ΔΙΕΘΝΕΣ
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΤΗΣ ΕΛΛΑΔΟΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«ΕΦΑΡΜΟΓΗ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ ΜΕ ΧΡΗΣΗ ΧΑΟΤΙΚΟΥ ΧΑΡΤΗ ΣΕ ΣΥΣΤΗΜΑ ΣΥΝΤΕΤΑΓΜΕΝΩΝ DRONE»

«Εικόνα»

Του φοιτητή
Σαμαρά Κωνσταντίνου
Αρ. Μητρώου: 516315

Επιβλέπων
Γιακουμής Άγγελος
Επίκουρος καθηγητής

Ημερομηνία 01/02/2022

Τίτλος Δ.Ε. Εφαρμογή κρυπτογράφησης με χρήση χαοτικού χάρτη σε σύστημα συντεταγμένων drone.
Κωδικός Δ.Ε. 21361
Ονοματεπώνυμο φοιτητή Σαμαράς Κωνσταντίνος
Ονοματεπώνυμο εισηγητή Γιακουμής Άγγελος
Ημερομηνία ανάληψης Δ.Ε. 15/10/2021
Ημερομηνία περάτωσης Δ.Ε. 01/02/2022

Βεβαιώνω ότι είμαι ο συγγραφέας αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, έχω καταγράψει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών, εικόνων και κειμένου, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επιπλέον, βεβαιώνω ότι αυτή η εργασία προετοιμάστηκε από εμένα προσωπικά, ειδικά ως διπλωματική εργασία, στο Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του ΔΙ.ΠΑ.Ε.

«Αφιέρωση»

Στην γυναίκα μου Ευρυδίκη και στην κόρη μου Αριάδνη.

Πρόλογος

Το αντικείμενο των ενσωματωμένων συστημάτων παρέχει την δυνατότητα σε έναν φοιτητή να διευρύνει το γνωστικό του εύρος σε μία ποικιλία ειδικοτήτων του τομέα της ηλεκτρονικής ώστε να συνδυάσει επιτυχώς υλικό με λογισμικό. Πέραν τούτου του παρέχει την δυνατότητα να συνδυάσει στο ενσωματωμένο σύστημα εφαρμογές και θεωρητικές αρχές που προέρχονται από άλλους κλάδους της επιστήμης και της μηχανικής ώστε να αποδοθεί μία πρακτική εφαρμογή.

Σε αυτήν την περίπτωση επέλεξα να σχεδιάσω και να εφαρμόσω σε ένα ενσωματωμένο σύστημα ένα μη γραμμικό μαθηματικό μοντέλο, συγκεκριμένα έναν χαοτικό χάρτη για την δημιουργία ενός κλειδιού κρυπτογράφησης για να κρυπτογραφεί τις συντεταγμένες ενός drone. Το ερέθισμα το έλαβα από τον συμφοιτητή και φίλο Ιατρόπουλο Απόστολο ο οποίος έχει πολυετή εμπειρία στον χώρο και ήταν καθοριστικό στην επιλογή μου.

Με το πέρας της εργασίας ωφελήθηκα καθώς απέκτησα εμπειρία στην χρήση της γλώσσας προγραμματισμού C τόσο στην συγγραφή λογισμικού όσο και στην συγγραφή του firmware για το ενσωματωμένο σύστημα, αλλά και στον γενικό σχεδιασμό του ενσωματωμένου συστήματος καθώς και στην κατανόηση των μεθόδων κρυπτογράφησης πληροφοριών.

Περίληψη

Με την χρήση του IDE της Visual Studio της Microsoft αναπτύχθηκε λογισμικό σε γλώσσα προγραμματισμού C το οποίο υπολογίζει γεννήτρια ακολουθίας τριανταδύο τυχαίων bit μέσω μιας εξίσωσης χαοτικής συνάρτησης ενός μονοδιάστατου χαοτικού χάρτη του οποίου οι μεταβλητοί συντελεστές επιλέγονται έτσι ώστε να βρίσκεται σε κατάσταση συνεχούς χάους και να παράγει τυχαίους πραγματικούς αριθμούς. Οι αριθμοί μετατρέπονται σε ακέραιοι, διαιρούνται με το δύο και συγκρίνονται ως προς την ακεραιότητα της διαίρεσης με τον λογικό τελεστή modulo ώστε να λαμβάνονται μηδέν ή ένα και έπειτα καταχωρούνται σε έναν πίνακα αποτελώντας ένα κλειδί κρυπτογράφησης.

Μέσω συνάρτησης βιβλιοθήκης παράγει τυχαίους ακέραιους αριθμούς που με τροποποίηση αντιπροσωπεύουν ένα σύστημα συντεταγμένων GPS το οποίο μετατρέπεται σε δυαδικό αριθμό μήκους τριανταδύο bit και καταχωρείται σε πίνακα. Οι δύο πίνακες πραγματοποιούν μεταξύ τους την λογική πράξη Exclusive Or και καταχωρούνται ως κρυπτογραφημένα δεδομένα.

Προκειμένου να λειτουργήσει το πρόγραμμα σε ζεύγος μικροελεγκτών ESP32 τροποποιήθηκε στο IDE της Arduino ώστε ο ένας να είναι πομπός και ο άλλος δέκτης. Ο πομπός διαχειρίζεται συσκευή GPS όπου μέσω της σειριακής λαμβάνει συντεταγμένες και αφού τις κρυπτογραφήσει τις εκπέμπει κάνοντας χρήση του πρωτοκόλλου επικοινωνίας Wi-Fi. Ο δέκτης λαμβάνει την κρυπτογραφημένη επικοινωνία και έχοντας το κλειδί κρυπτογράφησης αντιστρέφει την Exclusive Or και απεικονίζει την πληροφορία των συντεταγμένων σε πραγματικό χρόνο συγκρίνοντας την πληροφορία του πομπού με αυτήν του δέκτη ώστε να επιβεβαιωθεί απόλυτη ταύτιση μεταξύ τους.

Η πρακτική εφαρμογή ολοκληρώνεται με την εγκατάσταση του πομπού σε ένα τετρακόπτερο και πραγματοποιώντας μία δοκιμαστική ολιγόλεπτη πτήση ώστε να ληφθούν πραγματικές συντεταγμένες σε πραγματικό χρόνο.

«Encryption application using a chaotic map in a drone coordinate system»

«Konstantinos Samaras»

Abstract

Using Microsoft's Visual Studio IDE, a software was developed in the C programming language that calculates a thirty-two-bit random sequence generator through a chaotic equation of a one-dimensional chaotic map whose variable coefficients are selected so that it is in a state of continuous chaos and produces random real numbers. The numbers are converted to integers, divided by two, and compared in terms of the integrity of the division with the logical modulo operator to get zeroes or ones, and then entered into a table as an encryption key.

Through a library function it generates random integers that by modification represent a system of GPS coordinates which is converted to a binary number thirty-two bits long and entered in a table. The two tables perform the Exclusive Or logic operation together and are registered as encrypted data.

In order for the program to work in a pair of ESP32 microcontrollers it was modified in the Arduino IDE so that one is a transmitter and the other a receiver. The transmitter manages a GPS device where through the serial it receives coordinates and after encrypting them it transmits them using the Wi-Fi communication protocol. The receiver receives the encrypted communication and having the encryption key reverses the Exclusive Or and displays the coordinate information in real time comparing the information of the transmitter with that of the receiver in order to confirm complete identification between them.

The practical application is completed by installing the transmitter on a quadropter and performing a short test flight to obtain real-time coordinates.

Ευχαριστίες

Ευχαριστώ τους συναδέλφους μου Ιατρόπουλο Απόστολο για την βοήθεια του στην επιλογή του θέματος και Μπέλτσιο Κωνσταντίνο για τις συμβουλές τις γνώσεις του στα συστήματα μικροελεγκτών και ενσωματωμένων ώστε να δημιουργηθεί ένα βέλτιστο αποτέλεσμα. Ιδιαίτερα ευχαριστώ τους γονείς μου, τα αδέρφια μου, την γυναίκα μου και τα πεθερικά μου για την πολυετή και ατελείωτη υποστήριξη, αγάπη και υπομονή που έκαναν μέχρι αυτό το σημείο.

Περιεχόμενα

Κατάλογος Σχημάτων

Κατάλογος Πινάκων

Συντομογραφίες

Δ.Ε.	Διπλωματική Εργασία
ΔΙΠΑΕ	Διεθνές Πανεπιστήμιο Ελλάδος
Π.Ε.	Πτυχιακή Εργασία

Κεφάλαιο 1ο: Μελέτη

1.1 Εισαγωγή

Η μελέτη μιας εργασίας αποτελεί το πιο βασικό και σημαντικό μέρος μιας εργασίας καθώς εξυπηρετεί στην εξακρίβωση των τμημάτων της, στην πρόβλεψη ανεπιθύμητων καταστάσεων και στην πρόληψη εναντίων τους. Μία καλή μελέτη μπορεί να εξοικονομήσει πολύτιμο χρόνο και κόστος για το σύνολο των εμπλεκόμενων στην υλοποίηση της. Είναι κάτι το οποίο εφαρμόζεται σε κάθε καλή εργασία και αποτελεί ένδειξη της ποιότητας της και του επιπέδου επαγγελματισμού της.

Το σύνολο της εργασίας αφορά την πρακτική εφαρμογή της μεθόδου παραγωγής ενός κλειδιού κρυπτογράφησης με χρήση ενός χαοτικού χάρτη. Θα αναπτυχθεί λογισμικό που θα παράγει το κλειδί κρυπτογράφησης με την μέθοδο χαοτικού χάρτη και θα το χρησιμοποιεί για την κρυπτογράφηση των δεδομένων συντεταγμένων ενός συστήματος συντεταγμένων που αφορούν την τοποθεσία ενός μη επανδρωμένου εναέριου οχήματος (Unmanned Aerial Vehicle, UAV) [1] τις οποίες θα τις μεταδίδει σε έναν δέκτη που θα τις αποκρυπτογραφεί και θα τις απεικονίζει στην οθόνη ενός ηλεκτρονικού υπολογιστικού συστήματος.

Συγκεκριμένα η εφαρμογή μιας μεθόδου κρυπτογράφησης είναι μία πρακτική που υφίσταται από την αρχαιότητα η οποία στην εποχή της πληροφορίας έχει δεχτεί την προσοχή επιστημόνων και μηχανικών όσο ποτέ πριν άλλοτε στο σύνολο της ιστορίας της ανθρωπότητας. Ως μεθοδολογία περιλαμβάνει την δημιουργία ενός κλειδιού κρυπτογράφησης, της διαμόρφωσης των δεδομένων προς κρυπτογράφηση και του κλειδιού κρυπτογράφησης σε συγκεκριμένη μορφή δεδομένων, την μέθοδο σύμπλεξης τους για την επιτυχή κρυπτογράφηση των προς κρυπτογράφηση δεδομένων και την ανάστροφη διαδικασία για την επιτυχή αποκρυπτογράφηση των κρυπτογραφημένων δεδομένων στην αρχική τους πληροφορία [2].

Εμπνευσμένος από το μαθηματικό μοντέλο του χάους ο χαοτικός χάρτης είναι μία εξίσωση της οποία η κύρια ιδιαιτερότητα της είναι η ακραία μη γραμμική συμπεριφορά της που κατά συνέπεια δεν επιτρέπει κανένα της σημείο για οποιοδήποτε μήκος να υπάρχει η δυνατότητα γραμμικοποίησης του. Με την κατάλληλη σχεδίαση του και παραμετροποίηση του μπορεί να συμπεριληφθεί σε έναν αλγόριθμο ο οποίος θα παράγει ένα κλειδί κρυπτογράφησης. Η παραμετροποίηση του μπορεί να επιτρέψει για την παραγωγή διαφόρων καταστάσεων του χάους παρέχοντας στον μηχανικό αρκετές επιλογές λειτουργίας του[3].

Ο συνολικός αλγόριθμος θα επιτρέψει την ανάπτυξη ενός υλικολογισμικού το οποίο θα ελέγχει την λειτουργία μιας ενιαίας κατασκευής η οποία θα αποτελεί το υλικό μέρος της [4]. Αναφορικά οι εργασίες που θα εκτελεί το ενιαίο αυτό σύστημα θα είναι η λήψη συντεταγμένων τοποθεσίας, η κρυπτογράφηση/αποκρυπτογράφηση πληροφοριών συντεταγμένων, η ασύρματη μετάδοση τους μέσω πρωτοκόλλου επικοινωνίας, η πτήση και αιώρηση ενός μη επανδρωμένου εναέριου οχήματος και το σύστημα τηλεχειρισμού του.

Η σύνθεση όλων των ανωτέρω θα συμπεριλάβει το υλικό μέρος αλλά και το λογισμικό μέρος της εργασίας καθώς αυτά θα σχηματίσουν ένα ενσωματωμένο σύστημα ελεγχόμενο στον πυρήνα του από συστήματα μικροελεγκτών. Τα κύρια μέρη της τα οποία θα εξεταστούν με την σειρά είναι η κρυπτογράφηση, το σύστημα συντεταγμένων, τα συστήματα μικροελεγκτών, οι περιφερειακές συσκευές, το λογισμικό, το μη επανδρωμένο αεροσκάφος και το ενσωματωμένο σύστημα [5].

1.2 Ιστορική Αναδρομή

- **1900 π.Χ.:** Ανακαλύπτεται η αρχαιότερη χρήση της πρώιμης μορφής κρυπτογράφησης αντικατάστασης συμβόλου στην Αίγυπτο στον τάφο του Κνουμχοτέπ του 2ου. Η τεχνική αυτή χρησιμοποιούταν εκτενέστατα στην αρχαία Ελλάδα και Ρωμαϊκή αυτοκρατορία και θεωρούταν μη τυπική που σημαίνει πως απαιτούσε για την αποκρυπτογράφηση ένα κλειδί κρυπτογράφησης και της μαθηματικής μεθόδου εφαρμογής της. Η διασημότερη στρατιωτικής ανάπτυξης μέθοδος κρυπτογράφησης ονομαζόταν κρυπτογράφηση του Καίσαρα η οποία αντικαταστεί ένα γράμμα του αλφάβητου ενός κειμένου με άλλο γράμμα του αλφάβητου προς τα κάτω για καθορισμένο αριθμό θέσεων.
- **9ος αιώνας μ.Χ.:** Ο Άραβας μαθηματικός Al-Kindi ανέπτυξε μία μαθηματική μέθοδο ανάλυσης συχνότητας για την συστηματική παραβίαση μεθόδων κρυπτογράφησης που βασίζονται στην μέθοδο κρυπτογράφησης του Καίσαρα.
- **480 π.Χ.:** Η Βασίλισσα της Σπάρτης Γοργώ αποστέλλει μηνύματα στον σύζυγο της Βασιλιά Λεωνίδα στις Θερμοπύλες χαραγμένα σε μπρούτζινες πλάκες και καλυμμένες με κερί για να κρύψει και να αποτρέψει την ανάγνωση τους από μη εγκεκριμένους παραλήπτες.
- **Ιούλιος 1849:** Οι ναυτικές ένοπλες δυνάμεις κάνουν χρήση μικρής κλίμακας αερόστατων ως μη επανδρωμένα αεροσκάφη για πολεμικές επιχειρήσεις.
- **Αρχές 20ου αιώνα:** Ξεκινούν ουσιαστικές έρευνες και ανάπτυξη των μη επανδρωμένων αεροσκαφών.
- **1903:** Ο Ισπανός μηχανικός Leonardo Torres y Quevedo παρουσιάζει στην ακαδημία επιστημών του Παρισιού το "Telekino", ένα ασύρματο σύστημα ελέγχου ραδιοκυμάτων με απώτερο σκοπό την απομάκρυνση του ανθρώπινου στοιχείου από το πιλοτήριο των αεροσκαφών για την προστασία του.
- **1916:** Ο Archibald Montgomery Low αναπτύσσει ένα ασύρματο σύστημα ελέγχου μη επανδρωμένων αεροσκαφών για στόχους ασκήσεων σκοποβολής με την ονομασία "Aerial Target".
- **21 Μαρτίου 1917:** Ο Archibald Montgomery Low παρουσιάζει το μονόπλανο του Geoffrey de Havilland ως το αεροσκάφος που πέταξε χωρίς πιλότο μέσω ασύρματου ελέγχου δικής του επινόησης.
- **1935:** Ο αστέρας του κινηματογράφου και λάτρης των αεροσκαφών Reginald Denny κατασκεύασε το πρώτο τηλεχειριζόμενο αεροσκάφος σε κλίμακα.
- **1939-1945:** Ο Δεύτερος Παγκόσμιος Πόλεμος καθιστά μέγιστη προτεραιότητα μεταξύ των εμπλεκομένων την έρευνα και ανάπτυξη των συστημάτων κρυπτογράφησης τόσο για την προστασία των μεταδόσεων τους όσο και για την παραβίαση των αντιπάλων συστημάτων για συλλογή πληροφοριών, συμβάλλοντας στην διαρκή τεχνολογική ανάπτυξη του τομέα κρυπτογράφησης.
- **1945-1959:** Τα μη επανδρωμένα αεροσκάφη γνωρίζουν ελάχιστη τεχνολογική ανάπτυξη και θεωρούνται ως κάτι παραπάνω από τηλεχειριζόμενα αεροσκάφη.
- **Δεκαετία '50:** Ανακαλύπτεται το όφελος του πυριτίου στον κλάδο της ηλεκτρονικής που οδηγεί στην κατασκευή των ολοκληρωμένων κυκλωμάτων (Integrated Circuits, IC) μεταξύ αυτών και των Μικροελεγκτών και μικροεπεξεργαστών.
- **1959:** Ο πόλεμος του Βιετνάμ προκαλεί ανησυχία στην Αμερικανική στρατιωτική διοίκηση για τους πιλότους που καταρρίπτονται εντός εχθρικών εδαφών και την διάσωση τους και χρηματοδοτεί την έρευνα μη επανδρωμένων αεροσκαφών για πολεμικές επιχειρήσεις υψηλότερων απαιτήσεων.
- **Δεκαετίες '80 και '90:** Η σημαντική βελτίωση των ηλεκτρονικών συστημάτων τόσο σε απόδοση όσο και σε μέγεθος κατασκευής επέτρεψε την ανάπτυξη και κατασκευή μη επανδρωμένων αεροσκαφών φθηνού κόστους κατασκευής που είχε ενσωματωμένα διάφορα συστήματα όπως παρακολούθηση πραγματικού χρόνου, συστήματα καταγραφής συντεταγμένων και στόχευση και πλήξη στόχων με εκρηκτικές ύλες ενώ παράλληλα έγινε πιο αναλώσιμο από ποτέ.

1.3 Κρυπτογράφηση

Η κρυπτογράφηση αποτελεί στο σύνολο της μία πρακτική η οποία διακρίνεται από δύο χαρακτηριστικά. Το πρώτο είναι το κλειδί κρυπτογράφησης και το δεύτερο είναι ο τρόπος με τον οποίο το κλειδί κρυπτογράφησης κρυπτογραφεί τα δεδομένα. Προκειμένου να είναι πετυχημένη μία μέθοδος κρυπτογράφησης θα πρέπει αρχικά το κλειδί κρυπτογράφησης να κατασκευαστεί με μία μέθοδο η οποία να είναι και μυστική αλλά και να μην είναι δυνατόν να μπορεί να ανακαλυφθεί από μη εξουσιοδοτημένους παραλήπτες. Επίσης η μέθοδος κρυπτογράφησης των δεδομένων θα πρέπει να είναι μυστική αλλά και καλά σχεδιασμένη ώστε όταν πραγματοποιηθεί το σύνολο της διαδικασίας κρυπτογράφησης και αποκρυπτογράφησης τα αποκρυπτογραφημένα δεδομένα να είναι απολύτως πιστά με τα δεδομένα πριν την αποκρυπτογράφηση.

Η κρυπτογράφηση είναι ένας κλάδος στον οποίο τα μαθηματικά βρίσκουν μεγάλη πρακτική εφαρμογή καθώς η κύρια προσέγγιση πραγματοποιείται με την εφαρμογή διάφορων μαθηματικών μεθόδων οι οποίες σχεδιάζονται και αναπτύσσονται με τρόπο τέτοιο που να μειώνουν όσο περισσότερο γίνεται το ενδεχόμενο παραβίασης τους.

Σε σύγχρονες εφαρμογές οι μέθοδοι κρυπτογράφησης είναι το αποτέλεσμα ενός αλγόριθμου το αποτέλεσμα του οποίου κρίνεται από την εσωτερική δομή του και παραμετροποίηση του άρα συμπαιρένεται πως η όλη διαδικασία γίνεται σε ψηφιακό επίπεδο και πως πολλές διεργασίες αφορούν μετατροπές των δεδομένων από την αρχική τους μορφή σε συγκεκριμένη μορφή η οποία προκύπτει απαραίτητη για την επιτυχία της διαδικασίας.

1.3.1 Κλειδί Κρυπτογράφησης

Το κλειδί κρυπτογράφησης είναι ένα προϊόν το οποίο παρασκευάζεται στην μορφή ψηφιακής λέξης ορισμένου μεγέθους σε bit. Το τυπικό μήκος ενός κλειδιού κρυπτογράφησης που συνήθως απαντάται στις κοινές εφαρμογές κατασκευής κλειδιών κρυπτογράφησης είναι 128, 256 και 512 bit. Για τις ανάγκες της παρούσας εργασίας το μήκος του κλειδιού κρυπτογράφησης επιλέχθηκε να είναι στα 32 bit καθώς προκύπτει επαρκές για τις πληροφορίες που θα κρυπτογραφεί. Είναι το εργαλείο με το οποίο ο αλγόριθμος θα πραγματοποιήσει την μετατροπή του κειμένου σε μία ακατανόητη ακολουθία χαρακτήρων πραγματοποιώντας συνήθως μία αριθμητική ή λογική πράξη μεταξύ του κλειδιού και των χαρακτήρων.

Οι συνήθεις μέθοδοι κατασκευής κλειδιών κρυπτογράφησης ανήκουν σε δύο κύριες κατηγορίες, την συμμετρική και την ασυμμετρική. Η διαφορά τους βρίσκεται στο ότι στην συμμετρική όσοι έχουν εξουσιοδοτημένη πρόσβαση στις κρυπτογραφημένες πληροφορίες μοιράζονται όλοι το ίδιο κλειδί κρυπτογράφησης, ενώ στην ασυμμετρική το κλειδί κρυπτογράφησης είναι στην πραγματικότητα δύο κλειδιά, ένα δημόσιο και ένα προσωπικό όπου το προσωπικό είναι μυστικό και γνωστό μόνο στον κάτοχο του ενώ το δημόσιο είναι διαθέσιμο σε όποιον το χρειάζεται (συνήθως κάτοχος προσωπικού κλειδιού). Στο ασσυμετρικό σύστημα τα κλειδιά δεν είναι άσχετα κατασκευασμένα μεταξύ τους αλλά το προσωπικό κλειδί συσχετίζεται μαθηματικά με το δημόσιο και προκειμένου το προσωπικό να μπορέσει να αποκρυπτογραφήσει τις πληροφορίες στις οποίες έχει πρόσβαση θα πρέπει να το κάνει έμμεσα μέσω του δημόσιου κλειδιού κρυπτογράφησης, πράγμα που οδηγεί στο συμπέρασμα ότι το κύριο κλειδί κρυπτογράφησης είναι το δημόσιο και ο αλγόριθμος αναγνωρίζει τα προσωπικά κλειδιά μέσω της μαθηματικής σχέσης που έχουν με το δημόσιο προτού τα επιτρέψει να έχουν πρόσβαση στις κρυπτογραφημένες πληροφορίες.

Για τις ανάγκες της παρούσας εργασίας επιλέχθηκε η συμμετρική μέθοδος κατασκευής κλειδιού κρυπτογράφησης καθώς το παρών πλήθος συμμετεχόντων βρίσκεται στο ελάχιστο δυνατό, γεγονός που θέτει ανούσιο το επιπλέον επίπεδο ασφάλειας. Για την δημιουργία του κλειδιού κρυπτογράφησης η μαθηματική μέθοδος θα είναι αυτή του χαοτικού χάρτη μιας διάστασης. Γενικότερα το χάος στα μαθηματικά αφορά μαθηματικές συναρτήσεις/εξισώσεις που παρουσιάζουν έλλειψη γραμμικότητας οποιουδήποτε βαθμού. Αυτό το χαρακτηριστικό είναι χρήσιμο κυρίως για το γεγονός ότι είναι τόσο μη γραμμικό που δεν μπορεί να γραμμικοποιηθεί η χαρακτηριστική του καμπύλη σε κανένα σημείο της και κατά συνέπεια δεν μπορεί να εφαρμοστεί αντίστροφη μηχανική ώστε να επιτρέψει σε κάποιον να διαπιστώσει το κλειδί κρυπτογράφησης.

Ο χαοτικός χάρτης είναι μία εξελικτική συνάρτηση που παρουσιάζει χαοτική συμπεριφορά της οποίας το αποτέλεσμα προκύπτει από αντικατάσταση στο περιεχόμενο της για κάθε νέα τιμή της με την προηγούμενη τιμή της και μπορεί να είναι είτε διακριτό είτε συνεχές το αποτέλεσμα. Για τις ανάγκες της παρούσας εργασίας έγινε χρήση του ακόλουθου χάρτη.

$$x_i = A \sin\left(\frac{\omega}{x_{i-1}}\right) + B \tanh(x_{i-1})^2 \tag{2.1}$$

Ο συγκεκριμένος χαοτικός χάρτης είναι μονοδιάστατος και προέρχεται από μία δημοσίευση [6] στην οποία δοκιμάστηκε ως προς την αξιοπιστία της τυχαιότητας του. Αποτελείται από τέσσερις μεταβλητές (τις x, A, B και ω) οι οποίες αποτελούν τους συντελεστές του χαοτικού χάρτη και αναλόγως τις τιμές που θα έχουν ο χάρτης θα παράγει για κάθε επανάληψη του έναν τυχαίο πραγματικό αριθμό. Ο τρόπος με τον οποίο θα παράγονται οι τιμές του εξαρτώνται από τις τιμές των συντελεστών του χάρτη, καθώς αναλόγως τις τιμές των συντελεστών θα παράγει τιμές μέσω συγκεκριμένης κατάστασης χάους. Προκειμένου να επιλεγεί η επιθυμητή κατάσταση χάους που αφορά την κάθε εφαρμογή θα πρέπει να γίνει παραπομπή στο διχαλωτό γράφημα του κατασκευαστή του χαοτικού χάρτη το οποίο απεικονίζει για κάθε τιμή των συντελεστών του σε τι κατάσταση λειτουργίας θα βρίσκεται. Για τις ανάγκες της παρούσας εργασίας οι τιμές των συντελεστών του χαοτικού χάρτη έχουν επιλεγεί έτσι ώστε να βρίσκεται σε κατάσταση συνεχούς χάους και συγκεκριμένα για τιμές των συντελεστών του χαοτικού χάρτη που θα ισούνται με $A = 8, B = 15, \omega = 100$ *και* $x_{(0)} = 0{,}1$.

Σε αυτό το σημείο να ληφθεί υπόψιν πως το τυχαίο θα ήταν το ιδανικό και επιθυμητό αποτέλεσμα αλλά στο φυσικό σύμπαν δεν υπάρχει κάτι το αληθινά τυχαίο καθώς υπάρχει μία μόνιμη κατάσταση περίπλοκων μη γραμμικών συναρτήσεων που σχηματίζουν τεράστια συστήματα διαφορικών εξισώσεων μεταξύ τους διατηρώντας ένα απέραντο κοσμικό μοτίβο, επομένως τυπικά όλες οι γεννήτριες "τυχαίων" αριθμών ή μεταβλητών είναι μηχανές παραγωγής "ψευδοτυχαίων" αριθμών ή μεταβλητών με εξαίρεση αυτές που παράγουν σε κβαντικό επίπεδο. Έστω και έτσι όμως οι γεννήτριες που βασίζονται σε χαοτικούς χάρτες μπορούν να παράγουν με τόσο υψηλό παράγοντα τυχαιότητας αριθμούς κάνοντας το οποιοδήποτε μοτίβο τόσο περίπλοκο που άνετα μπορούν να θεωρηθούν αμελητέοι και τυχαίοι.

1.3.2 Δεδομένα προς Κρυπτογράφηση

Τα δεδομένα που προορίζονται για κρυπτογράφηση συνήθως είναι ποικιλόμορφα στην μορφή τους και αυτό συχνά δημιουργεί προβλήματα και σφάλματα στην διαδικασία εκτέλεσης του προγράμματος κρυπτογράφησης με κίνδυνο την κατάρρευση του καθώς αυτό οδηγείται σε απροσδόκητες καταστάσεις που δεν έχει προσδιοριστεί ο τρόπος διαχείρισης τους από αυτό. Το πρόβλημα εντοπίζεται στο γεγονός ότι ενώ το κλειδί κρυπτογράφησης συνήθως είναι σταθερό στην μορφή του και στο περιεχόμενο του, τα προς κρυπτογράφηση δεδομένα είναι μεταβαλλόμενα στο περιεχόμενο και στην μορφή τους.

Συμπερασματικά ο προγραμματιστής πρέπει να λάβει υπόψιν του πολλές παραμέτρους οι οποίες θα εξασφαλίσουν την ομαλή λειτουργία του προγράμματος, την ταχύτητα εκτέλεσης του και την ποιότητα του περιεχομένου του ώστε αυτό να "τρέχει" όσο το δυνατόν πιο βέλτιστα γίνεται.

Αρχικά θα πρέπει να χωρίσει τις διαδικασίες που θα εκτελεί το πρόγραμμα στα πιο βασικά της τμήματα. Για την συγκεκριμένη εργασία της οποίας το ζητούμενο είναι η κρυπτογράφηση του GPS σήματος ενός μη επανδρωμένου αεροσκάφους ώστε να το μεταδώσει σε εξουσιοδοτημένους παραλήπτες γίνεται αμέσως σαφές πως το πρόγραμμα θα χωριστεί σε δύο λειτουργίες δεδομένου πως η επικοινωνία σε αυτήν την εφαρμογή δεν είναι αμφίδρομη αλλά μονομερής. Δηλαδή υπάρχει ένας πομπός ο οποίος μόνο μεταδίδει πληροφορίες και υπάρχει ένας δέκτης που μόνο λαμβάνει σήμα, επομένως θα πρέπει να υπάρχει ένα πρόγραμμα που κρυπτογραφεί στην πηγή του αρχικού προς εκπομπή σήματος και ένα που αποκρυπτογραφεί στον παραλήπτη την κρυπτογραφημένη μετάδοση στο αρχικό σήμα στον δέκτη. Αυτό θα υλοποιηθεί με την δημιουργία μίας συνάρτησης η οποία θα διαβάζει το περιεχόμενο που λαμβάνει η σειριακή είσοδος του ενσωματωμένου συστήματος του πομπού το οποίο θα είναι σε μορφή συμβολοσειρών και με τις κατάλληλες αριθμητικές πράξεις θα το μετατρέπει σε μορφή ακολουθίας των 32 bit και θα επιστρέψει το αποτέλεσμα στο κυρίως πρόγραμμα. Αντίστοιχα στο firmware του δέκτη θα υπάρχει η συνάρτηση που θα διαβάζει την αποκρυπτογραφημένη ακολουθία και με τις κατάλληλες αριθμητικές πράξεις θα το μετατρέπει στην αρχική γραμματοσειρά.

1.3.3 Μέθοδος Κρυπτογράφησης

Με το πέρας όλων των προηγούμενων διαδικασιών του προγράμματος έχει πραγματοποιηθεί όλη η κατάλληλη προετοιμασία ώστε να μπορεί το πρόγραμμα να κρυπτογραφεί τα δεδομένα με το κλειδί κρυπτογράφησης. Η διαδικασία της κρυπτογράφησης συνοψίζεται στην τέλεση μίας αριθμητικής ή λογικής πράξης μεταξύ των προς κρυπτογράφηση δεδομένων και του κλειδιού κρυπτογράφησης.

Συγκεκριμένα για τις ανάγκες της παρούσας εργασίας τόσο τα προς κρυπτογράφηση δεδομένα όσο και το κλειδί κρυπτογράφησης έχουν μετατραπεί σε δυαδική μορφή ώστε να υπάρχει η δυνατότητα πέρα από την τέλεση αριθμητικών πράξεων μεταξύ τους, να μπορεί να πραγματοποιηθεί και η τέλεση των λογικών πράξεων. Για χάρη της σαφήνειας διευκρινίζεται πως αριθμητική πράξη είναι αυτή που κάνει χρήση (μεταξύ άλλων) των αριθμητικών τελεστών + (πρόσθεσης), -(αφαίρεσης), / ή ÷ (διαίρεσης) και * (πολλαπλασιασμού), ενώ λογική πράξη είναι αυτή που κάνει χρήση των λογικών τελεστών || (ή - OR), && (και - AND), ! (αναστρέφων - NOT) και ^ (αποκλειστική ή – EXCLUSIVE OR) των οποίων το αποτέλεσμα θα είναι πάντα δυαδικής φύσης και συγκεκριμένα θα είναι είτε το αληθές (TRUE) είτε το ψευδές (FALSE).

Στην συγκεκριμένη μέθοδο κρυπτογράφησης και αφού θα της είναι διαθέσιμα τα δεδομένα κρυπτογράφησης και το κλειδί κρυπτογράφησης στην τελική μορφή των ακολουθιών των 32 bit θα τελέσει μεταξύ τους την λογική πράξη XOR (Exclusive Or) αποδίδοντας μία νέα ακολουθία των 32 bit η οποία θα είναι ακατανόητη σε οποιονδήποτε μη εξουσιοδοτημένο παραλήπτη που τύχει να λάβει τα κρυπτογραφημένα δεδομένα. Για όλους τους λογικούς τελεστές υπάρχει αντίστοιχα και ένας λογικός πίνακας που αποδίδει το αποτέλεσμα των δύο ή και παραπάνω εισόδων σε αληθές ή ψευδές, όπου αληθές συμβολίζεται με 1 και ψευδές με 0. Για τον τελεστή XOR για δύο εισόδους η έξοδος του θα ισούται με 0 όταν και οι δύο είσοδοι θα είναι ίδιες, δηλαδή 0 και 0 ή 1 και 1, αλλιώς θα ισούται με 1 όταν οι είσοδοι θα είναι ανόμοιες, δηλαδή 0 και 1 ή 1 και 0. Ο ακόλουθος πίνακας ονομάζεται πίνακας αληθείας και απεικονίζει την έξοδο του τελεστή XOR για κάθε δυνατό συνδυασμό δυαδικής μορφής για δύο εισόδους του.

Πίνακας 1. Πίνακας αληθείας XOR.

x_1	x_2	y
0	0	0
0	1	1
1	0	1
1	1	0

Όπως περιεγράφηκε προηγουμένως, στον πίνακα διακρίνονται δύο είσοδοι x_1και x_2και το αποτέλεσμα της εξόδου τους y. Γίνεται αντιληπτό πως λόγω της δυαδικής φύσης των συντελεστών του πίνακα αληθείας, εφόσον υπάρχουν δύο είσοδοι τότε ο μέγιστος πιθανός συνδυασμός των εισόδων θα ισούται με $2^2 = 4$ όπου η δύναμη του 2 εκφράζει τον αριθμό εισόδων του τελεστή.

Το πρώτο βήμα για την πραγματοποίηση της διαδικασίας αποκρυπτογράφησης θα είναι να είναι γνωστό στο ενσωματωμένο σύστημα του δέκτη το κλειδί κρυπτογράφησης με το οποίο το ενσωματωμένο σύστημα του πομπού πραγματοποίησε την διαδικασία κρυπτογράφησης ώστε να μπορέσει να πραγματοποιήσει την αποκρυπτογράφηση. Αυτό το πετυχαίνει εκτελώντας στο πρόγραμμα του ακριβώς την ίδια συνάρτηση PRBG που χρησιμοποίησε ο πομπός με τον ίδιο χαοτικό χάρτη και με τις ίδιες τιμές συντελεστών του και για τον ίδιο αριθμό επαναλήψεων. Εφόσον είναι πιστά τα ανωτέρω και στα δύο ενσωματωμένα συστήματα, τότε θα μπορούν να παράγουν και τα δύο το ίδιο ακριβώς κλειδί κρυπτογράφησης εύρους 32 bit.

