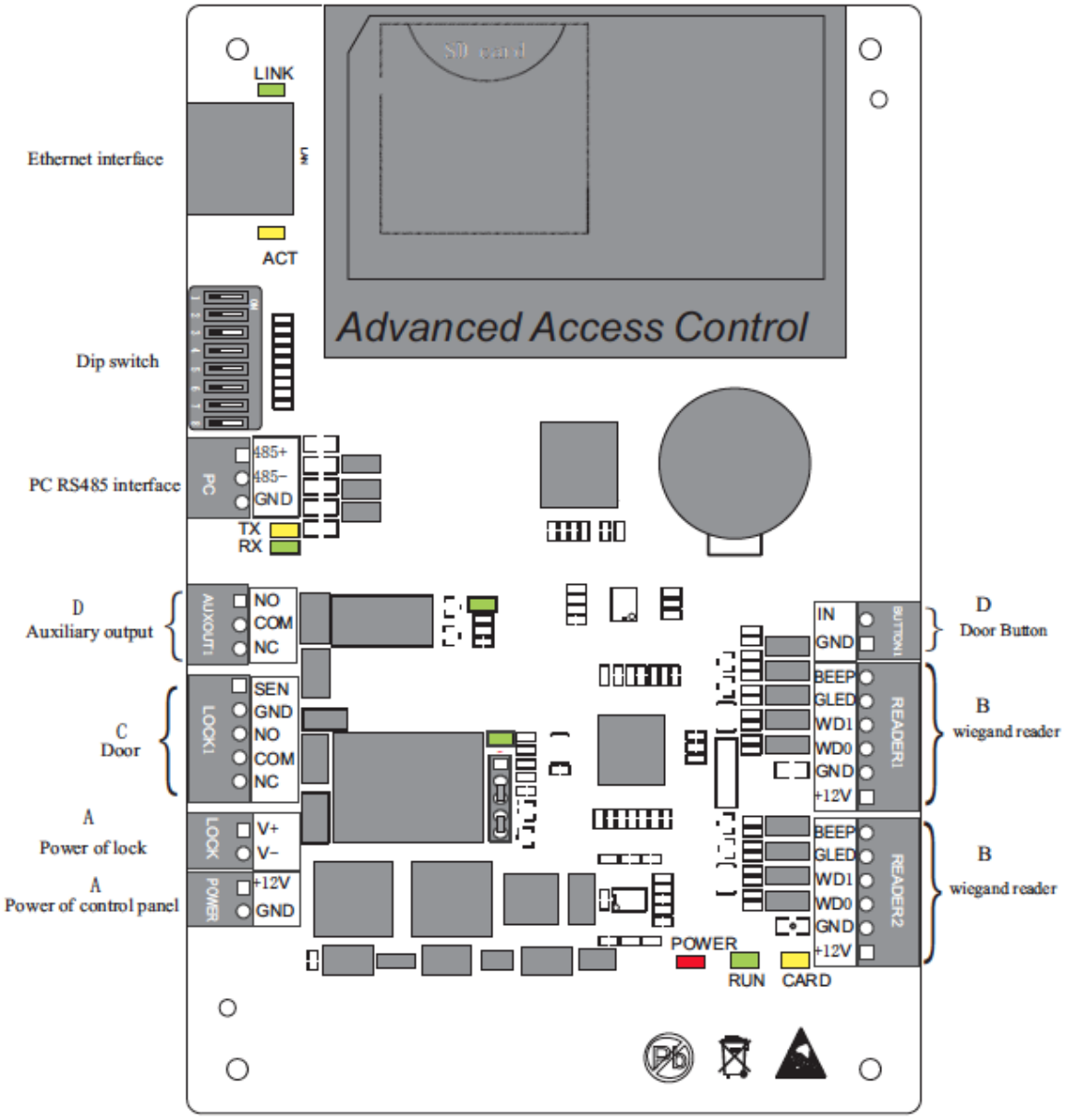
- Led POWER (κόκκινο) ένδειξη ότι το σύστημα είναι σε ενεργή κατάσταση
- Led RUN (πράσινο αναβοσβήνει) ένδειξη ότι το σύστημα είναι σε κατάσταση ηρεμίας.
- Led LINK (πράσινο): ένδειξη ενεργής σύνδεσης TCP / IP
- Led ACT (κίτρινο): ένδειξη μετάδοσης δεδομένων TCP / IP
- Led TX (κίτρινο): ένδειξη αποστολής δεδομένων RS-485
- Led RX (πράσινο): ένδειξη λήψης δεδομένων RS-485
- Led LOCK (πράσινο): ένδειξη ξεκλειδώματος
- Led CARD (κίτρινο): ένδειξη σήματος εισόδου αναγνώστη

2.2.4 I/O πίνακα ελέγχου

Ο πίνακας ελέγχου διαθέτει ένα πλήθος εισόδων και έξοδων που απαιτούνται για την αντίδραση του με το περιβάλλον.Όπως μπορούμε να παρατηρήσουμε στο σχήμα που ακολουθεί στην δεξιά πλευρά της πλακέτας έχουμε τις κλέμες για τους δύο αναγνώστες καθώς και την κλέμα για το μπουτόν εξόδου.

Στην αριστερή πλευρά της πλακέτας, από πάνω προς τα κάτω, υπάρχει η θύρα ethernet που είναι υπεύθυνη για την επικοινωνία με το δίκτυο. Ακριβώς από κάτω υπάρχουν τα dip switch του RS485, με τα οποία δηλώνουμε την διεύθυνση του πινάκα εφόσον έχουμε παραπάνω από έναν.

Στην συνέχεια ακολουθεί η κλέμα διασύνδεσης του RS485 καθώς και η βοηθητική έξοδος η οποία είναι πλήρως παραμετροποιήσιμη από το πρόγραμμα ανάλογα με τις απαιτήσεις. Συνήθως συνδέεται μια σειρήνα ή ένα κουδούνι. Επίσης έχουμε την κλέμα που είναι υπεύθυνη για την επικοινωνία με τον αισθητήρα καθώς και την επαφή του ρελέ που οδηγεί το ηλεκτρικό κυπρί της της πόρτας. Τέλος έχουμε την κλέμα που τροφοδοτεί την κλειδαριά καθώς και την κλέμα της τροφοδοσίας του συνολικού πίνακα.



Συγκεντρωτικά έχουμε :

ZKSOFTWARE C3-100 I/O	
Αναγνώστης καρτών	2
Μαγνητική επαφή	1
Ρελέ ελέγχου πόρτας	1
Button εξόδου	1
Auxiliary output (Βοηθητικό ρελέ)	1
RS485	1
TCP/IP	1

2.3 Αναγνώστης Wiegand ZKSoftware KR201E

Στην είσοδο του εργαστηρίου μικροϋπολογιστών εγκαταστάθηκε ο αναγνώστης KR201E.
Με κομψή και στιβαρή σχεδίαση, είναι εύκολο να συνδεθεί και να εγκατασταθεί σε οποιαδήποτε επιφάνεια. Ο αναγνώστης εγκαταστάθηκε στον τοίχο ακριβώς δίπλα στην πόρτα σε ύψος 1.40 m το οποίο είναι το ιδανικό για την ομαλή χρήση του.
Τα φώτα LED υποδεικνύουν εάν επιτρέπεται ή απαγορεύεται η πρόσβαση. σε κοντινή απόσταση έως 10 εκατοστά. Το γεγονός ότι αυτή η σειρά είναι αδιάβροχη, και οι θερμοκρασίες λειτουργίας μπορούν να κυμαίνονται από -20 º έως +65 º, είναι η ιδανική λύση για εσωτερική άλλα και εξωτερική εγκατάσταση.

2.3.1 Χαρακτηριστικά αναγνώστη

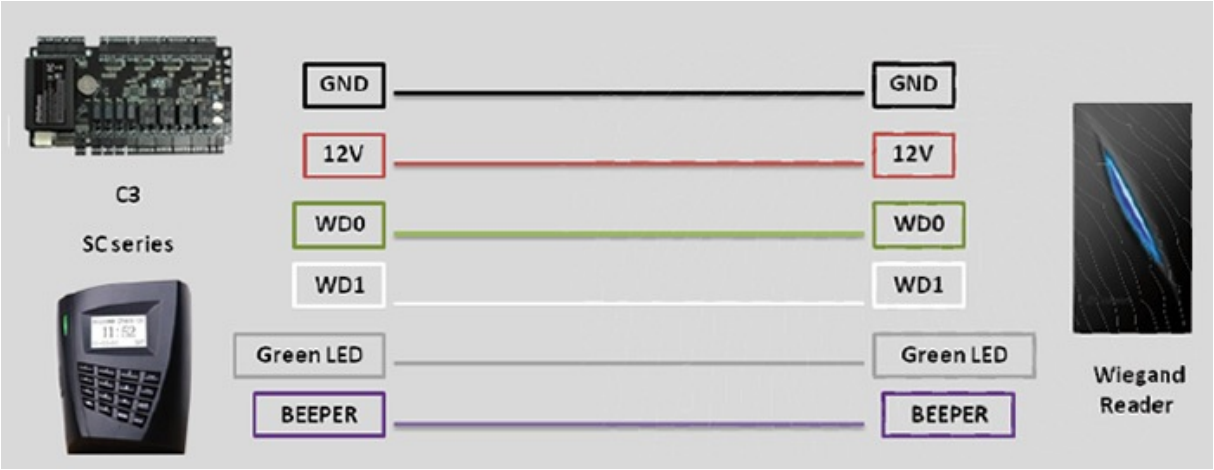
- 125KHz Proximity
- 26/34bit Wiegand
- Απόσταση ανάγνωσης 10 εκατοστά
- Εύκολο στην εγκατάσταση
- Προστασία από αντιστροφή πολικότητα
- Κομψή και στιβαρή σχεδίαση
- Αδιάβροχο πρότυπο IP65
- Led - Buzzer

2.3.2 Τεχνικές προδιαγραφές αναγνώστη

ZKSOFTWARE KR201E	
Απόσταση Ανάγνωσης	10 cm
Χρόνος ανάγνωσης κάρτας	300 ms
Τροφοδοσία	DC 6-14V / Max.70mA
Πρωτόκολλο κάρτας ανάγνωσης	26bit Wiegand
LED	2 χρώματα LED (Κόκκινο και πράσινο)
Beeper	Ναι
Θερμοκρασία Λειτουργίας	-20° to +65°C
Υγρασία Λειτουργίας	10% to 90%
Χρώμα	Μαύρο
Υλικό	ABS+PC
Διαστάσεις	84.5x44x16.8
Βάρος	55g
Δείκτης προστασίας	IP65

2.3.3 Επικοινωνία - Σύνδεση

Η συσκευή ανάγνωσης KR201E διαβάζει την εκτιθέμενη κάρτα και στέλνει τα δεδομένα στον πίνακα ελέγχου, ο οποίος και αποφασίζει αν θα δοθεί άδεια εισόδου στον κάτοχο της συγκεκριμένης κάρτας. Η επικοινωνία αυτή, μεταξύ πίνακα και αναγνώστη γίνεται με τη χρήση του πρότυπου Wiegand που είναι το πιο διαδεδομένο στον κόσμο των συστημάτων έλεγχου πρόσβασης.
Ο τρόπος σύνδεσης μεταξύ αναγνώστη και πίνακα έλεγχου παρουσιάζεται στο σχέδιο που ακολουθεί.



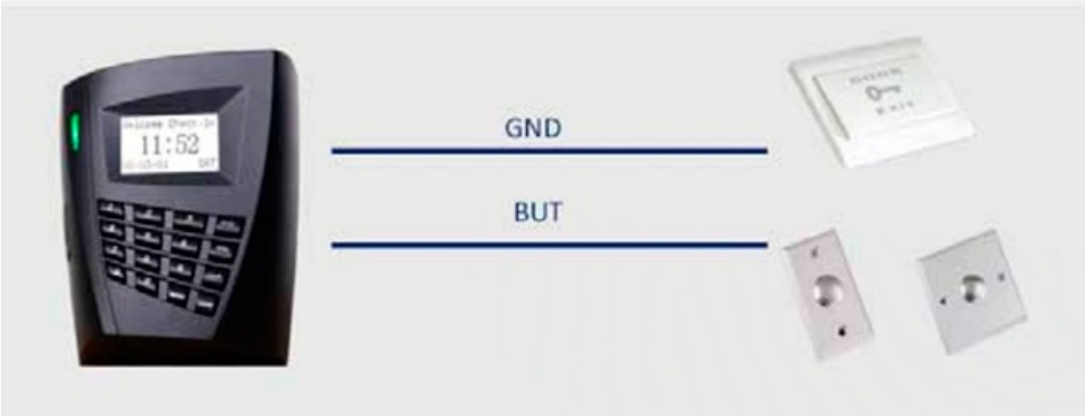
2.4 Μπουτόν έξοδου

Στο σύστημα ελέγχου πρόσβασης της εργασίας, πρέπει να υπάρχει η δυνατότητα να ανοίγει η πόρτα μέσα από την αίθουσα, για να εξέλθει κάποιος που βρίσκεται μέσα. Το RFID reader μαζί με την κεραία για τον εντοπισμό της RFID κάρτας βρίσκεται έξω από την πόρτα, άρα δεν υπάρχει η δυνατότητα σε κάποιον που βρίσκεται εντός της αίθουσας να περάσει την κάρτα του για να ανοίξει η πόρτα. Για τον λόγο αυτό προστέθηκαν δύο διακόπτες για την έξοδο από την αίθουσα.
Το πρώτο μπουτόν τοποθετήθηκε σε ύψος 1.40 m σε τοίχο διπλά από την έξοδο. Το δεύτερο, για διευκόλυνση, τοποθετήθηκε σε σημείο εύκολα προσβάσιμο ώστε ο διαχειριστής να μπορεί να ανοίξει την πόρτα χωρίς μετακίνηση από το γραφείο του.