Αφού το κλειδί κρυπτογράφησης είναι βέβαιο πως είναι γνωστό και στα δύο ενσωματωμένα συστήματα, ο δέκτης θα πρέπει να απομονώσει τα αρχικά δεδομένα του συστήματός συντεταγμένων με απόλυτη πιστότητα από τον πομπό. Αυτό το πετυχαίνει τελώντας την λογική πράξη XOR μεταξύ του κλειδιού κρυπτογράφησης και των κρυπτογραφημένων δεδομένων. Ο λόγος για τον οποίο συμβαίνει αυτό είναι διότι όσων αφορά την αριθμητική των λογικών τελεστών δεν υπάρχουν κρατούμενα όπως αν είχε υπάρξει αριθμητική τέλεση πράξεων. Έτσι το αποτέλεσμα των λογικών πράξεων ανταποκρίνεται στον πίνακα αληθείας του τελεστή με τον οποίο θα πραγματοποιηθεί η λογική πράξη. Αν για παράδειγμα έγινε μία λογική πράξη μεταξύ δύο αριθμών του δυαδικού αριθμητικού συστήματός, των 01011 και 10101 κάνοντας χρήση του λογικού τελεστή XOR, τότε σύμφωνα με τον πίνακα αληθείας της πράξης XOR το αποτέλεσμα των δύο δυαδικών αριθμών θα είναι το 11110. Προκειμένου να μπορέσουμε να αντιστρέψουμε την διαδικασία για να αποσπαστούν οι δύο αριθμοί που έδωσαν αυτό το αποτέλεσμα και εφόσον είναι γνωστός ο ένας από τους δύο, για παράδειγμα ο 01011, τότε πρέπει να εφαρμοστεί μεταξύ του 11110 και του 01011 ο λογικός τελεστής XOR ο οποίος θα είναι ο αντίστροφος του λογικού τελεστή XOR της πρώτης λογικής πράξης ως προς το αποτέλεσμα του. Δηλαδή όπου ο λογικός τελεστής XOR αποδίδει ένα αποτέλεσμα α κατά την πρώτη εκτέλεση, ο ίδιος λογικός τελεστής XOR θα αποδίδει το αντίστροφο αποτέλεσμα β κατά την δεύτερη εκτέλεση του. Επομένως αν εφαρμόσουμε τον λογικό τελεστή XOR στους δυαδικούς αριθμούς 11110 και 01011, τότε το αποτέλεσμα θα είναι ο αριθμός 10101 ο οποίος είναι ακριβώς αυτός με τον οποίο όταν εκτελέστηκε με τον λογικό τελεστή XOR με τον 01011 απέδωσε τον 11110.

Έτσι εφαρμόζοντας τον λογικό τελεστή XOR μεταξύ του κλειδιού κρυπτογράφησης εύρους 32 bit στην κρυπτογραφημένη δυαδική ακολουθία εύρους 32 bit για δεύτερη φορά, θα μπορέσει το πρόγραμμα να επαναφέρει τα αρχικά δεδομένα συστήματος συντεταγμένων στην αρχική δυαδική μορφή εύρους 32 bit που είχαν πριν την κρυπτογράφηση τους.

1.4 Σύστημα Συντεταγμένων

Τα συστήματα συντεταγμένων αποσκοπούν στο να παρέχουν σε έναν δέκτη ακριβή πληροφορία σχετικά με την θέση του στον πλανήτη. Η εφαρμογή αυτής της τεχνολογίας προέκυψε ιδιαίτερα χρήσιμη σε πολλούς τομείς όπως της ναυσιπλοΐας, έρευνας που εντοπίζεται σε εκτός πολιτισμού περιοχές και αεροπορίας. Γενικά σε όποια εφαρμογή αφορά την μετακίνηση μεταξύ συγκεκριμένων σημείων στην επιφάνεια του πλανήτη δηλαδή.

1.4.1 GPS (Global Pointing System)

Πρόκειται για ένα σύστημα πραγματικού χρόνου παροχής τοποθεσίας και ώρας οπουδήποτε στον πλανήτη υψηλής ακρίβειας χάρη σε ένα σύνολο δορυφόρων σε τροχιά, τοποθετημένων με τρόπο τέτοιο ώστε να υπάρχει πλήρη πλανητική κάλυψη από έναν ελάχιστο αριθμό δορυφόρων σε κάθε δεδομένη στιγμή. Αυτό είναι απαραίτητο επειδή έτσι είναι εφικτό, καθώς "κλειδώνει" μία συσκευή την τοποθεσία της, να μπορέσει το δορυφορικό δίκτυο να παρέχει πληροφορίες τοποθεσίας όχι μόνο σε ένα σύστημα αξόνων xy το οποίο αφορά τον μεσημβρινό και τον παράλληλο αλλά και τον άξονα z ο οποίος αφορά το ύψος στο οποίο βρίσκεται η συσκευή GPS.

Αρχικά το σύστημα συντεταγμένων ήταν γνωστό με την ονομασία Navstar GPS και αποτελούσε τεχνολογική ιδιοκτησία της κυβέρνησης των Ηνωμένων Πολιτειών της Αμερικής (ΗΠΑ) [7]. Μέχρι και σήμερα συνεχίζει να αποτελεί ιδιοκτησία της κυβέρνησης των ΗΠΑ απλώς έχει απλοποιηθεί η ονομασία του σε GPS και μπορεί να παρέχει πρόσβαση σε αυτό σε οποιονδήποτε έχει στην κατοχή του έναν δέκτη GPS. Αυτό το σύστημα συντεταγμένων αναπτύχθηκε ως απόπειρα να λυθούν τα προβλήματα που δημιουργούνταν από προγενέστερα συστήματα συντεταγμένων.

1.4.2 Το GPS ως μέρος του Ενσωματωμένου Συστήματος

Συμπερασματικά το GPS προκύπτει ως το ιδανικότερο σύστημα εντοπισμού συντεταγμένων καθώς η τεχνολογική του ανάπτυξη προσφέρει υψηλή αξιοπιστία του συστήματος και επομένως είναι το πλέον κατάλληλο σε σχέση με τα αντίστοιχα του. Λόγω των ανωτέρων θα είναι το σύστημα επιλογής το οποίο θα ενσωματωθεί στο ενσωματωμένο σύστημα το οποίο θα λειτουργήσει με το μη επανδρωμένο αεροσκάφος για την μετάδοση των συντεταγμένων του σε αληθινό χρόνο.

Η συσκευή στην οποία θα λειτουργεί το GPS θα είναι ένα module (ανεξάρτητη ολοκληρωμένη και αυτόνομη μονάδα) η οποία θα λειτουργεί σαν δέκτης και θα εντοπίζεται αποκλειστικά μόνο από το δορυφορικό δίκτυο των 24 δορυφόρων του συστήματος και θα λαμβάνει από αυτό τις πληροφορίες συντεταγμένων και ρολογιού που το αφορά ως δέκτης. Η συσκευή διαθέτει δική της βιβλιοθήκη με την βοήθεια της οποίας μετατρέπει την πληροφορία των συντεταγμένων της σε μία ακολουθία χαρακτήρων την οποία έπειτα την προωθεί στην σειριακή θύρα του συστήματος μικροελεγκτή του οποίου αποτελεί μέρος του ενσωματωμένου συστήματος. Όταν το ζεύγος των ενσωματωμένων επικοινωνήσουν μεταξύ τους και μεταβιβαστεί η πληροφορία από τον πομπό στον δέκτη, το firmware του δέκτη με την βοήθεια της βιβλιοθήκης της συσκευής GPS θα μετατρέψει την πληροφορία σε κατάλληλη μορφή ώστε να απεικονιστεί σε οθόνη. Η συσκευή GPS είναι σχεδιασμένη έτσι ώστε έχει 20 σημεία επαφής (10 σε κάθε πλευρά του) τύπου SMT σε κλίμακα του grid του μισού mill κατά το αυτοκρατορικό σύστημα (1,27mm κατά το μετρικό σύστημα) το οποίο είναι το μισό από αυτό που έχει καθοριστεί για τα πιο κοινά ολοκληρωμένα για τις αποστάσεις των ακροδεκτών τους. Αυτή η πληροφορία είναι σημαντική καθώς καθορίζει τον τρόπο με τον οποίο θα τοποθετηθεί η συσκευή GPS στην πλακέτα βακελίτη ώστε να ενωθεί με τις εισόδους/εξόδους του συστήματος μικροελεγκτή. Η συσκευή που θα χρησιμοποιηθεί

θα είναι συγκεκριμένα η PA6H της οποίας τα χαρακτηριστικά είναι ιδανικά για τους στόχους της παρούσας εργασίας [8].

Η ακρίβεια της συγκεκριμένης συσκευής είναι αρκετά υψηλή καθώς το σφάλμα της τοποθεσίας της φτάνει να 1,8 μέτρα σε σχέση με την πραγματική τοποθεσία του δέκτη ακόμη και ανάμεσα σε πυκνοκατοικημένες περιοχές όπου η απευθείας οπτική επαφή με τους δορυφόρους του δορυφορικού δικτύου του συστήματος περιορίζεται μερικές φορές στους τέσσερις δορυφόρους αλλά ποτέ δεν ήταν συνδεδεμένο με λιγότερους από τέσσερις. Η μεταβολή της τοποθεσίας κατά την μετακίνηση του δέκτη είναι μικρότερη από 10ms γεγονός που καθιστά την αντίδραση του συστήματος αρκετά ακαριαία ώστε να ληφθεί υπόψιν ως πραγματικού χρόνου. Η συμπερίληψη της δικής του βιβλιοθήκης συναρτήσεων λειτουργίας το κάνει ιδιαίτερα εύχρηστο για την διαχείριση του κατά την κατασκευή του firmware. Τέλος οι απαιτήσεις της σε ενέργεια για την σταθερή λειτουργία της είναι αρκετά χαμηλές ώστε να μπορεί με ευκολία μία μικρή πηγή ενέργειας όπως ένα power bank να παρέχει αυτονομία για τρεις με τέσσερις ώρες.

Ως συσκευή είναι εύκολα προσαρμόσιμη ώστε να μπορεί να προσαρμοστεί σε κάθε τύπου πλακέτα βακελίτη και να γίνει μέρος ενός ενσωματωμένου συστήματος καθώς οι δυνατότητες του είναι εξαιρετικά ωφέλιμες.

1.5 Συστήματα Μικροελεγκτών

Στον τομέα της αυτοματοποίησης και ολοκληρωμένων ηλεκτρονικών κυκλωμάτων ένα από τα μεγαλύτερα βοηθήματα στην διάθεση ενός ηλεκτρονικού μηχανικού είναι το σύστημα μικροελεγκτή το οποίο αφορά μία ηλεκτρονική τυπωμένη πλακέτα βακελίτη η οποία φέρει έναν μικροελεγκτή και έναν ελάχιστο αριθμό ηλεκτρονικών διατάξεων σχεδιασμένες ώστε να παρέχουν έναν ελάχιστο αριθμό παροχών και δυνατοτήτων τόσο στο επίπεδο διαχείρισης του μικροελεγκτή σχετικά με τις εισόδους/εξόδους του ή τις επί της πλακέτας διατάξεις όσο και προς το ανθρώπινο στοιχείο που επιθυμεί να το προσαρμόσει σε εφαρμογές πραγματικού κόσμου. Στην ενότητα αυτήν θα αναλυθεί το αντικείμενο αυτό ως προς το υλικό του, θα επεξηγηθεί η λειτουργία του και ο ρόλος του στο σύνολο της παρούσας εργασίας.

1.5.1 Μικροελεγκτές

Η μονάδα μικροελεγκτή (Micro Controller Unit - MCU) είναι μία συσκευή που αναπτύχθηκε την ίδια εποχή με τον μικροεπεξεργαστή με την ανακάλυψη της τεχνολογίας Ημιαγωγών – Μετάλλου – Οξειδίου (Metal – Oxide – Semiconductors, MOS) και έχει την δυνατότητα να μπορεί να διεξάγει διάφορες διεργασίες σε έναν καλό βαθμό αυτονομίας και αυτοματισμού [6]. Η συσκευή αυτή παρέχεται σε μορφή ολοκληρωμένου κυκλώματος σε διάφορες μορφές συσκευασίας σύμφωνα πάντα με τα παγκόσμια πρότυπα DIP, SOP/SOIC/SO, QFP, QFN/LCC, BGA και CSP έτσι ώστε να μπορεί να προσαρμοστεί με ευκολία σε τυπωμένη πλακέτα βακελίτη, σε βάση ολοκληρωμένου κυκλώματος, σε ράστερ ή σε διάτρητη πλακέτα βακελίτη ανάλογα με τον τύπο της συσκευασίας του. Η κύρια διαφορά ενός μικροελεγκτή και ενός μικροεπεξεργαστή είναι πως ο μικροελεγκτής όπως προαναφέρθηκε είναι ένα πλήρες υπολογιστικό σύστημα περιορισμένων δυνατοτήτων, ενώ ο μικροεπεξεργαστής είναι ένα σύστημα αριθμομηχανής σε μορφή ολοκληρωμένου κυκλώματος (Intergraded Circuit, IC) το οποίο διαβάζει, επεξεργάζεται και παράγει αριθμούς στις θύρες εισόδων/εξόδων του.

Επί της ουσίας είναι ένα ολοκληρωμένο υπολογιστικό σύστημα ικανό να διαχειριστεί έναν ορισμένο αριθμό περιφερειακών συσκευών καθώς διαθέτει μεταξύ άλλων έναν ελάχιστο αριθμό θυρών οι οποίες λειτουργούν ως είσοδοι/έξοδοι αναλόγως το πρόγραμμα του. Συγκεκριμένα στην δομή της κατασκευής

του περιέχεται ένας (τουλάχιστον) μικροεπεξεργαστής, μνήμες RAM και FLASH, ένας ταλαντωτής κρύσταλλος για την παροχή συχνότητας ρολογιού και θύρες εισόδων/εξόδων. Συνήθως απαιτείται από τον σχεδιαστή που θα τον χρησιμοποιήσει και εφαρμόσει στο σύστημα που σχεδιάζει να φροντίσει για την δημιουργία ή να γράψει ο ίδιος το πρόγραμμα που θα γραφτεί στην μνήμη του μικροελεγκτή το οποίο θα οδηγεί τις διάφορες ενέργειες που θα θέλει σύμφωνα με τον σχεδιασμό να εκτελεί το σύστημα του μικροελεγκτή. Το πρόγραμμα που γράφεται συγκεκριμένα για έναν μικροελεγκτή ονομάζεται firmware (Υλικολογισμικό) και θα αναλυθεί σε επόμενη ενότητα. Πολλοί σύγχρονοι μικροελεγκτές κατασκευάζονται πλέον έτσι που οι διαθέσιμοι πόροι τους να επιτρέπουν με κάποιες ρυθμίσεις και τροποποιήσεις σε προγράμματα οδηγών να μπορούν να διαθέτουν για την λειτουργία τους λειτουργικό σύστημα (Operating System, OS).

Υπάρχουν αρκετές εταιρίες που ειδικεύονται στην κατασκευή και παραγωγή ολοκληρωμένων κυκλωμάτων μικροελεγκτών με αποτέλεσμα να υπάρχει μεγάλη ποικιλία σε μικροελεγκτές με ιδιαίτερα σχεδιαστικά χαρακτηριστικά και δυνατότητες ώστε να υπάρχει η δυνατότητα από πλευράς μηχανικού ή γενικά του ανθρώπινου στοιχείου να επιλέξει με αρκετά υψηλή προσέγγιση την συσκευή μικροελεγκτή που ταιριάζει καλύτερα στον σχεδιασμό του. Ανάλογα το κόστος στο οποίο θέλει κανείς να επενδύσει για την επιλογή του μικροελεγκτή που θα καταλήξει στην εφαρμογή του, ο μικροελεγκτής μπορεί να είναι μιας εγγραφής ή επανεγγραφόμενος. Προφανώς ο μίας εγγραφής προκύπτει οικονομικότερος του επανεγγραφόμενου αλλά αν γραφτεί μία φορά το υλικολογισμικό στην μνήμη του η διαδικασία είναι μη αναστρέψιμη. Σε κάθε περίπτωση όταν ένας μηχανικός επιλέγει να ασχοληθεί με συσκευές μικροελεγκτών, προκειμένου να μπορέσει να τους προγραμματίσει είναι απαραίτητο να προμηθευτεί αφενός το λογισμικό της εταιρείας που κατασκευάζει τον μικροελεγκτή στο οποίο θα γράψει το υλικολογισμικό που θα τρέχει ο μικροελεγκτής, και αφετέρου την συσκευή που θα μετατρέπει το υλικολογισμικό από κείμενο οποιασδήποτε γλώσσας προγραμματισμού από αυτές που υποστηρίζει σε γλώσσα μηχανής και θα το γράφει στην μνήμη του μικροελεγκτή. Τέλος η ευχρηστία τους είναι τόσο υψηλή που πλέον συμπεριλαμβάνονται σε κάθε ηλεκτρονική συσκευή καθώς η παροχή λειτουργιών και ελέγχου που παρέχουν σε σχέση με το κόστος της συμπερίληψης τους είναι τέτοια που υπερκαλύπτει την διαφορά με πολλαπλάσιο συντελεστή καθώς σαφέστατα προσφέρουν υψηλή αναβάθμιση στα προϊόντα που συμπεριλαμβάνονται ως συσκευές.

Συγκεκριμένα ως συσκευή, παρόλο που ενδεικνύεται για διαχείριση αναλογικών σημάτων, από κατασκευής ο τρόπος διαχείρισης όλων των σημάτων στις θύρες εισόδων/εξόδων του είναι ψηφιακής λογικής. Οι περισσότεροι είναι σχεδιασμένοι να διαχειρίζονται τα σήματα στην λογική υψηλής στάθμης ή χαμηλής στάθμης όπου αντιπροσωπεύονται με μία διαφορά δυναμικού αντίστοιχα με 5V διαφορά δυναμικού τάσης για υψηλής στάθμης ή αλλιώς λογικό 1 και με 0V διαφορά δυναμικού τάσης για χαμηλής στάθμης ή αλλιώς λογικό 0. Οι πιο σύγχρονες συσκευές μικροελεγκτών λειτουργούν διαφορετικά έχοντας ορίσει για όριο την υψηλή στάθμη ίσο με 3,3V αλλά η λογική παραμένει η ίδια. Το κύριο πλεονέκτημα αυτής της επιλογής της ψηφιακής λειτουργίας είναι πως μειώνει την πιθανότητα σφάλματος κατά την μετάδοση της πληροφορίας των δεδομένων.

1.5.2 Βοηθητικές Ηλεκτρονικές Διατάξεις

Παρόλο που είναι αδιαμφισβήτητη η υπεροχή και οι δυνατότητες που μπορεί να παρέχει ένας μικροελεγκτής, αν δεν είναι συνδεσμολογημένος με τις κατάλληλες ηλεκτρονικές διατάξεις που θα συνθέτουν το συνδεσμολογικό μέρος του, δεν μπορεί να κάνει ουσιαστικά απολύτως τίποτα γιατί τόσο τα σήματα που παράγονται στους ακροδέκτες του, ακόμη και το να τροφοδοτηθεί κατάλληλα ώστε να μπορεί να λειτουργήσει σαν συσκευή είναι ενέργειες ανώφελες χωρίς τις κατάλληλες ηλεκτρονικές διατάξεις που θα παρέχουν αυτές τις δυνατότητες. Αυτό οφείλεται στο γεγονός ότι ένας μικροελεγκτής

σαν συσκευή, προκειμένου να επικοινωνήσει διαθέτει έναν ορισμένο αριθμό ακροδεκτών σύμφωνα με τον σχεδιασμό της κατασκευής του μέσω τον οποίων διαχειρίζεται τα σήματα που θα λάβει ή που θα παραγάγει.

Οι ηλεκτρονικές διατάξεις είναι κυκλώματα αποτελούμενα από ένα σύνολο ηλεκτρονικών στοιχείων όπως αντιστάσεων/πυκνωτών/πηνίων, διόδων/τρανζίστορ, ακόμη και ολοκληρωμένων κυκλωμάτων τα οποία έχουν σχεδιαστεί έτσι ώστε να είναι διαχειρίσιμα από τον μικροελεγκτή όταν αυτά θα είναι συνδεδεμένα με αυτόν. Ο σχεδιασμός τους προκύπτει από εξειδικευμένους μηχανικούς του αντικειμένου οι οποίοι θα καθορίσουν την γενική επιθυμητή λειτουργία του προς σχεδιασμού συστήματος, έπειτα θα διαχωρίσουν σε γενικά σύνολα τις διατάξεις ώστε να σχεδιαστούν λεπτομερώς, θα ακολουθήσει η δημιουργία προτύπων ώστε να δοκιμαστούν οι διατάξεις ως προς την επιθυμητή ανταπόκριση των λειτουργιών τους και τέλος, αναλόγως των αποτελεσμάτων θα προκύψει το τελικό σύστημα που θα είναι η σύνθεση μικροελεγκτή με βοηθητικές ηλεκτρονικές διατάξεις.

Γενικότερα το σύνολο των ηλεκτρονικών διατάξεων που περιβάλλουν έναν μικροελεγκτή αποτελούν τα όργανα του μικροελεγκτή με τα οποία του παρέχεται η δυνατότητα να επικοινωνεί, να αντιλαμβάνεται και να αλληλοεπιδρά με το περιβάλλον που τον περιβάλλει αναλόγως την διαχείριση τους. Όταν ένας μικροελεγκτής συνδεθεί με τις ηλεκτρονικές διατάξεις που θα ελέγχει προκειμένου να έχει την δυνατότητα να διαχειρίζεται είτε σήματα είτε το περιβάλλον γύρω του τότε πλέον το σύνολο των ηλεκτρονικών διατάξεων και του μικροελεγκτή ονομάζεται “σύστημα μικροελεγκτή”.

1.5.3 Συστήματα Μικροελεγκτών

Τα συστήματα μικροελεγκτών είναι το σύνολο ενός μικροελεγκτή με το ολοκληρωμένο σύνολο των διάφορων ηλεκτρονικών διατάξεων που χρησιμοποιεί ο μικροελεγκτής για έλεγχο, αντίληψη και διαμόρφωση του περιβάλλοντος του. Η ευχρηστία τους έγινε πολύ γρήγορα αντιληπτή από την κοινότητα των μηχανικών και ενσωματώθηκαν σε όλες τις ηλεκτρονικές και ηλεκτρικές εφαρμογές σε όλους τους τομείς καθώς από σχεδιασμού έχουν την δυνατότητα να ενσωματώνονται εύκολα και να αυτοματοποιούν ένα μεγάλο σύνολο λειτουργιών ώστε να διευκολύνουν τον χρήστη ως προς τις ενέργειες του στον μέγιστο δυνατό βαθμό απλούστευσης της χρήσης των διάφορων ηλεκτρικών και/ή ηλεκτρονικών συσκευών. Ένα από τα πιο σημαντικά πλεονεκτήματα που παρέχει ένα ολοκληρωμένο σύστημα μικροελεγκτή είναι πως περιλαμβάνει μία ηλεκτρονική διάταξη που επιτρέπει την μετατροπή ενός υλικολογισμικού που γράφτηκε σε γλώσσα προγραμματισμού που υποστηρίζει σε γλώσσα μηχανής και την εγγραφή του στην μνήμη του μικροελεγκτή. Η διάταξη αυτή ονομάζεται boot loader και διευκολύνει σε μεγάλο βαθμό το ανθρώπινο στοιχείο στο ζήτημα του λογισμικού μέρους του ενσωματωμένου συστήματος το οποίο θα περιγραφεί αναλυτικά σε επόμενη ενότητα.

Τα συστήματα μικροελεγκτών διακρίνονται σε δύο κύριες κατηγορίες. Η πρώτη αφορά αυτά που είναι μόνιμο μέρος των ηλεκτρονικών πλακετών βακελίτη στις συσκευές τις οποίες διαχειρίζονται. Η δεύτερη αφορά αυτόνομες ηλεκτρονικές πλακέτες βακελίτη οι οποίες μέσω των θυρών εισόδων/εξόδων που διαθέτουν μπορούν να χρησιμοποιηθούν επανειλημμένα ως μέρος διάφορων ηλεκτρικών και/ή ηλεκτρονικών συσκευών και είναι αποσπώμενο τμήμα σε σχέση με τις υπόλοιπες διατάξεις.

Μία πλήρη διάταξη συστήματος μικροελεγκτή που είναι ενσωματωμένη στην κύρια ηλεκτρονική πλακέτα βακελίτη μιας ηλεκτρικής ή/και ηλεκτρονικής συσκευής έχει σαφώς κάποια πλεονεκτήματα και μειονεκτήματα συγκριτικά με αυτές που ανήκουν στην κατηγορία των αποσπώμενων συστημάτων μικροελεγκτή όπου ορισμένα από τα κυριότερα θα αναφερθούν στην παρούσα εργασία. Επειδή είναι σχεδιασμένα στο σύνολο της κύριας ηλεκτρονικής πλακέτας βακελίτη απλοποιείται αυτομάτως το σύνολο του σχεδιασμού λόγω των απευθείας αγωγών χωρίς να χρειάζονται ενδιάμεσα σημεία επαφής

ελαττώνοντας την πιθανότητα σφάλματος ή κάποιου καταστροφικού γεγονότος λόγω κακής επαφής στο σημείο της ένωσης. Είναι καλύτερα διαχειρίσιμο το σύστημα μικροελεγκτή τόσο χωροταξικά στην κύρια πλακέτα κατά την διαδικασία σχεδιασμού από τον μηχανικό, όσο και από ογκομετρική άποψη στο τελικό προϊόν καθώς τα στοιχεία που το αποτελούν δεν είναι απαραίτητο να είναι όλα συγκεντρωμένα στο ίδιο μέρος της πλακέτας γεγονός που προσδίδει ευελιξία και ελευθερία στις επιλογές σχεδιασμού από πλευράς του μηχανικού.

Στην περίπτωση που ένα σύστημα μικροελεγκτή σχεδιαστεί έτσι ώστε να είναι αποσπώμενο από την κύρια ηλεκτρονική πλακέτα βακελίτη του προσδίδονται κάποια χαρακτηριστικά που συχνά το καθιστούν ως την καλύτερη δυνατή επιλογή για τον τελικό σχεδιασμό του προϊόντος. Ένας από τους πιο καλούς λόγους είναι πως κατά την διάρκεια της διαδικασίας αναζήτησης μιας βλάβης από έναν μηχανικό δοκιμής και επιβεβαίωσης (Test and Validation Engineer) είναι δυνατόν να αφαιρέσει την ύποπτη πλακέτα με ευκολία ώστε να καθορίσει αν είναι το αίτιο της βλάβης, εξοικονομώντας του πολύτιμο χρόνο. Ένας άλλος λόγος προτίμησης αυτού του σχεδιασμού είναι η δυνατότητα αντικατάστασης της πλακέτας με μία πιο σύγχρονη για τις ανάγκες αναβάθμισης της επίδοσης και λειτουργίας ολόκληρου του συστήματος ή/και της συσκευής ως σύνολο. Τα υπολογιστικά συστήματα συγκεκριμένα αποτελούν καλό παράδειγμα ευνοώντας την επιλογή αποσπώμενων ηλεκτρονικών πλακετών βακελίτη διότι κάνουν πολύ περισσότερη χρήση αντικατάστασης τους για λόγους βλάβης ή αναβάθμισης ολόκληρων των συστημάτων.

Στο ζήτημα των συστημάτων μικροελεγκτών που είναι διαθέσιμα στο εμπόριο υπάρχουν ήδη αρκετές εταιρείες που παρέχουν στο αγοραστικό κοινό έτοιμες λύσεις τόσο στο υλικό μέρος όσο και στο λογισμικό με μία από τις ηγετικές και πιο γνωστές στο ευρύ αγοραστικό κοινό να είναι η Arduino. Οι εταιρείες αυτές κατάφεραν να σχεδιάσουν τα συστήματα μικροελεγκτών με τέτοιο τρόπο ώστε να μπορούν άτομα με ελάχιστη εξειδίκευση στο αντικείμενο να μπορούν να ασχοληθούν με σχετική ευκολία τόσο στην πρακτική εφαρμογή του υλικού μέρους όσο και στο λογισμικό μέρος για την κατασκευή υλικολογισμικών λειτουργίας των συστημάτων μικροελεγκτών καθώς πολλές εταιρείες παρέχουν ακόμη και το περιβάλλον ανάπτυξης προγραμμάτων. Το IDE της εταιρείας Arduino για παράδειγμα είναι τόσο εύχρηστο που περιλαμβάνει στις βιβλιοθήκες πρωτοκόλλων επικοινωνιών των διάφορων συστημάτων μικροελεγκτών και πλακέτες από άλλες εταιρείες κατασκευής συστημάτων μικροελεγκτών όπως της εταιρείας ESP32. Επίσης περιλαμβάνει και πολλές βιβλιοθήκες συναρτήσεων για την διαχείριση συγκεκριμένων προγραμμάτων το οποίο θα αποσαφηνιστεί σε επόμενη ενότητα.

Μία έτοιμη και ολοκληρωμένη λύση που προσφέρεται στο εμπόριο για χρήση των μηχανικών αλλά ακόμη και τεχνικών είναι ο προγραμματιζόμενος λογικός ελεγκτής (Programmable Logic Controller, PLC). Πρόκειται για μία συσκευή που περιέχει ένα σύστημα μικροελεγκτή μέσα σε μία ανθεκτική θήκη η οποία παρέχει εξωτερικά σημεία σύνδεσης για την τροφοδοσία της αλλά και την επικοινωνία των θυρών εισόδων/εξόδων της. Πολλά μοντέλα αυτών των συσκευών φέρουν οθόνη και κουμπιά ως μέσο διεπαφής με το ανθρώπινο στοιχείο. Ο τρόπος προγραμματισμού είναι συγκεκριμένος αλλά έχει ποικιλομορφία καθώς υποστηρίζουν και κάποιες ψευδογλώσσες για διευκόλυνση του προγραμματισμού τους οι οποίες αναφορικά είναι η Ladder Diagram (LD), η Sequential Function Charts (SFC), η Function Block Diagram (FBD), η Structured Text (ST) και η Instruction List (IL). Πάραυτα είναι εφικτό να προγραμματιστούν και με γλώσσα προγραμματισμού, εφόσον την παρέχει ο κατασκευαστής, με χρήση ηλεκτρονικού υπολογιστή.

Για τις ανάγκες υλοποίησης της παρούσας εργασίας επιλέχτηκε ένα τέτοιο εμπορικό σύστημα μικροελεγκτή, συγκεκριμένα αυτό της εταιρείας ESP32 μοντέλο LOIN32 το οποίο παρέχει στις δυνατότητες του ενσωματωμένη κεραία, θύρα USB, εξωτερική τροφοδοσία, επικοινωνία πρωτοκόλλου

TX/RX, 36 ακροδέκτες από τους οποίους 5 είναι για την γείωση, 2 είναι για παροχή 3,3V, 2 είναι για παροχή 5V, και οι υπόλοιποι αφορούν θύρες εισόδων/εξόδων σημάτων. Στο δεύτερο κεφάλαιο που αφορά την υλοποίηση και κατασκευή του πρακτικού μέρους της εργασίας θα περιγραφεί αναλυτικά η εφαρμογή και ενσωμάτωση του συστήματος μικροελεγκτή στο σύνολο της κατασκευής [9].

1.6 Περιφερειακές Συσκευές

Οι περιφερειακές συσκευές αποτελούν ένα σπουδαίο κομμάτι των υπολογιστικών συστημάτων κάθε τύπου καθώς πρόκειται για μηχανήματα που κατασκευάστηκαν για συγκεκριμένες εργασίες και ταυτόχρονα να είναι απόλυτα ελεγχόμενες από το υπολογιστικό σύστημα. Τέτοιες συσκευές είναι ο εκτυπωτής, το ποντίκι και το πληκτρολόγιο που συναντά κανείς στην καθημερινότητα του ως τυπικά περιφερειακά του οικιακού υπολογιστικού συστήματος του.

Όταν το υπολογιστικό σύστημα είναι ένα σύστημα μικροελεγκτή οι περιφερειακές συσκευές έχουν μεγαλύτερο εύρος ποικιλιών και λειτουργιών διότι για τις ανάγκες του κάθε συστήματος μπορεί το σύνολο των περιφερειακών συσκευών να αποτελείται από συστοιχίες αισθητηρίων, ενδείκτες που μπορεί να είναι απλά στοιχεία LED, τύπου Seven Segment και οθόνες, κινητικά στοιχεία όπως ηλεκτροκινητήρες ακριβείας ή σερβοκινητήρες (servos) και διάφορες ηλεκτρονικές συσκευές όπως ένα GPS.

Πολλές συσκευές που μπορούν να ελεγχθούν από ένα σύστημα μικροελεγκτή εξυπηρετούν εξειδικευμένες λειτουργίες όπως ο δέκτης GPS. Αποτελεί ως συσκευή μία ανεξάρτητη, ολοκληρωμένη και αυτόνομη μονάδα η οποία απαιτεί μόνο τροφοδοσία προκειμένου να λειτουργήσει. Παρόλα αυτά δίνεται η δυνατότητα να ενσωματωθεί και να ελεγχθεί από ένα σύστημα μικροελεγκτή σαν περιφερειακή συσκευή για τις ανάγκες ενός ενσωματωμένου συστήματος. Η δυνατότητα αυτή είναι που το καθιστά κατάλληλο ως συσκευή για την συμπερίληψη του σε ένα σύστημα μικροελεγκτή για τον σχηματισμό ενός ενσωματωμένου συστήματος.

1.7 Λογισμικό

Το λογισμικό αποτελεί το έτερον ήμισυ του συνόλου του ενσωματωμένου συστήματος. Είναι απαραίτητο για να μπορέσει αυτό να λειτουργήσει έτσι ώστε να μπορεί να εκτελέσει ένα σύνολο λειτουργιών σύμφωνα με τον σχεδιασμό της εργασίας. Στην περίπτωση της παρούσας εργασίας και για τις ανάγκες λειτουργίας του ενσωματωμένου συστήματος είναι απαραίτητη η δημιουργία ενός firmware (υλικολογισμικού) και προκειμένου να πραγματοποιηθεί αυτό θα πρέπει πρώτα να αναπτυχθεί το software (λογισμικό) στο οποίο και θα βασιστεί. Ο λόγος για τον οποίο συμβαίνει αυτό είναι γιατί το λογισμικό έχει λιγότερους περιορισμούς σε παραμέτρους που πρέπει να ληφθούν υπόψιν επιτρέποντας έτσι στον προγραμματιστή μεγαλύτερα περιθώρια κινήσεων και ελευθερία στην ανάπτυξη του κώδικα ώστε αυτός να λειτουργήσει σύμφωνα με τα απαιτούμενα ζητούμενα. Με την επιτυχή υλοποίηση του δύναται έπειτα η βελτιστοποίηση του αναλόγως τις γνώσεις και δυνατότητες του μηχανικού.

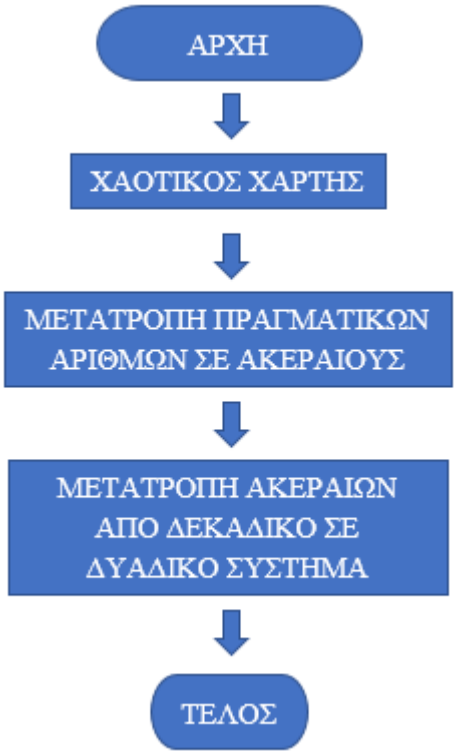
1.7.1 Software και Firmware

Το λογισμικό έχει εδραιωθεί γενικότερα να συμπεριλαμβάνει στην έννοια του οτιδήποτε αφορά ένα σε κώδικα προγράμματος σε οποιαδήποτε γλώσσα προγραμματισμού. Στην πράξη ως λογισμικό εννοείτε η οδηγία που δίνεται προς το υλικό ώστε αυτό να μπορέσει να λειτουργήσει με συγκεκριμένο και επιθυμητό τρόπο. Για τις ανάγκες υλοποίησης της παρούσας εργασίας το αρχικό λογισμικό λειτουργίας της θα γραφτεί σε ένα IDE ώστε να δοκιμαστούν πλήρως τα μέρη του ως προς την λειτουργία τους και

να συντεθούν σε ένα ενιαίο πρόγραμμα ώστε να δοκιμαστεί σαν ενιαία οντότητα για να διαπιστωθεί η σωστή λειτουργία του.

Το Firmware είναι μία ειδική κατηγορία λογισμικού που αναφέρεται στα προγράμματα που γράφονται ώστε να λειτουργούν και να διαχειρίζονται συγκεκριμένα μικροελεγκτές. Η ονομασία προκύπτει από την σύνθεση δύο Αγγλικών λέξεων, την firm που σημαίνει εφαρμοστό και την ware που σημαίνει προϊόν περιγράφοντας έτσι την ανάπτυξη ενός συγκεκριμένου τύπου προγράμματος που ονομάζεται υλικολογισμικό και που πρέπει να γραφτεί με τέτοιον τρόπο ώστε να μην ξεπερνά τους περιορισμούς του υλικού μέρους του μικροελεγκτή.

Αφού ολοκληρωθεί το λογισμικό σε μία αρχική μορφή και διακριβωθεί η ορθή λειτουργία του, αυτό θα πρέπει να τροποποιηθεί κατάλληλα ώστε να λειτουργήσει στα πλαίσια ενός μικροελεγκτή. Στην τελική του μορφή το υλικολογισμικό θα αποτελείται από την σύνθεση τριών αλγορίθμων σε έναν ενιαίο. Ο πρώτος θα παρασκευάζει το κλειδί κρυπτογράφησης και σχεδιάστηκε με βάση το διάγραμμα ροής που απεικονίζεται στο σχήμα 1.1.



Σχήμα 1-1: Διάγραμμα ροής κατασκευής κλειδιού κρυπτογράφησης

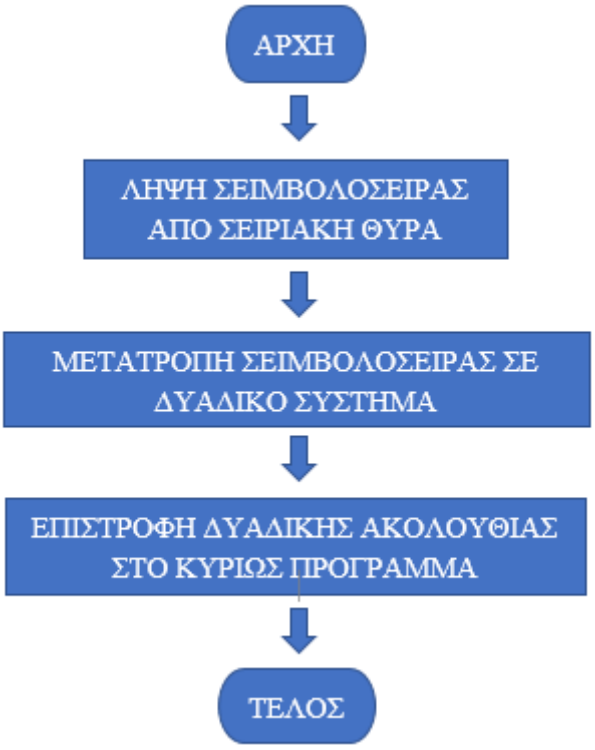
Όπου αρχικά παραμετροποιούνται οι αρχικές συνθήκες του χαοτικού χάρτη σύμφωνα με την επιλογή της κατάστασης λειτουργίας του ώστε να παραγάγει έναν τυχαίο πραγματικό αριθμό ο οποίος θα μετατραπεί σε ακέραιο μέσω μεθόδου στρογγυλοποίησης και τέλος θα γίνει μετατροπή του ακεραίου από το δεκαδικό σύστημα στο δυαδικό τελώντας μία λογική πράξη το αποτέλεσμα της οποίας θα αποδίδεται μεταξύ των λογικών αποτελεσμάτων **TRUE (1)** ή **FALSE(0)**. Αναλόγως το επιθυμητό μέγεθος του κλειδιού κρυπτογράφησης σε bit θα πρέπει να επαναληφθεί ο αλγόριθμος ισάριθμα ώστε να ληφθεί ο επιθυμητός αριθμός των bit που θα σχηματίζει σε σειρά μία ανάλογη ακολουθία bit.

Το σύνολο των ανωτέρω λειτουργιών και διαδικασιών ονομάζεται Γεννήτρια Ψευδοτυχαίων Αριθμών Bit (Pseudo Random Bit Generator - **PRBG**) και σε μελλοντικά διαγράμματα ροής για το υπόλοιπο της

παρούσας εργασίας το παραπάνω διάγραμμα ροής θα συνοψίζεται σε ένα μόνο κουτί με το όνομα **PRBG**.

Η σύντμηση των στοιχείων ενός αλγόριθμου σε ένα νέο στοιχείο είναι μία πρακτική που εφαρμόζεται για λόγους διευκόλυνσης και απλοποίησης κατά τον σχεδιασμό μελλοντικών διαγραμμάτων ροής καθώς χωρίς αυτήν την πρακτική θα μπορούσε το μέγεθος ενός εικονιζόμενου αλγόριθμου να γίνει τόσο μεγάλο ώστε αυτός να εκτείνεται σε μήκος αρκετών σελίδων και να μην είναι πλέον δυνατή η πλήρης μακροσκοπική απεικόνιση του σε μία οθόνη με αποτέλεσμα την αύξηση της πιθανότητας να παραληφθεί κάποιο σημαντικό στοιχείο του. Για όλα τα παραπάνω επινοήθηκε αυτή η πρακτική με την οποία μπορεί κανείς όταν επιθυμεί να δει αναλυτικά το περιεχόμενο του κουτιού που τον ενδιαφέρει να ανατρέξει στην σελίδα στην οποία εντοπίζεται το περιεχόμενο του ώστε να το εξετάσει μεμονωμένα. Τέτοιες πρακτικές είναι ιδιαίτερα επιθυμητές να εφαρμόζονται από πλευράς του μηχανικού καθώς έχουν ως απώτερο αποτέλεσμα έναν πρακτικό, κομψό και κυρίως λειτουργικό σχεδιασμό που βελτιστοποιεί το περιεχόμενο μιας μελέτης και κατ' επέκταση την μετέπειτα κατασκευή η οποία θα βασιστεί σε αυτήν.

Ο δεύτερος αλγόριθμος θα είναι αυτός της συνάρτησης μετατροπής τύπου χαρακτήρων από συμβολοσειρά στο δυαδικό αριθμητικό σύστημα και περιγράφεται στο διάγραμμα ροής που απεικονίζεται στο σχήμα 1.2.



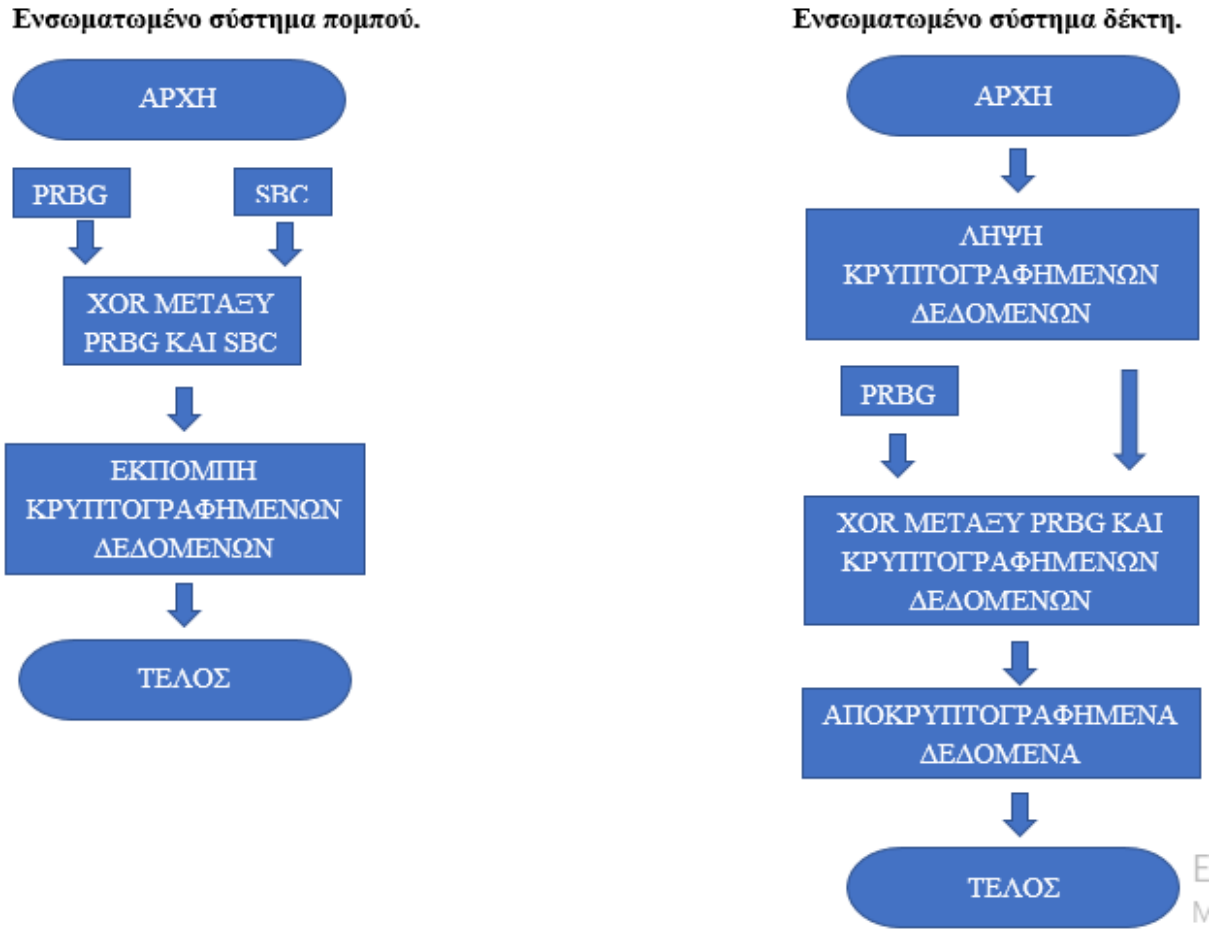
Σχήμα 1-2:Διάγραμμα ροής μετατροπής τύπων χαρακτήρων σε δυαδικό αριθμητικό σύστημα.

Στην σειριακή θύρα του συστήματος μικροελεγκτή λαμβάνονται τα δεδομένα που προέρχονται από την συσκευή GPS τα οποία είναι της μορφής συμβολοσειράς και θα μετατραπούν από κάθε χαρακτήρες τύπου character της συμβολοσειράς στην αντίστοιχη δυαδική μορφή τους ένα προς ένα και στην ίδια σειρά με την οποία λήφθηκαν. Η μετατροπή τους θα ανταποκρίνεται στην τιμή **ASCII** του κάθε χαρακτήρα η οποία θα είναι η αντίστοιχη του δυαδικού αριθμητικού συστήματος. Η κωδικοποίηση ASCII χρησιμοποιείται κατά κόρον από πολλούς μηχανικούς στον σχεδιασμό και την ανάπτυξη πολλών προγραμμάτων. Επί της ουσίας αποδίδει για κάθε χαρακτήρα του πληκτρολογίου μία αντίστοιχη τιμή

στο δεκαεξαδικό σύστημα αρίθμησης η οποία εφόσον είναι γνωστή στον προγραμματιστή μπορεί να την διαχειριστεί μέσα στο πρόγραμμα όπως θεωρεί αυτός καταλληλότερα. Με την ανάπτυξη των κατάλληλων συναρτήσεων δύναται να εισάγει την αρχική τιμή του χαρακτήρα ενδιαφέροντος και να μετατρέπεται από αυτήν στην αντίστοιχη τιμή του σε ένα άλλο αριθμητικό σύστημα όπως το δεκαδικό ή το δυαδικό. Για παράδειγμα, ο χαρακτήρας **'A'** του οποίου η αντιστοιχία σε κώδικα **ASCII** είναι ο δεκαδικού αριθμητικού συστήματος αριθμός **65** τότε ο αντίστοιχος αριθμός στο δυαδικό αριθμητικό σύστημα θα είναι ο αριθμός **1000001** και ο χαρακτήρας **'B'** του οποίου η αντιστοιχία σε κώδικα **ASCII** είναι ο δεκαδικού αριθμητικού συστήματος αριθμός **66** τότε ο αντίστοιχος αριθμός στο δυαδικό αριθμητικό σύστημα θα είναι ο αριθμός **1000010**.

Το σύνολο των ανωτέρω λειτουργιών και διαδικασιών ονομάζεται Μετατροπή Συμβολοσειράς σε Δυαδικό (String to Binary Converter - **SBC**) και σε μελλοντικά διαγράμματα ροής για το υπόλοιπο της παρούσας εργασίας το παραπάνω διάγραμμα ροής θα συνοψίζεται σε ένα μόνο κουτί με το όνομα **SBC** το οποίο θα εννοείται πως θα περιλαμβάνει το σύνολο του και πως θα μετατρέπει μία συμβολοσειρά στον αντίστοιχο δυαδικό αριθμό της ορισμένου και αμετάβλητου εύρους σύμφωνα με τις παραμέτρους που θα τις έχουν δοθεί.

Το διάγραμμα ροής του σχήματος 1.3 απεικονίζει τους δύο αλγόριθμους που θα εκτελούνται συγχρόνως στα δύο ενσωματωμένα συστήματα του εκπομπού και του δέκτη.



Σχήμα 1-3: Διάγραμμα ροής κρυπτογράφησης/αποκρυπτογράφησης σε συσκευές ενσωματωμένου συστήματος.

Όπου γίνεται άμεσα αντιληπτή η αναγκαιότητα ύπαρξης δύο προγραμμάτων καθώς χρειάζεται να εκτελείται ένας συγκεκριμένος αλγόριθμος στο ενσωματωμένο σύστημα που κρυπτογραφεί και εκπέμπει τα δεδομένα του GPS και ένας συγκεκριμένος αλγόριθμος στο ενσωματωμένο σύστημα που λαμβάνει και αποκρυπτογραφεί τα δεδομένα του GPS. Συγκεκριμένα στο ενσωματωμένο σύστημα που κρυπτογραφεί και εκπέμπει τα δεδομένα του GPS διακρίνονται τα κουτιά με τις ονομασίες PRBG και SBC των οποίων το περιεχόμενο τελεί την λογική πράξη XOR μεταξύ τους και έπειτα μεταδίδονται ως κρυπτογραφημένα δεδομένα από το σύστημα ασύρματης μετάδοσης του ενσωματωμένου στον χώρο. Αντίστοιχα στο ενσωματωμένο σύστημα που λαμβάνει και αποκρυπτογραφεί διακρίνεται το κουτί που συμβολίζει το σύστημα του δέκτη το οποίο λαμβάνει τα κρυπτογραφημένα δεδομένα από τον χώρο και τα μεταφέρει στο κύριο πρόγραμμα το οποίο με την σειρά του θα καλέσει την PRBG συνάρτηση ώστε να διακρίνει από τα κρυπτογραφημένα δεδομένα τα δεδομένα του GPS και το κλειδί κρυπτογράφησης. Έπειτα επιστρέφει στο κυρίως πρόγραμμα τα αποκρυπτογραφημένα δεδομένα του GPS.

Το σύνολο των ανωτέρω λειτουργιών και διαδικασιών διακρίνεται σε δύο διακριτές διαδικασίες όπου η μία ονομάζεται Κρυπτογράφηση και Εκπομπή Δεδομένων (Data Encryption and Transmission - **DET**) και η δεύτερη ονομάζεται Λήψη και Αποκρυπτογράφηση Δεδομένων (Data Reception and Decryption - **DRD**) και σε μελλοντικά διαγράμματα ροής για το υπόλοιπο της παρούσας εργασίας τα παραπάνω διαγράμματα ροής θα συνοψίζονται το κάθε ένα σε ένα μόνο κουτί με τα ονόματα **DET** και **DRD** τα οποία θα εννοείται πως θα περιλαμβάνουν το σύνολο τους όπως αυτό παρουσιάστηκε και πως το κάθε ένα θα εκπέμπει κρυπτογραφημένα δεδομένα και θα αποδίδει αποκρυπτογραφημένα δεδομένα αντίστοιχα.

1.8 Μη Επανδρωμένο Αεροσκάφος

Προερχόμενα από τον χώρο των τηλεκατευθυνόμενων οχημάτων τα μη επανδρωμένα αεροσκάφη διαφέρουν από ένα τηλεκατευθυνόμενο με τον ανώτερο τεχνολογικά εξοπλισμό που φέρουν που τα επιτρέπει να εκτελούν ενέργειες ανώτερης περιπλοκότητας σε σχέση με ένα τηλεκατευθυνόμενο. Αυτός είναι ένας από τους λόγους που τα τελευταία χρόνια έχουν γίνει το επίκεντρο του ενδιαφέροντος σε μαζικό επίπεδο από χομπίστες το υπόβαθρο των οποίων κυμαίνεται μεταξύ καθαρής ψυχαγωγίας και μηχανικών που θέλουν να δοκιμάσουν και να επεκτείνουν τα όρια των δυνατοτήτων των μη επανδρωμένων αεροσκαφών. Το κύριο χαρακτηριστικό τους είναι ότι δεν απαιτείται πιλότος στο σκάφος αν και απαιτείται η ύπαρξη επίγειου χειριστή ο οποίος πρέπει να επιτηρεί την λειτουργία του και αν κριθεί απαραίτητο να επέμβει στην λειτουργία του.

Η κύρια εξέλιξη των δυνατοτήτων τους οφείλεται στην υψηλή επιχορήγηση έρευνας που αφορά στρατιωτικές εφαρμογές οι οποίες απαιτούν πολύ συχνά ιδιαίτερα εξειδικευμένες λειτουργίες για εφαρμογή εν μέσω ενεργών στρατιωτικών επιχειρήσεων. Εξαιτίας αυτού τα μη επανδρωμένα έχουν εξελιχθεί σε δύο κύριες κατηγορίες. Στα ελικοφόρα και στα αεριωθούμενα όπου τα ελικοφόρα είναι αυτά που φέρουν έλικες με πιο εικονικά στο αντικείμενο τα τετρακόπτερα που όπως υποδηλώνει η ονομασία φέρουν τέσσερις βραχίονες με έναν έλικα στον καθένα και τα αεριωθούμενα είναι αυτά που πετάνε με κινητήρα jet.

Το εύρος των δυνατοτήτων ενός μη επανδρωμένου αεροσκάφους το τοποθετεί στο επίκεντρο ενδιαφέροντος ανάπτυξης τεχνολογιών του ίδιου ή γύρω από το ίδιο το αντικείμενο είτε για βελτίωση του με επεμβάσεις στο ίδιο ή με συνδετικές προς αυτό τεχνολογίες, είτε για αποτελεσματικότερη άμυνα και προστασία από αυτό. Για αυτόν τον σκοπό καλείται εξειδικευμένο επιστημονικό προσωπικό από τους τομείς της θεωρητικής και εφαρμοσμένης φυσικής, μηχανικών πληροφορικής, μηχανικών μηχανολόγων, μηχανικών ηλεκτρολόγων, μηχανικών ηλεκτρονικής και γενικότερα ειδικούς με

υπόβαθρο τεχνολογικών εφαρμογών ώστε να πραγματοποιούν έρευνα υψηλού επιπέδου για την επέκταση των γνωστικών ορίων του μη επανδρωμένου αεροσκάφους.

Στην κατασκευή τους συμπεριλαμβάνεται ένα σύστημα μικροελεγκτή το οποίο επιτρέπει μέχρι έναν βαθμό την επέκταση των δυνατοτήτων τους όπως την εγκατάσταση συστοιχιών αισθητηρίων είτε για την βελτίωση των λειτουργιών τους είτε για αντίληψη του περιβάλλοντα χώρου, την εγκατάσταση κινητηρίων για παρέμβαση και διαμόρφωση του περιβάλλοντα χώρου ή συνδυασμό των δύο για σχηματισμό ρομποτικού συστήματος εγκατεστημένο στο μη επανδρωμένο αεροσκάφος. Σημαντικό ρόλο παίζει το υλικολογισμικό που θα διαχειρίζεται τις λειτουργίες του ώστε να απαλλάξει τον χειριστή από έναν μεγάλο αριθμό επεμβάσεων από πλευράς του ώστε να μπορεί να ασχοληθεί με πιο σημαντικές πτυχές του ελέγχου. Το υλικολογισμικό ενός μη επανδρωμένου αεροσκάφους συνήθως αποτελεί το σύνολο περίπλοκων και εξελιγμένων αλγορίθμων αλλά μπορεί και να είναι κάποιο ευφυές σύστημα ή ακόμη και τεχνητή νοημοσύνη.

Με βάση τα ανωτέρω το μη επανδρωμένο αεροσκάφος είναι κατάλληλη επιλογή για να φέρει ένα σύστημα μικροελεγκτή το οποίο θα κρυπτογραφεί και θα εκπέμπει της πληροφορίες ενός GPS.

1.9 Ενσωματωμένο Σύστημα

Ένα από τα καλύτερα εργαλεία που υπάρχουν στην διάθεση ενός ηλεκτρονικού μηχανικού στην σύγχρονη εποχή είναι τα ψηφιακά ηλεκτρονικά, καθώς το εύρος των εφαρμογών τους μπορεί να δίνει απλές, κομψές και πρακτικές λύσεις στην υλοποίηση σχεδόν κάθε ιδέας, ζητούμενου και κατασκευής. Την κατηγορία αυτή την έχουν εμπλουτίσει τα συστήματα μικροελεγκτών τα οποία δίνουν την δυνατότητα σχηματισμού ενός ενσωματωμένου συστήματος το οποίο παρέχει την δυνατότητα μεγάλου ποσοστού αυτονομίας στην λειτουργία μιας κατασκευής. Στην παρούσα εργασία η εφαρμογή ενός ενσωματωμένου συστήματος προσφέρει όλα τα προαναφερθέντα πλεονεκτήματα καθώς μπορεί να διαχειριστεί και να ελέγχει όλα τα μέρη της κατασκευής. Το ζητούμενο που πρέπει να απαντηθεί σε αυτό το σημείο συνοπτικά είναι το τι ακριβώς είναι ένα ενσωματωμένο σύστημα και πως ακριβώς λειτουργεί.

Ένα ενσωματωμένο σύστημα προκύπτει από την σύνθεση διαφόρων συστημάτων σε ένα ενιαίο σύστημα. Η πιο συνηθισμένη του μορφή περιλαμβάνει απαραίτητα στο σύνολο της ένα σύστημα μικροελεγκτή, έναν ελάχιστο αριθμό περιφερειακών συσκευών και το κατάλληλο υλικολογισμικό για την εκτέλεση των προβλεπόμενων λειτουργιών του. Επί της ουσίας ένα ενσωματωμένο σύστημα είναι μία ολοκληρωμένη κατασκευή έτοιμη να λειτουργήσει αυτόνομα.

Οι σύγχρονες συσκευές πλέον στην πλειοψηφία τους αποτελούν ενσωματωμένα συστήματα που περιλαμβάνουν έξυπνους αλγόριθμους που στόχο έχουν την απαλλαγή από τον χρήστη των πιο απλών ενεργειών ώστε να απλοποιήσουν την καθημερινότητα του και παράλληλα να αυξήσουν την ποιότητα ζωής του. Το εύρος των λειτουργιών τους περιλαμβάνουν συστήματα ασύρματης και διαδικτυακής σύνδεσης και διαχείρισης, συστήματα συστοιχιών αισθητηρίων και συστήματα κινηματικών περιφερειακών συσκευών για μετακίνηση στον χώρο ή διαμόρφωση περιβάλλοντος χωρίς να περιορίζεται σε αυτά.

Κατά την ολοκλήρωση της κατασκευής της παρούσας εργασίας θα έχει συντεθεί ένα ενσωματωμένο σύστημα το οποίο θα αποτελείται από ένα ζεύγος συστημάτων μικροελεγκτή οι οποίοι θα επικοινωνούν μεταξύ τους ως πομπός και δέκτης κάνοντας χρήση του ασύρματου πρωτοκόλλου Wi-Fi, ο πομπός θα περιλαμβάνει μία περιφερειακή συσκευή GPS και θα τοποθετηθεί σε ένα μη επανδρωμένο αεροσκάφος και το σύνολο του θα το διαχειρίζεται ένα κατάλληλα ανεπτυγμένο firmware το οποίο θα κρυπτογραφεί

την πληροφορία του GPS δια της μεθόδου χαοτικού χάρτη στον πομπό και θα την αποκρυπτογραφεί στον δέκτη.

1.10 Περίληψη Κεφαλαίου

- Η παρούσα πτυχιακή εργασία αφορά την πρακτική εφαρμογή κρυπτογράφησης με την μέθοδο χαοτικού χάρτη σε δεδομένα συντεταγμένων GPS που αφορούν ένα μη επανδρωμένο αεροσκάφος.
- Η διαδικασία θα πραγματοποιηθεί μέσω συστήματος ζεύγους μικροελεγκτών όπου ο ένας θα λειτουργεί ως κρυπτογράφος και πομπός και ο δεύτερος θα λειτουργεί ως αποκρυπτογράφος και δέκτης.
- Το πρωτόκολλο επικοινωνίας που θα χρησιμοποιηθεί για την μεταφορά των δεδομένων από πομπό σε δέκτη θα είναι το Wi-Fi.
- Τα μέρη που συνθέτουν το σύνολο της εργασίας είναι η κρυπτογράφηση, το σύστημα συντεταγμένων, τα συστήματα μικροελεγκτών, οι περιφερειακές συσκευές, το λογισμικό, το μη επανδρωμένο αεροσκάφος και το ενσωματωμένο σύστημα.
- Η ανάπτυξη μιας εργασίας αποτελείται τουλάχιστον από δύο μέρη, από την μελέτη και από την κατασκευή της.
- Η κρυπτογράφηση είναι μία πρακτική που χρησιμοποιείται για την προφύλαξη πληροφοριών και δεδομένων από μη εξουσιοδοτημένους παραλήπτες.
- Το σύστημα συντεταγμένων είναι ένα εργαλείο που χρησιμοποιείται για την ακριβή εύρεση ενός σημείου στην παγκόσμια σφαίρα σε πραγματικό χρόνο.
- Σύστημα μικροελεγκτή ονομάζεται η συσκευή που φέρει τον μικροελεγκτή και όλες τις απαραίτητες ηλεκτρονικές διατάξεις που παρέχουν πρόσβαση σε όλες τις δυνατότητες της συσκευής.
- Περιφερειακές συσκευές ονομάζονται οι συσκευές που συνδέονται και ελέγχονται από ένα ολοκληρωμένο υπολογιστικό σύστημα.
- Το λογισμικό αποτελεί το έτερον ήμισυ του υλικού μέρους ενός υπολογιστικού συστήματος και αποτελείται από το πρόγραμμα που το οδηγεί ώστε να εκτελεί όλες τις προβλεπόμενες εργασίες του.
- Μη επανδρωμένο αεροσκάφος ονομάζεται ένα τηλεκατευθυνόμενο αεροσκάφος που δεν απαιτεί άνθρωπο πιλότο, έχει την δυνατότητα να λειτουργεί είτε αυτόνομα είτε με επίγειο χειριστή και μπορεί να μεταφέρει είτε φονικό είτε μη φονικό φορτίο.

Κεφάλαιο 2ο: Κατασκευή Εργασίας

2.1 Εισαγωγή

Μετά την ολοκλήρωση της μελέτης μιας εργασίας ακολουθεί η κατασκευή της με την υλοποίηση των μερών της και την σύνθεση τους σε ένα ολοκληρωμένο και λειτουργικό σύστημα. Η διαδικασία αυτή περιλαμβάνει πολλά βήματα καθώς μία νέα κατασκευή κατά την διάρκεια της υλοποίησης της είναι δυνατό να παρουσιάσει αναπάντεχα αποτελέσματα τα οποία είναι προϊόν απροσδόκητων καταστάσεων τα οποία δεν ήταν δυνατόν να προβλεφθούν στο στάδιο της μελέτης.

Μέρος της εργασίας ενός μηχανικού είναι να αναλύσει τα διάφορα τμήματα του συνόλου της εργασίας, να τα κατασκευάσει και να τα δοκιμάσει ανεξάρτητα το ένα από το άλλο ώστε να βεβαιωθεί για την ορθότητα της λειτουργίας τους προτού τα συνθέσει σε ένα πιο σύνθετο και περίπλοκο σύστημα. Οι κυριότεροι λόγοι για την επιλογή αυτής της μεθοδολογικής προσέγγισης είναι πρώτον διότι είναι πολύ πιο απλό και εύκολο να εντοπιστεί ένα απροσδόκητο πρόβλημα ή σφάλμα σε μία διάταξη που αποτελεί τμήμα ενός μεγαλύτερου συστήματος όταν αυτή είναι απομονωμένη από αυτό και δεύτερον για την αναλυτική καταγραφή και επιβεβαίωση των ορθών λειτουργιών της κάθε διάταξης προτού αυτή ενσωματωθεί στο σύνθετο σύστημα.

Πιο συγκεκριμένα για την κατασκευή μιας συσκευής που αποτελεί ένα ενσωματωμένο σύστημα πρέπει να υπάρχει από πλευράς εξειδίκευσης του μηχανικού που θα κάνει πράξη την μελέτη του ένα υπόβαθρο γνώσεων που να επιτρέψει την οργάνωση της διαδικασίας κατασκευής σε διάφορα τμήματα αλλά και την προτεραιότητα με την οποία θα αναπτυχθούν, ικανότητα λήψης μέτρησης ηλεκτρικών και φυσικών μεγεθών με χρήση κατάλληλων μετρητικών οργάνων, δυνατότητα ανάπτυξης λογισμικού με χρήση γλώσσας προγραμματισμού, ικανότητες κασσιτεροσυγκόλλησης μέσω χειρισμού σταθμών συγκολλήσεων και αποσυγκολλήσεων και γνώση πρώτων υλών και υλικών χωρίς να περιορίζεται σε αυτά.

Προκειμένου να υλοποιηθεί πλήρως η κατασκευή της παρούσας εργασίας θα πρέπει να διαχωριστεί σε ένα σύνολο ανεξάρτητων εργασιών των οποίων η επιτυχής μεμονωμένη ανάπτυξη της κάθε μίας θα δίνει νόημα στην ανάπτυξη της επόμενης σε σειρά εργασίας ώστε να μπορούν να συντεθούν σε ένα μεγαλύτερο σύνολο και να λειτουργήσουν σαν ολοκληρωμένη κατασκευή. Αρχικά θα αναπτυχθεί το λογισμικό καθώς αποτελεί το κύριο ζητούμενο της εργασίας με την έννοια ότι πρέπει να αναπτυχθεί ένα λογισμικό που να μπορεί να κρυπτογραφεί και να αποκρυπτογραφεί τα δεδομένα ενός GPS συστήματος συντεταγμένων ενός πομπού και ενός δέκτη. Εφόσον το λογισμικό λειτουργήσει με επιτυχία θα πρέπει στην συνέχεια το λογισμικό να διαμορφωθεί έτσι ώστε να λειτουργήσει σε ένα ζεύγος συστημάτων μικροελεγκτή και να προστεθούν και μερικές λειτουργίες, βιβλιοθήκες και συναρτήσεις που αφορούν το πρωτόκολλο επικοινωνίας Wi-Fi [10]. Με την ολοκλήρωση των ανωτέρω θα πρέπει να αναπτυχθεί πλακέτα βακελίτη η οποία θα συμπεριλαμβάνει αφενός το σύστημα μικροελεγκτή που θα υλοποιεί τον πομπό και αφετέρου την αυτόνομη συσκευή του GPS η οποία θα είναι ενσωματωμένη στο σύστημα μικροελεγκτή. Το άλλο σύστημα μικροελεγκτή που αποτελεί το ένα μέρος του ζεύγους συστημάτων μικροελεγκτή και που αποτελεί τον δέκτη θα είναι συνδεδεμένο με έναν ηλεκτρονικό υπολογιστή και θα απεικονίζει στην οθόνη του τα δεδομένα που θα λαμβάνει από τον πομπό. Επειδή το ζητούμενο της εργασίας θέλει τα GPS δεδομένα να ανταποκρίνονται στην τοποθεσία ενός μη επανδρωμένου αεροσκάφους η πλακέτα βακελίτη που θα φέρει το σύστημα μικροελεγκτή του δέκτη και το GPS θα προσαρμοστεί σε ένα μη επανδρωμένο αεροσκάφους τύπου τετρακόπτερου που σημαίνει πως θα πρέπει να έχει και αυτόνομη πηγή ενέργειας για την εξασφάλιση της λειτουργίας του.

Με την επιτυχή ολοκλήρωση όλων των ανωτέρω και την σύνθεση τους σε ένα ενιαίο ενσωματωμένο σύστημα θα πραγματοποιηθεί μία τελική δοκιμή η οποία αν θα είναι και αυτή επιτυχής θα έχει ολοκληρωθεί το σύνολο της παρούσας εργασίας.

2.2 Ανάπτυξη λογισμικού

Η ανάπτυξη ενός λογισμικού αποτελεί κρίσιμο κομμάτι της κατασκευής της παρούσας εργασίας για πολλούς λόγους. Θα πρέπει αρχικά να μπορεί να εκτελεί με επιτυχία και ακρίβεια το κεντρικό ζητούμενο της πτυχιακής το οποίο είναι αυτό της κρυπτογράφησης και αποκρυπτογράφησης μιας πληροφορίας. Στην μελέτη της εργασίας αυτής περιεγράφηκε με σαφήνεια το θεωρητικό υπόβαθρο όλων των τμημάτων της διαδικασίας αυτής καθώς και δημιουργηθήκανε και οι αλγόριθμοι η οποίοι απεικονίζουν τα τμήματα του αλγόριθμου που θα υλοποιούν τις συναρτήσεις που θα εκτελούν και θα παράγουν τα τμήματα αυτά. Στο κεφάλαιο αυτό θα παρουσιαστεί το πώς ακριβώς θα υλοποιηθούν αυτά στο πρώτο στάδιο ανάπτυξης του προγράμματος κρυπτογράφησης και αποκρυπτογράφησης

Η γλώσσα προγραμματισμού στην οποία θα αναπτυχθεί το πρόγραμμα είναι η C [11]. Η C σαν γλώσσα προγραμματισμού χρησιμοποιείται περισσότερο από μηχανικούς που ασχολούνται με την ανάπτυξη υλικολογισμικού για την λειτουργία των μικροελεγκτών καθώς επιτρέπει στον μηχανικό να διαχειριστεί με τον κώδικα του την συσκευή και την μνήμη της κοντά στο επίπεδο μηχανής. Τα δύο κύρια χαρακτηριστικά της είναι πρώτον πως δεν έχει μεγάλο όγκο εντολών αλλά εκτελεί τις εργασίες της με χρήση συναρτήσεων και δεύτερον είναι μία δομημένη γλώσσα προγραμματισμού στην φιλοσοφία της.