2.4.1 Τεχνικές προδιαγραφές μπουτόν

Zksoftware Exit Button	
Διαστάσεις	86μ*86π (mm)
Υλικό κατασκευής	Πλαστικό
Βάρος	0,12 Kg
Εγγύηση Ποιότητας	2 χρόνια
Current Rating	10A 48VDC max

2.4.2 Επικοινωνία - Σύνδεση



Το μπουτόν έχει δυο ακροδέκτες, οι οποίοι συνδέονται στα I/O του πίνακα ελέγχου. Όταν πατηθεί κλείνει το κύκλωμα και περνάει ρεύμα στον δεύτερο ακροδέκτη.
Αυτό έχει σαν αποτέλεσμα ο πίνακας να εντοπίζει την ύπαρξη ρεύματος, άρα να δίνει εντολή για να ανοίξει η πόρτα. Όσο το μπουτόν δεν είναι πατημένο, το κύκλωμα παραμένει ανοιχτό, άρα δεν δίνεται εντολή για άνοιγμα της πόρτας. Τα δυο μπουτόν συνδέθηκαν παράλληλα.

2.5 Μαγνητική επαφή

Για τον έλεγχο της θέσης της πόρτας του εργαστηριού τοποθετήθηκε μια μαγνητική επαφή Αποτελείται από 2 μέρη: το σταθερό μέρος (επαφή) τοποθετημένο στο σταθερό σημείο της θύρας και από το κινητό μέρος (μαγνήτης) τοποθετημένο στο κινητό μέρος της θύρας.
Η μαγνητική επαφή διαθέτει δυο ακροδέκτες. Οι ακροδέκτες του συνδέονται στα I/O του πίνακα ελέγχου. Ο διακόπτης ελέγχεται από ένα εφαρμοσμένο μαγνητικό πεδίο, με τη βοήθεια μαγνητικής επαγωγής από το ένα άκρο του αισθητήρα στο άλλο.
Όσο τα δυο άκρα δεν βρίσκονται πολύ κοντά (2-3 cm) το ένα στο άλλο τότε το κύκλωμα παραμένει ανοιχτό και έτσι δεν περνάει ρεύμα. Στην περίπτωση που τα δύο άκρα βρίσκονται σε επαφή ή τουλάχιστον πολύ κοντά τότε το κύκλωμα κλείνει και με αυτό τον τρόπο περνάει ρεύμα, το οποίο εντοπίζει ο πίνακας ελέγχου και έτσι αντιλαμβάνεται ότι η πόρτα παραμένει κλειστή.

2.6 Ηλεκτρικό Κυπρί

Για την αυτοματοποίηση της πόρτας του εργαστηριού έπρεπε να γίνουν κάποιες μετατροπές. Έτσι αλλάχτηκε η συμβατική κλειδαριά με ηλεκτρικό κυπρί, το οποίο εγκαταστάθηκε στην κάσα.
Το ηλεκτρικό κυπρί αποτελείται από μία γλώσσα που συγκρατεί την πόρτα στη θέση της μέσω ενός ηλεκτρικού μηχανισμού. Μόλις δοθεί η ανάλογη εντολή από τον πινάκα έλεγχου και σταλεί ρεύμα στο μηχανισμό, τότε η γλώσσα αφήνεται ελεύθερη και η πόρτα ανοίγει.
Το ηλεκτρικό κυπρί που τοποθετήθηκε είναι fail secure. Αυτό σημαίνει ότι στην περίπτωση διακοπής ρεύματος η πόρτα παραμένει κλειστή. Η μηχανική κλειδαριά μπορεί να χρησιμοποιηθεί για την έξοδο από την ασφαλή πλευρά. Η τάση τροφοδοσίας είναι 12VDC, η οποία προσφέρει αθόρυβη λειτουργία. Το συγκεκριμένο κυπρί είναι επίσης 100% λειτουργιάς, έτσι ώστε να μπορεί να διαρρέεται από ηλεκτρικό ρεύμα για μεγάλα χρονικά διαστήματα χωρίς να προκαλείται πρόβλημα στο πηνίο του. Αυτό μας εξασφαλίζει ότι

μπορούμε να κρατήσουμε την πόρτα ανοιχτή για συγκεκριμένες ώρες που μπορεί να απαιτηθεί από τον διαχειριστή.

2.6.2 Τεχνικές προδιαγραφές

Ηλεκτρικό Κυπρί	
Διαστάσεις	240μ*25π (mm)
Τάση λειτουργίας	12VDC
Βάρος	0,41 Kg
Ένταση λειτουργίας	240mA

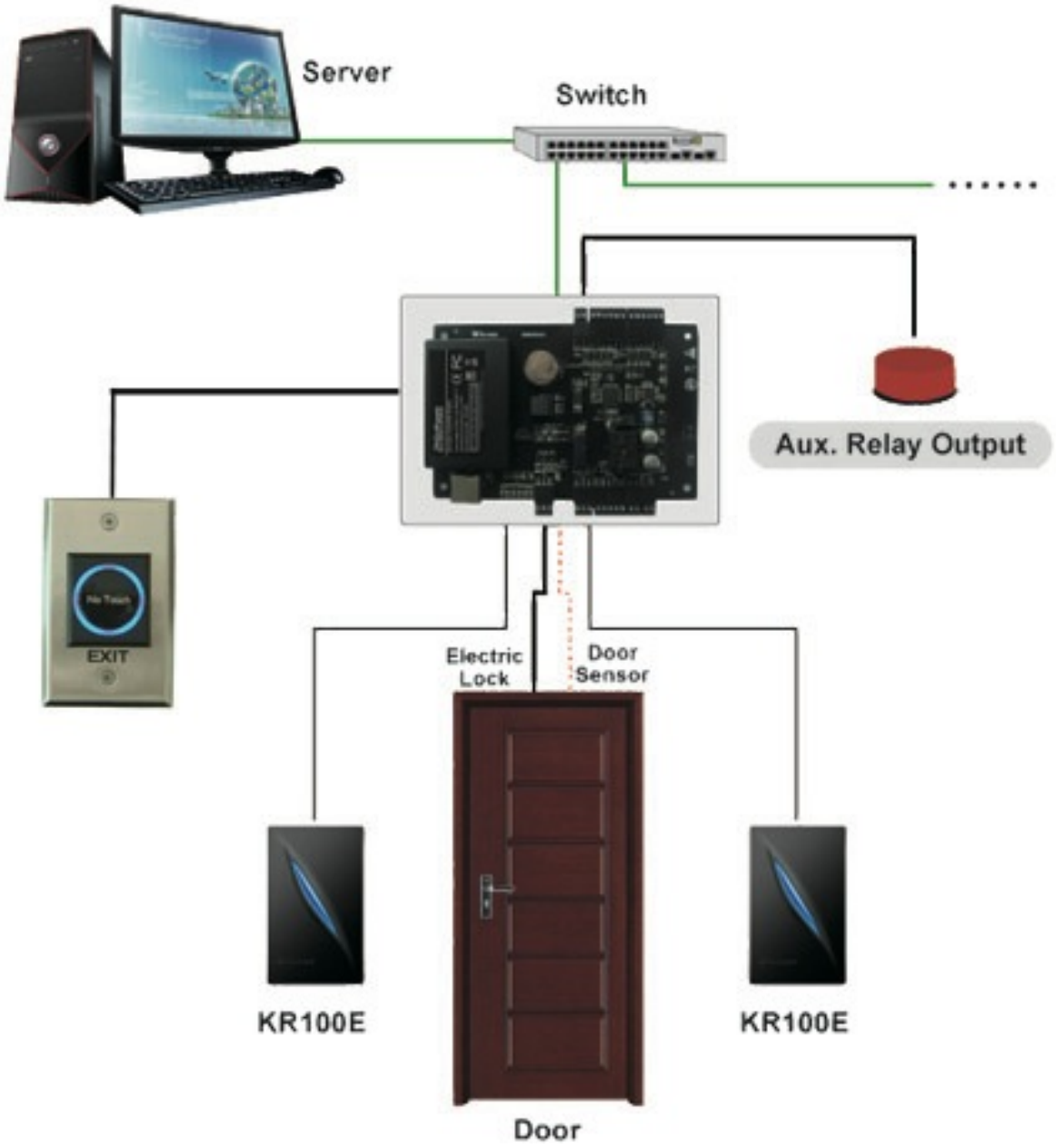
2.7 Σειρήνα Εσωτερικού Χώρου

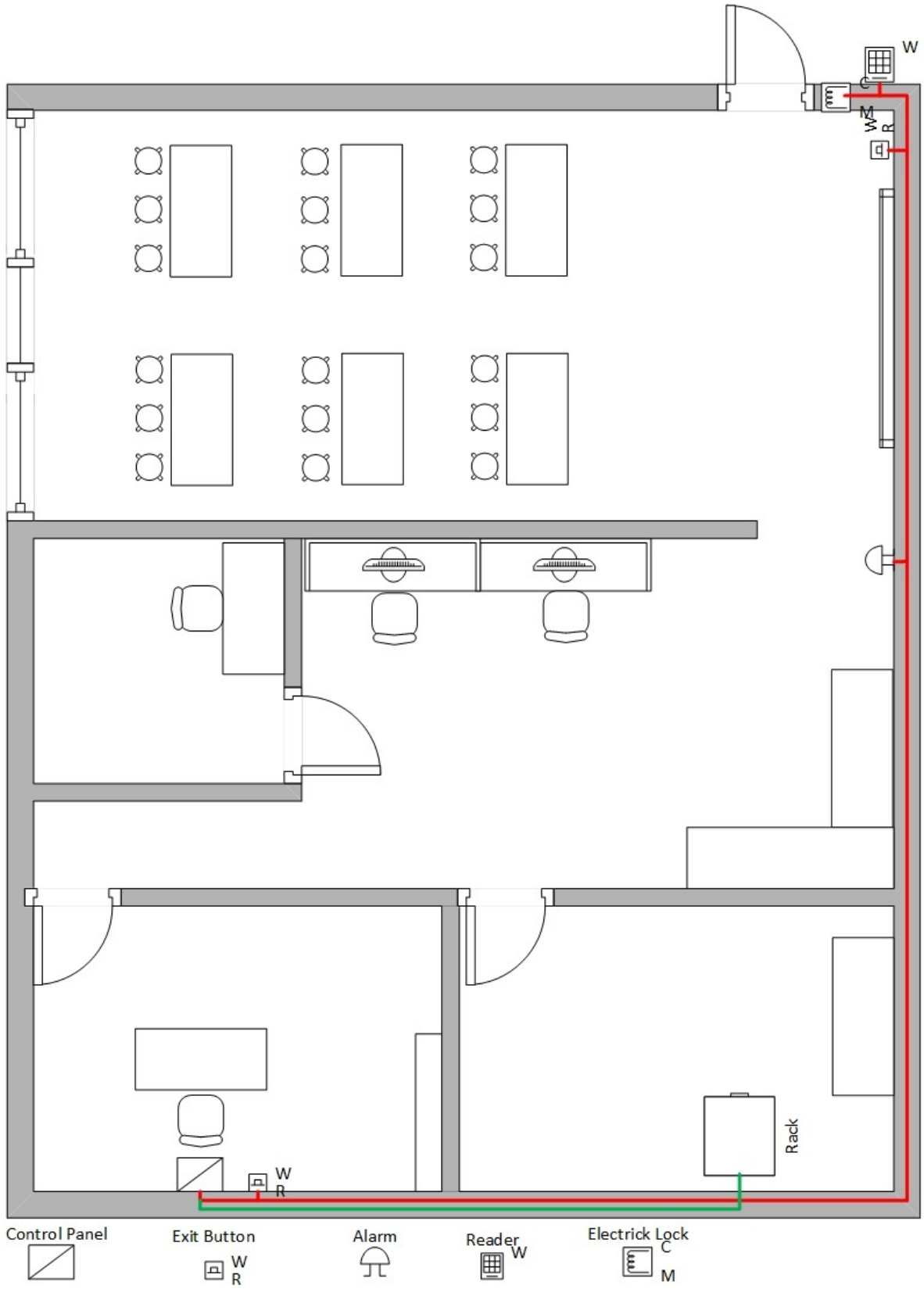
Στον εσωτερικό χώρο του εργαστηρίου τοποθετήθηκε μια σειρήνα. Η σειρήνα είναι ένα πολύ βασικό μέρος του συστήματος γιατί χάρη σε αυτή ενημερωνόμαστε ότι υπάρχει κάποιο πρόβλημα στον χώρο μας. Έτσι σε περίπτωση παραβίασης της πόρτας ο πίνακας έλεγχου θα ενεργοποιήσει την σειρήνα που θα μας προειδοποιήσει ηχητικά άλλα και οπτικά ότι κάποιος προσπαθεί να εισέλθει στον χώρο μας.
Με το πρόγραμμα του συστήματος μπορούμε να δημιουργήσουμε πάμπολλες συνθήκες για το πότε θέλουμε να χτυπάει η σειρήνα.
Η σειρήνα τοποθετήθηκε σε δυσπρόσιτο σημείο ώστε κανείς να μην έχει πρόσβαση σε αυτή παρά μόνο με σκάλα. Είναι μικρή σε μέγεθος και αρκετά διακριτική. Η τροφοδοσία της γίνεται με καλώδιο από τον πινάκα έλεγχου του συστήματος και συνδέεται στο βοηθητικό ρελέ του.
Η ένταση της είναι 108db και μαζί με τον φάρο που διαθέτει ενσωματωμένο, αναβοσβήνει σε κατάσταση συναγερμού ώστε να γίνεται πάντα αντιληπτό σε όλους γύρω ότι υπάρχει κάποιο πρόβλημα με το χώρο.