Το μεγάλο προτέρημα της ως γλώσσα προγραμματισμού προέρχεται από το γεγονός ότι βασίζεται στην ύπαρξη των έτοιμων συναρτήσεων που είναι οργανωμένες σε βιβλιοθήκες αλλά για έναν έμπειρο προγραμματιστή του παρέχεται η δυνατότητα να αναπτύξει τις δικές του συναρτήσεις τις οποίες μπορεί να τις οργανώσει σε δική του βιβλιοθήκη ή βιβλιοθήκες. Αυτό είναι τρομερό προτέρημα καθώς ο προγραμματιστής που θα αναπτύξει το δικό του σύνολο συναρτήσεων σε μία βιβλιοθήκη δικής του επινόησης εξασφαλίζει αφενός με μεγάλη βεβαιότητα πως το περιεχόμενο της θα λειτουργήσει χωρίς προβλήματα με τον βέλτιστο δυνατό τρόπο και αφετέρου γνωρίζει ακριβώς το περιεχόμενο τους και πως ακριβώς να το αξιοποιήσει.

Αρχικά θα αναπτυχθεί το πρόγραμμα σε ένα ολοκληρωμένο περιβάλλον ανάπτυξης (Integrated Development Environment, IDE) το οποίο περιέχει έναν κειμενογράφο παραμετροποιημένο ειδικά για την σύνταξη προγραμμάτων ώστε να ανιχνεύει τα συντακτικά λάθη από πλευράς του προγραμματιστή. Συγκεκριμένα θα είναι αυτό το Visual Studio της Microsoft. Με την ολοκλήρωση του κώδικα που θα αντιπροσωπεύει το σύνολο του προγράμματος θα πρέπει με κάποιον τρόπο αυτό να μετατραπεί σε γλώσσα μηχανής, σε μία ακολουθία μηδενικών και άσων δηλαδή που να εξηγεί στην μηχανή τις ενέργειες που πρέπει να εκτελέσει. Το εργαλείο που εκτελεί αυτήν την μετατροπή ονομάζεται μεταγλωττιστής (compiler). Κατά την διάρκεια της μεταγλώττισης μπορεί να εντοπίσει πολλά πιθανά λάθη, να τα αναγνωρίσει και να ενημερώσει τον προγραμματιστή για αυτά με την μορφή ενός μηνύματος σφάλματος.

2.2.1 Ανάπτυξη προγράμματος Κλειδιού Κρυπτογράφησης

Το θεμελιώδες ζητούμενο ολόκληρης της εργασίας είναι η ανάπτυξη της συνάρτησης η οποία θα παράγει το κλειδί κρυπτογράφησης κάνοντας χρήση ενός μονοδιάστατου χαοτικού χάρτη. Η ιδιαιτερότητα του είναι πως λόγω της ακραίας μη γραμμικότητας του περιεχομένου του το αποτέλεσμα του έχει υψηλότατο παράγοντα τυχαιότητας παρέχοντας έτσι ένα σύνολο πραγματικών τυχαίων αριθμών. Ο χαοτικός χάρτης είναι ήδη γνωστό από την μελέτη πως έμπρακτα είναι μία μη γραμμική

εξίσωση, που το περιεχόμενο της περιγράφεται ως $x_i = A\sin\left(\frac{\omega}{x_{i-1}}\right) + B\tanh(x_{i-1})^2$. Αναλύοντας το περιεχόμενο της προκύπτει πως αποτελείται από τέσσερις μεταβλητές οι οποίες σύμφωνα με την μελέτη θα έχουν τις ακόλουθες τιμές: $A = 8, B = 15, \omega = 100\ και\ x_{(0)} = 0{,}1$. Διακρίνεται πως οι τρεις τιμές ανήκουν στο σύνολο των ακεραίων αριθμών και η μία τιμή ανήκει στο σύνολο των πραγματικών αριθμών. Επομένως θα πρέπει να δηλωθούν στο πρόγραμμα τέσσερις μεταβλητές, τρεις τύπου integer και μία τύπου float.

Επίσης κάποιες από τις πράξεις δεν συμπεριλαμβάνονται στις τυπικές βιβλιοθήκες συναρτήσεων που συνήθως συμπεριλαμβάνονται σχεδόν σε όλα τα προγράμματα, τις <stdio.h> και <stdlib.h> και επομένως χωρίς την συμπερίληψη της κατάλληλης βιβλιοθήκης δεν θα μπορεί να τις υπολογίσει διότι δεν θα τις αναγνωρίσει. Αυτές οι πράξεις είναι ο υπολογισμός του ημιτόνου, της υπερβολικής συνεφαπτομένης και του υπολογισμού των δυνάμεων.

Αρχικά πρέπει να γραφτεί η εξίσωση σε μορφή που θα μπορεί να ερμηνευτεί από τον μεταγλωττιστή κατά την διαδικασία της μεταγλώττισης του πηγαίου κώδικα. Έτσι η εξίσωση θα πρέπει να γραφτεί ως εξής: X=A*sin(C/(X-1))+B*tanhpow((X-1), 2); Ακολούθως για να μπορέσει να αναγνωρίσει ο μεταγλωττιστής τις συναρτήσεις sin(), tanh() και pow() θα πρέπει να συμπεριλάβει στο κύριο πρόγραμμα και το αρχείο βιβλιοθήκης <math.h>. Τέλος η ανωτέρω μαθηματική έκφραση επιδέχεται βελτιστοποίηση καθώς η συνάρτηση pow() απαιτεί αρκετό χρόνο για την εκτέλεση της και έτσι το τμήμα της μαθηματικής έκφρασης tanhpow((X-1), 2) μπορεί να μετατραπεί κατάλληλα ώστε να μπορεί να εκφραστεί και ως (tanh(X-1)*tanh(X-1)). Με την εφαρμογή όλων των ανωτέρω η τελική μαθηματική έκφραση της εξίσωσης θα είναι X=A*sin(C/(X-1))+B*(tanh(X-1)*tanh(X-1));. Το αποτέλεσμα κάθε νέας κατάστασης της προκύπτει από την επίλυση για την προηγούμενη της κατάσταση. Για κάθε επανάληψη το αποτέλεσμα της εξίσωσης αυτής που θα προκύπτει θα ανήκει στο σύνολο των πραγματικών αριθμών και θα έχει αρκετά δεκαδικά ψηφία.

Με την λύση της εξίσωσης θα προκύψει ένας πραγματικός αριθμός ο οποίος θα έχει κάποιον ελάχιστο αριθμό δεκαδικών ψηφίων των οποίων ο αριθμός θα προκύπτει από την ακρίβεια με την οποία έχει παραμετροποιηθεί η μεταβλητή στην οποία καταχωρείται. Για τον λόγο αυτό είναι καλύτερα η μεταβλητή του X να είναι τύπου double παρά τύπου float. Όπως αναφέρθηκε και στην μελέτη η εξίσωση που εφαρμόζεται για την παραγωγή των τυχαίων αυτών πραγματικών αριθμών προέρχεται από μία εργασία με τίτλο “Medical Data Encryption based on a Modified Sinusoidal 1D Chaotic Map and Its Microcontroller Implementation” και έχει ήδη δοκιμαστεί στο πακέτο δοκιμών τυχαιότητας NIST, ένα σύνολο 15 διαφορετικών τεστ το οποίο και πέρασε με επιτυχία βεβαιώνοντας τον παράγοντα τυχαιότητας του χαοτικού χάρτη όπως φαίνεται και στην εικόνα 2.1 όπου ο χαοτικός χάρτης περνάει όλες τις δοκιμές με επιτυχία. Η επιτυχία προκύπτει από τα αποτελέσματα των δοκιμών καθώς η τιμή πιθανότητας P-value πρέπει να είναι ανώτερη από έναν συντελεστή α=0,01και από την εικόνα αυτό επαληθεύεται από την στήλη P-value όπου και οι δεκαπέντε δοκιμές έχουν πράγματι αποτέλεσμα μεγαλύτερο του συντελεστή α.

No.	Test	Chi-square P-Value	Rate
1	Frequency	0.911413	50/50
2	BlockFrequency	0.534146	50/50
3	CumulativeSums	0.816537	50/50
4	Runs	0.779188	49/50
5	LongestRun	0.010237	50/50
6	Rank	0.494392	49/50
7	FFT	0.137282	50/50
8	NonOverlappingTemplate	0.883171	50/50
9	OverlappingTemplate	0.779188	49/50
10	Universal	0.935716	49/50
11	ApproximateEntropy	0.911413	49/50
12	RandomExcursions	0.022503	30/30
13	RandomExcursionsVariant	0.082177	30/30
14	Serial	0.085587	48/50
15	LinearComplexity	0.816537	50/50

Εικόνα 2-1.: Αποτελέσματα επαλήθευσης της τυχαιότητας του χαοτικού χάρτη μέσω του πακέτου δοκιμών NISTμε παραμετροποίηση των μεταβλητών του για x=0,1, A=3, B=2 και ω=10000.

Τον τυχαίο αυτόν αριθμό στην συνέχεια τον επεξεργάζεται η συνάρτηση κάνοντας χρήση της συνάρτησης floor() η οποία τελεί στρογγυλοποίηση του αριθμού προς τον ακέραιο που αποτελεί τον συντελεστή του αριθμού. Αυτό σημαίνει πως αν για παράδειγμα ο ακέραιος αριθμός του πραγματικού αριθμού ήταν για παράδειγμα το εφτά, είτε ο αριθμός ήταν ο 7,00000001 είτε ο 7,99999999 η στρογγυλοποίηση θα πραγματοποιούνταν πάντοτε προς τα κάτω και το αποτέλεσμα θα ήταν ο ακέραιος 7. Και ενώ κανονικά η διαδικασία αυτή είναι η σωστή για την πορεία του προγράμματος, ένας έμπειρος προγραμματιστής γνωρίζει πως καταχωρώντας το περιεχόμενο της μεταβλητής που περιέχει τον πραγματικό τυχαίο αριθμό σε μία μεταβλητή τύπου int ο μεταγλωττιστής αυτήν την ενέργεια θα την πράξει αυτομάτως καθιστώντας αχρείαστη την χρήση της συνάρτησης floor() βελτιστοποιώντας τον κώδικα με αντίτιμο ένα μήνυμα προειδοποίησης για απώλεια δεδομένων λόγω αυτόματης μετατροπής από τύπο double σε τύπο integer. Από την στιγμή που παραχθεί ο τυχαίος αριθμός ο τρόπος με τον οποίο θα αξιοποιηθεί αποτελεί μέρος της μεθοδολογίας κρυπτογράφησης και συγκεκριμένα της διαδικασίας της παρασκευής του κλειδιού κρυπτογράφησης.

Ο ακέραιος που θα προκύψει θα επεξεργαστεί μέσω τέλεσης με τον αριθμητικό τελεστή % (modulo) ο οποίος μπορεί να εφαρμοστεί μόνο σε μεταβλητές τύπου integer ή σε ακέραιες σταθερές. Ο συγκεκριμένος τελεστής έχει την ιδιαιτερότητα να αποδίδει το υπόλοιπο της διαίρεσης μεταξύ δύο ακεραίων και θα δίνει ως υπόλοιπο μηδέν εάν η διαίρεση είναι τέλεια ή αλλιώς το υπόλοιπο που μπορεί να αντιστοιχεί στην διαίρεση. Κάνοντας χρήση στην συνάρτηση αυτού του τελεστή μεταξύ του ακέραιου που προκύπτει από την έως τώρα επεξεργασία και της σταθερής 2 το αποτέλεσμα του modulo θα είναι πάντοτε είτε μηδέν είτε ένα. Το αποτέλεσμα αυτής της τέλεσης εφόσον είναι γνωστή η δυαδική του φύση μπορεί να καταχωρείται σε μία μεταβλητή τύπου bool η οποία καταλαμβάνει στην μνήμη χώρο ίσου με ένα byte, συμβάλλοντας στην βελτιστοποίηση του κώδικα.

Όλη η ανωτέρω διαδικασία αποσκοπεί στο να παραχθεί ένα μηδέν ή ένας άσος. Το αρχικό ζητούμενο παρόλα αυτά είναι να παραχθεί ένα κλειδί κρυπτογράφησης μήκους 32 bit και όχι μόνο ενός bit. Για την επίτευξη αυτού είναι αναγκαίο η ανωτέρω διαδικασία να μπει ολόκληρη σε έναν βρόγχο επανάληψης τύπου for ο οποίος θα πρέπει να παραμετροποιηθεί για 32 επαναλήψεις. Μέσα στον βρόγχο αυτόν για κάθε επανάληψη του το αποτέλεσμα του θα καταχωρείται σε έναν πίνακα μήκους 32 θέσεων ξεκινώντας από την πρώτη θέση του πίνακα για την πρώτη επανάληψη του βρόγχου και για κάθε νέα επανάληψη, αναλόγως τον αύξοντα αριθμό της θα καταχωρεί στην αντίστοιχη θέση του πίνακα το

αποτέλεσμα της διαδικασίας το οποίο όπως αναφέρθηκε προηγουμένως θα είναι δυαδικής φύσης και ως εκ τούτου ο πίνακας θα είναι τύπου bool.

Η C γλώσσα προγραμματισμού έχει κάποιες ιδιαιτερότητες και μία από αυτές είναι πως δεν είναι φιλική προς τους πίνακες, ή τουλάχιστον προς την διαχείριση τους. Αν και στην πράξη αυτό το συμπέρασμα προκύπτει από όσους αγνοούν κάποιες λεπτομέρειες του σχεδιασμού της. Υπάρχει ένας προβληματισμός ως προς την επιστροφή ενός ολόκληρου πίνακα από μία συνάρτηση στο κυρίως πρόγραμμα ή προς οπουδήποτε, ενώ το ίδιο δεν ισχύει για άλλες μεταβλητές. Ο λόγος για τον οποίο συμβαίνει αυτό είναι γιατί στην C ο πίνακας επί της ουσίας είναι δείκτης, μία μεταβλητή η οποία "δείχνει" σε μία συγκεκριμένη θέση μνήμης και συγκεκριμένα στην θέση μνήμης που καταλαμβάνει η πρώτη θέση του πίνακα. Έχοντας αυτό υπόψιν και γνωρίζοντας την λογική με την οποία μία συνάρτηση που δουλεύει δείκτες επιστρέφει πίσω έναν δείκτη παραμετροποιείται η συνάρτηση κατάλληλα ώστε να επιστρέφει το περιεχόμενο ενός πίνακα στην κύρια συνάρτηση του προγράμματος. Με όλα τα ανωτέρω το τελικό αποτέλεσμα είναι μία συνάρτηση που παράγει ένα κλειδί κρυπτογράφησης το περιεχόμενο του οποίου κατασκευάστηκε με χρήση χαοτικού χάρτη και είναι πλέον στην διάθεση του κύριου προγράμματος ώστε να το χρησιμοποιήσει για την κρυπτογράφηση δεδομένων. Ο κώδικας της συνάρτησης απεικονίζεται στο σχήμα 2.2 στο οποίο διακρίνονται οι μεταβλητές που ορίζονται ως συντελεστές της συνάρτησης, ο βρόγχος for και η παραμετροποίηση του ώστε να επαναληφθεί 32 φορές και το περιεχόμενο του που περιλαμβάνει την εξίσωση του χαοτικού χάρτη, την συνάρτηση floor() και τον πίνακα bstr στον οποίο θα καταχωρηθούν τα bit που θα σχηματίσουν το κλειδί κρυπτογράφησης μετά την εφαρμογή του τελεστή modulo (%).

```
/*Initialization of chaotic map variables*/
float X=0.1;
int A=8;
int B=15;
int C=100;
for (i=0; i<32; ++i)//Pseudo random bit generator.
    {
    X=A*sin(C/(X-1))+B*(tanh(X-1)*tanh(X-1));//1D Chaotic map equation.
    int result=floor(X);//Round down to closest int.
    bstr[i]= result % 2; //Transform each int from each i to bin, then store in 1D array.
```

Εικόνα 2-2: Συνάρτηση κλειδιού κρυπτογράφησης.

2.2.2 Επεξεργασία και τροποποίηση δεδομένων προς κρυπτογράφηση.

Τα προς κρυπτογράφηση δεδομένα μπορούν να υπάρχουν σε πολλές μορφές και σε διάφορα μεγέθη καθώς και σε ευμετάβλητα μεγέθη. Για τον λόγο αυτόν είναι απαραίτητο ο μηχανικός να προσδιορίσει την αρχική τους μορφή με την οποία λαμβάνονται σε όλο τους το εύρος ώστε να είναι γνωστή η μορφή και ο τύπος τους μέχρι τις πιο ακραίες καταστάσεις τους. Έχοντας αυτήν την γνώση υπόψιν του μπορεί να σχεδιάσει ένα κατάλληλο πρόγραμμα που θα είναι ικανό για την επεξεργασία τους χωρίς τον κίνδυνο να υπάρξει κάποια απροσδιόριστη κατάσταση η οποία θα μπορούσε να το οδηγήσει στην κατάρρευση του.

Στο στάδιο αυτό της κατασκευής είναι γνωστό πως το επιθυμητό ζητούμενο είναι η λήψη δεδομένων συντεταγμένων από ένα GPS και να κρυπτογραφηθούν με το κλειδί κρυπτογράφησης. Καθώς είναι γνωστό πως το κλειδί κρυπτογράφησης είναι μία ακολουθία μήκους 32 bit της οποίας η μορφή δεν θα μεταβληθεί και ούτε θα μετατραπεί, η λογική επιβάλει πως και τα δεδομένα που θα κρυπτογραφηθούν θα πρέπει να είναι στην μορφή ακολουθίας 32 bit. Επειδή όμως στο στάδιο αυτό η πρόσβαση στα δεδομένα της συσκευής GPS δεν είναι ακόμη διαθέσιμη θα πρέπει να προσομοιωθεί με κάποιον

λογισμικό τρόπο αυτή η λειτουργία ώστε να μπορεί να κατασκευαστεί το λογισμικό κρυπτογράφησης και να μπορεί να δοκιμαστεί η ορθότητα της λειτουργίας του.

Ένα σύστημα συντεταγμένων που χρησιμοποιείται ακόμη και σήμερα είναι αυτό των αξόνων των μεσημβρινών και των παράλληλων. Οι μεσημβρινοί είναι οι νοητές ευθείες γραμμές που διαγράφουν από τον έναν πόλο του πλανήτη στον άλλον και η μεταξύ τους απόσταση μετριέται σε μοίρες. Ο κύριος μεσημβρινός θεωρείται αυτός που τέμνει το Greenwich και αριθμείται με μηδέν. Από αυτό το σημείο χωρίζονται σε δύο μεσημβρινούς, αυτούς που βρίσκονται δυτικά του Greenwich ονομάζονται Δυτικοί Μεσημβρινοί και το εύρος τους σε μοίρες εκτείνεται από 0° έως 180° και συμπεριλαμβάνει και τις υποδιαιρέσεις σε λεπτά (') και δευτερόλεπτα (") της μοίρας και σε αυτούς που βρίσκονται ανατολικά του Greenwich και ονομάζονται Ανατολικοί Μεσημβρινοί και το εύρος τους σε μοίρες εκτείνεται από 0° έως 180° αντίστοιχα καλύπτοντας έτσι σε επίπεδο πλάνο 360° περιμετρικά του πλανήτη. Οι παράλληλοι είναι ομόκεντροι κύκλοι οι οποίοι είναι κάθετοι στους μεσημβρινούς. Ο κύριος παράλληλος εντοπίζεται στο ύψος του ισημερινού, το σημείο δηλαδή όπου ο παράλληλος έχει την μεγαλύτερη διάμετρο, μετριούνται σε μοίρες όπως και οι μεσημβρινοί και στο κύριο παράλληλο αποδίδεται η τιμή των 0°. Από τον κύριο παράλληλο εκτείνονται οι παράλληλοι προς τον Βορρά οι οποίοι έχουν εύρος τιμών σε μοίρες από 0° έως 90° και ονομάζονται Παράλληλοι του Βόρειου Ημισφαίριου και οι παράλληλοι προς τον Νότο οι οποίοι έχουν εύρος τιμών σε μοίρες από 0° έως 90° και ονομάζονται Παράλληλοι του Νότιου Ημισφαίριου αντίστοιχα.

Πολλές σύγχρονες εφαρμογές αποδίδουν την τοποθεσία κάνοντας χρήση αυτού του συστήματος συντεταγμένων αξόνων x και y αποδίδοντας δύο ακέραιους και την ακρίβεια με σημείο υποδιαστολής και πέντε δεκαδικά ψηφία. Ως εκ' τούτου προκύπτει πως συνολικά ο αριθμός αποτελείται από ένα σύνολο επτά ψηφίων στο δεκαδικό αριθμητικό σύστημα και για την εφαρμογή που προορίζεται η αγνόηση της υποδιαστολής σε αυτό το στάδιο δεν επηρεάζει με κάποιον τρόπο την λειτουργία του προγράμματος. Η συνάρτηση rand() είναι σχεδιασμένη ώστε να μην δέχεται όρισμα και όταν καλείται από το πρόγραμμα η εκτέλεση της λειτουργίας της έχει ως αποτέλεσμα την παραγωγή ενός τυχαίου ακέραιου αριθμού από το 0 μέχρι το 32767. Το χαρακτηριστικό αυτό έχει την προοπτική να δώσει λύση αλλά όχι ακριβώς όπως το αποδίδει η συνάρτηση. Το πρόβλημα εντοπίζεται σε τρία σημεία, το ένα είναι πως το μέγιστο μέγεθος των ψηφίων που μπορεί να αποδώσει η συγκεκριμένη συνάρτηση για κάθε φορά που θα καλείται είναι πέντε ψηφία, το δεύτερο είναι πως το αποτέλεσμα κάθε κλήσης της συνάρτησης μπορεί να είναι ευμετάβλητο καθώς το μέγεθος του αποτελέσματος θα κυμαίνεται μεταξύ ενός και πέντε ψηφίων και το τρίτο είναι πως το σύστημα συντεταγμένων αποδίδεται σε ένα σύνολο επτά ψηφίων και όχι πέντε. Αυτό δεν εξυπηρετεί στην λειτουργία του προγράμματος καθώς για λόγους ομαλής λειτουργίας είναι επιθυμητό η μορφή των προς κρυπτογράφηση δεδομένων να είναι ορισμένη και αμετάβλητη.

Μία απλή και κομψή λύση για το πρόβλημα αυτό ώστε το αποτέλεσμα της συνάρτησης rand() να έχει τα επιθυμητά χαρακτηριστικά είναι να καταχωρείται το αποτέλεσμα της σε μία μεταβλητή και έπειτα στο περιεχόμενο της μεταβλητής αυτής να προστίθεται μία σταθερά με την τιμή 1000000. Το αποτέλεσμα της πρόσθεσης αυτής θα αποδίδει έναν αριθμό ο οποίος θα είναι αφενός μήκους επτά ψηφίων και αφετέρου θα είναι αμετάβλητος ως προς το μήκος του. Επομένως συμπαιρένεται από το αποτέλεσμα πως η λύση αυτή είναι κατάλληλη για τις ανάγκες δοκιμής της λειτουργίας της συνάρτησης αυτής αλλά και για την δοκιμή της συνολικής κρυπτογράφησης. Το επόμενο βήμα θα είναι η μετατροπή των προς κρυπτογράφηση δεδομένων από το δεκαδικό αριθμητικό σύστημα στο δυαδικό.

Η διαδικασία μετατροπής ενός αριθμού του δεκαδικού αριθμητικού συστήματος στο δυαδικό περιλαμβάνει την συνεχή διαίρεση του αριθμού με την σταθερά δύο μέχρι να καταλήξει είτε σε τέλεια

είτε σε ατελή διαίρεση και έπειτα να πάρει το υπόλοιπο κάθε πράξης με την σειρά από την τελευταία πράξη στην πρώτη και να το γράψει με την ίδια σειρά από αριστερά προς τα δεξιά. Για παράδειγμα αν ο αριθμός που προορίζεται να μετατραπεί στο δυαδικό αριθμητικό σύστημα είναι ο 127 τότε θα πρέπει να διαιρεθεί με την ακόλουθη διαδικασία που απεικονίζεται στην εικόνα 2.3.

$$151 \div 2 = 75, \textit{υπόλοιπο} = 1.$$

$$75 \div 2 = 37, \textit{υπόλοιπο} = 1.$$

$$37 \div 2 = 18, \textit{υπόλοιπο} = 1.$$

$$18 \div 2 = 9, \textit{υπόλοιπο} = 0.$$

$$9 \div 2 = 4, \textit{υπόλοιπο} = 1.$$

$$4 \div 2 = 2, \textit{υπόλοιπο} = 0.$$

$$2 \div 2 = 1, \textit{υπόλοιπο} = 0.$$

$$1 \div 2 = 0, \textit{υπόλοιπο} = 1.$$

Εικόνα 2-3: Παράδειγμα μετατροπής από δεκαδικό σε δυαδικό αριθμητικό σύστημα.

Και ξεκινώντας την καταγραφή των υπολοίπων κάθε διαίρεσης από την τελευταία πράξη προς την πρώτη θα προκύψει ο δυαδικός αριθμός 10010011 ο οποίος είναι ο αντίστοιχος 151 του δεκαδικού αριθμητικού συστήματος. Για την επαλήθευση του η διαδικασία μετατροπής ενός δυαδικού αριθμού στο δεκαδικό αριθμητικό σύστημα πρέπει κάθε στοιχείο του να πολλαπλασιαστεί με μία δύναμη της βάσης δύο όπου η δύναμη προκύπτει από την αύξουσα σειρά του στοιχείου από δεξιά προς τα αριστερά με αρχική τιμή το 0 και τελείται ως εξής:

$$1 \times 2^7 + 0 \times 2^6 + 0 \times 2^5 + 1 \times 2^4 + 0 \times 2^3 + 1 \times 2^2 + 1 \times 2^1 + 1 \times 2^0$$

Όπου πράγματι το αποτέλεσμα είναι 151 που ταιριάζει με την αρχική τιμή που προοριζόταν για μετατροπή.

Η ανωτέρω διαδικασία πρέπει να γραφτεί σε κώδικα με κατάλληλο τρόπο ώστε να εκτελεί την διαδικασία μετατροπής χωρίς να υπάρχουν σφάλματα κατά την εκτέλεση της. Ένας βέλτιστος τρόπος είναι με προσεκτική διαχείριση της μνήμης στην οποία καταχωρείται η κάθε τιμή bit προς bit με χρήση της συνάρτησης malloc(). Ο κώδικας της συνάρτησης που παράγει και τροποποιεί τα προς κρυπτογράφηση δεδομένα απεικονίζεται στο σχήμα 2.4 όπου δημιουργείται μία συνάρτηση με όνομα get_bits με ορίσματα δύο μεταβλητές τύπου integer με περιεχόμενα έναν επταψήφιο αριθμό και έναν διψήφιο αριθμό. Ο επταψήφιος αντιπροσωπεύει την μία συντεταγμένη και ο διψήφιος τον επιθυμητό αριθμό σε bit ο οποίος ισούται με 32. Έπειτα δηλώνεται μία μεταβλητή τύπου integer ως δείκτης στο περιεχόμενο της οποίας θα καταχωρείται στην θέση μνήμης που δείχνει και θα είναι η μεταβολή της μνήμης της με τον τρόπο που εκτελείται μέσα στον βρόγχο for. Η πρακτική αυτή είναι αρκετά προχωρημένη και πρέπει να εφαρμόζεται μόνο από προχωρημένους και έμπειρους προγραμματιστές καθώς η μέθοδος προγραμματισμού δυναμικής μνήμης επεμβαίνει στις θέσεις μνήμης ενός προγράμματος και αν δεν γίνει σωστά θα έχει καταστροφικές συνέπειες στην εκτέλεση του προγράμματος.

```
int *get_bits(int n, int bits_wanted){//get_bits is a function with pointer, n contains a seven digit integer
    int *bits = (int*) malloc(sizeof(int) * bits_wanted);
    int k;
    for(k=0; k<bits_wanted; k++){
        int mask = 1 << k;
        int masked_n = n & mask;
        int the_bit = masked_n >> k;
        bits[k] = the_bit;
    }
    return bits;
}
```

Εικόνα 2-4: Συνάρτηση μετατροπής δεκαδικού αριθμού σε δυαδικό.

Με την ολοκλήρωση των συναρτήσεων που παρουσιάστηκαν σε αυτήν την ενότητα ολοκληρώνεται το τμήμα του προγραμματισμού που αφορά την μετατροπή των δεδομένων στην επιθυμητή μορφή τους ώστε να μπορεί να πραγματοποιηθεί η διαδικασία κρυπτογράφησης τους η οποία αφορά άλλο τμήμα της κατασκευής του λογισμικού.

2.2.3 Ανάπτυξη Λογισμικού Κρυπτογράφησης

Η έννοια της κρυπτογράφησης περιλαμβάνει αρκετές έννοιες που πρέπει να είναι κατανοητές από τον σχεδιαστή της μεθόδου που θα εφαρμοστεί. Κατά κύριο λόγο αφορά τον σχεδιασμό και την εφαρμογή μιας μαθηματικής μεθόδου για την κωδικοποίηση ενός κειμένου ώστε να μην μπορεί να αναγνωστεί από μη εξουσιοδοτημένους παραλήπτες. Επομένως αφορά κυρίως μαθηματικές εφαρμογές και γνώσεις παρά λεκτικές και γλωσσικές ικανότητες από πλευράς του μηχανικού που θα σχεδιάσει το σύνολο της κρυπτογράφησης.

Για την δημιουργία του κλειδιού κρυπτογράφησης εφαρμόστηκε η μαθηματική μέθοδος χαοτικού χάρτη και για τα προς κρυπτογράφηση δεδομένα πραγματοποιήθηκαν αρκετές αριθμητικές μετατροπές ώστε να καταλήξουν σε μία επιθυμητή μορφή. Πέρα του ότι όλες οι ανωτέρω διαδικασίες ήταν απαραίτητες να εκτελεστούν για τον συγκεκριμένο σχεδιασμό, η διαδικασία τους συμβάλει στην περιπλοκότητα του συνόλου της κρυπτογράφησης αυξάνοντας τον παράγοντα προστασίας τους από απόπειρα παραβίασης τους από μη εγκεκριμένους παραλήπτες και συμπερασματικά προκύπτει πως είναι επιθυμητή η υπερβολική εφαρμογή μαθηματικών πράξεων, μετατροπών και μεθόδων.

Με την ίδια λογική επιλέγεται και η διαδικασία με την οποία θα χρησιμοποιηθεί το κλειδί κρυπτογράφησης ώστε να κρυπτογραφηθούν τα ευαίσθητα περιεχομένου δεδομένα. Καθώς τα προς κρυπτογράφηση δεδομένα αλλά και το κλειδί κρυπτογράφησης εκφράζονται ως αριθμοί του δυαδικού αριθμητικού συστήματος προκύπτει η επιλογή να μπορεί να εφαρμοστεί μεταξύ τους οποιαδήποτε αριθμητική πράξη αλλά και οποιαδήποτε λογική πράξη όπως ήδη έχει περιγραφεί στην μελέτη της παρούσας εργασίας στο πρώτο κεφάλαιο στην ενότητα 1.3.3 μέθοδος κρυπτογράφησης. Επιλέγοντας την τέλεση της λογικής πράξης XOR μεταξύ του κλειδιού κρυπτογράφησης και του δυαδικού αριθμού που αντιπροσωπεύει τα δεδομένα GPS προκύπτει ένας νέος αριθμός ο οποίος είναι η κρυπτογραφημένη ασφαλή πληροφορία των δεδομένων GPS. Στο σχήμα 2.5 διακρίνεται το τμήμα του κώδικα που τελεί την λογική πράξη XOR μεταξύ των μεταβλητών τύπου πίνακα που περιέχουν το κλειδί κρυπτογράφησης και την πληροφορία GPS.

```
int crypted[32];
for (i=0; i<bits_wanted; i++){
    crypted[i] = bstr[i] ^ bits[i];}
```

Εικόνα 2-5: Κώδικας κρυπτογράφησης.

Όπως στο πρόγραμμα που εκτελεί την διαδικασία κρυπτογράφησης, το πρόγραμμα που θα εκτελεί την διαδικασία αποκρυπτογράφησης θα πρέπει αρχικά να καταχωρήσει τα ληφθέντα κρυπτογραφημένα δεδομένα σε μία μεταβλητή τύπου bool. Στην συνέχεια θα πρέπει να εκτελέσει την ίδια συνάρτηση δημιουργίας του κλειδιού κρυπτογράφησης που εκτέλεσε το πρόγραμμα που εκτέλεσε την κρυπτογράφηση στον πομπό με την ίδια ακριβώς εξίσωση χαοτικού χάρτη και με την ίδια ακριβώς παραμετροποίηση του έτσι ώστε να είναι ικανό να παραγάγει το ίδιο ακριβώς κλειδί κρυπτογράφησης. Συμπερασματικά προκύπτει πως θα πρέπει ο προγραμματιστής να φροντίσει στο πρόγραμμα αποκρυπτογράφησης να υπάρχει ακριβώς η ίδια συνάρτηση παραγωγής κλειδιού κρυπτογράφησης με αυτήν που υπάρχει στο πρόγραμμα κρυπτογράφησης. Ο λόγος που είναι απαραίτητο αυτό είναι πως για την αποκρυπτογράφηση των κρυπτογραφημένων δεδομένων θα πρέπει να τελευτεί η λογική πράξη XOR μεταξύ αυτών και του κλειδιού κρυπτογράφησης ώστε να αποκρυπτογραφηθούν και να ανακτηθούν στην αρχική τους μορφή των 32 bit που είχαν πριν την κρυπτογράφηση. Έπειτα θα πρέπει να εκτελεστεί με την αντίστροφη σειρά η διαδικασία μετατροπών που τα μετέτρεψε από τύπου συμβολοσειράς σε δυαδική μορφή. Με την ανάκτηση τους στην αρχική τους μορφή θα είναι πλέον στον ίδιο τύπο δεδομένων που ήταν όταν λήφθηκαν από την συσκευή GPS και θα έχει ολοκληρωθεί με επιτυχία η διαδικασία κρυπτογράφησης/αποκρυπτογράφησης.

Με τα ανωτέρω συμπαιρένεται πως με την ανάπτυξη του κώδικα και την εκτέλεση του δοκιμάζεται η λειτουργία του στα διάφορα τμήματα του και συναρτήσεις και αποδεικνύεται πως η αρχική ιδέα είναι δυνατόν να υλοποιηθεί για το πλήρες περιεχόμενο της και να λειτουργήσει όπως σχεδιάστηκε στην μελέτη του.

2.3 Σύστημα μικροελεγκτή

Η εφαρμογή των συστημάτων μικροελεγκτών σε διάφορες ηλεκτρικές και/ή ηλεκτρονικές εφαρμογές αποτελεί ένα βήμα αναβάθμισης τους καθώς οι δυνατότητες τους ως ολοκληρωμένα υπολογιστικά συστήματα επιτρέπουν την ενσωμάτωση συστημάτων που επεκτείνουν τον αριθμό λειτουργιών και εξ’ αποστάσεως προσβασιμότητας τους συμβάλλοντας στην αυτοματοποίηση των περισσότερων ενεργειών εκτελώντας τις αυτόνομα είτε εν μέρη είτε εξ’ ολοκλήρου. Εξ’ αιτίας αυτού του χαρακτηριστικού τους βρίσκονται στο επίκεντρο σχεδόν κάθε συσκευής ώστε να αναλαμβάνουν και να διαχειρίζονται μία πληθώρα ενεργειών απαλλάσσοντας τον χρήστη από έναν μεγάλο βαθμό εργασιών διευκολύνοντας τον. Το χαρακτηριστικό της ανάθεσης της αυτονομίας είναι το σημείο κλειδί των συστημάτων μικροελεγκτών το οποίο προκαλεί την τόσο υψηλή απήχηση τους καθώς συνδυάζει την ανάληψη εργασιών και της διαχείρισης τους για έναν αριθμό συνθηκών που μπορεί να προβλέψει ο μηχανικός που θα σχεδιάσει το σύστημα αλλά και την ταχύτητα με την οποία θα τις εκτελέσει χάρη στην υπολογιστική ισχύ του.

Ένας μικροελεγκτής μπορεί να ληφθεί υπόψιν ως ένα αυτόνομο σύστημα επειδή συμπεριλαμβάνει στην κατασκευή του έναν ή και περισσότερους μικροεπεξεργαστές, μνήμη και περιφερειακά και έχει την δυνατότητα, αναλόγως τον σχεδιασμό να σχηματισθεί ως ένα ενσωματωμένο σύστημα. Η πλειοψηφία των μικροελεγκτών που χρησιμοποιούνται σήμερα είναι ενσωματωμένοι σε άλλα μηχανήματα, όπως αυτοκίνητα, τηλέφωνα, συσκευές και περιφερειακά για συστήματα υπολογιστών. Χάρη στα προχωρημένα τεχνολογικά συστήματα μικροελεγκτών ορισμένα ενσωματωμένα συστήματα είναι πολύ εξελιγμένα όμως πολλά έχουν ελάχιστες απαιτήσεις για την μνήμη και για το μέγεθος του προγράμματος που θα περιέχουν, λειτουργούν χωρίς λειτουργικό σύστημα και η πολυπλοκότητα του υλικολογισμικού που γράφεται στην μνήμη τους είναι χαρακτηριστικά χαμηλή. Οι τυπικές συσκευές που μπορούν να συνδεθούν στις θύρες εισόδου/εξόδου περιλαμβάνουν συσκευές ραδιοσυχνοτήτων, LED, διακόπτες, ρελέ, αισθητήρες, ηλεκτρομαγνητικές βαλβίδες και μικρές ή προσαρμοσμένες οθόνες

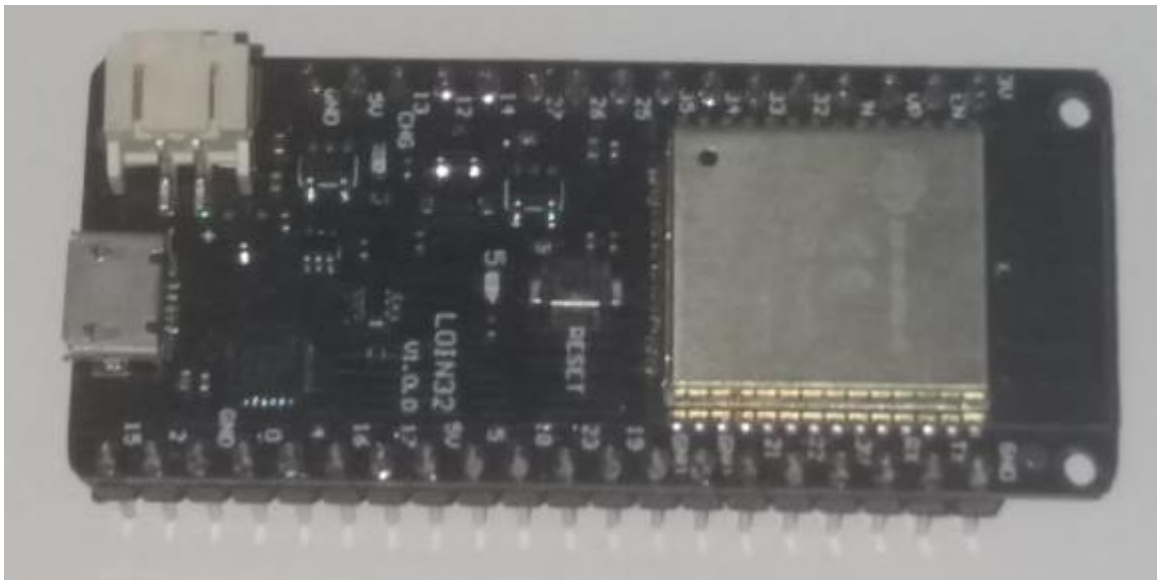
υγρών κρυστάλλων για δεδομένα όπως θερμοκρασία, υγρασία, επίπεδο φωτός κ.λπ. Τα ενσωματωμένα συστήματα συνήθως δεν έχουν πληκτρολόγιο, οθόνη, δίσκους , εκτυπωτές ή άλλες αναγνωρίσιμες συσκευές εισόδου/εξόδου ενός συμβατικού οικιακού ηλεκτρονικού υπολογιστή και ενδέχεται να μην υπάρχουν καθόλου συσκευές οποιουδήποτε είδους διεπαφής ανθρώπινης αλληλεπίδρασης με το σύστημα μικροελεγκτή.

Η κατασκευή συμπεριλαμβάνει ένα σύστημα μικροελεγκτών στου οποίου την μνήμη θα γραφτεί το πρόγραμμα με το οποίο θα μπορεί να εκτελεί έναν απαραίτητο αριθμό εργασιών για την ορθή και ολοκληρωμένη λειτουργία του συνόλου της κατασκευής. Το σύστημα μικροελεγκτή αποτελείται από ένα ζεύγος συστημάτων μικροελεγκτών τα οποία προορίζονται να εδραιώσουν μεταξύ τους επικοινωνία. Το πρωτόκολλο επικοινωνίας είναι το Wi-Fi που σημαίνει πως το ένα σύστημα μικροελεγκτή θα πρέπει να λειτουργεί ως server και το άλλο να λειτουργεί ως client. Η κύρια εργασία των δύο συστημάτων θα χωριστεί στα δύο και θα ανατεθεί από μισή σε κάθε σύστημα μικροελεγκτή. Το ένα θα συλλέγει τα δεδομένα συντεταγμένων από την συσκευή GPS, θα τα κρυπτογραφεί και θα τα εκπέμπει μέσω της κεραίας του και το άλλο θα λαμβάνει τα κρυπτογραφημένα δεδομένα μέσω της κεραίας του, θα τα αποκρυπτογραφεί και θα τα εμφανίζει στην οθόνη του υπολογιστή.

2.3.1 Το σύστημα μικροελεγκτή ESP32

Ένα από τα πιο διαδεδομένα συστήματα μικροελεγκτή για την ευχρηστία του είναι το ESP32. Παρέχει στον χρήστη για τον σχεδιασμό του μία πληθώρα συστημάτων και τις βιβλιοθήκες με τις οποίες μπορεί να τα λειτουργήσει και να τα παραμετροποιήσει. Αυτό που ενδιαφέρει στην συγκεκριμένη κατασκευή είναι το συμπεριλαμβανόμενο σύστημα ασύρματης επικοινωνίας Wi-Fi. Κοντά σε αυτό έχει πολλά άλλα χαρακτηριστικά που το καθιστούν κατάλληλο ως επιλογή του υλικού μέρους για την υλοποίηση της κατασκευής.

Συγκεκριμένα ο μικροελεγκτής που φέρει είναι ο ESP-WROOM-32 της Espressif ο οποίος περιέχει διπύρηνο μικροεπεξεργαστή ο οποίος λειτουργεί με ταχύτητα των 240MHz και είναι εξοπλισμένος με flash μνήμη 4MB χωρητικότητας η οποία επικοινωνεί με το ενσύρματο πρωτόκολλο επικοινωνίας SPI. Η μνήμη του δύναται να επεκταθεί στα 16MB χωρητικότητας. Οι δυνατότητες συνδεσιμότητας του περιλαμβάνουν το Wi-Fi 802,11b/g/n πρωτόκολλο ασύρματης επικοινωνίας με χαρακτηριστικά τα συστήματα ασφαλείας WEP και WPA/WPA2 PSK/Enterprise, ολοκληρωμένο κύκλωμα κρυπτογράφησης που υποστηρίζει τους αλγόριθμους AES/SHA2/Elliptical Curve Cryptography/RSA-4096, Μέγιστη ισχύ για μετάδοση δεδομένων: 19,5 dBm@11b, 16,5 dBm@11g, 15,5 dBm@11n και ευαισθησία μέγιστης λήψης ίση με -97 dBm και το πρωτόκολλο ασύρματης επικοινωνίας Bluetooth 4.0 LE. Παρέχει 32 θύρες εισόδων/εξόδων από τις οποίες οι 26 είναι ψηφιακές θύρες εισόδων/εξόδων στα 3,3V με δυνατότητα PWM, 18 θύρες εισόδων αναλογικού σήματος, 3 θύρες ενσύρματης επικοινωνίας πρωτοκόλλου UART, 3 θύρες ενσύρματης επικοινωνίας πρωτοκόλλου SPI, 2 θύρες ενσύρματης επικοινωνίας πρωτοκόλλου I2C, 2 θύρες εξόδου DAC και 2 θύρες ενσύρματης επικοινωνίας πρωτοκόλλου I2S. Παρέχει κατάσταση ύπνου με μέγιστη κατανάλωση τα 5μA και διεπαφή μπαταρίας Λιθίου με δυνατότητα φόρτισης τα 500mA. Στο σχήμα 2.6 απεικονίζεται το σύστημα μικροελεγκτή όπου στις δύο επιμήκεις πλευρές του διακρίνονται τα σημεία επαφής των θυρών εισόδων/εξόδων τα οποία είναι διαμπερή, ο μικροελεγκτής ο οποίος είναι το μεγάλο τετράγωνο ασημένιο αντικείμενο τοποθετημένο στο δεξί άκρο του όπου ακόμη πιο δεξιά διακρίνεται η τυπωμένη κεραία του, επάνω αριστερά η διεπαφή της μπαταρίας και αριστερά η θύρα USB.



Εικόνα 2-6: Σύστημα μικροελεγκτή ESP32.

Από τα ανωτέρω χαρακτηριστικά αυτό που ξεχωρίζει στην κατασκευή της παρούσας εργασίας είναι το πρωτόκολλο ασύρματης επικοινωνίας Wi-Fi το οποίο θα αξιοποιηθεί για την μετάδοση και λήψη μεταξύ των δύο συστημάτων μικροελεγκτών των κρυπτογραφημένων δεδομένων.

2.3.2 Ανάπτυξη του Υλικολογισμικού

Στην ενότητα 2.2 περιεγράφηκε η ανάπτυξη του λογισμικού που εκτελεί την διαδικασία κρυπτογράφησης μεταξύ των δεδομένων GPS και του κλειδιού κρυπτογράφησης. Το λογισμικό αυτό όμως είναι μόνο ένα μέρος του πλήρους προγράμματος που θα λειτουργήσει στα δύο συστήματα μικροελεγκτών.

Όσων αφορά το αντικείμενο των υπολογιστικών συστημάτων και συγκεκριμένα αυτών των μικροελεγκτών, το υλικολογισμικό αποτελεί μια συγκεκριμένη κατηγορία λογισμικού υπολογιστικού συστήματος που παρέχει τον έλεγχο χαμηλού επιπέδου για το συγκεκριμένο υλικό μιας συσκευής. Το υλικολογισμικό θα πρέπει να περιέχει τις βασικές λειτουργίες σε μορφή συναρτήσεων της συσκευής που αποτελεί το σύστημα μικροελεγκτή αλλά και την δυνατότητα να παρέχει υπηρεσίες αποσπώμενου υλικού σε λογισμικό υψηλότερου επιπέδου, όπως είναι για παράδειγμα τα λειτουργικά συστήματα. Για συσκευές που είναι πιο απλά κατασκευασμένες συγκρινόμενες με άλλες όπως είναι οι μικροελεγκτές που έχουν περιορισμένες δυνατότητες, το υλικολογισμικό μπορεί να λειτουργεί ως το πλήρες λειτουργικό σύστημα της συσκευής μικροελεγκτή, εκτελώντας με αυτόν τον τρόπο όλες τις λειτουργίες ελέγχου, παρακολούθησης και χειρισμού των δεδομένων.

Επομένως λαμβάνοντας υπόψιν τις περιορισμένες δυνατότητες του υπολογιστικού συστήματος μικροελεγκτή θα πρέπει να συμπεριληφθεί το λογισμικό που γράφτηκε στο IDE της Visual Studio της Microsoft το οποίο εκτελεί τις διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης σε ένα πιο σύνθετο υλικολογισμικό το οποίο θα πρέπει να εκτελεί περισσότερες λειτουργίες. Αρχικά θα πρέπει να συμπεριλάβει στο υλικολογισμικό του τον τρόπο ανάγνωσης της συσκευής του GPS σήματος σε κάποια από τις σειριακές του εισόδους του συστήματος μικροελεγκτή και συγκεκριμένα στις θύρες εισόδων/εξόδων RX/TX. Αυτό σημαίνει πως θα συνδεθούν αντίστοιχα στις θύρες εισόδων/εξόδων RX/TX που φέρει η συσκευή GPS. Ο τρόπος σύνδεσης γίνεται ενσύρματα και περιλαμβάνει κάποιες ιδιαιτερότητες κατά την υλοποίηση του. Η κυριότερη εκ των οποίων είναι πως θα πρέπει η TX θύρα

του συστήματος μικροελεγκτή, η οποία είναι αυτή που θα μεταδίδει τα δεδομένα του συστήματος μικροελεγκτή προς την συσκευή GPS, να συνδεθεί με την RX θύρα της συσκευής GPS και αντίστοιχα η TX θύρα της συσκευής GPS, η οποία είναι αυτή που θα μεταδίδει τα δεδομένα της συσκευής GPS προς το σύστημα μικροελεγκτή, να συνδεθεί με την RX θύρα του συστήματος μικροελεγκτή διαφορετικά δεν θα εδραιωθεί η επικοινωνία μεταξύ συστήματος μικροελεγκτή και συσκευής GPS και το πρωτόκολλο επικοινωνίας δεν θα είναι δυνατόν να εφαρμοστεί.

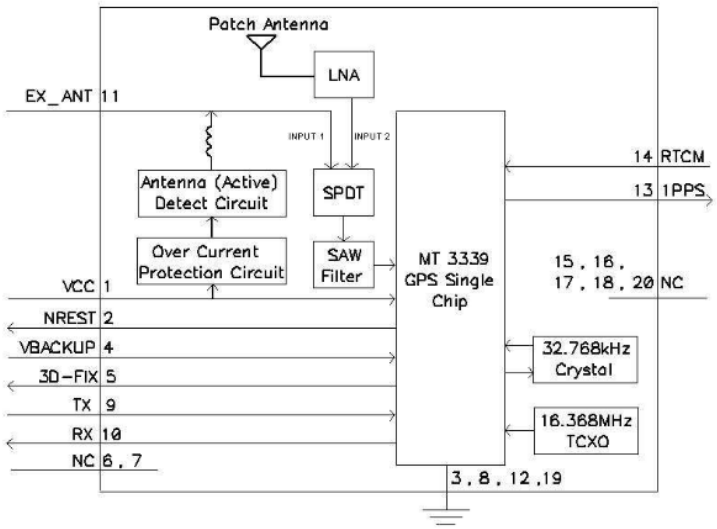
2.3.3 Υλικολογισμικό και Υλικό Συσκευής GPS

Για να γραφτεί σωστά το υλικολογισμικό που αφορά την συσκευή GPS θα πρέπει αρχικά να είναι γνωστές οι θύρες εισόδων/εξόδων της συσκευής GPS και να συνδεθούν σωστά και κατάλληλα με τις ανάλογες και απαραίτητες θύρες εισόδων/εξόδων του συστήματος μικροελεγκτή.

- Συγκεκριμένα, όπως φαίνεται στο σχήμα 2.7 θα πρέπει αρχικά να τροφοδοτηθεί η συσκευή GPS συνδέοντας τους ακροδέκτες με την αρίθμηση 1 και 3,8,12 και 19. Στον ακροδέκτη με την αρίθμηση 1 θα πρέπει να συνδεθεί η διαφορά δυναμικού τάσης η οποία σύμφωνα με το Datasheet της συσκευής GPS θα πρέπει να ισούται με 3,3V η οποία μπορεί να παρέχεται απευθείας από το σύστημα μικροελεγκτή καθώς φέρει την δυνατότητα. Ένας παράγοντας που πρέπει να ληφθεί υπόψιν και πρέπει να εξετάζεται είναι το αν η παροχή από το σύστημα μικροελεγκτή μπορεί να παρέχει και το απαιτούμενο ρεύμα κατανάλωσης της συσκευής GPS. Σύμφωνα με τα Datasheet του συστήματος μικροελεγκτή και της συσκευής GPS προκύπτει πως η μέγιστη κατανάλωση της συσκευής GPS κατά την λειτουργία της ισούται με 25mA και πως η μέγιστη παροχή ρεύματος του συστήματος μικροελεγκτή ισούται με 40mA, επομένως η παροχή του συστήματος μικροελεγκτή υπερκαλύπτει της ανάγκες τροφοδοσίας της συσκευής GPS και έτσι μπορεί να συνδεθεί απευθείας σε αυτήν χωρίς να υπάρξει κάποιο πρόβλημα στην κατάσταση λειτουργίας της.
- Οι ακροδέκτες με αρίθμηση3,8,12 και 19 αφορούν την γείωση της συσκευής GPS και η σωστή διασύνδεση τους απαιτεί αρχικά την μεταξύ τους βραχυκύκλωση και έπειτα να συνδεθούν σε κάποια από τις γειώσεις του συστήματος μικροελεγκτή. Αυτό συμβαίνει διότι στο σύστημα μικροελεγκτή οι γειώσεις του μικροελεγκτή είναι ήδη συνδεδεμένες μεταξύ τους βάση σχεδιασμού μέσω της πλακέτας βακελίτη στην οποία είναι τοποθετημένος ενώ η συσκευή GPS δεν είναι τοποθετημένη σε πλακέτα βακελίτη αλλά είναι μία αυτόνομη μονάδα σε μορφή ολοκληρωμένου κυκλώματος.
- Οι ακροδέκτες με την αρίθμηση 6, 7, 15,16,17, 18 και 20 έχουν την ένδειξη NC που σημαίνει πως πρέπει να παραμείνουν ασύνδετοι.
- Ο ακροδέκτης με την αρίθμηση 2 αφορά τον διακόπτη επαναφοράς της συσκευής ο οποίος ενεργοποιείται όταν θα εφαρμοστεί σε αυτόν διαφορά δυναμικού που θα ισούται με το μηδέν. Εφόσον στον σχεδιασμό αυτό είναι κάτι το οποίο προκύπτει όχι μόνο αχρείαστο αλλά και ανεπιθύμητο, θα είναι βραχυκυκλωμένο με την διαφορά δυναμικού της τροφοδοσίας έτσι ώστε κατά την ενεργή κατάσταση λειτουργίας της συσκευής GPS να παραμένει μόνιμα σε κατάσταση υψηλής διαφοράς δυναμικού και να μην έρχεται ποτέ σε κατάσταση διαφοράς δυναμικού ίσης με το μηδέν.
- Ο ακροδέκτης με την αρίθμηση 4 αφορά την εφεδρική είσοδο ισχύος για την διατήρηση των δεδομένων RTC και πλοήγησης. Καθώς δεν είναι μέρος του σχεδιασμού της εργασίας και δεν επηρεάζει με κάποιον τρόπο την συνολική κατασκευή με το αν θα παραμείνει ασύνδετος ο συγκεκριμένος ακροδέκτης, θα μείνει ως έχει, δηλαδή μη συνδεδεμένος.
- Ο ακροδέκτης με την αρίθμηση 5 αφορά την ένδειξη κλειδώματος του σήματος τριών διαστάσεων. Δίνει την επιλογή να τοποθετηθεί ένας φωτεινός ενδείκτης ο οποίος θα ενημερώνει για το πότε η συσκευή του δέκτη GPS θα έχει εντοπιστεί από τουλάχιστον τέσσερις δορυφόρους του δορυφορικού δικτύου εντοπισμού θέσης ώστε να μπορεί να λάβει την πληροφορία της τοποθεσίας της.
- Οι ακροδέκτες με την αρίθμηση 9 και 10 αφορούν τις θύρες εισόδου/εξόδου σειριακής επικοινωνίας και ονομάζονται αντίστοιχα TX και RX. Στην κατασκευή θα συνδεθούν με τις

αντίστοιχες θύρες εισόδου/εξόδου σειριακής επικοινωνίας TX/RX του συστήματος μικροελεγκτή.

- Ο ακροδέκτης με την αρίθμηση 11 αφορά την θύρα σύνδεσης εξωτερικής κεραίας. Καθώς δεν έχει συμπεριληφθεί στον αρχικό σχεδιασμό και δεν επηρεάζει με κάποιον αρνητικό τρόπο την κατασκευή με το να παραμείνει ασύνδετος δεν θα συνδεθεί πουθενά.
- Ο ακροδέκτης με την αρίθμηση 13 αφορά την παροχή τροφοδοσίας διαφοράς δυναμικού 2,8V για CMOS τεχνολογία. Καθώς δεν έχει συμπεριληφθεί στον αρχικό σχεδιασμό και δεν επηρεάζει με κάποιον αρνητικό τρόπο την κατασκευή με το να παραμείνει ασύνδετος δεν θα συνδεθεί πουθενά.
- Ο ακροδέκτης με την αρίθμηση 14 αφορά είσοδο σειριακών δεδομένων DGPS RTCM. Καθώς δεν έχει συμπεριληφθεί στον αρχικό σχεδιασμό και δεν επηρεάζει με κάποιον αρνητικό τρόπο την κατασκευή με το να παραμείνει ασύνδετος δεν θα συνδεθεί πουθενά.



Εικόνα 2-7: Σχεδιάγραμμα συσκευής GPS.

Επιπλέον είναι απαραίτητη η συμπερίληψη μίας ηλεκτρονικής διάταξης για την καλύτερη και ομαλότερη λειτουργία της συσκευής GPS. Συγκεκριμένα το να συνδεσμολογηθεί ένας φωτεινός ενδείκτης στον ακροδέκτη με αρίθμηση 5 ώστε να μπορεί να ενημερωθεί ο χρήστης για την κατάσταση επικοινωνίας του δέκτη με το δορυφορικό δίκτυο θα είναι μία ωφέλιμη παροχή στο σύνολο της κατασκευής. Επίσης το να προστεθεί στην είσοδο της τροφοδοσίας στον ακροδέκτη με αρίθμηση 1 ένα χωρητικό στοιχείο θα ωφελήσει στην σταθεροποίηση της μέσης τιμής τροφοδοσίας.

Για όλα τα ανωτέρω επιλέχθηκε η υλοποίηση τους σε μία διάτρητη πλακέτα βακελίτη. Οι διάτρητες πλακέτες βακελίτη προσφέρουν κάποια σημαντικά οφέλη κατά την διαδικασία της πρώιμης υλοποίησης μιας πλακέτας όπως τον εύκολο πειραματισμό των αγωγών που βρίσκονται μεταξύ των ηλεκτρονικών στοιχείων καθώς η υλοποίηση αυτών των αγωγών πραγματοποιείται με την τοποθέτηση καλωδίων τα οποία συγκολλούνται μόνο τα άκρα τους στο σημείο ένωσης των ηλεκτρονικών στοιχείων με την διάτρητη πλακέτα βακελίτη. Ένα άλλο όφελος είναι ότι προσφέρει χωροταξική ευελιξία στον μηχανικό ώστε να δοκιμάσει στην επιφάνεια της διάτρητης πλακέτας βακελίτη πολλούς και διάφορους συνδυασμούς στοιχείων ώστε να διαπιστώσει έμπρακτα την πιο βολική χωροταξία των ηλεκτρονικών υλικών σε σχέση με τους αγωγούς που θα τα ενώνουν. Το κύριο χαρακτηριστικό των διάτρητων πλακετών βακελίτη είναι πως το επίπεδο τους είναι συμμετρικά διαμπερές σε μορφή πλέγματος όπου η κάθε τρύπα απέχει ίσα από το κέντρο της με όλες τις διπλανές της με την πρότυπη πιστοποιημένη απόσταση των 2,53 χιλιοστών του μέτρου. Η απόσταση αυτή απαντάται στην κατασκευή των ολοκληρωμένων κυκλωμάτων όπου η μεταξύ απόσταση των ακροδεκτών τους από το κέντρο τους είναι

ίση με 2,53 χιλιοστά του μέτρου. Τέλος η διάτρητη πλακέτα βακελίτη παρέχει από την μία πλευρά της γύρω από κάθε τρύπα μία ομόκεντρη επιφάνεια χαλκού ώστε να μπορεί αφενός να συγκολληθεί ο ακροδέκτης ενός υλικού στοιχείου έτσι ώστε αυτό να μπορεί να παραμείνει σταθερό στην πλακέτα και αφετέρου να μπορούν να συγκολληθούν οι άκρες των καλωδίων που θα χρησιμέψουν ως αγωγοί της κατασκευής.

Καθώς η συσκευή GPS ανήκει σε μία ιδιαίτερη κατηγορία σχεδιασμού από την εταιρεία που την κατασκεύασε διότι πρώτον οι αποστάσεις των ακροδεκτών της απέχουν μεταξύ τους από το κέντρο τους 1,265 χιλιοστών του μέτρου το οποίο είναι το μισό σε απόσταση από το τυποποιημένο σύνηθες για τέτοιες συσκευές και δεύτερον οι ακροδέκτες της συσκευής δεν είναι σχεδιασμένοι για να εφαρμόζονται σε διαμπερή ηλεκτρονική πλακέτα βακελίτη αλλά έχουν κατασκευαστεί έτσι ώστε να ανήκουν στην κατηγορία ηλεκτρονικών στοιχείων επιφανείας όπου τα ηλεκτρονικά στοιχεία αυτά κολλιούνται απευθείας στην επιφάνεια της ηλεκτρονικής πλακέτας βακελίτη σε ειδικά προσχεδιασμένες επιφάνειες χαλκού για το στοιχείο που πρόκειται να υποδεχτούν. Για τον λόγο αυτόν πραγματοποιήθηκε ειδικά σχεδιασμένη προσαρμογή ώστε να εφαρμοστεί η συσκευή στο πλέγμα της διάτρητης πλακέτας βακελίτη των αποστάσεων μεταξύ των διαμπερών τρυπών της των 2,53 χιλιοστών του μέτρου όπως φαίνεται στο σχήμα 2.8.

Όπως μπορεί να διακριθεί για κάθε ακροδέκτη της συσκευής GPS συγκολλήθηκε ένας ακροδέκτης αγωγός καλωδίου ο οποίος στην συνέχεια πέρασε διαμπερές από την διάτρητη πλακέτα βακελίτη ώστε να συγκολληθεί από την άλλη πλευρά στα σημεία χαλκού κάθε τρύπας της και να προσαρμοστεί με αυτόν τον τρόπο η κλίμακα του πλέγματος των ακροδεκτών της συσκευής στην κλίμακα του πλέγματος της διάτρητης πλακέτας βακελίτη. Τέτοιες πρακτικές εφαρμόζονται ως πρόχειρη λύση όταν τον το στάδιο της κατασκευής βρίσκεται ακόμη στο μέσο της υλοποίησης προκειμένου να επικεντρωθεί η προσπάθεια στην επιτυχή λειτουργία της συσκευής ως κύκλωμα.

Εικόνα 2-8: Τροποποίηση προσαρμογής συσκευής GPS στην διάτρητη πλακέτα βακελίτη.

Στην συνέχεια όταν λειτουργήσει σε βασικό επίπεδο η κατασκευή για το σύνολο των ηλεκτρονικών διατάξεων, συσκευών και συστημάτων πραγματοποιούνται διορθώσεις που προβλέπουν πλέον λεπτομέρειες στον σχεδιασμό οι οποίες δεν είχαν διακριθεί σε προηγούμενο σχεδιαστικό στάδιο.

Για την υλοποίηση της ηλεκτρονικής διάταξης που θα περιλαμβάνει έναν φωτεινό ενδείκτη επιλέχθηκε ένα LED κόκκινου φωτός. Τα LED είναι φθηνά ηλεκτρονικά στοιχεία που υπάρχουν σε πληθώρα στην αγορά και είναι εύκολη η συμπερίληψη τους στο σύνολο μίας διάταξης. Συγκεκριμένα θα συνδεθεί ορθά πολωμένο στον ακροδέκτη με αρίθμηση 5, δηλαδή η κάθοδος της διόδου LED θα συγκολληθεί στον ακροδέκτη 5 της συσκευής GPS και στην άνοδο θα συγκολληθεί το ένα άκρο μίας αντίστασης με ωμική τιμή ίσης των 330Ω και το άλλο της άκρο θα συγκολληθεί με τον ακροδέκτη με αρίθμηση 8 ο οποίος είναι ένας από τις γειώσεις της συσκευής GPS. Τα αρχικά της σύντμησης LED αντιστοιχούν στις Αγγλικές λέξεις Light Emitting Diode (Δίοδος Εκπομπής Φωτός) η οποία αφορά στο σύνολο της ως ηλεκτρονικό στοιχείο μία πηγή φωτός κατασκευασμένη από ένα υλικό ημιαγωγού το οποίο έχει την ιδιότητα να εκπέμπει φως όταν διαρρέεται από ένα ελάχιστο ρεύμα. Επί της ουσίας τα ελεύθερα ηλεκτρόνια που υπάρχουν στο υλικό ημιαγωγού ανασυνδυάζονται με τις οπές των κατιόντων, των θετικά φορτισμένων ατόμων δηλαδή, στις ασθενές στιβάδες ηλεκτρονίων των ατόμων και

απελευθερώνοντας κατά συνέπεια ενέργεια στην μορφή φωτονίων. Το χρώμα του φωτός που αποδίδει το LED (το οποίο αντιστοιχεί στην ενέργεια των φωτονίων) καθορίζεται από την ενέργεια που απαιτείται για να διασχίσουν τα ηλεκτρόνια το διάκενο ζώνης του ημιαγωγού. Το λευκό φως προκύπτει από την μίξη πολλαπλών ημιαγωγών ή εναλλακτικά από την εφαρμογή ενός επιπλέον στρώματος φωσφόρου επί του υλικού ημιαγωγού το οποίο θα λειτουργεί ως πηγή φωτός στη συσκευή ημιαγωγού. Ως ηλεκτρονικά εξαρτήματα πρωτοεμφανίστηκαν το 1962 και τα πρώτα LED εκπέμπαν φως στο υπέρυθρο φάσμα (IR) το οποίο ήταν χαμηλής έντασης. Τα υπέρυθρα LED χρησιμοποιούνται μέχρι σήμερα σε εφαρμογές τηλεχειρισμού όπως για παράδειγμα αυτά που χρησιμοποιούνται σε μεγάλη ποικιλία ηλεκτρονικών ειδών ευρείας κατανάλωσης για οικιακή χρήση. Τα πρώτα LED ορατού φωτός ήταν χαμηλής έντασης και περιορίζονταν φασματικά στην χρωματική περιοχή του κόκκινου. Τα πρώτα LED χρησιμοποιήθηκαν συχνά ως ενδεικτικές λυχνίες, αντικαθιστώντας μικρούς λαμπτήρες πυρακτώσεως και σε οθόνες επτά τμημάτων για τον σχηματισμό αριθμών. Οι πιο πρόσφατες τεχνολογικές εξελίξεις έχουν δημιουργήσει LED που εκπέμπουν στο ορατό, υπεριώδες (UV) και υπέρυθρο φάσμα με υψηλή, χαμηλή και ενδιάμεση απόδοση έντασης του φωτός όπως για παράδειγμα λευκά LED κατάλληλα για φωτισμό δωματίου ή/και εξωτερικού χώρου. Η ανάπτυξη της τεχνολογίας των LED έχει οδηγήσει στην δημιουργία νέων τύπων οθονών και αισθητήρων, ενώ οι υψηλοί ρυθμοί εναλλαγής τους είναι χρήσιμοι στην προηγμένη τεχνολογία επικοινωνιών με εφαρμογές τόσο διαφορετικές μεταξύ τους όπως ο αεροφωτισμός, τα φώτα νεράιδων, προβολείς αυτοκινήτου, στη διαφήμιση, γενικός φωτισμός, σήματα κυκλοφορίας, φλας κάμερας, κηπευτικά φώτα καλλιέργειας και ιατρικές συσκευές. Τα LED έχουν πολλά πλεονεκτήματα σε σχέση με τις πηγές φωτός πυρακτώσεως όπως είναι η χαμηλότερη κατανάλωση ενέργειας, η μεγαλύτερη διάρκεια ζωής, βελτιωμένη φυσική στιβαρότητα, μικρότερο μέγεθος και ταχύτερους ρυθμούς εναλλαγής. Σε αντιστοιχία αυτών των χαρακτηριστικών, τα μειονεκτήματα των LED περιλαμβάνουν ηλεκτρικούς περιορισμούς στη χαμηλή τάση και γενικά στην ισχύ συνεχούς ρεύματος (όχι εναλλασσόμενου ρεύματος), αδυναμία παροχής σταθερού φωτισμού από μια παλμική πηγή τροφοδοσίας συνεχούς ή εναλλασσόμενου ρεύματος και μικρότερη μέγιστη θερμοκρασία λειτουργίας και αποθήκευσης θερμοκρασίας. Τα LED συνήθως χρειάζονται ηλεκτρονικά εξαρτήματα υποστήριξης για να λειτουργήσουν.