2.7.1 Τεχνικές προδιαγραφές

Σειρήνα	
Διαστάσεις (ΥxΠ)	122.0mm x 43.0mm
Τάση λειτουργίας	12VDC
Ακουστική ισχύς	108 dB / 1 m
Κατανάλωση ρεύματος	250 mA

2.8 Σχέδια συστήματος - κάτοψη

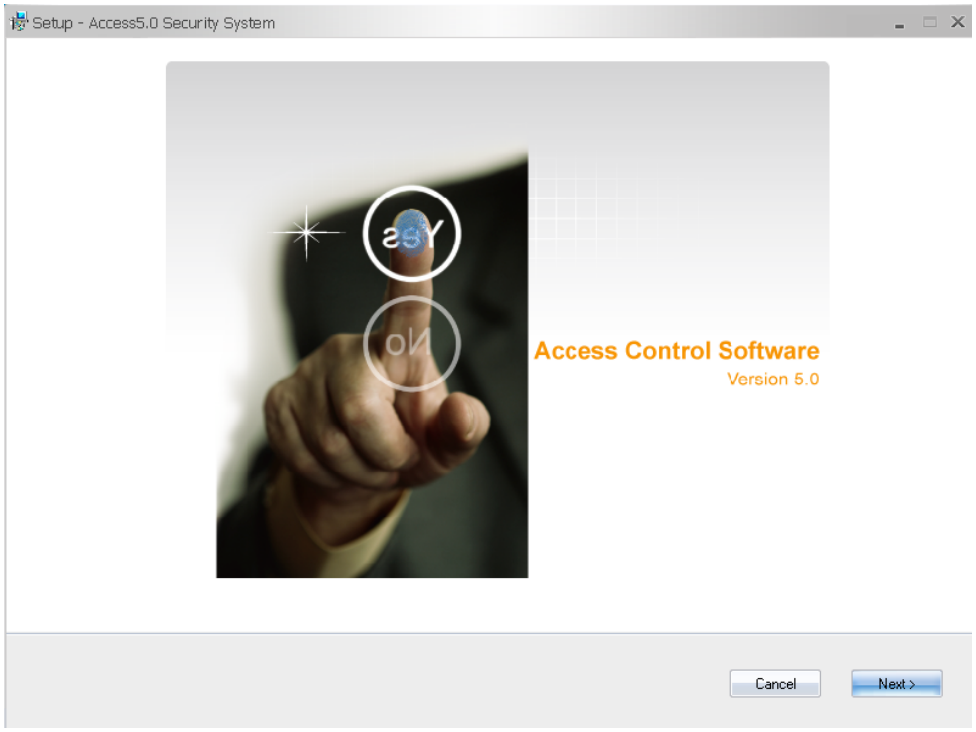


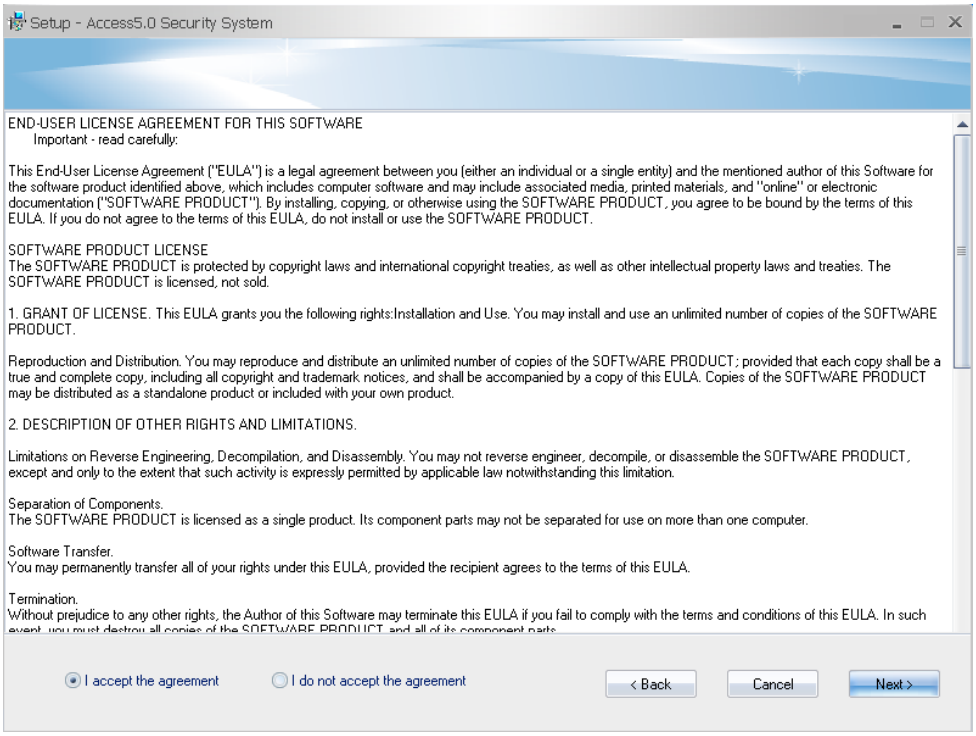

W
C
M
W
R
W
R
Rack
Control Panel
Exit Button
W
R
Alarm
Reader
W
Electrick Lock
C
M

ΚΕΦΑΛΑΙΟ 3.

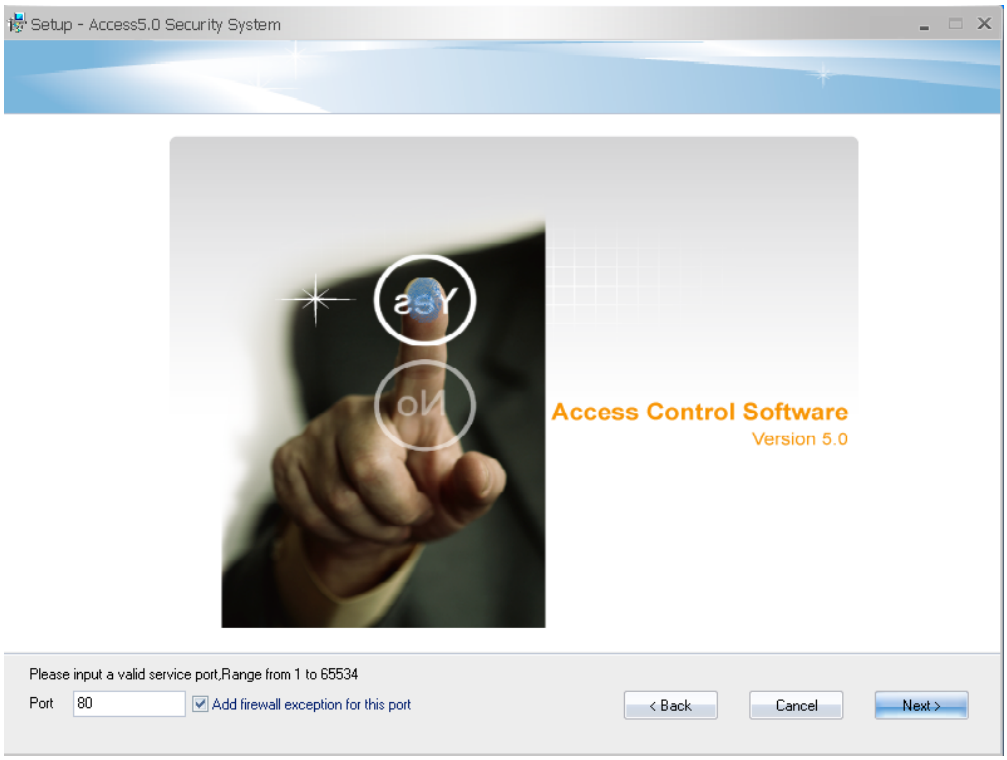
3.1 Εγκατάσταση λογισμικού

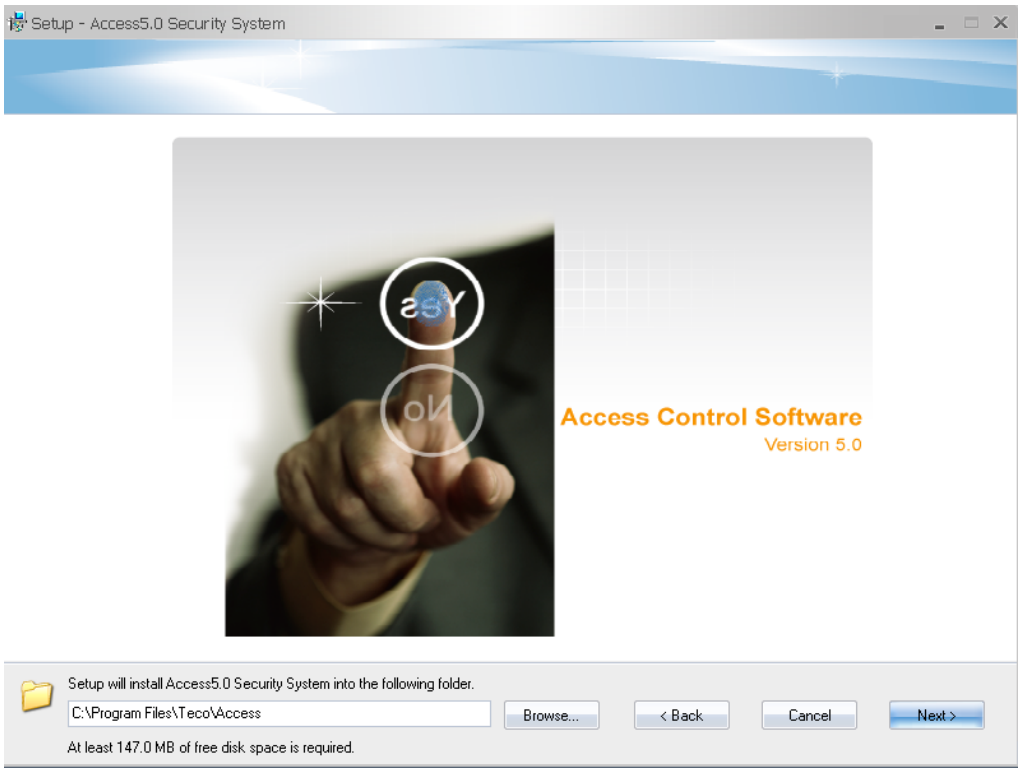
Εισάγουμε το CD του προγράμματος στο Drive του υπολογιστή μας.
Μετά από μερικά δευτερόλεπτα μας εμφανίζεται το παράθυρο που ακολουθεί. Πατάμε Next