Τα σήματα συνεχούς ρεύματος θεωρούνται λανθασμένα ως σήματα καθαρά χωρίς θόρυβο και με χαρακτηριστικό το ότι είναι ορισμένο ως σήμα 0Hz. Στην πραγματικότητα όμως είναι ένα σύνολο διάφορων σημάτων θορύβου με εύρος συχνοτήτων από σχεδόν 0HZ μέχρι την κλίμακα των GHz τα οποία όμως έχουν ακραία χαμηλό πλάτος έτσι ώστε να απεικονίζονται σαν σταθερή γραμμή όταν αυτά ανιχνεύονται στον παλμογράφο και είναι δυνατόν κάποια από αυτά τα σήματα να φιλτραριστούν με την εφαρμογή ενός χωρητικού στοιχείου σε μορφή ηλεκτρονικής διάταξης. Το ηλεκτρονικό στοιχείο που φέρει χωρητικές ιδιότητες ονομάζεται πυκνωτής και είναι ένα από τα τρία βασικά ηλεκτρονικά στοιχεία μεταξύ των αντιστάσεων και των πηνίων. Ένας πυκνωτής είναι μια συσκευή που μπορεί να αποθηκεύει ηλεκτρική ενέργεια σε μορφή ηλεκτρικού πεδίου και είναι ένα παθητικό ηλεκτρονικό στοιχείο με δύο ακροδέκτες που μπορεί να έχουν ή όχι πολικότητα. Το ηλεκτρικό μέγεθος που διαχειρίζεται ένας πυκνωτής είναι γνωστό ως χωρητικότητα. Η χωρητικότητα υπάρχει συνήθως παντού στα ηλεκτρονικά και ηλεκτρικά κυκλώματα σε παρασιτική μορφή ακόμη και μεταξύ οποιωνδήποτε δύο ή και περισσότερων ηλεκτρικών αγωγών, το στοιχείο ενός πυκνωτή είναι ένα εξάρτημα που έχει σχεδιαστεί για να προσθέτει εσκεμμένα χωρητικότητα συγκεκριμένου μεγέθους σε ένα κύκλωμα. Η φυσική μορφή του ως ηλεκτρονικό στοιχείο και η κατασκευή τους ποικίλλει ευρέως καθώς υπάρχουν πολλοί τύποι πυκνωτών οι οποίοι βρίσκονται σε κοινή χρήση στις πρακτικές εφαρμογές σύνθεσης ηλεκτρονικών κυκλωμάτων. Οι περισσότεροι πυκνωτές περιέχουν τουλάχιστον δύο ακροδέκτες οι οποίοι οδηγούν σε μεταλλικές πλάκες ή σε επιφάνειες μεταξύ των οποίων εφαρμόζεται για την μεταξύ του μόνωση ένα

διηλεκτρικό μέσο. Οι πλάκες αυτές μπορεί να είναι από ένα φύλλο, λεπτό φιλμ, συντηγμένο σφαιρίδιο μετάλλου ή ηλεκτρολύτης. Το μη αγώγιμο διηλεκτρικό εφαρμόζεται με σκοπό την αύξηση της χωρητικότητας φόρτισης του πυκνωτή και τα υλικά που χρησιμοποιούνται συνήθως ως διηλεκτρικά μέσα περιλαμβάνουν το γυαλί, κεραμικό, πλαστικό φιλμ, χαρτί, μαρμαρυγία, αέρα και στρώματα οξειδίου. Οι πυκνωτές χρησιμοποιούνται ευρέως ως μέρη ηλεκτρικών και ηλεκτρονικών κυκλωμάτων σε πολλές κοινές ηλεκτρικές συσκευές. Όταν εφαρμόζεται μια διαφορά ηλεκτρικού δυναμικού (τάση) στους ακροδέκτες ενός πυκνωτή όπως για παράδειγμα όταν ένας πυκνωτής συνδέεται σε μια μπαταρία, ένα ηλεκτρικό πεδίο αναπτύσσεται κατά μήκος του διηλεκτρικού προκαλώντας τη συλλογή καθαρού θετικού φορτίου στην μια του πλάκα και συγκεκριμένα σε αυτήν που είναι συνδεδεμένη στον θετικό πόλο της μπαταρίας ενώ στην αντίστοιχη πλάκα που είναι συνδεδεμένη στον αρνητικό πόλο της μπαταρίας προκαλείται η συλλογή καθαρού αρνητικού φορτίου. Στην πραγματικότητα δεν ρέει καθόλου ρεύμα μέσω του διηλεκτρικού, ωστόσο υπάρχει μια ροή φορτίου μέσω του κυκλώματος πηγής. Εάν η κατάσταση αυτή διατηρηθεί επαρκώς για ένα ελάχιστο χρονικό διάστημα το ρεύμα μέσω του κυκλώματος της πηγής παύει να ρέει. Εάν όμως εφαρμοστεί μια χρονικά μεταβαλλόμενη τάση στους ακροδέκτες του πυκνωτή η πηγή υφίσταται μία συνεχή ροή ρεύματος λόγω των κύκλων φόρτισης και εκφόρτισης του πυκνωτή. Λαμβάνοντας όλα τα ανωτέρω υπόψιν θα συγκολληθούν στην διάτρητη πλακέτα βακελίτη που φέρει την συσκευή GPS δύο πυκνωτές σε μεταξύ τους παραλληλία πρώτον για να φιλτράρουν τους ανεπιθύμητους θορύβους του συνεχούς ρεύματος και δεύτερον για να σταθεροποιήσουν την τροφοδοσία λειτουργίας της συσκευής στον χρόνο συναρτήσει την τάση. Αυτό συμβαίνει διότι στις ηλεκτροτεχνικές ιδιότητες των πυκνωτών ισχύει πως οι χωρητικότητες δύο ή και περισσότερων πυκνωτών προστίθενται όταν αυτοί συνδεσμολογηθούν παράλληλα ο ένας προς τον άλλον. Προκύπτει απαραίτητη η χρήση δύο πυκνωτών καθώς από τα φύλλα δεδομένων της συσκευής GPS ο κατασκευαστής παρέχει την πληροφορία πως το συγκεκριμένο χωρητικό στοιχείο θα πρέπει να ισούται με χωρητικότητα 1,01 μF. Για τον σχηματισμό διάταξης η οποία θα είναι δυνατόν να αποδώσει αυτήν την τιμή χωρητικότητας καθώς δεν υπάρχει στο εμπόριο τυποποιημένο στοιχείο με τέτοια τιμή χωρητικότητας υπάρχουν δύο πιθανές λύσεις που μπορούν να αποδώσουν αυτήν την τιμή. Η πρώτη λύση θα είναι να γίνει χρήση μεταβλητού πυκνωτή ο οποίος θα μπορεί να ρυθμιστεί με ακρίβεια στην τιμή των 1,01 μF. Τα μειονεκτήματα της λύσης αυτής είναι πως πρώτον ένας τέτοιος πυκνωτής κοστίζει πολύ περισσότερο από έναν τυποποιημένο πυκνωτή συγκεκριμένης χωρητικής τιμής και δεύτερον ένας τέτοιος πυκνωτής καταλαμβάνει περισσότερο χώρο σε όγκο από ότι ένας τυποποιημένος πυκνωτής συγκεκριμένης χωρητικής τιμής. Η δεύτερη λύση είναι να εξεταστεί η κατά προσέγγιση υλοποίηση μιας διάταξης πυκνωτών οι οποίοι να μπορούν κάνοντας χρήση δύο ή και περισσότερων πυκνωτών να αποδώσουν την συγκεκριμένη χωρητική τιμή. Στο εμπόριο υπάρχουν διαθέσιμοι πυκνωτές ηλεκτρολυτικού τύπου οι οποίοι φέρουν την χωρητική τιμή του ενός μF επομένως απομένει να καλυφτούν ακόμη 0,01 μF ή αλλιώς 10 nF. Και πάλι στο εμπόριο υπάρχουν διαθέσιμοι πυκνωτές διαφόρων τύπων οι οποίοι φέρουν την χωρητική τιμή των δέκα nF. Οι διαφορές που παρουσιάζουν μεταξύ τους οι διάφοροι τύποι είναι τέτοιες που για την λειτουργία και εφαρμογή του κυκλώματος δεν το επηρεάζουν με κάποιον ιδιαίτερο τρόπο επομένως μπορεί να επιλεγεί ένας πυκνωτής δέκα nF οποιουδήποτε τύπου. Με την επιλογή δύο πυκνωτών θα πρέπει κατά την υλοποίηση της κατασκευής να δοθεί προσοχή στην σύνδεση του ηλεκτρολυτικού πυκνωτή καθώς οι πυκνωτές αυτού του τύπου έχουν πολικότητα που σημαίνει πως έχει σημασία σε ποιο δυναμικό θα συνδεθεί ο κάθε ακροδέκτης του. Θα πρέπει στην συσκευή GPS οι πυκνωτές να συγκολληθούν και οι δύο με το ένα άκρο των ακροδεκτών τους στον ακροδέκτη με αρίθμηση 1 της συσκευής GPS και με το άλλο άκρο τους στον ακροδέκτη με αρίθμηση 3 της συσκευής GPS όπου για τον ηλεκτρολυτικό ισχύει πως ο ακροδέκτης που φέρει την ένδειξη “+” θα πρέπει να συγκολληθεί στον ακροδέκτη με αρίθμηση 1 της συσκευής GPS και ο

ακροδέκτης που φέρει την ένδειξη "-" θα πρέπει να συγκολληθεί στον ακροδέκτη με αρίθμηση 3 της συσκευής GPS.

Όπως διακρίνεται στο σχήμα 2.8 η διάτρητη πλακέτα βακελίτη στην οποία έχει προσαρμοστεί η συσκευή GPS περιβάλλεται από ακροδέκτες τύπου header αρσενικούς. Αυτό συμβαίνει διότι υπάρχει άλλη μία πλακέτα η οποία φέρει το σύστημα μικροελεγκτή και μία βάση η οποία υλοποιήθηκε με ακροδέκτες τύπου header θηλυκούς έτσι ώστε να μπορεί να δεχθεί την διάτρητη πλακέτα βακελίτη που φέρει την συσκευή GPS έτσι ώστε να είναι αποσπώμενη.

Το υλικολογισμικό που αφορά την διαχείριση της συσκευής GPS θα εκτελεί έναν ελάχιστο αριθμό διεργασιών από πλευράς του συστήματος μικροελεγκτή όπου πρωτίστως θα ανιχνεύει την ύπαρξη της συσκευής GPS, θα την τροφοδοτεί προκειμένου να λειτουργεί με επάρκεια και τέλος θα λαμβάνει από αυτήν μέσω σειριακής επικοινωνίας τα δεδομένα της συσκευής GPS τα οποία θα αποτελούνται από τις συντεταγμένες σε σύστημα τριών διαστάσεων και από τις πληροφορίες χρόνου. Τα δεδομένα αυτά θα παρέχονται από το δίκτυο δορυφόρων που βρίσκονται σε τροχιά, στο σύνολο τους είναι 24 αλλά η συσκευή του δέκτη πρέπει να ανιχνευτεί από τουλάχιστον τέσσερις ώστε να δώσει τις πληροφορίες του στίγματος της στο σύστημα μικροελεγκτή. Τα δεδομένα που δέχεται ως δέκτης η συσκευή GPS τα προωθεί μέσω της σειριακής της εξόδου προς την σειριακή θύρα του συστήματος μικροελεγκτή σε μορφή δεδομένων ακολουθίας χαρακτήρων. Επομένως στο υλικολογισμικό συμπεριλαμβάνεται η βιβλιοθήκη με την ονομασία <HardwareSerial.h> με την οποία γίνεται η διαχείριση από το σύστημα μικροελεγκτή των δεδομένων που εμφανίζονται στην σειριακή είσοδο του συστήματος μικροελεγκτή συγκεκριμένα για την συσκευή GPS η οποία είναι συνδεδεμένη σε αυτό ώστε να μπορεί να αναγνωρίζει σωστά τις ακολουθίες δεδομένων ως προς το που αρχίζει το σύνολο του κάθε πακέτου δεδομένων και που τελειώνει. Με όλα τα παραπάνω ολοκληρώνεται η ενότητα που αφορά το υλικό μέρος της συσκευής GPS και το τμήμα του υλικολογισμικού που χρειάζεται για το σύστημα μικροελεγκτή που λειτουργεί ως πομπός.

2.3.4 Πρωτόκολλο επικοινωνίας Wi-Fi στο υλικολογισμικό της κατασκευής

Το Wi-Fi αντιπροσωπεύει ένα σύνολο πρωτοκόλλων ασύρματου δικτύου που έχει βασιστεί στο σύνολο προτύπων IEEE 802.11 τα οποία συνήθως εφαρμόζονται σε τοπική δικτύωση συσκευών για την πρόσβαση τους στο διαδίκτυο επιτρέποντας σε κοντινές ψηφιακές συσκευές την ανταλλαγή δεδομένων μέσω του δρομολογητή. Τα ασύρματα αυτά δίκτυα είναι τα πιο ευρέως χρησιμοποιούμενα δίκτυα υπολογιστών στον κόσμο τα οποία χρησιμοποιούνται παγκοσμίως σε οικιακά δίκτυα και δίκτυα μικρών γραφείων για τη σύνδεση σε αυτά επιτραπέζιων και φορητών ηλεκτρονικών υπολογιστών, tablet, smartphone, σύγχρονων έξυπνων τηλεοράσεων, εκτυπωτών και έξυπνων ηχείων για την μεταξύ τους σύνδεση μέσω του ασύρματου δρομολογητή αλλά και για τη σύνδεση τους στο διαδίκτυο και γενικότερα σε σημεία όπου παρέχεται η ασύρματη πρόσβαση σε δημόσιους χώρους όπως σε καφετέριες, ξενοδοχεία, βιβλιοθήκες και αεροδρόμια για την παροχή δημόσιας πρόσβασης στο διαδίκτυο συγκεκριμένα για κινητές συσκευές. Το Wi-Fi αποτελεί σήμα κατατεθέν της μη κερδοσκοπικής εταιρείας Wi-Fi Alliance η οποία περιορίζει τη χρήση του όρου Wi-Fi σε προϊόντα που ολοκληρώνουν με επιτυχία τις δοκιμές πιστοποίησης διαλειτουργικότητας. Το πρωτόκολλο Wi-Fi χρησιμοποιεί πολλά από τα πρωτόκολλα του συνόλου IEEE 802 και έχει σχεδιαστεί έτσι ώστε να συνεργάζεται άψογα με το ενσύρματο πρωτόκολλο επικοινωνίας Ethernet. Οι συμβατές συσκευές μπορούν να δικτυωθούν μέσω ασύρματων σημείων πρόσβασης μεταξύ τους καθώς και με ενσύρματες συσκευές και το Διαδίκτυο. Οι διαφορετικές εκδόσεις του Wi-Fi καθορίζονται από διάφορα πρότυπα πρωτοκόλλου IEEE 802.11 όπου οι διάφορες τεχνολογίες ραδιοτηλεπικοινωνιών καθορίζουν τις ζώνες ραδιοφώνου και τις μέγιστες περιοχές και ταχύτητες που μπορούν να επιτευχθούν. Το Wi-Fi

χρησιμοποιεί συχνότερα τις ζώνες ραδιοφώνου SHF 2,4 GHz (120 mm) UHF και 5 GHz (60 mm). Αυτές οι ζώνες υποδιαιρούνται σε πολλά κανάλια. Τα κανάλια μπορούν να κοινοποιηθούν μεταξύ των δικτύων, αλλά μόνο ένας πομπός μπορεί να εκπέμπει τοπικά σε ένα κανάλι ανά πάσα στιγμή. Οι ζώνες κύματος του Wi-Fi έχουν σχετικά υψηλή απορρόφηση και λειτουργούν καλύτερα για χρήση σε οπτική επαφή. Πολλά κοινά εμπόδια όπως τοίχοι, κολώνες και οικιακές συσκευές μπορεί να μειώσουν σημαντικά την εμβέλεια αλλά αυτό βοηθά επίσης στην ελαχιστοποίηση των παρεμβολών μεταξύ διαφορετικών δικτύων σε πολυσύχναστα περιβάλλοντα. Ένα σημείο πρόσβασης (hotspot) το οποίο έχει την δυνατότητα να το παρέχει ένας δρομολογητής έχει συχνά εμβέλεια περίπου 20 μέτρων σε εσωτερικούς χώρους, ενώ ορισμένα σύγχρονα σημεία πρόσβασης πετυχαίνουν εμβέλεια σε αποστάσεις έως και 150 μέτρων σε εξωτερικούς χώρους. Η κάλυψη ενός σημείου πρόσβασης μπορεί να είναι μηδαμινή με κάλυψη ενός μικρού χώρου με τοίχους που εμποδίζουν τα ραδιοκύματα ή να καλύπτει αποστάσεις της τάξεως των τετραγωνικών χιλιομέτρων χρησιμοποιώντας πολλά επικαλυπτόμενα σημεία πρόσβασης με επιτρεπόμενη περιαγωγή μεταξύ τους.

Συνήθως η κάλυψη ενός σημείου πρόσβασης που βρίσκεται σε επικοινωνία με ένα άλλο είναι αρκετά περιορισμένη επιτρέποντας στην καλύτερη των περιπτώσεων ασύρματη επικοινωνία σε ακτίνα μερικών δεκάδων μέτρων. Η ιδιότητα αυτή μπορεί να φανεί χρήσιμη σε περιπτώσεις που η ασύρματη επικοινωνία πρέπει να παραμείνει κρυφή από συστήματα ανίχνευσης μεγάλου εύρους ισχύος εκπεμπόμενων σημάτων. Για την περίπτωση της κατασκευής το σύστημα ασύρματης επικοινωνίας πρωτοκόλλου Wi-Fi είναι ενσωματωμένο στο σύστημα μικροελεγκτή και μπορεί να το διαχειριστεί μέσω χρήσης βιβλιοθήκης. Στο υλικολογισμικό η βιβλιοθήκη που πρέπει να συμπεριληφθεί προκειμένου να ενεργοποιηθεί η δυνατότητα χρήσης του ενσωματωμένου συστήματος Wi-Fi είναι η "WiFi.h". Προκειμένου να μπορέσει να λειτουργήσει το σύστημα ασύρματης επικοινωνίας πρωτοκόλλου Wi-Fi είναι απαραίτητο να οριστεί το ένα σύστημα μικροελεγκτή ως server και το άλλο σύστημα μικροελεγκτή ως client. Συγκεκριμένα το σύστημα μικροελεγκτή του πομπού θα είναι αυτό του server και το σύστημα μικροελεγκτή του δέκτη θα είναι αυτό του client. Καθώς θα εγκατασταθεί σε κάθε σύστημα μία ελαφρώς διαφορετική εκδοχή του ίδιου υλικολογισμικού στο κάθε υλικολογισμικό θα υπάρξουν και τροποποιήσεις οι οποίες θα μοιάζουν λεπτομέρειες αλλά είναι απαραίτητες για την ορθή λειτουργία του κάθε συστήματος μικροελεγκτή. Όταν γίνεται λόγος πως το σύστημα μικροελεγκτή που θα λειτουργεί ως δέκτης θα οριστεί παράλληλα και ως client (πελάτης) εννοείται πως στο υλικολογισμικό του θα συμπεριληφθεί η βιβλιοθήκη <HTTPClient.h> η οποία περιέχει το σύνολο των απαραίτητων δομών και συναρτήσεων οι οποίες όταν χρησιμοποιηθούν κατάλληλα στο σύνολο του υλικολογισμικού θα του επιτρέψουν να λειτουργήσει με το αναγνωριστικό client στο πρωτόκολλο του διαδικτύου ώστε να το αναγνωρίζει ένας server (διακομιστής). Ο ορισμός ως client περιλαμβάνει αλλά δεν περιορίζεται στον σχηματισμό ενός μικρού λογισμικού προγράμματος που λειτουργεί σε επιτραπέζιους ηλεκτρονικούς υπολογιστές. Η κύρια λειτουργία του χρησιμοποιείται για τη λήψη υπηρεσιών από έναν ή και περισσότερους διακομιστές και λειτουργεί σε συσκευές που προορίζονται ως “πελάτες” όπως είναι οι φορητοί υπολογιστές, οι επιτραπέζιοι ηλεκτρονικοί υπολογιστές είτε αυτοί είναι οικιακοί είτε είναι δημόσιοι. Ο τρόπος με τον οποίο το κάνει αυτό είναι κάνοντας αιτήματα προς τον διακομιστή και να αναμένει έως ότου αυτός ανταποκριθεί ή όχι. Είναι ένα λειτουργικό σύστημα που έχει σχεδιαστεί για χρήση σε διακομιστή. Όταν γίνεται λόγος πως το σύστημα μικροελεγκτή που θα λειτουργεί ως πομπός θα οριστεί παράλληλα και ως server (διακομιστής) εννοείται πως στο υλικολογισμικό του θα συμπεριληφθεί η βιβλιοθήκη "ESPAsyncWebServer.h" η οποία περιέχει το σύνολο των απαραίτητων δομών και συναρτήσεων οι οποίες όταν χρησιμοποιηθούν κατάλληλα στο σύνολο του υλικολογισμικού θα του επιτρέψουν να λειτουργήσει με το αναγνωριστικό sever στο πρωτόκολλο του διαδικτύου ώστε να μπορεί να αναγνωρίζεται από τα υπόλοιπα αντικείμενα

του διαδικτύου ως διακομιστής. Ο ορισμός ως διακομιστής περιλαμβάνει αλλά δεν περιορίζεται στον σχηματισμό ενός σύνθετου και προχωρημένου σε τεχνογνωσία λογισμικού προγράμματος που λειτουργεί σε ειδικής κατασκευής ηλεκτρονικούς υπολογιστές οι οποίοι πληρούν έναν ελάχιστο αριθμό προϋποθέσεων σε χαρακτηριστικά υλικού ώστε να μπορεί να υποστηρίξει την σταθερή, συνεχή και ορθή λειτουργία ενός διακομιστή. Η κύρια λειτουργία του χρησιμοποιείται για την παροχή υπηρεσιών σε πολλούς πελάτες και έχει την ιδιότητα να εξυπηρετήσει πολλούς πελάτες ταυτόχρονα και είναι πολύ προηγμένο λογισμικό σύστημα.

2.4 Υλοποίηση υλικού μέρους της κατασκευής

Με τον όρο υλικό περιγράφεται το μέρος της κατασκευής που συνθέτει το απτό σύνολο από το οποίο αποτελείται η κατασκευή και περιλαμβάνει όλα της τα μέρη τα οποία είναι το ζεύγος συστημάτων των μικροελεγκτών, η συσκευή GPS, το μη επανδρωμένο αεροσκάφος και το σύστημα τηλεχειρισμού του. Γενικότερα ως έννοια αφορά το υλικό μέρος ενός ηλεκτρονικού υπολογιστικού συστήματος το οποίο περιλαμβάνει τα φυσικά μέρη του όπως είναι το κουτί του, την κεντρική μονάδα επεξεργασίας (CPU), τον σκληρό δίσκο, την μητρική πλακέτα, την μνήμη του, το τροφοδοτικό, την κάρτα γραφικών, την κάρτα ήχου, την οθόνη, το ποντίκι, το πληκτρολόγιο, τα ηχεία και τον εκτυπωτή. Αντίθετα, το λογισμικό είναι το σύνολο των οδηγιών που μπορούν να αποθηκευτούν σε ένα μέσο αποθήκευσης όπως είναι ο σκληρός δίσκος ενός οικιακού ηλεκτρονικού υπολογιστή ή όπως είναι η μνήμη ενός μικροελεγκτή και να εκτελεστούν από το υλικό. Το υλικό έχει την ονομασία hardware με την έννοια πως είναι πιο άκαμπτο σε ότι αφορά τις αλλαγές ενώ το λογισμικό αντίστοιχα έχει την ονομασία software επειδή είναι πρακτικά πολύ ευκολότερη η μεταβολή του περιεχομένου του σε απαραίτητες αλλαγές που τυχών προκύψουν. Το υλικό κατευθύνεται συνήθως από το λογισμικό για να εκτελέσει οποιαδήποτε εντολή. Ο συνδυασμός υλικού και λογισμικού σχηματίζει ένα χρησιμοποιήσιμο υπολογιστικό σύστημα αν και είναι δυνατό να υπάρξουν άλλα συστήματα που το σύνολο τους να υλοποιείται μόνο με υλικό.

Οι ηλεκτρονικοί υπολογιστές είναι ένας από τους πιο συνηθισμένους τύπους υπολογιστικών συστημάτων λόγω της ευελιξίας τους και της σχετικά χαμηλής τιμής τους. Οι επιτραπέζιοι ηλεκτρονικοί υπολογιστές διαθέτουν ένα σύνολο περιφερειακών συσκευών όπως είναι η οθόνη, το πληκτρολόγιο, το ποντίκι και το κουτί του υπολογιστή. Το κουτί του υπολογιστή περιέχει το σύνολο του υλικού του μέρους όπως τη μητρική πλακέτα, τις σταθερές ή αφαιρούμενες μονάδες δίσκων για αποθήκευση των δεδομένων, το τροφοδοτικό και μπορεί να περιέχει άλλες περιφερειακές συσκευές, όπως για παράδειγμα έναν δρομολογητή ή άλλες διεπαφές δικτύου. Ορισμένες παραλλαγές επιτραπέζιων ηλεκτρονικών υπολογιστών ενσωμάτωσαν τις περιφερειακές συσκευές της οθόνης και του πληκτρολογίου στο ίδιο κουτί με την μητρική πλακέτα, τον επεξεργαστή και το τροφοδοτικό. Φυσικά ο διαχωρισμός των διαφόρων μερών σε αυτόνομα τμήματα επιτρέπει στο χρήστη την δυνατότητα να μπορεί να τακτοποιήσει τα τμήματα αυτά κατά προσωπική προτίμηση σε μια ευχάριστη και άνετη προς τον ίδιο διάταξη με έμφαση στη διαχείριση των καλωδίων ισχύος και μεταξύ τους δεδομένων.

Οι φορητοί υπολογιστές (Laptops) έχουν σχεδιαστεί με σημείο αναφοράς την φορητότητα με αποτέλεσμα την αυξημένη αυτονομία και βελτιστοποιημένη κατανάλωση ισχύος αλλά η λειτουργία τους παραμένει παρόμοια με τους επιτραπέζιους ηλεκτρονικούς υπολογιστές. Παρέχουν την δυνατότητα να αξιοποιούν εξαρτήματα χαμηλότερης κατανάλωσης ή μειωμένου μεγέθους με χαμηλότερη απόδοση από έναν επιτραπέζιο ηλεκτρονικό υπολογιστή παρόμοιου κόστους. Οι φορητοί υπολογιστές συμπεριλαμβάνουν το πληκτρολόγιο στο σύνολο τους, την οθόνη και τον επεξεργαστή σε ένα κουτί. Η οθόνη στο αναδιπλούμενο επάνω κάλυμμα του κουτιού μπορεί να κλείσει για την μεταφορά του κυρίως για προστασία της οθόνης και του πληκτρολογίου. Αντί για ποντίκι οι φορητοί υπολογιστές φέρουν μία επιφάνεια αφής ή μοχλό κατάδειξης. Τα tablet είναι φορητοί υπολογιστές όπου

το πληκτρολόγιο είναι πλέον μία ψηφιακή οντότητα η οποία απεικονίζεται σε μία ειδικού τύπου οθόνης η οποία ονομάζεται οθόνη αφής και χρησιμοποιείται ως κύρια συσκευή εισόδου διεπαφής. Τα tablet ως συσκευές γενικά ζυγίζουν λιγότερο και είναι μικρότερα από τους φορητούς ηλεκτρονικούς υπολογιστές. Ορισμένα tablet συμπεριλαμβάνουν στο σύνολο της κατασκευής τους πτυσσόμενα πληκτρολόγια ή προσφέρουν συνδέσεις σε ξεχωριστά εξωτερικά πληκτρολόγια μέσω των θυρών εισόδων/εξόδων. Ορισμένα μοντέλα φορητών ηλεκτρονικών υπολογιστών διαθέτουν αποσπώμενο πληκτρολόγιο με το οποίο επιτρέπεται στο ηλεκτρονικό υπολογιστικό σύστημα να εναλλάσσεται μεταξύ tablet με οθόνη αφής και tablet με πληκτρολόγιο.

Το κουτί του ηλεκτρονικού υπολογιστή περιέχει τα περισσότερα τεμάχια του υπολογιστικού συστήματος και παρέχει την μηχανική υποστήριξη και προστασία για όλα τα εσωτερικά στοιχεία όπως είναι η μητρική πλακέτα, οι μονάδες δίσκων αποθήκευσης δεδομένων, οι κάρτες μνήμης, οι κάρτες γραφικών και το τροφοδοτικό, τα μέρη δηλαδή των οποίων το υλικό δεν περιέχεται σε κάποια προστατευτική συσκευασία και παράλληλα ελέγχει και κατευθύνει τη ροή του αέρα για να πετυχαίνει όσο το δυνατόν αποδοτικότερη ψύξη πάνω από τα εσωτερικά εξαρτήματα. Το κουτί παρέχει επίσης ένα σημαντικό μέρος προστασίας του συστήματος με τον έλεγχο των ηλεκτρομαγνητικών παρεμβολών που εκπέμπονται από τον υπολογιστή και προστατεύει τα εσωτερικά μέρη από την ενδεχόμενη ηλεκτροστατική εκφόρτιση η οποία μπορεί να φτάσει στιγμιαία ακόμη και την κλίμακα των GigaVolt. Τα μεγάλα κουτιά συνήθως ονομάζονται πύργοι και παρέχουν χώρο για αρκετούς δίσκους αποθήκευσης δεδομένων ή για την τοποθέτηση στο εσωτερικό τους άλλων περιφερειακών και συνήθως είναι τοποθετημένοι στο πάτωμα, ενώ τα κουτιά των επιτραπέζιων ηλεκτρονικών υπολογιστών που υπάρχουν συνήθως στα σπίτια κατά μέσο όρο παρέχουν λιγότερο χώρο περιορίζοντας έτσι την πιθανότητα επέκτασης. Τα υπολογιστικά συστήματα που υλοποιούνται σε μορφή όπου όλα τα διάφορα τμήματα θα συμπεριλαμβάνονται σε ένα κουτί και συμπεριλαμβάνουν στο σύνολο τους και την οθόνη ενσωματωμένη στο ίδιο κουτί. Οι φορητοί ηλεκτρονικοί υπολογιστές απαιτούν κουτιά που παρέχουν προστασία από κρούσεις και κραδασμούς για την προστασία της μονάδας από ζημιές και υλικές φθορές.

Το κύριο τμήμα που αποτελεί την βάση και το επίκεντρο ενός ηλεκτρονικού υπολογιστικού συστήματος είναι η μητρική πλακέτα. Το κύριο σώμα ονομάζεται "πλακέτα" και με αυτόν τον όρο περιγράφεται ένα αντικείμενο του οποίου η πρώτη ύλη σχηματίζεται από βακελίτη το οποίο είναι συνθετικό υλικό επάνω στο οποίο εφαρμόζεται μία στρώση χαλκού. Στις μητρικές πλακέτες η διαδικασία κατασκευής τους απαιτεί την δημιουργία πλακετών επενδυμένων με χαλκό οι οποίες είναι ιδιαίτερα λεπτές σε πάχος και σε ποσότητα τεμαχίων τουλάχιστον διψήφιο. Σχεδιάζονται έτσι ώστε να τοποθετηθούν οι μία επάνω στην άλλη προκειμένου να ενσωματωθούν σε ένα σώμα που θα σχηματίσει με το σύνολο του την μητρική πλακέτα. Προτού την ενσωμάτωση των μεμονωμένων φύλλων πλακετών σε ένα σώμα, το κάθε φύλλο θα χαραχτεί και θα καθαριστεί από το πλεόνασμα χαλκού αφήνοντας μόνο τον χαλκό που θα σχηματίζει το απαραίτητο σύστημα αγωγών για την ηλεκτρική μεταφορά δεδομένων και ισχύος μέσα από αυτούς. Παρόλο το γεγονός ότι μία μητρική πλακέτα μπορεί να αποτελείται από δεκάδες στρώσεις, μόνο δύο από αυτές τις στρώσεις θα φέρουν ηλεκτρονικά στοιχεία τα οποία θα σχηματίζουν ηλεκτρονικές διατάξεις και αυτές θα είναι οι δύο ορατές πλευρές της μητρικής πλακέτας. Το ενσωματωμένο σύνολο κυκλωμάτων που διαθέτει συνδέει επάνω της αλλά και μεταξύ τους τις υπόλοιπες συσκευές του ηλεκτρονικού υπολογιστή συμπεριλαμβανομένης της Κεντρικής Μονάδας Επεξεργασίας (CPU), της προσωρινής μνήμης RAM, των μονάδων ανάγνωσης ή/και αποθήκευσης δίσκων (CD, DVD, σκληρού δίσκου ή οποιουδήποτε άλλου) καθώς και τυχόν περιφερειακά που συνδέονται μέσω των θυρών εισόδων/εξόδων ή των υποδοχών επέκτασης του υπολογιστικού συστήματος. Τα ολοκληρωμένα κυκλώματα (IC) που εμπεριέχονται στο σύνολο ενός ηλεκτρονικού υπολογιστικού συστήματος περιέχουν συνήθως δισεκατομμύρια της κλίμακας των νανόμετρων

($10^{-9}m$) τρανζίστορ πεδίου μετάλλου-οξειδίου-ημιαγωγού (MOSFET). Οι συσκευές που συνδέονται άμεσα με ή κατά τμήμα της μητρικής πλακέτας περιλαμβάνουν:

- Την Κεντρική Μονάδα Επεξεργασίας (CPU) η οποία εκτελεί τους περισσότερους από τους υπολογισμούς και εκτελεί τον κύριο όγκο των συνολικών επεξεργασιών που απαιτούνται για την ορθή και ομαλή λειτουργία ενός υπολογιστή και αναφέρεται συχνά ως ο εγκέφαλος του υπολογιστή. Καθώς λαμβάνει τις οδηγίες του προγράμματος του λειτουργικού συστήματος από τη μνήμη τυχαίας πρόσβασης (RAM) στις θύρες εισόδων του τις ερμηνεύει και τις επεξεργάζεται ώστε στη συνέχεια να αποστέλλει μέσω των θυρών εξόδων του τα αποτελέσματα των εργασιών επεξεργασίας και μέσω των αγωγών της μητρικής πλακέτας έτσι ώστε οι σχετιζόμενες και ελεγχόμενες από αυτόν συσκευές να μπορούν να εκτελέσουν και να λειτουργήσουν σύμφωνα με τις οδηγίες που θα λάβουν. Η Κεντρική Μονάδα Επεξεργασίας επί της ουσίας είναι ένας μικροεπεξεργαστής ο οποίος κατασκευάζεται σε μορφή ολοκληρωμένου κυκλώματος (IC) μετάλλου-οξειδίου-ημιαγωγού (MOS). Όταν αυτός τοποθετηθεί στην βάση του μέσω της οποίας θα επικοινωνεί με τα υπόλοιπα συστήματα και συσκευές προκύπτει απαραίτητη η εφαρμογή και χρήση μιας ψήκτρας που η λειτουργία της είναι η απαγωγή θερμοκρασίας από το ολοκληρωμένο κύκλωμα για την αποτροπή της υπερθέρμανσης του και καταστροφικού γεγονότος για αυτόν. Η λειτουργία μίας ψήκτρας μπορεί να υλοποιηθεί με διάφορους τρόπους και στην πιο συνήθη μέθοδο η ψήκτρα ως υλικό είναι μία σύνθετη κατασκευή καθώς αποτελείται από ένα συμπαγές μεταλλικό μέρος θερμοδυναμικά σχεδιασμένο για την μέγιστη δυνατή απαγωγή θερμότητας από το ολοκληρωμένο κύκλωμα και συμπληρώνεται από την προσθήκη ενός ανεμιστήρα για την εξασφάλιση της ταχύτερης διέλευσης του αέρα μέσα από τα πλευρά του μεταλλικού σώματος για βέλτιστη λειτουργία της απαγωγής θερμότητας. Μία άλλη μέθοδος υλοποίησης ψήκτρας που είναι λιγότερο διαδεδομένη εφαρμόζεται τοποθετώντας ένα σύστημα ψύξης νερού και η μέθοδος αποκαλείται υδρόψυξη η οποία χρησιμοποιεί ένα σύστημα σωληνώσεων για την κυκλοφορία νερού μέσα σε αυτό που σχηματίζουν ένα κλειστό κύκλωμα και που καταλήγουν στο ολοκληρωμένο κύκλωμα σε ένα τερματικό το οποίο λειτουργεί ως εναλλάκτης θερμότητας καθώς το νερό απαγάγει την θερμοκρασία από το ολοκληρωμένο και επιστρέφει μέσω του κλειστού κυκλώματος σωληνώσεων στο ψυγείο το οποίο μειώνει την θερμοκρασία του νερού στην αρχική τυπική τιμή του. Οι περισσότερες και νεότερες Κεντρικές Μονάδες Επεξεργασίας περιλαμβάνουν μια μονάδα επεξεργασίας γραφικών (GPU) ενσωματωμένη στο ίδιο ολοκληρωμένο κύκλωμα. Η συχνότητα των κύκλων μηχανής της Κεντρικής Μονάδας Επεξεργασίας εξαρτάται από την ταχύτητα του ρολογιού της και καθορίζει το πόσο γρήγορα θα εκτελεί τις διεργασίες της και μετριέται σε GHz με τις τυπικές τιμές εμπορίου να βρίσκονται μεταξύ 1 GHz και 5 GHz. Χαρακτηριστικό στοιχείο των Κεντρικών Μονάδων Επεξεργασίας είναι η δυνατότητα του υπερχρονισμού της που βελτιώνει την απόδοση της με κόστος τον μεγαλύτερο θερμικό συντελεστή εις βάρος της με συμπέρασμα την αναγκαιότητα για υψηλότερη ψύξη.
- Το σύμπλεγμα ολοκληρωμένων κυκλωμάτων το οποίο συμπεριλαμβάνει ένα σημείο γεφύρωσης το οποίο μεσολαβεί στην επικοινωνία μεταξύ της Κεντρικής Μονάδας Επεξεργασίας και των υπόλοιπων συσκευών του υπολογιστικού συστήματος συμπεριλαμβανομένης της κύριας μνήμης του, συμπεριλαμβάνει και ένα δεύτερο σημείο γεφύρωσης το οποίο συνδέεται με το πρώτο σημείο γεφύρωσης που αναφέρθηκε προ λίγου και υποστηρίζει τις διάφορες βοηθητικές διεπαφές και τους διαχωριστές διαύλων μεταφοράς δεδομένων και τέλος ένα ολοκληρωμένο κύκλωμα Super I/O το οποίο είναι συνδεδεμένο μέσω του δεύτερου σημείου γεφύρωσης το οποίο υποστηρίζει τις πιο αργές και παλαιού τύπου συσκευές όπως τις σειριακές θύρες, την παρακολούθηση υλικού από το υπολογιστικό σύστημα και έλεγχο των ανεμιστήρων.
- Την μνήμη τυχαίας πρόσβασης (RAM) είναι η μνήμη η οποία αποθηκεύει τον κώδικα και τα δεδομένα στα οποία έχει ενεργή πρόσβαση η Κεντρική Μονάδα Επεξεργασίας. Για παράδειγμα όταν εκκινείται η εκτέλεση ενός προγράμματος περιήγησης ιστού στο υπολογιστικό σύστημα τότε το πρόγραμμα αυτό καταλαμβάνει έναν ελάχιστο χώρο αποθήκευσης στην μνήμη αυτήν και αποθηκεύεται στη μνήμη RAM για όλη την χρονική διάρκεια στην οποία το πρόγραμμα θα εκτελείται μέχρι την στιγμή που θα κλείσει το πρόγραμμα περιήγησης ιστού. Τυπικά πρόκειται για έναν τύπο δυναμικής μνήμης RAM (DRAM) όπως και η σύγχρονη DRAM (SDRAM), όπου

τα ολοκληρωμένα κυκλώματα μνήμης τεχνολογίας MOS αποθηκεύουν δεδομένα σε κυψέλες μνήμης που αποτελούνται από MOSFET και πυκνωτές τεχνολογίας MOS. Η μνήμη RAM διατίθεται συνήθως σε διπλές ενσωματωμένες συσκευές μνήμης (DIMM) σε μεγέθη των 2 GB, 4 GB και 8 GB και ακόμη μεγαλύτερη.

- Την μνήμη μόνο για ανάγνωση (ROM), η οποία είναι συνήθως ένα μη πτητικό ολοκληρωμένο κύκλωμα μνήμης το οποίο αποθηκεύει δεδομένα σε κελιά μνήμης τεχνολογίας MOSFET αιωρούμενης πύλης. Στο περιεχόμενο της έχει αποθηκεμένο το BIOS το οποίο είναι το πρώτο πρόγραμμα που εκτελείται όταν ο υπολογιστής ενεργοποιηθεί από κατάσταση απενεργοποίησης, μια διαδικασία γνωστή ως “Bootstrapping”, “Booting” ή “Booting up”. Το BIOS (Basic Input Output System) περιλαμβάνει το υλικολογισμικό εκκίνησης, διαχείρισης θυρών εισόδων/εξόδων και διαχείρισης ενέργειας. Οι μητρικές πλακέτες των τελευταίων γενιών χρησιμοποιούν ενοποιημένη διεπαφή υλικολογισμικού (UEFI) αντί για το BIOS.
- Τους διαχωριστές διαύλων που συνδέουν την Κεντρική Μονάδα Επεξεργασίας με διάφορες εσωτερικές συσκευές και για την επέκταση καρτών για γραφικά και ήχο.
- Την συμπληρωματική μπαταρία CMOS (Complementary MOS) η οποία τροφοδοτεί τη μνήμη τεχνολογίας CMOS για την ημερομηνία και την ώρα στο ολοκληρωμένο κύκλωμα του BIOS. Η μπαταρία αυτή είναι μια μπαταρία ρολογιού.
- Την κάρτα γραφικών η οποία διαχειρίζεται και επεξεργάζεται τα γραφικά του ηλεκτρονικού υπολογιστικού συστήματος. Οι πιο ισχυρές κάρτες γραφικών είναι πιο κατάλληλες για να χειρίζονται απαιτητικές εργασίες όπως είναι η αναπαραγωγή βιντεοπαιχνιδιών ή η εκτέλεση λογισμικού γραφικών υπολογιστή. Μια κάρτα γραφικών περιέχει μια μονάδα επεξεργασίας γραφικών (GPU) από την οποία διαχειρίζεται και μια μνήμη για δεδομένα γραφικών (συνήθως είναι τύπου SDRAM) και τα δύο κατασκευασμένα σε μορφή ολοκληρωμένου κυκλώματος τεχνολογίας MOS.
- Τα MOSFET ισχύος τα οποία αποτελούν την αυτόνομη μονάδα ρυθμιστή της τάσης (VRM) η οποία ελέγχει την τιμή της τάσης που θα λαμβάνουν το σύνολο των συσκευών που σχηματίζουν το υλικό μέρος του ηλεκτρονικού υπολογιστικού συστήματος για την τροφοδοσία τους.

Το μεγαλύτερο μέρος από τα ανωτέρω συμπεριλαμβάνεται στο σύνολο ενός μικροελεγκτή ο οποίος σχηματίζει σε μορφή ολοκληρωμένου κυκλώματος ένα ηλεκτρονικό υπολογιστικό σύστημα τεχνολογίας μονοξειδίου μετάλλου-ημιαγωγού (MOS) το οποίο αποτελείται από έναν ή και περισσότερους μικροεπεξεργαστές μαζί με μνήμη διάφορων τύπων και προγραμματιζόμενες περιφερειακές διατάξεις που σχηματίζουν τις θύρες εισόδου/εξόδου. Η μνήμη προγράμματος με τη μορφή σιδηροηλεκτρικής RAM, NOR flash ή OTP ROM περιλαμβάνεται επίσης συνήθως στο ολοκληρωμένο κύκλωμα του μικροελεγκτή καθώς και μια μικρής χωρητικότητας RAM. Οι μικροελεγκτές έχουν σχεδιαστεί έτσι ώστε να μπορούν να εφαρμοστούν σε ενσωματωμένες εφαρμογές σε αντίθεση με τους μικροεπεξεργαστές που χρησιμοποιούνται σε ηλεκτρονικά υπολογιστικά συστήματα ή σε άλλες εφαρμογές γενικής χρήσης που σχηματίζουν σύστημα από ένα σύνολο διάφορων διακριτών ολοκληρωμένων κυκλωμάτων. Στην σύγχρονη ισχύουσα ορολογία ένας μικροελεγκτής είναι παρόμοιος αλλά λιγότερο εξελιγμένος από ένα σύστημα που περιέχεται σε ένα ολοκληρωμένο κύκλωμα (SoC). Ένα SoC μπορεί να περιλαμβάνει μία συσκευή μικροελεγκτή ως ένα από τα στοιχεία του αλλά συνήθως τον ενσωματώνει σε μία πλήρη διάταξη μαζί με προηγμένα περιφερειακά όπως συμβαίνει σε μία μονάδα επεξεργασίας γραφικών (GPU), σε μία μονάδα ασύρματου δικτύου Wi-Fi και σε έναν ή περισσότερους συνεπεξεργαστές. Οι συσκευές μικροελεγκτών χρησιμοποιούνται σε προϊόντα και συσκευές των οποίων ο έλεγχος πραγματοποιείται αυτόματα όπως γίνεται με τα συστήματα ελέγχου κινητήρα αυτοκινήτων, τις εμφυτεύσιμες ιατρικές συσκευές, τα τηλεχειριστήρια, τις μηχανές γραφείου, τις συσκευές, τα ηλεκτρικά εργαλεία, τα παιχνίδια και άλλα ενσωματωμένα συστήματα που συμπεριλαμβάνουν συσκευή μικροελεγκτή. Σε σχέση με τα ηλεκτρονικά υπολογιστικά συστήματα όπου ο μικροεπεξεργαστής, η μνήμη και οι συσκευές εισόδου/εξόδου είναι διακριτές και αυτόνομες οντότητες, το μειωμένο τους μέγεθος και κόστος των συσκευών μικροελεγκτών καθιστούν οικονομικό τον ψηφιακό έλεγχο ακόμη περισσότερων συσκευών και διεργασιών. Οι συσκευές μικροελεγκτών

μικτού σήματος είναι κοινές, οι οποίες ενσωματώνουν αναλογικά στοιχεία που απαιτούνται για τον έλεγχο μη ψηφιακών ηλεκτρονικών συστημάτων. Στο πλαίσιο της τεχνολογίας του Διαδικτύου των πραγμάτων οι μικροελεγκτές είναι ένα οικονομικό και δημοφιλές μέσο συλλογής δεδομένων, ανίχνευσης και ενεργοποίησης του φυσικού κόσμου ως συσκευές τεχνολογικής αιχμής. Ορισμένοι μικροελεγκτές μπορεί να χρησιμοποιούν λέξεις τεσσάρων bit και να λειτουργούν σε συχνότητες τόσο χαμηλές όσο 4 kHz για χαμηλή κατανάλωση ενέργειας (μονοψήφιες τιμές σε milliwatts ή σε microwatts). Παρέχουν γενικότερα την δυνατότητα να διατηρούν σταθερή λειτουργικότητα ενώ αναμένουν ένα συμβάν το οποίο αναλόγως το πώς είναι ορισμένο στο υλικολογισμικό του θα αντιδράσει με συγκεκριμένο τρόπο, όπως είναι το πάτημα ενός κουμπιού ή κάποια άλλη ενέργεια που θα οδηγήσει σε διακοπή μιας κατάστασης. Η κατανάλωση ενέργειας κατά τη διάρκεια της αδράνειας στην οποία το ρολόι, η Κεντρική Μονάδα Επεξεργασίας και τα περισσότερα περιφερειακά είναι απενεργοποιημένα αγγίζει την κλίμακα των nanowatt καθιστώντας πολλές από αυτές τις συσκευές κατάλληλες για μακροχρόνιες εφαρμογές που κάνουν χρήση πηγών τροφοδοσίας με μπαταρίες. Άλλοι μικροελεγκτές μπορεί να έχουν κρίσιμους ρόλους για την απόδοση, όπου μπορεί να χρειαστεί να λειτουργούν περισσότερο σαν επεξεργαστής ψηφιακού σήματος (DSP), με υψηλότερες ταχύτητες ρολογιού και κατανάλωση ενέργειας.

2.4.1 Εφαρμογή συστήματος μικροελεγκτή με περιφερειακή συσκευή

Η χρήση και εφαρμογή στο σύνολο της κατασκευή ενός από τα πιο δημοφιλή συστήματα μικροελεγκτή με κύριο χαρακτηριστικό την ευχρηστία του όπως είναι το ESP32 παρέχει έναν σημαντικό παράγοντα πλεονεκτημάτων. Καθώς η συσκευή του μικροελεγκτή είναι εξ' ορισμού μία αυτόνομη συσκευή σχεδιασμένη να λειτουργεί όπως οποιοδήποτε ηλεκτρονικό υπολογιστικό σύστημα παρέχει την δυνατότητα τοποθέτησης του σε μία ηλεκτρονική πλακέτα βακελίτη ειδικά σχεδιασμένη και προετοιμασμένη ώστε να αξιοποιεί κατά το βέλτιστο τις διαθέσιμες θύρες εισόδων/εξόδων και τροφοδοσίας και το σύνολο αυτό αποτελεί το σύστημα μικροελεγκτή. Εφόσον το υλικολογισμικό έχει αναπτυχθεί και έχει ήδη δοκιμαστεί ως προς την λειτουργία του αυτό που απομένει είναι η σωστή εφαρμογή και ο τρόπος διασύνδεσης του με το υπόλοιπο υλικό έτσι ώστε να επικοινωνεί σωστά μαζί τους και να λειτουργήσει το σύνολο της κατασκευής σωστά.

Τα κύρια χαρακτηριστικά ενός συστήματος μικροελεγκτή πρέπει τουλάχιστον να ανταποκρίνονται στις ελάχιστες απαιτήσεις της κατασκευής, επομένως πρέπει να είναι γνωστά εκ των προτέρων και για το σύστημα μικροελεγκτή που θα εφαρμοστεί στην συγκεκριμένη κατασκευή έχουν ως εξής: Όπως έχει ήδη αναφερθεί πως ο μικροελεγκτής που φέρει είναι ο ESP-WROOM-32 της Espressif ο οποίος περιέχει διπύρηνο μικροεπεξεργαστή και λειτουργεί στην ταχύτητα επεξεργασίας των 240 MHz. Είναι εξοπλισμένος με flash μνήμη 4 MB χωρητικότητας η οποία επικοινωνεί με το ενσύρματο πρωτόκολλο επικοινωνίας SPI και η μνήμη του δύναται να επεκταθεί στα 16 MB συνολικής χωρητικότητας. Οι δυνατότητες ασύρματης συνδεσιμότητας του συμπεριλαμβάνουν το Wi-Fi 802,11 b/g/n πρωτόκολλο ασύρματης επικοινωνίας με χαρακτηριστικά τα συστήματα κυβερνοασφαλείας WEP και WPA/WPA2 PSK/Enterprise, το ολοκληρωμένο κύκλωμα κρυπτογράφησης που υποστηρίζει τους αλγόριθμους AES/SHA2/Elliptical Curve Cryptography/RSA-4096, μέγιστη ισχύ για μετάδοση δεδομένων: 19,5 dBm@11b, 16,5 dBm@11g, 15,5 dBm@11n και ευαισθησία μέγιστης λήψης ίση με -97 dBm και το πρωτόκολλο ασύρματης επικοινωνίας Bluetooth 4.0 LE. Διαθέτει 32 θύρες εισόδων/εξόδων από τις οποίες οι 26 είναι ψηφιακές θύρες εισόδων/εξόδων στα 3,3V με δυνατότητα PWM, 18 θύρες εισόδων αναλογικού σήματος, 3 θύρες ενσύρματης επικοινωνίας πρωτοκόλλου UART, 3 θύρες ενσύρματης επικοινωνίας πρωτοκόλλου SPI, 2 θύρες ενσύρματης επικοινωνίας πρωτοκόλλου I2C, 2 θύρες εξόδου

DAC και 2 θύρες ενσύρματης επικοινωνίας πρωτοκόλλου I2S. Παρέχει κατάσταση ύπνου με μέγιστη κατανάλωση τα 5 μA και διεπαφή μπαταρίας Λιθίου με δυνατότητα φόρτισης τα 500 mA.

Από τα ανωτέρω θα αξιοποιηθούν οι δυνατότητες του μικροελεγκτή και της μνήμης στην οποία θα εγγραφεί το υλικολογισμικό και μία θύρα ενσύρματης επικοινωνίας στην οποία θα συνδεθεί η αυτόνομη συσκευή GPS. Συγκεκριμένα για τον σχηματισμό αυτής της κατασκευής θα χρειαστεί να αξιοποιηθεί μία διάτρητη πλακέτα βακελίτη η οποία θα χρησιμεύσει ως βάση για τον σχηματισμό του πλήρους συστήματος. Η διάτρητη πλακέτα βακελίτη αποτελείται από ένα συνθετικής προέλευσης υλικό το οποίο κατασκευάζεται συγκεκριμένα για την υλοποίηση και δημιουργία πρωτοτύπων ηλεκτρονικών κυκλωμάτων. Τα χαρακτηριστικά του ως υλικού το περιγράφουν ως ένα λεπτό και άκαμπτο φύλλο πλαστικής ύλης με διηλεκτρικές ιδιότητες με τρύπες που έχουν γίνει σε προκαθορισμένα διαστήματα σε σχέδιο πλέγματος συνήθως μοτίβου ενός τετραγώνου πλέγματος με μεταξύ τους απόσταση 0,1 ίντσες (2,54 χιλιοστά του μέτρου). Αυτές οι τρύπες περιβάλλονται ομόκεντρα από στρόγγυλες ή τετράγωνες χάλκινες επενδύσεις επί της επιφάνειας της πλακέτας οι οποίες επενδύσεις χρησιμεύουν στην κασσιτεροκόλληση μεταξύ τους και των ακροδεκτών των ηλεκτρονικών στοιχείων που θα τις διαπεράσουν, αν και υπάρχουν και πλακέτες που είναι διάτρητες αλλά οι τρύπες δεν περιβάλλονται από χάλκινη επένδυση. Η φθηνή διάτρητη πλακέτα βακελίτη φέρει χάλκινη επένδυση μόνο στη μία πλευρά της ενώ οι διάτρητες πλακέτες βακελίτη που είναι καλύτερης ποιότητας φέρουν επένδυση χαλκού και στις δύο επιφάνειες τους. Το κύριο χαρακτηριστικό είναι ότι κάθε χάλκινη επένδυση που περιβάλει ομόκεντρα κάθε τρύπα του πλέγματος είναι ηλεκτρικά απομονωμένη από τις υπόλοιπες που σημαίνει ότι ο κατασκευαστής του κυκλώματος πρέπει να πραγματοποιήσει όλες τις συνδέσεις μεταξύ των ηλεκτρονικών στοιχείων οι οποίες θα χρησιμέψουν ως ηλεκτρικοί αγωγοί δεδομένων ή ισχύος, είτε με σύρμα περιέλιξης πηνίου είτε με τεχνικές καλωδίωσης από σημείο σε σημείο. Διακριτά ηλεκτρονικά στοιχεία συγκολλούνται στην πρωτότυπη πλακέτα όπως οι αντιστάσεις, οι πυκνωτές, τα πηνία, τα τρανζίστορ και τα ολοκληρωμένα κυκλώματα. Το υλικό του υποστρώματος ονομάζεται βακελίτης και είναι συνήθως κατασκευασμένο από μία σύνθεση χαρτοπολτού ελασματοποιημένου με φαινολική ρητίνη (όπως το FR-2) ή εποξειδικό πολυστρωματικό υλικό ενισχυμένο με υαλοβάμβακα (FR-4). Το σύστημα πλέγματος με μεταξύ τους απόσταση των 0,1 ιντσών (2,54 χιλιοστά του μέτρου) μπορεί να δεχτεί ολοκληρωμένα κυκλώματα σε πακέτα DIP και πολλούς άλλους τύπους ηλεκτρονικών στοιχείων διαμπερούς οπής. Η διάτρητη πλακέτα βακελίτη δεν έχει σχεδιαστεί για τη δημιουργία πρωτοτύπων κυκλωμάτων που στον σχεδιασμό τους φέρουν ηλεκτρονικά στοιχεία επιφανειακής τοποθέτησης. Πριν από την υλοποίησης ενός κυκλώματος σε διάτρητη πλακέτα βακελίτη οι θέσεις των ηλεκτρονικών στοιχείων και των αγωγών των ηλεκτρονικών συνδέσεων σχεδιάζονται συνήθως με λεπτομέρεια είτε σε χαρτί, είτε με εργαλεία λογισμικού ώστε να υπάρχει μία σχετικά βελτιστοποιημένη χωροταξική διάταξη. Ωστόσο τα πρωτότυπα σχετικά μικρής κλίμακας, με την έννοια ότι περιλαμβάνουν μικρό αριθμό ηλεκτρονικών στοιχείων σε ποσότητα και η μεταξύ τους συνδέσεις είναι απλές, κατασκευάζονται συχνά απευθείας χρησιμοποιώντας μία υπερμεγέθη διάτρητη πλακέτα βακελίτη. Ένα λογισμικό για σχεδιασμό διατάξεων Τυπωμένων Πλακετών Κυκλωμάτων παρέχει την δυνατότητα παραμετροποίησης και για τη δημιουργία διατάξεων διάτρητων πλακετών βακελίτη. Στην περίπτωση αυτή ο σχεδιαστής τοποθετεί χωροταξικά τα ηλεκτρονικά στοιχεία με τρόπο τέτοιο ώστε όλες οι ενώσεις να συμπίπτουν σε αντιστοιχία ενός πλέγματος με μεταξύ τους αποστάσεις των 0,1 ιντσών (2,54 χιλιοστά του μέτρου). Κατά την όδευση των συνδέσεων μπορούν να χρησιμοποιηθούν περισσότερες από 2 στρώσεις χαλκού καθώς οι πολλαπλές επικαλύψεις των πλακετών δεν αποτελούν πρόβλημα για τα μονωμένα καλώδια. Την στιγμή που οριστικοποιηθεί η τελική διάταξη τα ηλεκτρονικά στοιχεία συγκολλούνται στις προκαθορισμένες θέσεις τους με έμφαση στον προσανατολισμό των ηλεκτρονικών στοιχείων που φέρουν πόλωση όπως είναι οι ηλεκτρολυτικοί πυκνωτές, οι δίοδοι και τα ολοκληρωμένα

κυκλώματα. Στη συνέχεια πραγματοποιούνται οι διάφορες ηλεκτρικές διασυνδέσεις σύμφωνα με τον σχεδιασμό και τις απαιτήσεις της διάταξης. Μία καλή πρακτική εφαρμογή είναι να πραγματοποιείται το μεγαλύτερο μέρος της όδευσης χωρίς να προστεθεί επιπλέον καλώδιο. Αυτό πραγματοποιείται λυγίζοντας τους υπάρχοντες ακροδέκτες των ηλεκτρονικών στοιχείων οι οποίοι προεξέχουν από την επιφάνεια της πλακέτας προς την επιθυμητή κατεύθυνση τους, κόβοντας το επιπλέον μήκος και συγκολλώντας το καλώδιο για να πραγματοποιηθεί η απαιτούμενη ηλεκτρική σύνδεση. Μια άλλη καλή πρακτική εφαρμογή αρνείται να λυγίσει τους προεξέχοντες ακροδέκτες των ηλεκτρονικών στοιχείων και να τα χρησιμοποιήσει για όδευση, ισχυριζόμενη ότι αυτό καθιστά την αφαίρεση ενός εξαρτήματος σε αργότερο χρόνο δύσκολη ή ακόμη και αδύνατη όπως σε πιθανή επέμβαση επισκευής. Εάν για κάποιο λόγο χρειαστεί να χρησιμοποιηθούν επιπλέον καλώδια ή χρησιμοποιούνται ήδη στην πλακέτα όλα τα διαθέσιμα καλώδια, συνήθως οι οδεύσεις δρομολογούνται εξ ολοκλήρου στη χάλκινη πλευρά των διάτρητων πλακετών βακελίτη με κασσιτεροκόλληση επειδή σε αντίθεση με τις ταινίες αγωγών οι χάλκινες επενδύσεις των οπών δεν είναι μεταξύ τους συνδεδεμένες και η μόνη οπή που περιβάλλεται από χάλκινη επένδυση είναι ήδη κατειλημμένη από τον ακροδέκτη ενός ηλεκτρονικού στοιχείου. Τα κατάλληλα για χρήση καλώδια που συνιστώνται σε τέτοιες εφαρμογές κυμαίνονται από μεμονωμένα καλώδια όπως αυτό του verowire (σμάλτο σύρμα χαλκού με μόνωση πολυουρεθάνης που κατά τη συγκόλληση λιώνει) έως γυμνό χάλκινο σύρμα ανάλογα με τις ατομικές προτιμήσεις του σχεδιαστή. Για μονωμένα καλώδια προτιμάται το λεπτό σύρμα συμπαγούς πυρήνα ή αλλιώς μονόκλωνο με μόνωση ανθεκτική στη θερμοκρασία όπως το Kynar ή το Tefzel. Σε πολλές περιπτώσεις συνηθίζεται καθώς είναι απαραίτητο να χρησιμοποιείται ένα ειδικό εργαλείο απογύμνωσης καλωδίων το οποίο συμπεριλαμβάνει μια λεπτή ατσάλινη λεπίδα με μια σχισμή στην οποία απλά εισάγεται το καλώδιο και στη συνέχεια εξάγεται με ευκολία αφήνοντας ένα καθαρό και απογυμνωμένο άκρο. Αυτό το καλώδιο αναπτύχθηκε αρχικά για συναρμολόγηση κυκλώματος με την τεχνική περιτύλιξης καλωδίων, αλλά χρησιμεύει επίσης καλά για μικροσκοπική καλωδίωση από σημείο σε σημείο σε διάτρητη πλακέτα βακελίτη. Το απογυμνωμένο χάλκινο σύρμα είναι χρήσιμο κατά τη συγχώνευση πολλών συνδέσεων για να σχηματιστεί ένας ηλεκτρικός δίαυλος όπως είναι η γείωση του κυκλώματος και όταν υπάρχει αρκετός χώρος για την σωστή όδευση των συνδέσεων. Οι σκόπιμες γεφυρώσεις συγκόλλησης μπορούν να χρησιμοποιηθούν για την μεταξύ τους σύνδεση των γειτονικών χάλκινων επενδύσεων όταν είναι απαραίτητο. Απαιτείται προσεκτικός συντονισμός χεριού και ματιού για να αποφευχθεί η πρόκληση ακούσιων βραχυκυκλωμάτων. Τα κυκλώματα που υλοποιούνται σε διάτρητες πλακέτες βακελίτη δεν είναι απαραίτητα εύθραυστα αλλά και πάλι είναι λιγότερο ανθεκτικά στις κρούσεις από τις πλακέτες τυπωμένων κυκλωμάτων λόγω του διάτρητου πλέγματος το οποίο προσδίδει αδυναμία στην συνοχή του υλικού.

Λαμβάνοντας υπόψιν όλα τα ανωτέρω για την προσαρμογή του συστήματος μικροελεγκτή σε μία τέτοια διάτρητη πλακέτα βακελίτη θα πρέπει να συνυπολογιστούν κάποιοι παράμετροι όπως το σύνολο των συσκευών που θα προσαρμοστούν σε αυτήν, το σύνολο των ακροδεκτών της κάθε συσκευής καθώς και ποιοι από αυτούς θα ενωθούν μεταξύ τους και το πρότυπο των μεταξύ τους αποστάσεων για το αν θα ανήκουν στο ίδιο πρότυπο με αυτό της διάτρητης πλακέτας βακελίτη. Το σύστημα μικροελεγκτή του ESP-32 περιλαμβάνει στο πακέτο του ως προϊόν δύο σειρές ακροδεκτών οι οποίοι είναι μεταξύ τους μονωμένοι ώστε να παρέχεται η δυνατότητα προς τον σχεδιαστή να τους συγκολλήσει στην πλακέτα του συστήματος μικροελεγκτή η οποία έχει κατασκευαστεί με την πρόβλεψη να μπορεί να συμπεριλάβει τους ακροδέκτες αυτούς. Οι προσθήκη των ακροδεκτών στην πλακέτα του συστήματος μικροελεγκτή αποτελεί μία επέκταση διευκόλυνσης με πρακτικό τρόπο καθώς επιτρέπει καλύτερη πρόσβαση στις θύρες εισόδων/εξόδων του συστήματος μικροελεγκτή. Για την συσκευή GPS όπως προαναφέρθηκε έχει κατασκευαστεί ήδη η προσαρμογή της με την βοήθεια διάτρητης πλακέτας βακελίτη για την

προσαρμογή των μεταξύ αποστάσεων των ακροδεκτών από 0,05 της ίντσας σε 0,1 της ίντσας όπως είναι δηλαδή το τυπικό πρότυπο των αποστάσεων των ακροδεκτών για το πακέτο DIP των ολοκληρωμένων κυκλωμάτων. Για καλύτερη πρακτικότητα στην διάτρητη πλακέτα βακελίτη θα τοποθετηθούν οι αντίστοιχοι "θηλυκοί" ακροδέκτες που ταιριάζουν με αυτούς τους "αρσενικούς" ακροδέκτες του συστήματος μικροελεγκτή οι οποίοι θα εξυπηρετούν ως ένα είδους βάση η οποία θα επιτρέπει να αποσπάται κατά βούληση από αυτήν το σύστημα μικροελεγκτή. Για τον ίδιο λόγο η ίδια ακριβώς τοποθέτηση βάσης θα υλοποιηθεί επί της διάτρητης πλακέτας βακελίτη για την συσκευή GPS ώστε να της επιτρέψει να είναι αποσπώμενη. Με την τοποθέτηση των "βάσεων" του συστήματος μικροελεγκτή και της συσκευής GPS απομένει να συγκολληθούν οι ηλεκτρικοί αγωγοί δεδομένων και παροχής ισχύος μεταξύ μικροελεγκτή και συσκευής GPS που θα εξυπηρετήσουν στην ορθή λειτουργία του συνολικού συστήματος.

Το καλώδιο ως απτό αντικείμενο υλικού περιγράφεται ως ένα ενιαίο και συνήθως κυλινδρικό, εύκαμπτο και μακρόστενο επιμήκης σκέλος ή ράβδος από μέταλλο. Τα καλώδια χρησιμοποιούνται σε πληθώρα εφαρμογών τόσο στην μηχανολογία όσο και στην ηλεκτρολογία για να φέρουν μηχανικά φορτία ή ηλεκτρικά/ηλεκτρονικά ρεύματα και τάσεις ισχύος και τηλεπικοινωνιακά σήματα. Το καλώδιο δύναται να παρέχεται είτε γυμνό καθαρό μέταλλο είτε ως επενδυμένο με κάποιο υλικό συνήθως μονωτικό και το μεταλλικό στέλεχος σχηματίζεται κατά την κατασκευή του έλκοντας το μέταλλο μέσα από μια οπή σε μια μήτρα ή πλάκα έλξης όσο αυτό βρίσκεται σε αρκετά υψηλή θερμοκρασία στην οποία η κατάσταση του να είναι ημίρρευστη κάνοντας το αρκετά μαλακό ώστε να διευκολυνθεί η μορφοποίηση του. Οι μονάδες μέτρησης των καλωδίων διατίθενται σε διάφορα τυπικά μεγέθη βάση συγκεκριμένων προτύπων όπως αυτά προκύπτουν από ειδικούς οργανισμούς που τα ορίζουν εξ' αρχής σε έναν αριθμό μέτρησης. Ο όρος "καλώδιο" χρησιμοποιείται επίσης πιο αυθαίρετα για να περιγράψει μία δέσμη τέτοιων κλώνων όπως για παράδειγμα γίνεται με τον όρο "σύρμα πολλαπλών κλώνων" που η πιο σωστή του ονομασία και περιγραφή είναι η "συρματόσχοινο" στη επιστήμη της μηχανολογίας ή "καλώδιο" στην επιστήμη του ηλεκτρισμού. Το σύρμα διατίθεται σε μορφές συμπαγούς πυρήνα, λανθάνοντος ή πλεκτού. Η μορφή της διατομής του μεταλλικού μέρους του καλωδίου συνήθως είναι κυκλική αλλά μπορεί να κατασκευαστεί και σε τετράγωνες, εξαγωνικές, πεπλατυσμένες ορθογώνιες ή άλλες διατομές είτε για διακοσμητικούς σκοπούς είτε για συγκεκριμένων απαιτήσεων τεχνικούς σκοπούς όπως είναι τα πηνία φωνής υψηλής απόδοσης στα μεγάφωνα. Το καλώδιο έχει πολλές χρήσεις και αποτελεί την πρώτη ύλη πολλών σημαντικών κατασκευαστών όπως είναι η βιομηχανία συρμάτινων διχτυών, τα μηχανικά ελατήρια, η κατασκευή συρμάτινων υφασμάτων και η κλώση συρματόσχοινων. Το συρμάτινο ύφασμα όλων των βαθμών αντοχής και λεπτότητας του πλέγματος χρησιμοποιείται για κοσκίνισμα και κοσκίνισμα μηχανημάτων, για την αποστράγγιση χαρτοπολτού, για σήτες παραθύρων και για πολλούς άλλους σκοπούς. Τεράστιες ποσότητες σύρματος αλουμινίου, χαλκού, νικελίου και χάλυβα χρησιμοποιούνται για καλώδια τηλεφώνου και δεδομένων και ως αγωγοί στη μετάδοση ηλεκτρικής ενέργειας και στη θέρμανση. Η ζήτηση του για περιφράξεις είναι υψηλή και καταναλώνεται πολύ στην κατασκευή κρεμαστών γεφυρών, κλουβιών, στην κατασκευή έγχορδων μουσικών οργάνων και επιστημονικών οργάνων. Ο άνθρακας και το σύρμα από ανοξείδωτο χάλυβα ελατηρίου έχουν σημαντικές εφαρμογές σε μηχανικά ελατήρια για κρίσιμα εξαρτήματα/εξαρτήματα που κατασκευάζονται για της ανάγκες της αυτοκινητοβιομηχανίας. Για την κατασκευή χρήσιμου καλωδίου δεν έχουν τις απαραίτητες φυσικές ιδιότητες όλα τα μέταλλα και τα μεταλλικά κράματα καθιστώντας ένα συγκεκριμένο εύρος κατάλληλων μετάλλων για την κατασκευή καλωδίων. Τα μέταλλα πρέπει απαραίτητα να είναι όλκιμα και ανθεκτικά στην ένταση από την ποιότητα της οποίας εξαρτάται κυρίως η χρησιμότητα του καλωδίου. Τα κύρια μέταλλα που είναι κατάλληλα για την κατασκευή καλωδίων με σχεδόν ίδια ολκιμότητα είναι η πλατίνα, ο άργυρος, ο σίδηρος, ο χαλκός, το αλουμίνιο και ο χρυσός και

μόνο από αυτά και ορισμένα από τα κράματά τους με άλλα μέταλλα, κυρίως από ορείχαλκο και από μπρούτζο, κατασκευάζονται τα καλώδια. Με προσεκτική επεξεργασία είναι δυνατόν να παραχθεί εξαιρετικά λεπτό καλώδιο. Τα χάλκινα καλώδια μπορεί να επικαλύπτονται με άλλα μέταλλα όπως είναι ο κασσίτερος, το νικέλιο και το ασήμι για την προσαρμογή τους σε διαφορετικές αντοχές θερμοκρασιών, να παρέχουν λίπανση και να προσφέρουν ευκολότερη αφαίρεση της μόνωσης τους από τον χαλκό.

Με βάση τα ανωτέρω και όπως ήδη περιεγράφηκε σε προηγούμενη ενότητα θα συγκολληθούν καλώδια τα οποία θα λειτουργήσουν ως ηλεκτρικοί αγωγοί για την μεταφορά των δεδομένων και για την τροφοδοσία ισχύος μεταξύ του συστήματος μικροελεγκτή και της συσκευής GPS. Συγκεκριμένα θα συγκολληθούν από την επιφάνεια της διάτρητης πλακέτας βακελίτη που είναι επενδυμένη με χάλκινες επιφάνειες στις οποίες έχουν συγκολληθεί οι ακροδέκτες των βάσεων οι οποίοι βρίσκονται στην επιφάνεια της άλλης πλευράς της πλακέτας η οποία δεν φέρει κάποια επένδυση. Τα καλώδια είναι μονού συμπαγούς πυρήνα ή αλλιώς μονόκλωνα ο οποίος έχει διάμετρο 0,4 χιλιοστών του μέτρου και περιβάλλεται από μία επένδυση μονωτικού υλικού η οποία προστατεύει από τυχών βραχυκυκλώματα μειώνοντας την πιθανότητα του να συμβεί ένα τέτοιο γεγονός. Προκειμένου να πραγματοποιηθεί η συγκόλληση των ηλεκτρικών αγωγών πρέπει να τοποθετηθεί αρχικά το καλώδιο επί της διάτρητης πλακέτας βακελίτη από την όψη των συγκολλημένων ακροδεκτών μεταξύ εκείνων των ακροδεκτών με τους οποίους θα συγκολληθεί προκειμένου να σχηματιστεί ένας μεταξύ τους ηλεκτρικός αγωγός που θα τους ενώνει και θα πρέπει να μορφοποιηθεί κατάλληλα ώστε να μην διασταυρώνεται όσο γίνεται με άλλους αγωγούς και να έχει ένα ελάχιστο μήκος ώστε να περισσεύει μία μικρή ποσότητα στο μήκος του ώστε να προκύψει επαρκές για την λειτουργία του. Στην συνέχεια θα πρέπει να κοπεί αφού έχει καθοριστεί το ελάχιστο μήκος του και να αφαιρεθούν μερικά χιλιοστά του μέτρου από την μόνωση του καλωδίου από κάθε του άκρο έτσι ώστε να μείνει καθαρό το μέταλλο και να μπορεί να συγκολληθεί στον ακροδέκτη του κάθε άκρου του. Επομένως θα συγκολληθούν καλώδια μεταξύ των ακροδεκτών του συστήματος μικροελεγκτή και της συσκευής GPS ώστε να παρέχει το σύστημα του μικροελεγκτή στην συσκευή GPS τροφοδοσία από τον ακροδέκτη του συστήματος μικροελεγκτή στάθμης τάσεως ίσης με 3,3V στον ακροδέκτη τροφοδοσίας της συσκευής GPS, από τον ακροδέκτη του συστήματος μικροελεγκτή στάθμης τάσεως ίσης με 3,3V στον ακροδέκτη NRESET της συσκευής GPS, από τον ακροδέκτη σειριακής επικοινωνίας RX του συστήματος μικροελεγκτή με τον ακροδέκτη σειριακής επικοινωνίας TX της συσκευής GPS, από τον ακροδέκτη σειριακής επικοινωνίας TX του συστήματος μικροελεγκτή με τον ακροδέκτη σειριακής επικοινωνίας RX της συσκευής GPS, από τον ακροδέκτη της γείωσης του συστήματος μικροελεγκτή στον έναν ακροδέκτη από τους τέσσερις της κοινής γείωσης της συσκευής GPS και τέλος μεταξύ όλων των ακροδεκτών των γειώσεων της συσκευής GPS. Έτσι θα έχει ολοκληρωθεί η κατάλληλη και ορθή σύνδεση της συσκευής GPS ως περιφερειακή συσκευή του συστήματος μικροελεγκτή προκειμένου να είναι ελεγχόμενη από αυτό και να του παρέχει με πιστότητα της πληροφορίες συντεταγμένων που θα λαμβάνει από το δορυφορικό δίκτυο ως προς την ακριβή τοποθεσία του σε πραγματικό χρόνο.