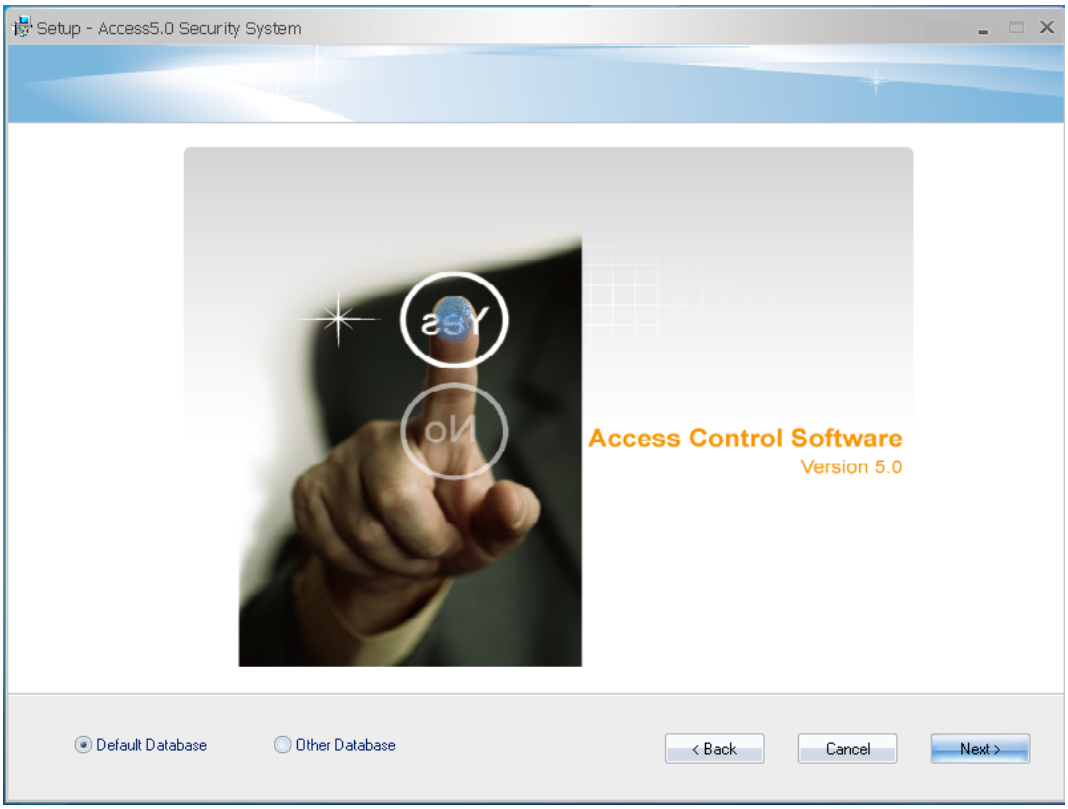


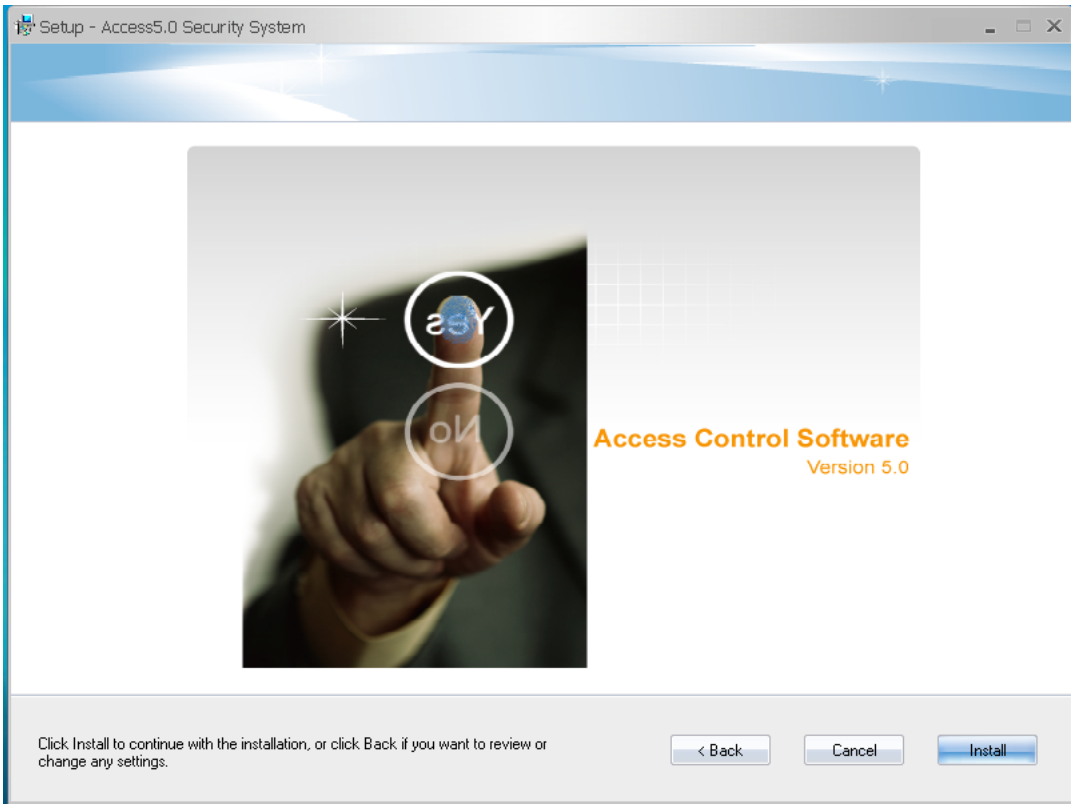
Στο επόμενο παράθυρο τικάρουμε στο Add Firewall exception to this port και πατάμε Next

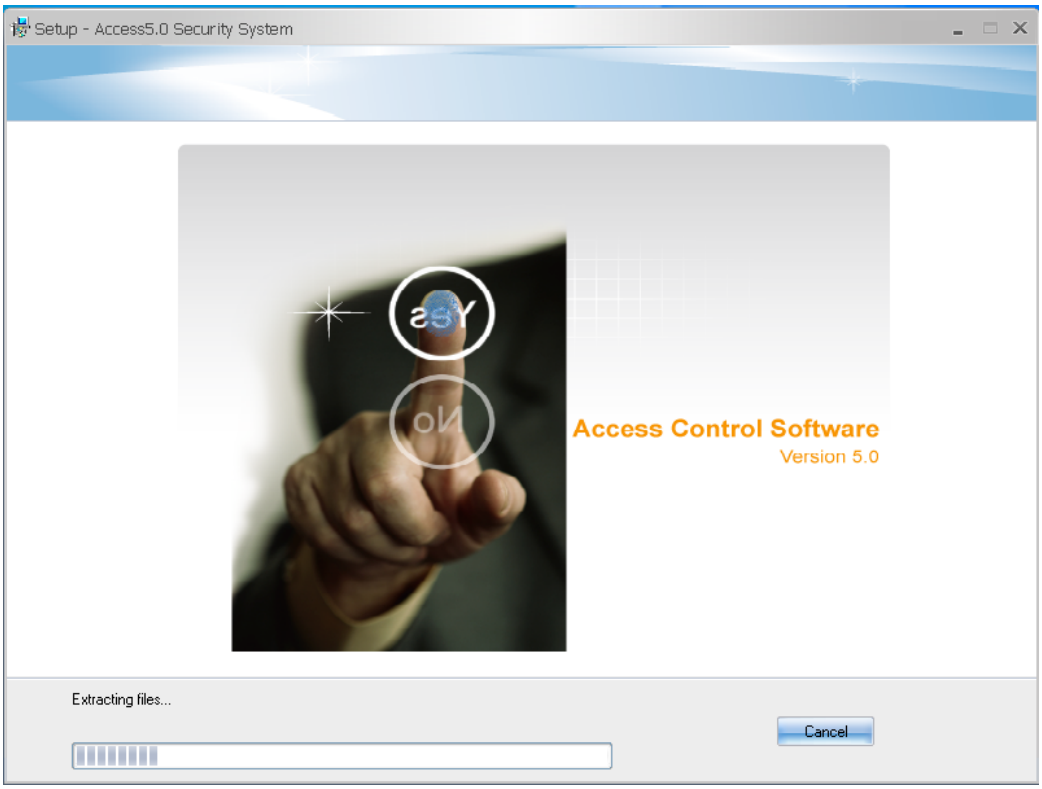


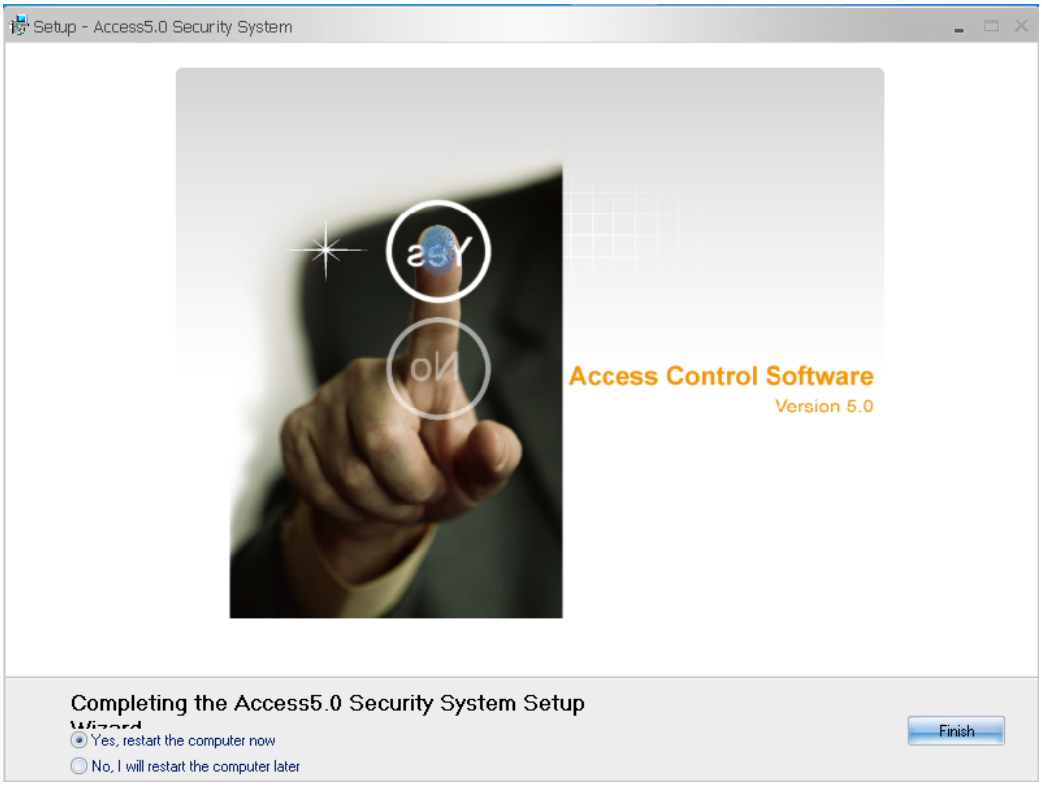


Επιλέγουμε το Default Database και πατάμε Next









Επιλέγουμε το Finish και κάνουμε επανεκκίνηση στον υπολογιστή μας.

3.2 Επισκόπηση των καρτελών προγράμματος

Διαχείριση προσωπικού: Η διαχείριση προσωπικού κυρίως περιέχει τα ακόλουθα τρία μέρη: [Κλάδος/Τμήμα], [Προσωπικό] και [Κάρτα εισόδου/εξόδου]. Μετά την κατηγοριοποίηση του προσωπικού βάσει των τμημάτων, μπορούν εύκολα, να χορηγηθούν «πακέτα» δικαιωμάτων στο προσωπικό ενός τμήματος.

Διαχείριση συσκευών: Χρησιμοποιείται κυρίως για την προσθήκη, εύρεση και διαγραφή του πίνακα ελέγχου πρόσβασης. Ο χρήστης έχει τη δυνατότητα να διαμοιράσει τη συσκευή, λογικά, με τη χρήση περιοχών. Με αυτόν τον τρόπο η συσκευή μπορεί να φιλτραριστεί ανά περιοχές κατά την παρακολούθηση. Επίσης ο χρήστης έχει τη δυνατότητα να επιτρέψει τους διαχειριστές τον έλεγχο της συσκευής σε κάποιες περιοχές μέσω [Ρυθμίσεις Συστήματος] – [Χρήστης].

Ρυθμίσεις θύρας: Κατά την προσθήκη, από τον χρήστη, του πίνακα ελέγχου πρόσβασης, το σύστημα θα εισάγει αυτόματα τις θύρες του αντίστοιχου αριθμού σύμφωνα με τις παραμέτρους του πίνακα ελέγχου. Ο χρήστης δε χρειάζεται λοιπόν, να κάνει την εισαγωγή χειροκίνητα, όμως πρέπει να ορίσει τις παραμέτρους για την κάθε θύρα ανάλογα με τις εκάστοτε ανάγκες.

Χρονική ζώνη πρόσβασης: Μετά την προσθήκη της χρονικής ζώνης, ο χρήστης μπορεί να την επιλέξει όταν ένα επίπεδο πρόσβασης προστίθεται μέσω [Επίπεδα Πρόσβασης]. Σε αυτή την περίπτωση, η χρονική ζώνη θα χρησιμοποιηθεί ως η ώρα ανοίγματος της θύρας για το προσωπικό, εντός του πεδίου της δυνατότητας ελέγχου. Κάθε ζώνη περιέχει τις ημέρες της εβδομάδας, από Κυριακή έως Σάββατο, τρεις κατηγορίες αργίας και αντίστοιχα η κάθε ημέρα, περιέχει τρία χρονικά διαστήματα.

Έλεγχος πρόσβασης αργιών: Αφού προστεθούν οι μέρες αργίας και καθοριστεί το είδος τους, ο χρήστης μπορεί να θέσει χρονικά διαστήματα για συγκεκριμένο τύπο αργίας σε μια χρονική ζώνη.

Επίπεδο πρόσβασης: Είναι ο πυρήνας του συστήματος και αντιπροσωπεύει τον συνδυασμό των θυρών με δικαιώματα πρόσβασης εντός των διαστημάτων ελέγχου πρόσβασης

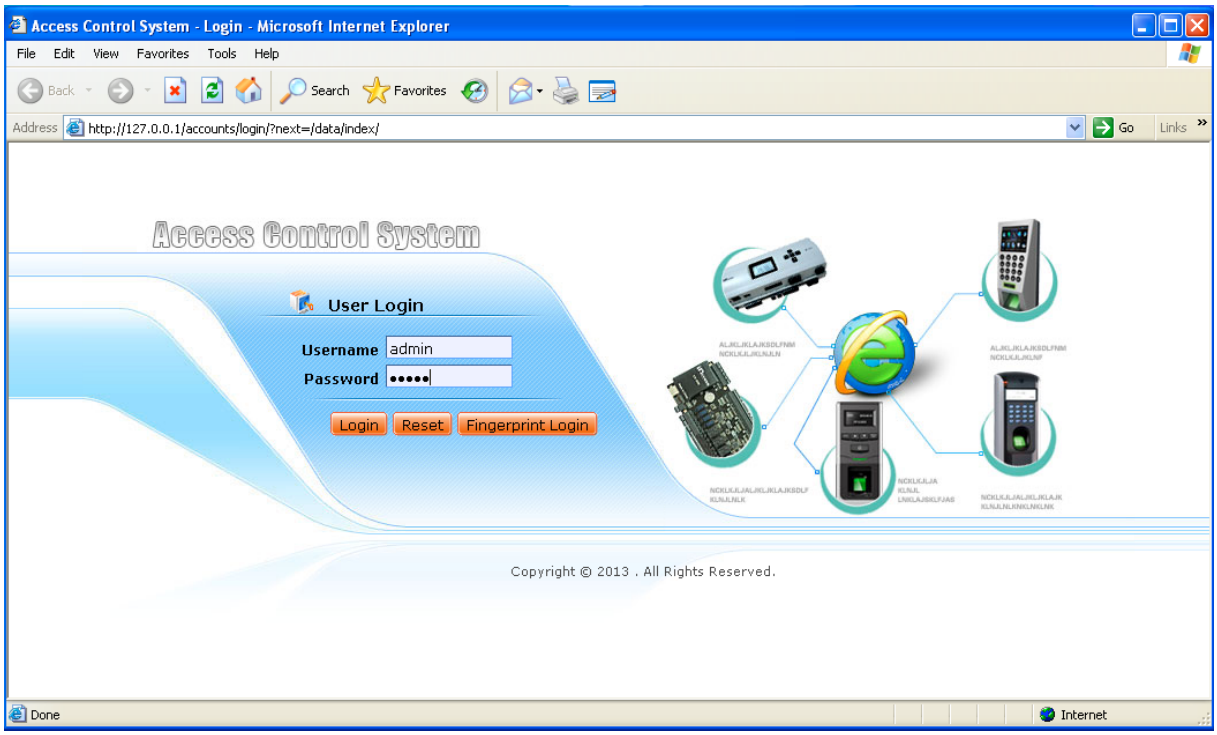
Σε αυτή την καρτέλα ορίζουμε ποιος έχει το προνόμιο πρόσβασης για το άνοιγμα της πόρτας καθώς και σε ποια ζώνη ώρας.

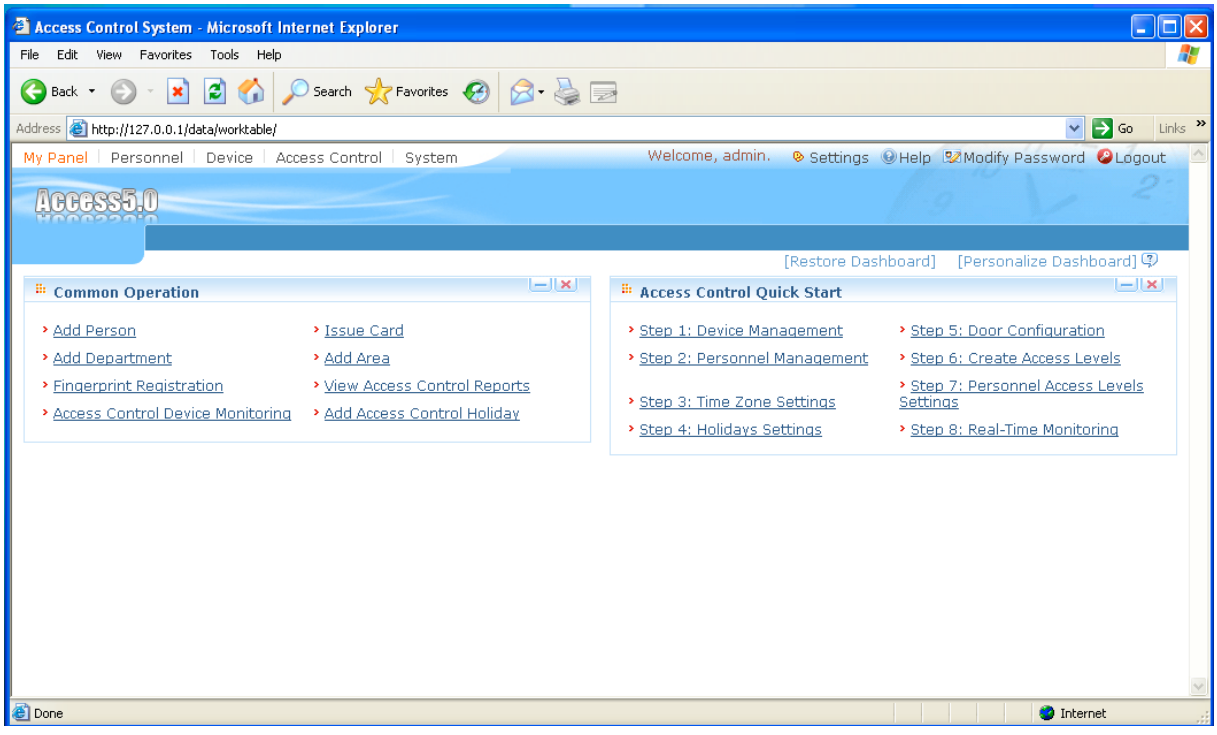
3.3 Σύνδεση στο σύστημα

Η προεπιλεγμένη πόρτα του συστήματος είναι η 80. Εάν για παράδειγμα η διεύθυνση IP (IP address) του διακομιστή (server) είναι η 192.168.1.10 , κάθε client με σύνδεση στο δίκτυο μπορεί να έχει πρόσβαση στο σύστημα απευθείας μέσω του http://192.168.1.10:80 (ή http://192.168.1.10) στο πρόγραμμα περιήγησης. Εάν αυτό το URL δεν είναι διαθέσιμο στον client, παρακαλώ βεβαιωθείτε ότι το port 80 δεν είναι απενεργοποιημένο από το firewall του server. Εάν είναι απενεργοποιημένο, παρακαλώ προσθέστε το port 80 ως εξαίρεση στο firewall (προτείνεται), ή κλείστε το firewall (δεν προτείνεται).

Εισάγετε το όνομα χρήστη και τον κωδικό πρόσβασης (το αρχικό όνομα χρήστη και ο κωδικός πρόσβασης είναι και τα δύο «admin»), για να εισέλθετε στο σύστημα. Αφού συνδεθείτε με τον προεπιλεγμένο λογαριασμό χρήστη, προτείνεται, να αλλάξετε τον αρχικό κωδικό πρόσβασης και να βεβαιωθείτε για την ασφάλειά του.

Αφού συνδεθείτε στο σύστημα, μπαίνετε στο [My Panel] interface.

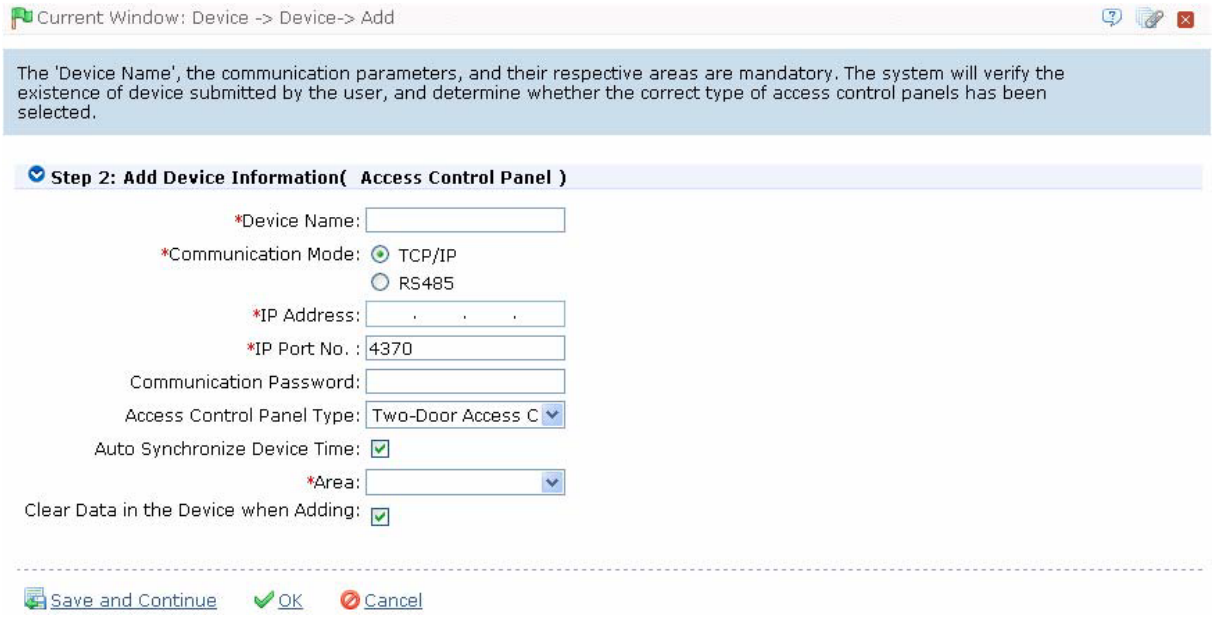




3.4 Διαχείριση συσκευών

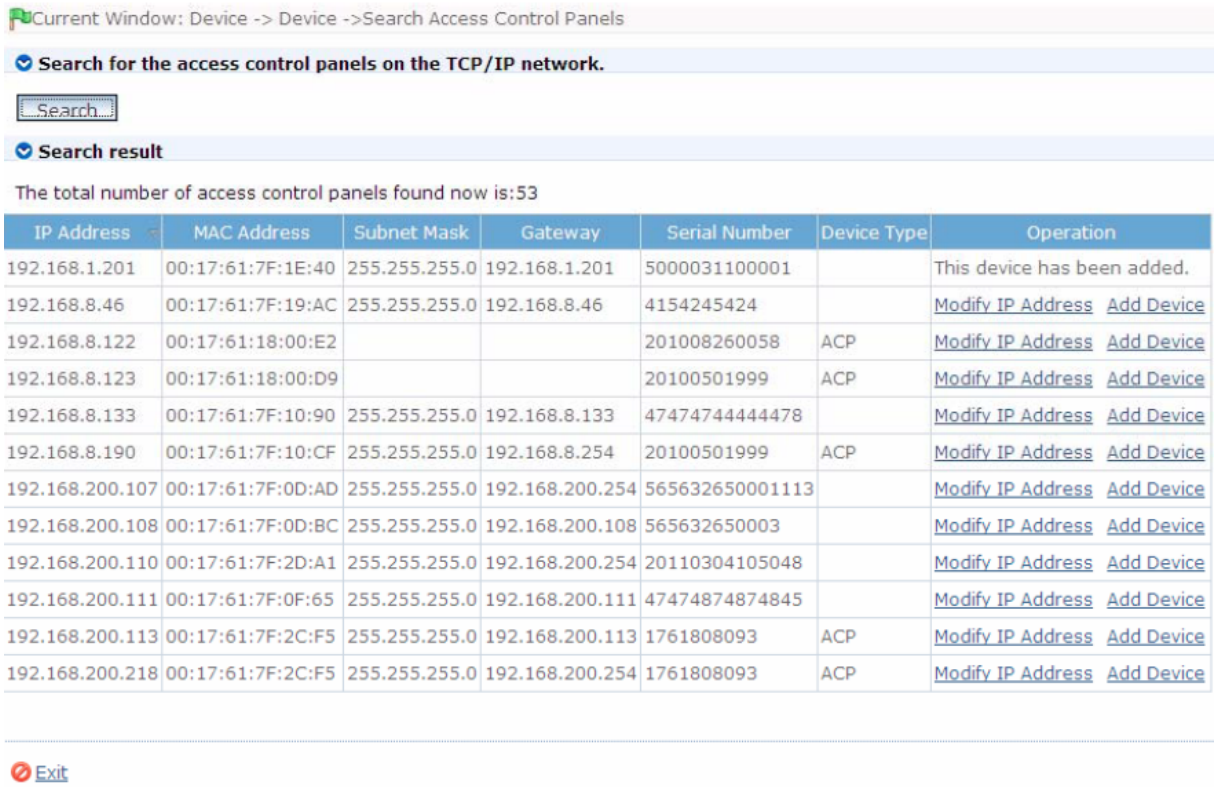
Πιέστε [Device] στην αριστερή πάνω γωνία του [My Panel] για να εισέλθετε στη μονάδα διαχείρισης συσκευών.

1. Πιέστε το μενού [Area Setting] και τροποποιείστε την περιοχή που έχει προστεθεί κατά την αρχικοποίηση του συστήματος. Π.χ συμπληρώστε όνομα, εταιρεία κ.ο.κ. Για να τροποποιήσετε την προεπιλεγμένη περιοχή, δεν απαιτείται η επιλογή της παραπάνω περιοχής. Ο χρήστης έχει τη δυνατότητα να προσθέσει και άλλες περιοχές ανάλογα με τις ανάγκες του και η σχέση μεταξύ των περιοχών ρυθμίζεται σύμφωνα με τη δομή της κάθε εταιρείας, επιχείρησης ή ιδρύματος.
2. Κάντε κλικ στο μενού [Device]. Δυο τύποι συσκευών υποστηρίζονται από το σύστημα, πίνακας ελέγχου πρόσβασης και δικτυακό recorder video.
(1) Για τον πίνακα ελέγχου πρόσβασης, υπάρχουν δύο τρόποι για την εισαγωγή συσκευών στο λογισμικό.
Πατήστε το κουμπί [Add] και επιλέξτε να προσθέσετε τον πίνακα ελέγχου πρόσβασης. Το ακόλουθο interface εμφανίζεται (TCP/IP mode):

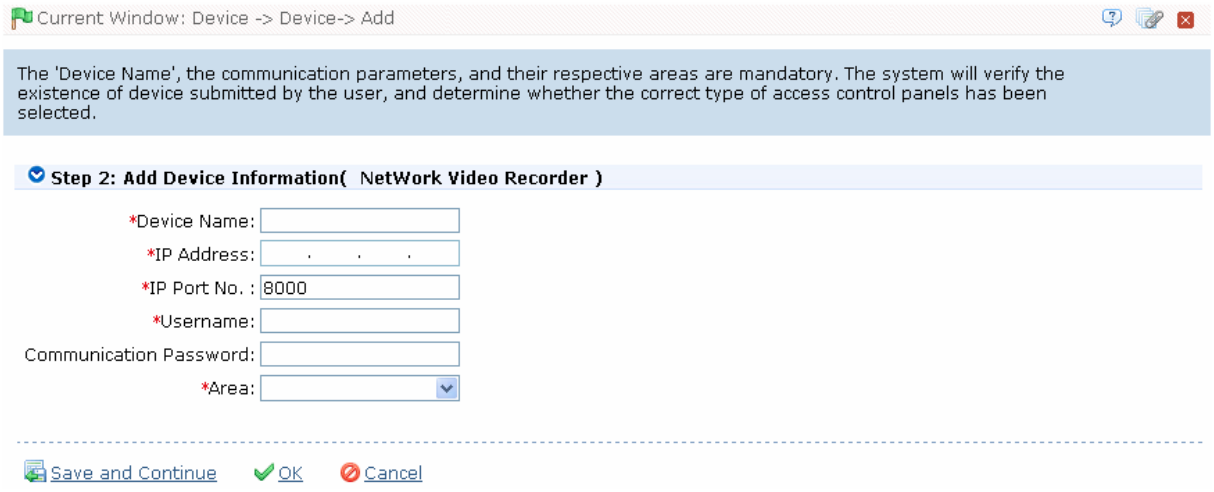


Συμπληρώστε το όνομα συσκευής, παραμέτρους επικοινωνίας (όπως IP address, IP port number ή διεύθυνση 485, serial port number, baud rate), επιλέξτε την κατάσταση επικοινωνίας (communication mode), τον τύπο του πίνακα ελέγχου πρόσβασης (access control panel) και την περιοχή στην οποία ανήκει. Το όνομα της συσκευής προτείνεται να είναι, όσο το δυνατόν, απλό.
Ο κωδικός πρόσβασης επικοινωνίας (communication password) θα εισάγεται για συσκευές των οποίων ο κωδικός έχει οριστεί. Ο κωδικός επικοινωνίας για όλες τις νέες συσκευές είναι κενός από προεπιλογή.
Αφού γίνει η εισαγωγή της συσκευής, για να αποφευχθεί η κακόβουλη πρόσβαση στο σύστημα, ο χρήστης μπορεί να χρησιμοποιήσει [Modify Communication Password] μέσω [Access Control] – [Door Setting] – [Door Management] ώστε να ορίσει τον κωδικό πρόσβασης επικοινωνίας.
Αλλαγή σε two-door και two-way mode: Επιλέγεται μόνο σε περιπτώσεις στις οποίες four-door και one-way access control panel χρησιμοποιούνται ως two-door και two-way access control panel. Ο χρήστης δε χρειάζεται να επιλέξει αυτή τη ρύθμιση σε άλλες περιπτώσεις.

Προτείνεται ο χρήστης να επιλέξει τη ρύθμιση auto synchronize device time ώστε να διαβεβαιώσει ότι ο χρόνος στον πίνακα ελέγχου πρόσβασης είναι ίδιος με αυτόν στον server.
Clear Data in the Device when Adding. Ορίζεται ως προεπιλογή, και όπως αναφέρει και ο τίτλος, μετά την εισαγωγή της συσκευής στο σύστημα, θα διαγράψει τα δεδομένα που υπάρχουν αποθηκευμένα στη συσκευή. Όλα τα access levels θα διαγραφούν, όμως τα αρχεία καταγραφής συμβάντων θα παραμείνουν. Αν προσθέσετε συσκευή μόνο για επίδειξη ή δοκιμή του συστήματος, μην το τσεκάρετε.
Κάντε κλικ στο κουμπί [OK]. Εάν εμφανιστεί ένα παράθυρο διαλόγου, κάντε κλικ στο [OK], και το σύστημα θα προσπαθήσει να συνδέσει τη συσκευή. Εάν το σύστημα απαιτεί επιτυχή σύνδεση, κάντε κλικ στο [OK], και το σύστημα θα ξεκινήσει την εισαγωγή της συσκευής.
Η καινούρια συσκευή που προσθέσατε, μπορεί να βρεθεί στη λίστα των συσκευών.
Ένας άλλος τρόπος για να εισάγουμε συσκευή, είναι μέσω [Search Access Control Panel]. Το αποτέλεσμα μετά την εύρεση είναι παρόμοιο με την παρακάτω εικόνα:



Κάντε κλικ στο [Add Device] στη στήλη [Operation] για να εμφανιστεί ένα παράθυρο διαλόγου ώστε να τροποποιήσετε το όνομα της συσκευής. Η IP address είναι προεπιλεγμένη για το σύστημα, ο χρήστης παρόλα αυτά έχει τη δυνατότητα να την αλλάξει με ένα συνοπτικό όνομα ανάλογα με τις ανάγκες του. Αφού πατήσετε [OK], η συσκευή προστίθεται επιτυχώς.
(2) Στο new device adding interface, επιλέξτε να προσθέσετε ένα network video recorder και κάντε κλικ στο [Next]. Το ακόλουθο interface εμφανίζεται:



Ο χρήστης καλείται να συμπληρώσει τις ακόλουθες πληροφορίες, όπως IP address, IP port, User name κτλ. Μετά από αυτό κάντε κλικ στο [OK] για να τερματίσετε τη διαδικασία εισαγωγής νέας συσκευής.

Το σύστημα υποστηρίζει Hikvision network video recorder. Για περισσότερες πληροφορίες παρακαλώ διαβάστε το software user manual.

3.5 Διαχείριση προσωπικού

Εισέλθετε στις ρυθμίσεις [Personnel] από το μενού στην πάνω αριστερή γωνία.

Κάντε κλικ στο [Department] για να μπείτε στο interface του department management και αλλάξτε το προεπιλεγμένο όνομα department σε πραγματικό όνομα (όπως το όνομα της εταιρείας ή της επιχείρησης ή του ιδρύματος). Στη συνέχεια, ο χρήστης μπορεί να δημιουργήσει μια δομή καταλόγου των departments με σαφή ιεραρχική σειρά, σύμφωνα με τις πραγματικές ανάγκες.

Ο χρήστης μπορεί να χρησιμοποιήσει την κατηγοριοποίηση του προσωπικού από τα departments σύμφωνα με τις πραγματικές ανάγκες, για παράδειγμα, μπορεί να ταξινομήσει το προσωπικό σε τάξεις, θαλάμους ή σε τμήματα της εταιρείας.

Κάντε κλικ στο [Personnel] για να μπείτε στη διαχείριση του προσωπικού. Κλικ στο [Add] για να δείτε το ακόλουθο interface:

Το παρακάτω μέρος είναι οι βασικές πληροφορίες του προσωπικού. Οι αριθμοί προσωπικού μπορεί να είναι είτε αριθμοί εργατικών καρτών, είτε φοιτητικών καρτών, όμως οι αριθμοί δεν πρέπει να επαναλαμβάνονται. Η συμπλήρωση του department είναι υποχρεωτική. Άλλες πληροφορίες μπορούν να συμπληρωθούν προαιρετικά από τον χρήστη ανάλογα με τις ανάγκες.

Εάν ο χρήστης χρειαστεί να εκδώσει μια κάρτα για νέο προσωπικό, αυτό μπορεί να εισάγει τον αριθμό της κάρτας απευθείας στο πλαίσιο κειμένου πίσω από τον αριθμό της κάρτας (ή να περάσει την κάρτα από card reader).

Το κάτω μέρος περιλαμβάνει κυρίως τη ρύθμιση των προνομίων πρόσβασης. Εάν απαιτείται, το υπάρχον επίπεδο πρόσβασης να εντοπιστεί για τον χρήστη, επιλέξτε το απευθείας από

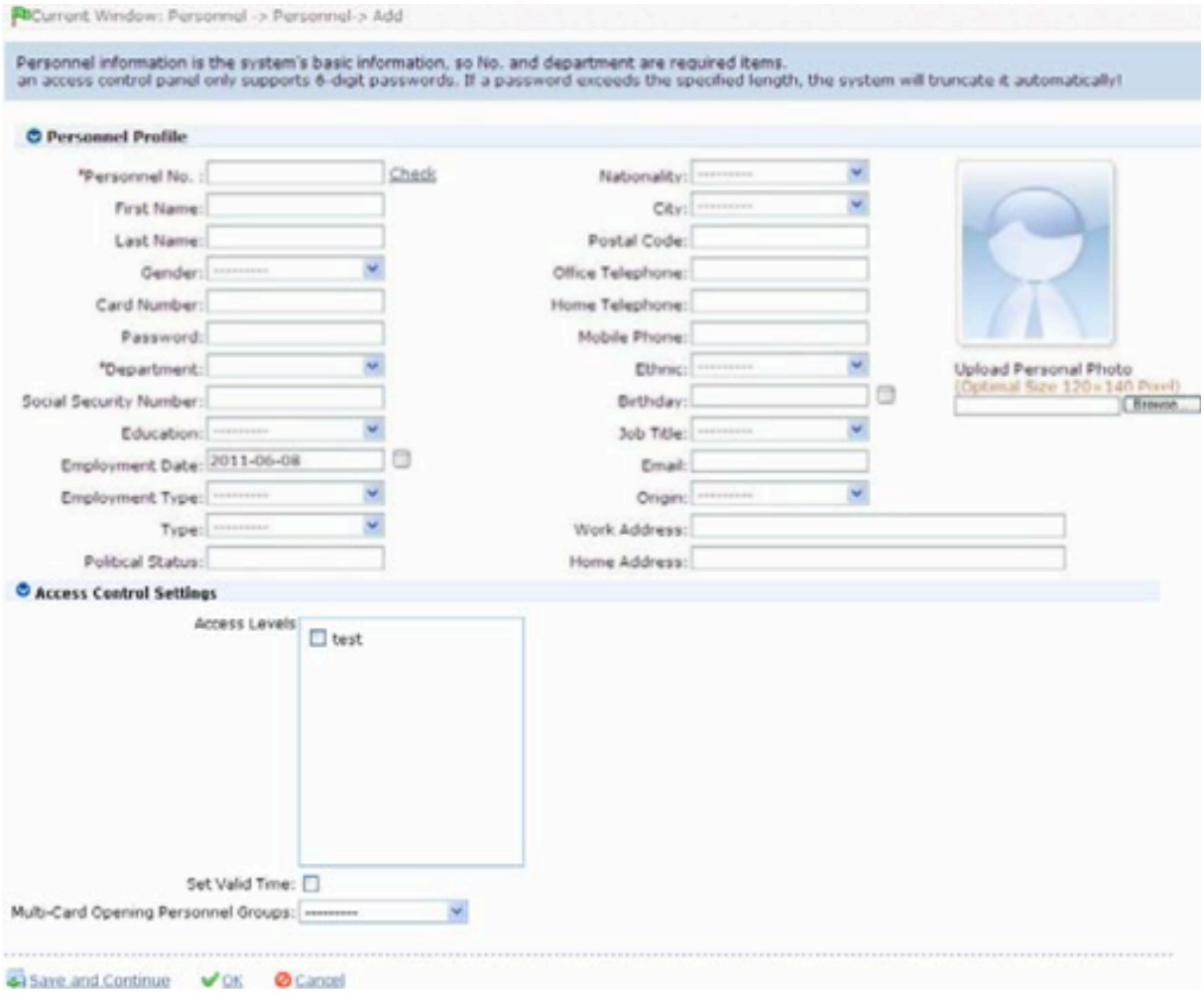
αυτή την τοποθεσία (Εάν δεν έχει προστεθεί επίπεδο πρόσβασης στο σύστημα μπορείτε να δείτε την υπόδειξη με τα κόκκινα γράμματα στην παραπάνω εικόνα). Η ρύθμιση του ενεργού χρόνου είναι εφαρμόσιμη για τους επισκέπτες ή άλλες περιστάσεις στις οποίες το προσωπικό έχει δικαιώματα ανοίγματος της θύρας. Η χρήση multi-card για ομάδα προσωπικού προβλέπεται για τη λειτουργία multi-card door opening. Εάν αυτή η λειτουργία δεν χρησιμοποιείται, αφήστε την κενή.

Σημείωση: Υπάρχουν δύο λειτουργίες στο σύστημα, για ρύθμιση της πρόσβασης του προσωπικού.

Η πρώτη γίνεται ως εξής: προσθέστε προσωπικό (χωρίς ρύθμιση επιπέδου πρόσβασης) μέσω [Personnel] – [Personnel], προσθέστε επίπεδο πρόσβασης μέσω [Access Control] – [Access Levels] και τελικά ρυθμίστε τα επίπεδα πρόσβασης προσωπικού μέσω [Access Control] – [Personnel Access Levels].

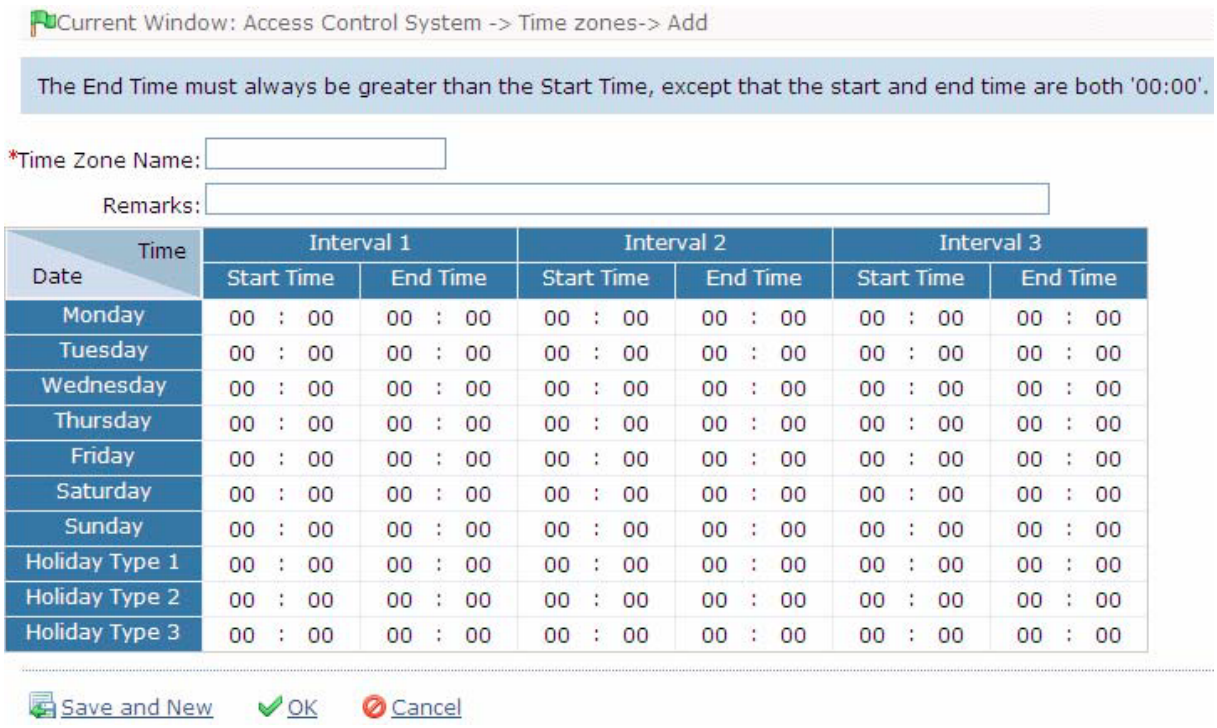
Η δεύτερη γίνεται με την προσθήκη επιπέδου πρόσβασης από [Access Control] – [Access Levels] και επιλογή επιπέδου πρόσβασης απευθείας όταν προστίθεται ή επεξεργάζεστε το προσωπικό μέσω [Personnel] – [Personnel].

Η επίδειξη παρακάτω αναφέρεται στην πρώτη λειτουργία.



3.6 Χρονική ζώνη πρόσβασης

Η χρονική ζώνη [24-hour Accessible] έχει προστεθεί ως προεπιλογή στο σύστημα. Κάθε χρονική ζώνη, περιλαμβάνει ημέρες από Κυριακή έως Σάββατο και τρία είδη αργίας καθένα από τα οποία περιέχει τρία χρονικά διαστήματα.
Παράδειγμα 1: [Effective Time Zone] η ενεργός ώρα της θύρας, από Δευτέρα έως Παρασκευή μέσα σε αυτή την ζώνη ώρας είναι 08:00-12:00, 13:00-18:00, 19:00-21:00, αυτό για τις αργίες [Holiday Type 1] είναι 08:00-22:00 και για τον δεύτερο τύπο αργίας [Holiday Type 2] είναι 12:00-23:00, ενώ τρίτο είδος δεν υπάρχει [Holiday Type 3].



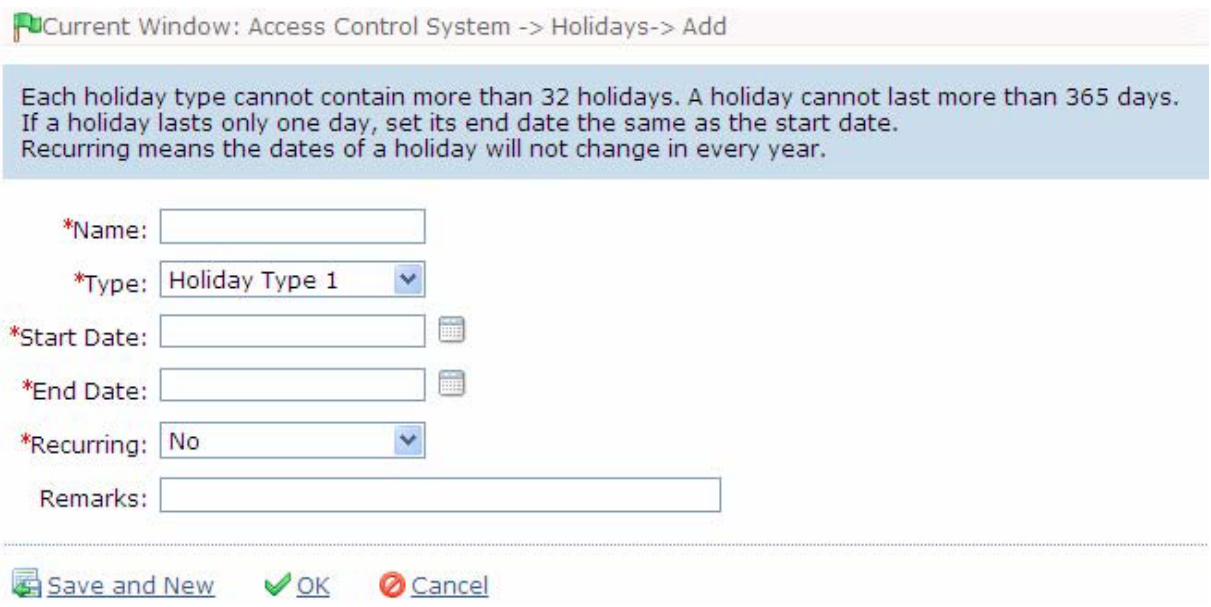
Τα ακόλουθα σημεία πρέπει να ληφθούν υπ' όψιν:

1. Τρία χρονικά διαστήματα είναι διαθέσιμα για κάθε ημέρα. Εάν ο χρήστης χρησιμοποιεί μόνο το ένα ή τα δύο από αυτά, μπορεί να κρατήσει την προεπιλεγμένη τιμή για τα υπόλοιπα ένα ή δυο χρονικά διαστήματα (00:00-00:00).
2. Εάν το [Holiday Type 3] δεν έχει ακόμα οριστεί, κρατείστε την προεπιλεγμένη τιμή (00:00-00:00) για τα τρία χρονικά διαστήματα μέσα στην χρονική ζώνη.
3. Δεν θα πρέπει να υπάρχει καμία επικάλυψη του χρόνου μεταξύ των τριών διαστημάτων.

Αφού οριστεί η χρονική ζώνη, ορίστε τη ως την ενεργό χρονική ζώνη της θύρας.

3.7 Έλεγχος πρόσβασης αργίας

Εάν δεν απαιτείται έλεγχος πρόσβασης κατά τις μέρες αργίας, παρακαλώ παραλείψατε αυτό το μέρος και κρατείστε την προεπιλεγμένη τιμή (00:00-00:00) για τα αντίστοιχα χρονικά διαστήματα στη χρονική ζώνη πρόσβασης.
Για να προσθέσετε έλεγχο πρόσβασης κατά τις ημέρες αργίας, απαιτείται να επιλέξετε έναν από τους τύπους αργίας από τους τρεις τύπους που είναι διαθέσιμοι στο σύστημα. Εκτός από την κατηγοριοποίηση των αργιών, η λειτουργία του τύπων αργίας χρησιμοποιείται κυρίως για την ημέρα που έχει οριστεί ως αργία, όταν το σύστημα επιλέξει κατά προτεραιότητα το διάστημα της αργίας από τις επιλεγμένες χρονικές ζώνες, ως τον ενεργό χρόνο (συμπεριλαμβανομένων ενεργών γεγονότων θύρας και ενεργού χρόνου ανοίγματος της θύρας για το προσωπικό), δηλαδή, όταν το σύστημα επιλέξει χρονικά διαστήματα από τις χρονικές ζώνες, το επίπεδο προτεραιότητας των αργιών τύπων 1, 2 και 3 είναι υψηλότερο από το διάστημα Κυριακής-Σαββάτου.
Κάντε κλικ στο [Add] για να δείτε το ακόλουθο interface:



Η επίσημη αργία της Διεθνούς Ημέρα Εργασίας, προστίθεται εδώ. Μετά τον συνδυασμό του με το [Time Zones Demo] από το παραπάνω παράδειγμα, όταν ο χρόνος είναι μεταξύ της ημερομηνίας έναρξης και λήξης, λόγω του ότι ο τύπος αργίας [Labor Day] είναι [Holiday Type 1], όταν ο [Time Zones Demo] χρησιμοποιείται για την θύρα ως ενεργή χρονική ζώνη και είναι ενεργή από 8:00 έως 22:00, τότε η θύρα είναι μη προσβάσιμη για άλλη ώρα.

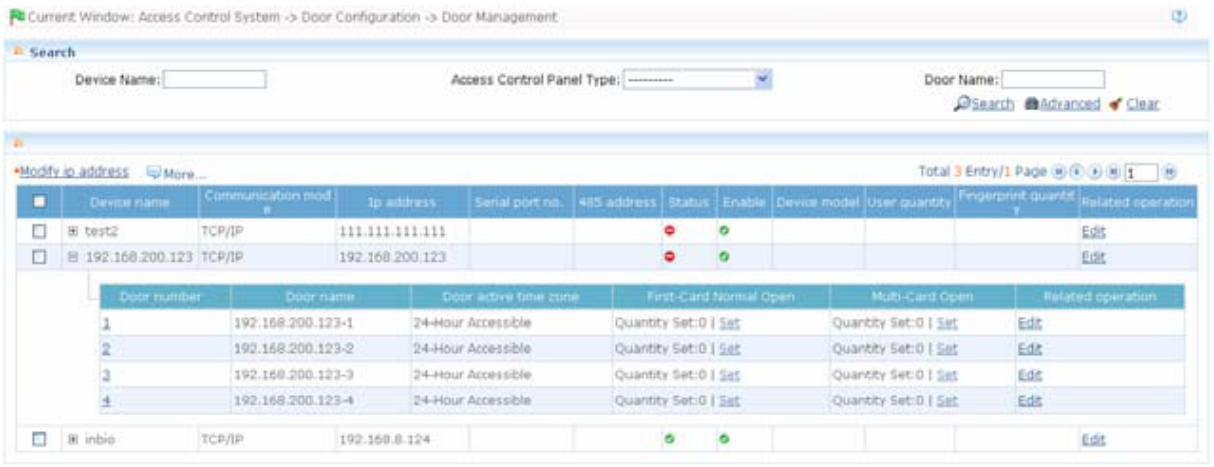
«Πρόσβαση αργιών», ως μια ευρύτερη έννοια περιέχει άλλες αργίες που απαιτούν ειδική μεταχείριση, εκτός από νόμιμες αργίες, όπως το γεγονός ότι η θύρα πρέπει να είναι ανοικτή, όπως τις υπόλοιπες ημέρες, τα Σαββατοκύριακα. Ο χρήστης πρέπει να ορίσει αυτές τις ειδικές ημερομηνίες, όπως τις αργίες, ως συγκεκριμένο τύπο αργίας, στο σύστημα.

Σημειώσεις:

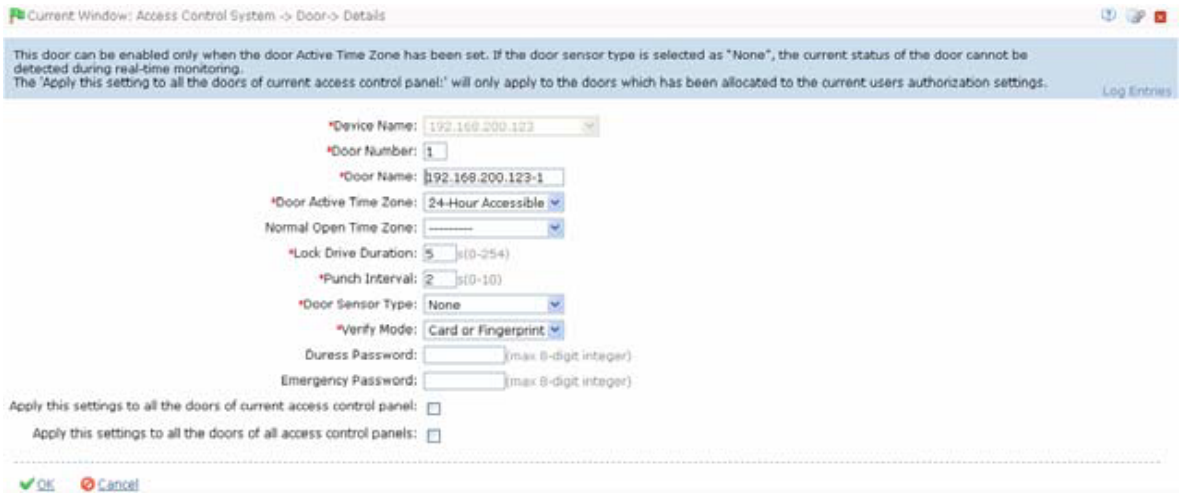
- Χρόνος έναρξης και λήξης για τη ρύθμιση της αργίας δε μπορεί να ξεπερνά σε διάρκεια τον ένα χρόνο.
- Ο αριθμός αργιών που περιέχεται σε κάθε τύπο δε μπορεί να ξεπερνά τις 32.

3.8 Ρυθμίσεις θύρας

Μετά την προσθήκη της συσκευής στο [Device], εισέλθετε στο [Access Control]. Η νέα προσθήκη πληροφοριών για τον πίνακα ελέγχου και η αντίστοιχη λίστα των θυρών βρίσκεται στο [Door Setting] – [Door Management]:



Κάντε κλικ στο [Edit] για τις σχετικές λειτουργίες και παραμέτρους της θύρας για τον πίνακα ελέγχου, όπως φαίνεται παρακάτω:



Door Name, είναι ο συνδυασμός του ονόματος της συσκευής και ο προεπιλεγμένος αριθμός της θύρας. Υπάρχει η δυνατότητα τροποποίησης τους από τον χρήστη.
Door Sensor Type, μπορεί να επιλεχθεί ανάλογα με τις πραγματικές ανάγκες του χρήστη. Οι άλλες παράμετροι επίσης μπορούν να συμπληρωθούν ανάλογα με τις ανάγκες παρόλα αυτά, οι προεπιλεγμένες τιμές μπορούν να παραμείνουν εφόσον δεν υπάρχουν συγκεκριμένες απαιτήσεις.
Τα δύο check boxes στο κάτω μέρος χρησιμοποιούνται από τον χρήστη ώστε να εφαρμόσει τις ρυθμίσεις αυτές και σε άλλες θύρες με σκοπό να αποφύγει την επαναλαμβανόμενη διαδικασία για την ίδια ρύθμιση.

Σημειώσεις
Αν ο χρήστης πρέπει να χρησιμοποιήσει τις λειτουργίες του κανονικού ανοίγματος με την πρώτη κάρτα, άνοιγμα με πολλές κάρτες, anti-pass back, interlock και linkage, μπορούν να εισχωρηθούν από τα σχετικά κουμπιά στη σελίδα [Access] – [Door Setting]. Παρακαλώ προσφύγετε στο εγχειρίδιο χρήστη για παραπάνω λεπτομέρειες.

3.9 Ρυθμίσεις επιπέδων πρόσβασης

Πριν από την κατανομή των προνομίων πρόσβασης στο προσωπικό, προσθέστε τα επίπεδα πρόσβασης που διατίθενται για τη χρήση συγκεκριμένων ομάδων, τα οποία αποτελούνται κυρίως από το συνδυασμό της χρονικής ζώνης πρόσβασης και της πρόσβασης θύρας. Συγκεκριμένα, ποια χρονική ζώνη, ανοίγει ποια θύρα.
Μπείτε στο [Access Control] – [Access Levels] και κάντε κλικ στο [Add] για να δείτε το interface επεξεργασίας.
Ο χρήστης χρειάζεται μόνο να επιλέξει χρονική ζώνη και ποια θύρα θα ελέγχει.

Σημειώσεις
Η χρονική ζώνη πρόσβασης η οποία έχει επιλεχθεί εδώ είναι προκαθορισμένη στο [Access Control] – [Access Time Zone]. Αυτό σημαίνει ότι η χρονική ζώνη μπορεί να είναι ίδια με την ενεργή χρονική ζώνη των θυρών.

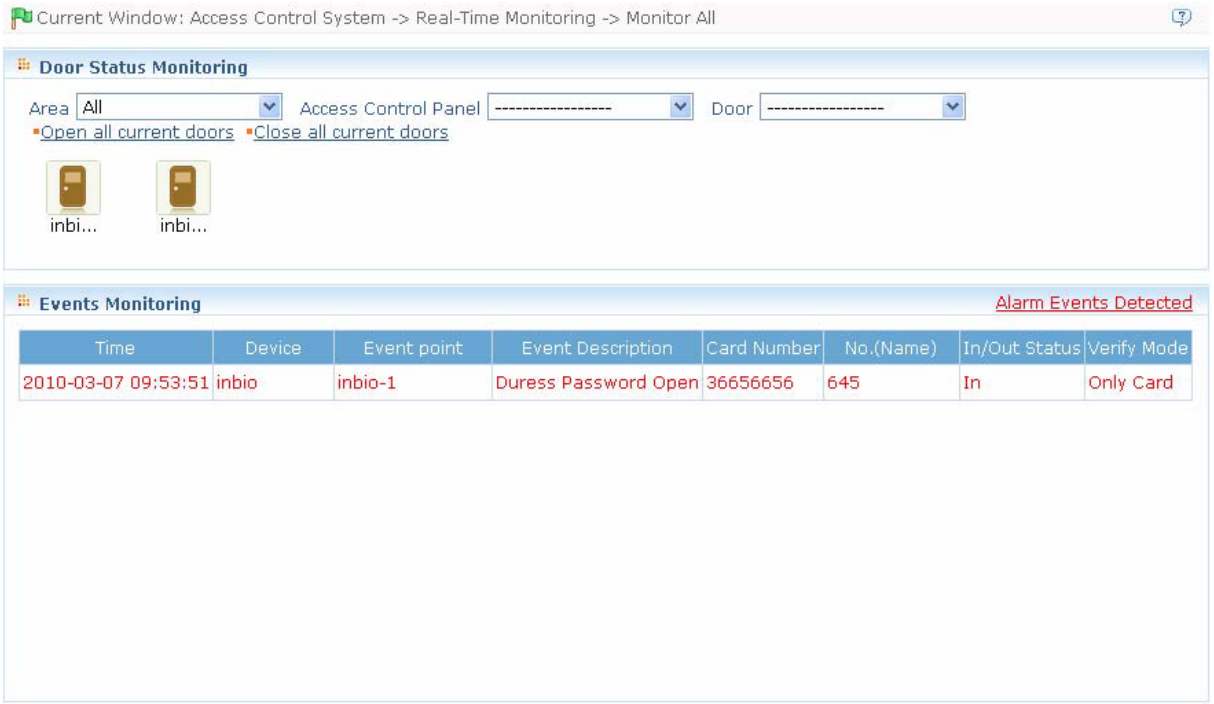
3.10 Ρυθμίσεις επιπέδων πρόσβασης προσωπικού

Μπείτε στο [Access Control] – [Personnel Access Levels] – [Display with Access Levels], κάντε κλικ στο [Add Personnel] για να εισάγετε το προσωπικό που επιθυμείτε στο επιλεγμένο επίπεδο πρόσβασης. Μπορείτε επίσης να δείτε ή να διαγράψετε το υπάρχον προσωπικό του επιλεγμένου επιπέδου πρόσβασης.
Όταν ο χρήστης έχει ενεργοποιημένο το [Display as Personnel], αφού επιλέξει ένα συγκεκριμένο πρόσωπο στην αριστερή πλευρά, μπορεί να δει το επίπεδο πρόσβασης που ισχύει για αυτό. Εκτελέστε τη λειτουργία [Add Access Level] για να προσθέσετε άτομα στην ομάδα με τα περισσότερα προνόμια πρόσβασης ή [Delete Level Access] για να τα διαγράψετε.

Σημειώσεις
Το σύστημα, μπορεί να ανταποκριθεί στις ανάγκες της κατανομής δικαιωμάτων πρόσβασης κατά ομάδες ή χωριστά. Όταν ο χρήστης εκτελεί αυτή τη λειτουργία, μπορεί να χρησιμοποιήσει την αναζήτηση του συστήματος για να μάθει το απαιτούμενο επίπεδο πρόσβασης ή το προσωπικό για την ακριβή κατανομή των δικαιωμάτων.

3.11 Καταγραφή και γεγονότα σε πραγματικό χρόνο

Μπείτε στο [Access Control] – [Real-time Monitoring] – [Monitor all] όπως φαίνεται στο παρακάτω σχήμα:

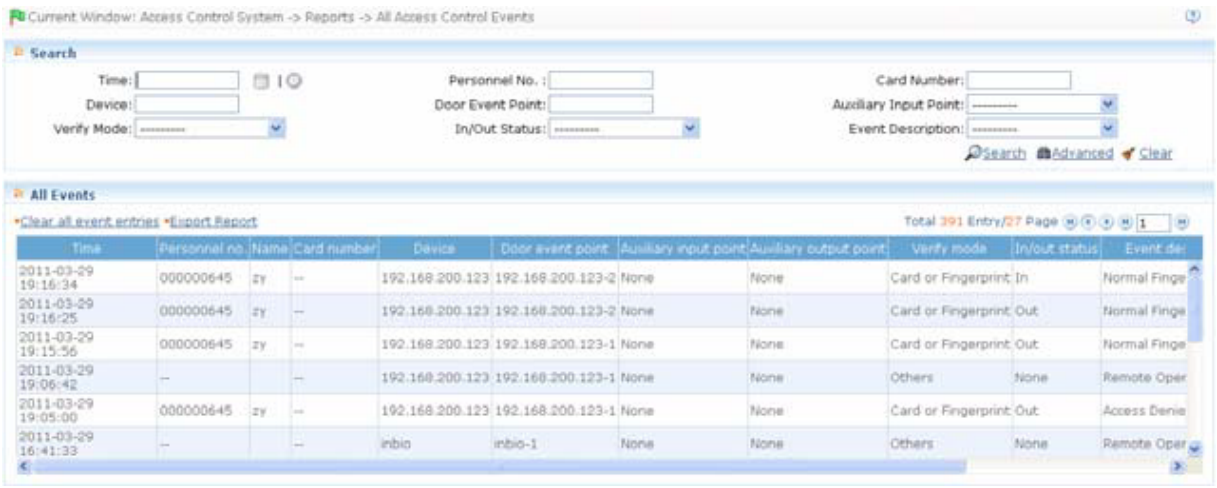


Το σύστημα παρέχει απεικόνιση της κατάστασης της θύρας και των γεγονότων σε πραγματικό χρόνο. Ο χρήστης μπορεί να αλλάξει τις ρυθμίσεις στα κουτιά drop-down στην Area, πίνακα ελέγχου και τη θύρα, για να περιορίσει ή να διευρύνει το πεδίο εφαρμογής της παρακολούθησης. Η προεπιλεγμένη ρύθμιση του συστήματος είναι να παρακολουθεί όλες τις θύρες υπό τον πίνακα ελέγχου τις οποίες ο τρέχων χρήστης έχει δικαιώματα θέασης.
Όταν ο χρήστης αλλάζει στο [Alarm Event], το σύστημα θα απεικονίσει μόνο τα γεγονότα που ενεργοποιούν τον συναγερμό.

Σημειώσεις
1. Παρακαλώ ανατρέξτε στο εγχειρίδιο, στο κεφάλαιο απεικόνιση σε πραγματικό χρόνο [real-time monitoring] για πιο λεπτομερείς περιγραφές.

3.12 Αναφορές

Κατά την εισαγωγή στην αναφορά μέσω [Access Control], ο χρήστης έχει τη δυνατότητα να δει [All Access Control Events] και [Personnel Access Levels] ανάλογα με τις ανάγκες του. Εάν ο χρήστης θέλει να δει το [Access Control Exception Events], μπορεί να βρει σχετικές καταγραφές μέσω της λειτουργίας εύρεσης του συστήματος.



ΒΙΒΛΙΟΓΡΑΦΙΑ

- http://en.wikipedia.org/wiki/Access_control
- http://www.zktechnology.eu
- http://www.zktechnology.eu/index.php/categories-11/access-controllers/c3-rfid
- http://www.zktechnology.eu/index.php/categories-11/accesories/wiegand-readers
- http://www.zktechnology.eu/index.php/categories-11/accesories/push-buttons
- http://www.vroumeliotis.gr/Access-Control-Έλεγχος-εισόδου-Ελεγχος-Πρόσβασης
- Security manager Τευχος 30 Ηλεκτρονικές Κλειδαριές - Ανοίγοντας νέους δρόμους
- Security manager Τευχος 37 Συστήματα ελέγχου πρόσβασης: Θα έχουν το “πάνω χέρι” στα ενοποιημένα συστήματα
- Security manager Τευχος 36 Η ενοποίηση δύο “κόσμων” : Σύγκλιση φυσικού και IT ελέγχου πρόσβασης
- Security manager Τευχος 37 Οι εξελίξεις στα πληκτρολόγια access control
- Security manager Τευχος 30 Ηλεκτρονικές Κλειδαριές: Ανοίγοντας νέους δρόμους
- Security manager Τευχος 26 Καρταναγνώστης: Τα μυστικά της σωστής επιλογής και εγκατάστασης