2.5 Σύνθεση Συστήματος Μικροελεγκτή με Μη Επανδρωμένο Εναέριο Όχημα

Με την ολοκλήρωση του συστήματος μικροελεγκτή ως υλικού μέρους το οποίο περιλαμβάνει την τοποθέτηση του σε διάτρητη πλακέτα βακελίτη με την εγκατάσταση της συσκευής GPS ως περιφερειακή συσκευή και του υλικολογισμικού με το οποίο θα εκτελεί τις απαραίτητες λειτουργίες σύμφωνα με τις οδηγίες του, το επόμενο βήμα της υλοποίησης της κατασκευής απαιτεί την τοποθέτηση του σε ένα μη επανδρωμένο εναέριο όχημα (Unmanned Aerial Vehicle, UAV) και την εκτέλεση

κάποιων δοκιμών ως προς την ικανοποιητική απόδοση του συνόλου των λειτουργιών του καθώς και την ανταπόκριση του ως προς το αρχικό ζητούμενο.

Με τον όρο “μη επανδρωμένο εναέριο όχημα” (Unmanned Aerial Vehicle, UAV) περιγράφεται το κοινώς γνωστό ως drone το οποίο είναι ένα αεροσκάφος που δεν φέρει άνθρωπο πιλότο, πλήρωμα ή επιβάτες. Τα μη επανδρωμένα εναέρια οχήματα αποτελούν στοιχεία ενός συστήματος μη επανδρωμένων αεροσκαφών (Unmanned Aircraft System, UAS) το οποίο περιλαμβάνει την απαραίτητη τοποθέτηση ενός χειριστή εδάφους και ενός συστήματος επικοινωνιών με το μη επανδρωμένο εναέριο όχημα. Η πτήση των μη επανδρωμένων εναέριων οχημάτων μπορεί να λειτουργεί υπό χρήση τηλεχειρισμού από επίγειο άνθρωπο χειριστή ως τηλεχειριζόμενο αεροσκάφος (Remotely Piloted Aircraft, RPA) ή σε ένα εύρος διαφόρων βαθμών αυτονομίας όπως είναι η χρήση του βοηθητικού συστήματος αυτόματου πιλότου μέχρι πλήρως αυτόνομα στην λειτουργία τους αεροσκάφη που δεν περιλαμβάνουν καμία απολύτως πρόβλεψη για ανθρώπινη παρέμβαση οποιασδήποτε μορφής. Τα μη επανδρωμένα εναέρια οχήματα όταν αρχικά αναπτύχθηκαν κατά τον εικοστό αιώνα, η τεχνολογική τους ανάπτυξη προοριζόταν για στρατιωτικές αποστολές που θεωρούνταν σχεδόν απαξιωτικές για τους πιλότους και λαμβάνονταν υπόψιν ως αγγαρείες όμως καθώς η τεχνολογική τους εξέλιξη συνέχισε να παρουσιάζει διαρκή πρόοδο, κατά τον εικοστό πρώτο αιώνα αναβαθμίστηκαν σε ουσιαστικά και αξιόπιστα αποκτήματα για την συντριπτική πλειοψηφία των περισσότερων στρατιωτικών δυνάμεων της οικουμένης. Καθώς παράλληλα παρουσίασαν και οι τεχνολογίες ελέγχου σημαντική βελτίωση ενώ το κόστος κατασκευής σε μαζική παραγωγή μειώθηκε η χρήση τους επεκτάθηκε περαιτέρω καθώς εφαρμόζονται και σε πολλές μη στρατιωτικές εφαρμογές. Αναφορικά και χωρίς να περιορίζονται σε αυτές τις μη στρατιωτικές δραστηριότητες περιλαμβάνονται οι αεροφωτογραφίες, οι παραδόσεις προϊόντων και αγαθών, η γεωργία, η αστυνόμευση και επιτήρηση των αστικών περιοχών, οι επιθεωρήσεις υποδομής, η επιστήμη, το λαθρεμπόριο και οι αγώνες drone.

Το μη επανδρωμένο εναέριο όχημα που θα χρησιμοποιηθεί για την υλοποίηση της κατασκευής της παρούσας εργασίας ανήκει στην κατηγορία των τετρακόπτερων που η ονομασία αναφέρεται στον τρόπο με τον οποίο κατορθώνει το μη επανδρωμένο εναέριο όχημα να πετύχει την αιώρηση του στον χώρο κάνοντας χρήση τεσσάρων ελίκων οι οποίοι είναι εφαρμοσμένοι ο καθένας στον άξονα ενός ηλεκτροκινητήρα ακριβείας γνωστών και ως σερβοκινητήρες. Οι σερβοκινητήρες με την σειρά τους τοποθετούνται στο άκρο ενός βραχίονα που αποτελεί τμήμα του σώματος του μη επανδρωμένου εναέριου αεροσκάφους σχηματίζοντας τελικά μία τοποθέτηση σχήματος σταυρού. Οι στροφές του κάθε κινητήρα ελέγχονται από ένα σύστημα μικροελεγκτή του οποίου αποτελούν μέρος του ως περιφερειακές συσκευές του και ο τρόπος με τον οποίο τους ελέγχει γίνεται μέσω μιας άλλης ομάδας περιφερειακών συσκευών οι οποίες ανήκουν στην ομάδα των αισθητηρίων οι οποίες παρέχουν το σύνολο των πληροφοριών για το κατά πόσο το μη επανδρωμένο όχημα βρίσκεται παράλληλα με την βαρυτική έλξη του πλανήτη ώστε να αιωρείται σε συγκεκριμένο ύψος σε σχέση με αυτόν και για το αν πλέει προς κάποια κατεύθυνση της επιφάνειας του και τις οδηγίες για αυτές τις παραμέτρους τις δέχεται από το υλικολογισμικό που έχει αποθηκεμένο στο ολοκληρωμένο κύκλωμα της μνήμης του. Εφόσον είναι δυνατόν για το συγκεκριμένο μη επανδρωμένο εναέριο όχημα να λειτουργήσει στο σύνολο των αναμενόμενων λειτουργιών του έτσι ώστε να μπορεί να ληφθεί υπόψιν ως αυτόνομη συσκευή από έναν βαθμό και πάνω, είναι γνωστό πως ελέγχεται η διαχείριση του από ένα σύστημα μικροελεγκτή και λειτουργεί σύμφωνα με τις οδηγίες ενός υλικολογισμικού που είναι γραμμένο στην μνήμη του τότε μπορεί να θεωρηθεί ως ένα ανεξάρτητο ενσωματωμένο σύστημα. Οι δυνατότητες του περιλαμβάνουν ένα αρκετά κομψό αλγόριθμο κατάλληλα διαμορφωμένο για την ομαλή λειτουργία της αιώρησης του μη επανδρωμένου εναέριου αεροσκάφους είτε είναι σε κατάσταση αδράνειας είτε εκτελεί ένα σύνολο μετακινήσεων μέσα στον χώρο. Ο έλεγχος του πραγματοποιείται με την χρήση ενός συστήματος

τηλεχειρισμού όπου συγκεκριμένα υπάρχει ένα σύστημα επικοινωνίας μεταξύ των δύο διακριτών συσκευών του μη επανδρωμένου εναέριου οχήματος και του τηλεχειρισμού του. Ο τηλεχειρισμός διαθέτει πέρα από το σύστημα που σχηματίζει την διάταξη του πομπού και μία σύνθετη συστοιχία διάφορων διακόπτων με τους οποίους μπορεί ο επίγειος χειριστής να ελέγξει πλήρως ολόκληρο το σύνολο των παρεχόμενων λειτουργιών ελέγχου του.

Το σύστημα μικροελεγκτή αποτελεί ανεξάρτητη οντότητα από αυτήν του μη επανδρωμένου εναέριου οχήματος και το σύστημα επικοινωνίας του θα είναι διαφορετικό από αυτό του μη επανδρωμένου αεροσκάφους. Αυτό συμβαίνει διότι το συγκεκριμένο μη επανδρωμένο αεροσκάφος δεν διαθέτει στο σύνολο των λειτουργιών του την δυνατότητα παροχής δεδομένων που να αφορούν την ακριβή τοποθεσία του σε σύστημα συντεταγμένων με αποτέλεσμα να γνωρίζουμε κατά προσέγγιση την τοποθεσία του για όσο αυτό θα βρίσκεται εντός του ορατού πεδίου του επίγειου χειριστή του. Επομένως υποχρεωτικά για να μπορεί να παρέχει την πληροφορία των συντεταγμένων του θα πρέπει να επιτραπεί η αναβάθμιση του με την προσθήκη υλικού αυτού του συστήματος στο σύνολο των λειτουργιών του. Καθώς ο σχεδιασμός του υλικού μέρους του συστήματος μικροελεγκτή βρίσκεται σε αρχικό και πειραματικό στάδιο΄ και δεδομένου πως υπάρχουν περιθώρια για περαιτέρω μελλοντικές δοκιμές και εφαρμογές διατάξεων για σειρά επεκτατικών αναβαθμίσεων το σύστημα μικροελεγκτή θα εφαρμοστεί στο εξωτερικό μέρος τους μη επανδρωμένου εναέριου αεροσκάφους με τρόπο τέτοιο ώστε να δοκιμαστεί η κατασκευή προς το πλήρως εύρος των ορθών λειτουργιών της ώστε να επαληθευτεί η αναμενόμενη λειτουργία της ως ένα ενιαίο ενσωματωμένο σύστημα.

2.6 Υλοποίηση Ενσωματωμένου Συστήματος

Όταν το υλικό μέρος της κατασκευής ολοκληρωθεί σε μία ενιαία κατασκευή της οποίας η περιπλοκότητα περιλαμβάνει μεταξύ άλλων τουλάχιστον ένα σύστημα μικροελεγκτή, έναν ελάχιστο αριθμό εμπλεκόμενων ηλεκτρικών και/ή ηλεκτρονικών συσκευών, ένα ή περισσότερα πρωτόκολλα επικοινωνίας και υλικολογισμικό ή/και λογισμικό τότε θεωρείται πως έχει σχηματιστεί ένα λειτουργικό ενσωματωμένο σύστημα. Ως ενσωματωμένο σύστημα ονομάζεται ένα σύστημα υλικού υπολογιστικού συστήματος του οποίου ο σχεδιασμός βασίζει στο επίκεντρο του έναν μικροελεγκτή με υλικολογισμικό που έχει σχεδιαστεί για να εκτελεί μια αποκλειστική λειτουργία είτε ως ανεξάρτητο σύστημα είτε ως μέρος ενός μεγαλύτερου συστήματος. Γενικότερα επειδή τα ενσωματωμένα συστήματα είναι μία σχετικά πρόσφατη τεχνολογική προσθήκη στην καθημερινότητα ο ορισμός του δεν έχει καταλήξει ακόμη σε κάτι το απόλυτο αλλά περιγράφεται ως κάτι γενικό. Στον πυρήνα του συστήματος βρίσκεται ένα ολοκληρωμένο κύκλωμα το οποίο ονομάζεται μικροελεγκτής και είναι σχεδιασμένο να εκτελεί υπολογισμούς για λειτουργίες σε πραγματικό χρόνο όμοιο με ένα ηλεκτρονικό υπολογιστικό σύστημα. Οι πολυπλοκότητα της σύνθεσης του πυρήνα κυμαίνεται από την συμπερίληψη ενός μόνο μικροελεγκτή μέχρι την συμπερίληψη μίας αλληλένδετης συστοιχίας μικροελεγκτών με συνδεδεμένα σε αυτήν περιφερειακά και/ή διάφορα δίκτυα συμπεριλαμβανομένου αυτών της πλήρους αυτοματοποιημένης και αυτόνομης λειτουργίας χωρίς καμία ανθρώπινη παρέμβαση μέχρι τις εφαρμογές συστημάτων διεπαφής που κάνουν χρήση πολύπλοκων γραφικών περιβαλλόντων χρήστη (Graphic User Interface, GUI). Η πολυπλοκότητα ενός ενσωματωμένου συστήματος ποικίλλει σημαντικά ανάλογα με την εργασία για την οποία έχει σχεδιαστεί και δεν είναι δυνατόν να καθοριστεί με απόλυτο ορισμό. Οι εφαρμογές του ενσωματωμένου συστήματος κυμαίνονται από ψηφιακά ρολόγια και φούρνους μικροκυμάτων μέχρι και υβριδικά ηλεκτρικά οχήματα (Electric Vehicles, EV) και ηλεκτρονικά συστήματα και συσκευές. Μέχρι και το 98% όλων των μικροελεγκτών που κατασκευάζονται σε παγκόσμια κλίμακα χρησιμοποιούνται σε σχηματισμό ενσωματωμένων συστημάτων. Η διαχείριση των ενσωματωμένων συστημάτων μπορεί να πραγματοποιείται από μικροελεγκτές, από επεξεργαστές ψηφιακού σήματος (DSP), από GPU

τεχνολογία και συστοιχίες πυλών, από προγραμματιζόμενες συστοιχίες πεδίου πύλης (FPGA) και από ολοκληρωμένα κυκλώματα ειδικής εφαρμογής (ASIC). Αυτά τα συστήματα διαχείρισης επεξεργασίας είναι εξοπλισμένα με ειδικές ηλεκτρονικές διατάξεις σχεδιασμένες για τον χειρισμό ηλεκτρικών και/ή μηχανικών συστημάτων διεπαφής προς το ανθρώπινο στοιχείο. Το λογισμικό των ενσωματωμένων συστημάτων που ορίζει τον τρόπο λειτουργίας του ονομάζεται υλικολογισμικό και αποθηκεύεται σε ένα ολοκληρωμένο κύκλωμα μνήμης τύπου μόνο για ανάγνωση ή μνήμης τύπου flash που εκτελούνται με περιορισμένους πόρους υλικού ηλεκτρονικού υπολογιστικού συστήματος. Τα ενσωματωμένα συστήματα αλληλοεπιδρούν με τον φυσικό κόσμο μέσω των περιφερειακών συσκευών που μπορούν να συνδεθούν σε αυτό αξιοποιώντας τις θύρες εισόδου/εξόδου που διαθέτει. Η βασική δομή ενός ενσωματωμένου συστήματος περιλαμβάνει στοιχεία όπως ο αισθητήρας του οποίου η λειτουργία περιγράφεται ως μία συσκευή που μετράει και μετατρέπει μία ορισμένη φυσική ποσότητα σε ένα αντίστοιχο ηλεκτρικό σήμα το οποίο στη συνέχεια μπορεί να ερμηνευτεί από έναν μηχανικό ενσωματωμένων συστημάτων ή οποιοδήποτε ηλεκτρονικό όργανο μέτρησης το οποίο υπάρχει ως ηλεκτρονική διάταξη στο ενσωματωμένο το οποίο έχει την δυνατότητα αποθήκευσης της μετρούμενης ηλεκτρικής/φυσικής ποσότητας στην μνήμη του ενσωματωμένου συστήματος, έναν μετατροπέα ADC ο οποίος είναι ένας μετατροπέας ενός αναλογικού σήματος σε ψηφιακό σήμα ο οποίος μετατρέπει το αναλογικό σήμα που ανιχνεύει ο αισθητήρας σε ένα αντίστοιχο ψηφιακό σήμα, έναν επεξεργαστή και ASIC όπου οι επεξεργαστές αξιολογούν τα δεδομένα σύμφωνα με τις οδηγίες που παρέχει το υλικολογισμικό για να διαμορφώσουν τα δεδομένα τις εξόδου και να αποθηκευτούν στη μνήμη του ενσωματωμένου συστήματος, έναν μετατροπέα DAC ο οποίος είναι ένας μετατροπέας ψηφιακού σήματος σε ένα αντίστοιχο αναλογικό σήμα και μετατρέπει τα ψηφιακά δεδομένα που παράγονται από τον επεξεργαστή σε αναλογικά δεδομένα και από έναν ενεργοποιητή ο οποίος συγκρίνει το σήμα της εξόδου που παράγεται από τον μετατροπέα DAC με την πραγματική αποθηκεμένη έξοδο και αποθηκεύει την εγκεκριμένη έξοδο.

Το σύνολο της κατασκευής της παρούσας εργασίας αποτελεί ένα ενιαίο σύστημα το οποίο αποτελείται από την σύνθεση διάφορων διακριτών στοιχείων έτσι ώστε κατά την λειτουργία του να παρέχει ένα ορισμένο σύνολο λειτουργιών. Το επίκεντρο του συστήματος που θα διαχειρίζεται και θα ελέγχει τις διάφορες λειτουργίες του το σχηματίζουν ένα ζεύγος συστημάτων μικροελεγκτών τα οποία συστήματα εξάγουν τις οδηγίες για την πλήρη λειτουργία τους από το υλικολογισμικό που διαθέτει το κάθε ένα σύστημα μικροελεγκτή αποθηκεμένο στην μνήμη του. Το κάθε ένα από τα υλικολογισμικά των δύο συστημάτων μικροελεγκτών έχει αναπτυχθεί κατά τέτοιο τρόπο ώστε το ένα να αποτελεί μέρος του άλλου έτσι που να είναι επί της ουσίας ένα σύνθετο υλικολογισμικό των δύο μερών. Τα συστήματα μικροελεγκτών σε συνδυασμό με το υλικολογισμικό που έχουν αποθηκεμένο στις μνήμες τους αποτελεί τον πυρήνα του ενσωματωμένου συστήματος γύρω από τον οποίο θα σχηματιστεί το υπόλοιπο ενσωματωμένο σύστημα. Το ένα σύστημα μικροελεγκτή θα εκτελεί χρέη δέκτη και θα λειτουργεί στα πλαίσια του IDE της Arduino σε ένα οικιακό ηλεκτρονικό υπολογιστικό σύστημα όπου η λειτουργία του θα είναι να λαμβάνει με χρήση του ασύρματου πρωτοκόλλου Wi-Fi κρυπτογραφημένα δεδομένα συντεταγμένων σε πραγματικό χρόνο από το σύστημα μικροελεγκτή του πομπού τα οποία θα αποκρυπτογραφεί και θα τα απεικονίζει στο απεικονιστικό του IDE της Arduino. Το άλλο σύστημα μικροελεγκτή θα εκτελεί χρέη πομπού και θα είναι συνδεδεμένο σε αυτό μία συσκευή GPS την οποία θα ελέγχει και θα διαχειρίζεται, θα κρυπτογραφεί τα δεδομένα που θα λαμβάνει από την συσκευή GPS και θα τα μεταδίδει στον δέκτη. Το σύστημα μικροελεγκτή του πομπού θα εγκατασταθεί στο σώμα ενός μη επανδρωμένου εναέριου οχήματος ώστε να το αναβαθμίσει με την προσθήκη σε αυτό ενός συστήματος παροχής πληροφοριών GPS. Μέρος της συνολικής αναβάθμισης περιλαμβάνει και την μέθοδο κρυπτογράφησης ως πρακτική εφαρμογή για τις συντεταγμένες ενός μη επανδρωμένου

εναέριου οχήματος όπου η μέθοδος κρυπτογράφησης αφορά την κατασκευή ενός κλειδιού κρυπτογράφησης κάνοντας χρήση ενός χαοτικού χάρτη, μία μαθηματική μέθοδος ανεπτυγμένη στην θεωρεία του χάους που αφορά μία συνεχή μορφή χάους η οποία παρουσιάζει την ανάπτυξη της χαρακτηριστικής της σε προοδευτική μη γραμμικότητα καθιστώντας αδύνατη την οποιαδήποτε απόπειρα γραμμικοποίησης της. Συμπεριλαμβανομένου και του συστήματος μικροελεγκτή που είναι υπεύθυνο για τις κινηματικές λειτουργίες του μη επανδρωμένου εναέριου οχήματος και αυτού που θα ελέγχει την μετάδοση πληροφοριών του συστήματος τηλεχειρισμού το σύνολο του ενσωματωμένου θα περιέχει τέσσερα συστήματα μικροελεγκτών τα οποία θα ελέγχουν και θα διαχειρίζονται το σύνολο των λειτουργιών του. Το ένα κύριο μέρος του ενσωματωμένου συστήματος θα είναι η συσκευή του πομπού που θα κρυπτογραφεί δεδομένα συντεταγμένων και θα τα μεταδίδει στην συσκευή του δέκτη που θα τα αποκρυπτογραφεί και θα τα απεικονίζει ελεγχόμενη από το ζεύγος μικροελεγκτών. Το επόμενο κύριο μέρος του ενσωματωμένου συστήματος θα είναι η συσκευή που θα διαχειρίζεται και θα ελέγχει τις λειτουργίες του συστήματος τηλεχειρισμού και θα τις διαβιβάζει στο σύστημα λήψης του μη επανδρωμένου εναέριου οχήματος από το δικό του εγκατεστημένο σύστημα μικροελεγκτή. Το τελευταίο κύριο μέρος του ενσωματωμένου συστήματος θα είναι η συσκευή του μη επανδρωμένου εναέριου οχήματος το οποίο οι περιγραφή των λειτουργιών του συνοψίζονται σε πτήση όπου θα ελέγχει το επίπεδο της αιώρησης του ως προς την κατεύθυνση της δύναμης επιτάχυνσης της βαρύτητας της γης και την πλεύση της στο επίπεδο αυτό, καθώς και την λήψη των μεταδιδόμενων πληροφοριών από το σύστημα τηλεχειρισμού της. Όλα τα ανωτέρω συνθέτουν ένα πλήρες ενσωματωμένο σύστημα.

Στο σχήμα 2.9 απεικονίζεται η πληροφορία του συστήματος GPS όπως αυτή λαμβάνεται από το δορυφορικό δίκτυο στην συσκευή δέκτη GPS και έπειτα όπως αυτή λαμβάνεται από το σύστημα μικροελεγκτή μέσω της σειριακής εισόδου και ερμηνεύεται από το υλικολογισμικό του ώστε να εμφανιστεί στην τελική του μορφή.

```
Location: 40.617440,22.958838  Date/Time: 1/31/2022 20:30:35.00
Location: 40.617440,22.958838  Date/Time: 1/31/2022 20:30:35.00
Location: 40.617440,22.958838  Date/Time: 1/31/2022 20:30:35.00
HTTP Response code: 200
Location: 40.617440,22.958838  Date/Time: 1/31/2022 20:30:35.00
Location: 40.617440,22.958838  Date/Time: 1/31/2022 20:30:35.00
Location: 40.617440,22.958838  Date/Time: 1/31/2022 20:30:35.00
Location: 40.617440,22.958838  Date/Time: 1/31/2022 20:30:35.00
HTTP Response code: 200
Location: 40.617440,22.958838  Date/Time: 1/31/2022 20:30:35.00
Location: 40.617440,22.958838  Date/Time: 1/31/2022 20:30:35.00
Location: 40.617440,22.958838  Date/Time: 1/31/2022 20:30:35.00
Location: 40.617440,22.958838  Date/Time: 1/31/2022 20:30:35.00
```

Εικόνα 2-9: Απεικόνιση πληροφοριών συντεταγμένων στον διακομιστή πριν την κρυπτογράφηση.

Όπως διακρίνεται στο σχήμα 2.9 καθώς το GPS είναι ένα σύστημα παροχής συντεταγμένων σε πραγματικό χρόνο απεικονίζει τις πληροφορίες που αφορούν την τοποθεσία του δέκτη στον χώρο σε μοίρες ως προς τον μεσημβρινό και τον παράλληλο αλλά και σε πραγματικό χρόνο σε μορφή ημερομηνίας και ώρας.

Αντίστοιχα στο σχήμα 2.10 απεικονίζεται η ίδια πληροφορία όπως αυτή μεταδόθηκε στον πελάτη.

```
Location: 40.617440,22.958835  Date/Time: 1/31/2022 20:30:33.00
Location: 40.617440,22.958837  Date/Time: 1/31/2022 20:30:34.00
Location: 40.617440,22.958837  Date/Time: 1/31/2022 20:30:34.00
Location: 40.617440,22.958837  Date/Time: 1/31/2022 20:30:34.00
Location: 40.617440,22.958837  Date/Time: 1/31/2022 20:30:34.00
Location: 40.617440,22.958837  Date/Time: 1/31/2022 20:30:34.00
Location: 40.617440,22.958837  Date/Time: 1/31/2022 20:30:34.00
Location: 40.617440,22.958838  Date/Time: 1/31/2022 20:30:35.00
Location: 40.617440,22.958838  Date/Time: 1/31/2022 20:30:35.00
Location: 40.617440,22.958838  Date/Time: 1/31/2022 20:30:35.00
Location: 40.617442,22.958842  Date/Time: 1/31/2022 20:30:36.00
Location: 40.617442,22.958842  Date/Time: 1/31/2022 20:30:36.00
Location: 40.617442,22.958842  Date/Time: 1/31/2022 20:30:36.00
Location: 40.617442,22.958842  Date/Time: 1/31/2022 20:30:36.00
Location: 40.617442,22.958842  Date/Time: 1/31/2022 20:30:36.00
```

Εικόνα 2-10: Απεικόνιση πληροφοριών συντεταγμένων στον πελάτη μετά την αποκρυπτογράφηση.

Όπως διακρίνεται στο σχήμα 2.10 η απεικόνιση της πληροφορίας της συσκευής του δέκτη GPS απεικονίζεται με πιστότητα στο σύστημα μικροελεγκτή που λειτουργεί ως δέκτης καθώς παρέχει τις ίδιες συντεταγμένες τοποθεσίας στην ίδια χρονική στιγμή. Μετά την απεικόνιση της πληροφορίας της συσκευής GPS στον διακομιστή κρυπτογραφήθηκε για την ασύρματη μετάδοση της στον πελάτη ο οποίος την απεικόνισε μορφολογικά σωστά που σημαίνει πως και η διαδικασία κρυπτογράφησης/αποκρυπτογράφησης λειτούργησε τέλεια και σε πραγματικό χρόνο.

2.7 Περίληψη Κεφαλαίου

- Το λογισμικό αποτελεί το σύνολο οδηγιών με το οποίο ένα πρόγραμμα μπορεί να κατανοήσει το τι ακριβώς πρέπει να κάνει κατά την διάρκεια της εκτέλεσης του.
- Ένα πρόγραμμα για να αναπτυχθεί πρέπει να γραφτεί σε έναν ειδικό κειμενογράφο ο οποίος έχει εργαλεία υποστήριξης σωστής ανάπτυξης του. Προκειμένου να αναπτυχθεί ένα λογισμικό Είναι απαραίτητη από πλευράς προγραμματιστή η καλή γνώση τουλάχιστον μίας γλώσσας προγραμματισμού.
- Μία γλώσσα προγραμματισμού είναι το εργαλείο ενός προγραμματιστή για να υλοποιήσει την δομή των οδηγιών προς το υλικό ενός υπολογιστικού συστήματος ώστε αυτό να μπορέσει να εκτελέσει ένα σύνολο επιθυμητών ενεργειών και λειτουργιών. Ο ειδικός κειμενογράφος στον οποίο αναπτύσσεται ένα πρόγραμμα περιλαμβάνει ένα εργαλείο το οποίο ονομάζεται μεταγλωττιστής και μεταγλωττίζει τον κώδικα από την γλώσσα προγραμματισμού σε γλώσσα μηχανής.
- Το υλικό μέρος μιας κατασκευής περιγράφει όλο το μέρος της το οποίο είναι απτό. Διαφέρει κατά κύριο λόγο από το λογισμικό στο ότι δεν είναι τόσο εύκολη η μεταβολή και η διαμόρφωση του όταν αυτή μορφοποιηθεί.
- Ένα σύστημα μικροελεγκτή περιέχει στον πυρήνα του ένα ολοκληρωμένο κύκλωμα το οποίο ονομάζεται μικροελεγκτής και στην ουσία αποτελεί ένα υπολογιστικό σύστημα περιορισμένων δυνατοτήτων. Το σύστημα μικροελεγκτή είναι ένα PCB που με τις διατάξεις που περιέχει υποβοηθά τον μικροελεγκτή να διαχειρίζεται τις θύρες επικοινωνίας, τις εξόδους εισόδους και τις παροχές ισχύος.
- Το υλικολογισμικό είναι μία συγκεκριμένη μορφή λογισμικού που συνήθως απευθύνεται για εφαρμογή σε έναν μικροελεγκτή. Θα πρέπει η ανάπτυξη του να γίνεται με τέτοιο τρόπο ώστε να ανταποκρίνεται στις δυνατότητες του συστήματος μικροελεγκτή αλλά και για το σύνολο των λειτουργιών για το οποίο προορίζεται το σύστημα μικροελεγκτή.
- Το σύστημα GPS είναι μία μέθοδος παροχής συντεταγμένων σε έναν δέκτη σε αληθινό χρόνο.

- Ένα module περιγράφει έναν τύπο συσκευής η οποία είναι σχεδιασμένη να λειτουργεί για το σύνολο των λειτουργιών της τελείως αυτόνομα και συνήθως κατασκευάζεται με τέτοιον τρόπο που να αποτελεί περιφερειακή συσκευή ενός συστήματος μικροελεγκτή.
- Με τον όρο ενσωματωμένο σύστημα περιγράφεται το σύνολο διάφορων συσκευών ή διατάξεων με διαφορετική λειτουργία μεταξύ τους που μπορούν να σχηματίσουν ένα ενιαίο σύστημα με πυρήνα ένα ή και περισσότερα συστήματα μικροελεγκτή τα οποία περιλαμβάνουν στο περιεχόμενο της μνήμης τους το υλικολογισμικό λειτουργίας τους.
- Το ενσωματωμένο σύστημα της κατασκευής της παρούσας εργασίας αποτελείται από την σύνθεση τριών διακριτών συσκευών.
- Η μία από τις τρεις συσκευές που συνθέτουν το ενσωματωμένο σύστημα θα εκτελεί την διαδικασία κρυπτογράφησης/αποκρυπτογράφησης των δεδομένων μιας συσκευής GPS και την μετάδοση τους μεταξύ ενός εκπομπού και δέκτη. Στο περιεχόμενο της θα περιέχει δύο συστήματα μικροελεγκτών.
- Η επόμενη συσκευή που συνθέτει το ενσωματωμένο σύστημα αφορά τον τηλεχειρισμό του μη επανδρωμένου εναέριου οχήματος η οποία σχηματίζει ένα σύστημα τηλεχειρισμού με χρήση διάφορων διακοπτών οι οποίοι ελέγχονται από ένα σύστημα μικροελεγκτή που είναι εγκατεστημένο στην συσκευή και που αναλαμβάνει την μετάδοση των σημάτων των διακοπτών προς το σύστημα λήψης του μη επανδρωμένου εναέριου οχήματος.
- Η τελευταία συσκευή που συνθέτει το ενσωματωμένο σύστημα αφορά ένα μη επανδρωμένο εναέριο αεροσκάφος το οποίο ελέγχεται από ένα εγκατεστημένο σε αυτό σύστημα μικροελεγκτή που ελέγχει τις λειτουργίες πτήσης και αιώρησης του, καθώς και την λήψη των οδηγιών από τον επίγειο χειριστή του και την ερμηνεία τους.

Κεφάλαιο 3ο: Συμπεράσματα και προτάσεις βελτίωσης

3.1 Εισαγωγή

Κατά την ολοκλήρωση του συνόλου ενός έργου όπως αυτό της παρούσας πτυχιακής εργασίας είναι καλή αλλά και απαραίτητη πρακτική η καταγραφή των συμπερασμάτων από το αποτέλεσμα της συνολικής λειτουργίας της και γενικότερα από ότι αξιοσημείωτο συνέβη κατά την μελέτη και υλοποίηση των διάφορων μερών της που την συνθέτουν. Ο κύριος λόγος για τον οποίο αυτό είναι απαραίτητο είναι διότι τα συμπεράσματα επικεντρώνουν στα κύρια σημεία τα οποία είναι τα κρισιμότερα για το σύνολο της εργασίας και παρέχουν τις κατάλληλες πληροφορίες για την ανάπτυξη άλλων εργασιών που θα βασίζονται σε αυτήν κατά μέρος ή εξολοκλήρου για την ανάπτυξη πιο βελτιωμένων συστημάτων ή για την βελτίωση της παρούσας. Μεταξύ των συμπερασμάτων αναπτύσσεται και ένα σύνολο προτάσεων για πιθανούς τρόπους βελτίωσης της ή συνέχισης της κατά κάποιων μερών της ή του συνόλου της ή ακόμη και συμπερίληψης της σε ένα μεγαλύτερο σύνολο μιας άλλης εργασίας.

3.2 Συμπεράσματα Μελέτης

Από την μελέτη της εργασίας προκύπτουν αρκετά συμπεράσματα από την διαδικασία του γενικού αρχικού σχεδιασμού μέχρι τον καταληκτικό λεπτομερή σχεδιασμό. Αρχικά προκύπτει πως η μέθοδος κρυπτογράφησης αποτελεί ένα κρίσιμο στοιχείο συστήματος που πρέπει να συμπεριλαμβάνεται όχι κατά κόρον αλλά σε συγκεκριμένες μόνο περιπτώσεις και αυτό γιατί η μεγαλύτερη αδυναμία μίας μεθόδου κρυπτογράφησης είναι η συχνότητα χρήσης της. Καθώς μία μέθοδος κρυπτογράφησης γίνεται όλο και πιο δημοφιλής σημαίνει παράλληλα πως όλο και περισσότερος κόσμος θα ασχολείται με το περιεχόμενο της και την κατανόηση του με όλο και περισσότερες προσεγγίσεις, ενώ οι άνθρωποι που

θα επιχειρούν να ανακαλύψουν τρόπους για να την παραβιάσουν θα αυξάνονται με γεωμετρικούς ρυθμούς. Η συγκεκριμένη μέθοδος είναι σίγουρα άξια προσοχής διότι η μέθοδος με την οποία παράγεται το κλειδί κρυπτογράφησης προσδίδει έναν βαθμό πολυπλοκότητας που φαίνεται να είναι πρακτικά αδύνατο για κάποιον να βρει τρόπο να την παραβιάσει διότι ακόμη και να γνωρίζει πως το κλειδί κρυπτογράφησης παρασκευάστηκε με την μέθοδο χαοτικού χάρτη θα πρέπει να ανακαλύψει οπωσδήποτε την εξίσωση του χαοτικού χάρτη και έπειτα θα πρέπει να ανακαλύψει τις ακριβείς τιμές που χρησιμοποιήθηκαν για τον κάθε συντελεστή του χαοτικού χάρτη. Πέρα από τον τρόπο παραγωγής κρυπτογράφησης η μέθοδος κρυπτογράφησης των δεδομένων προσθέτει στην περιπλοκότητα επομένως προκύπτει πως αν μπορεί να δει κανείς την όλη διαδικασία της μελέτης της κατασκευής ως μία διαδικασία της οποίας το κάθε βήμα θα χτιστεί με βάση το προηγούμενο βήμα της τότε το κάθε βήμα προσθέτει μία αύξηση του βαθμού δυσκολίας παραβίασης του που συμβαίνει με εκθετικό ρυθμό.

Η διαδικασία ανάπτυξης λογισμικού που να εκτελεί την διαδικασία κρυπτογράφησης αφού αυτή έχει μία φορά καθοριστεί πρέπει να ακολουθήσει μία συγκεκριμένη μέθοδο ώστε να προκύψει ένα βέλτιστο τελικό προϊόν που θα εκτελεί τις λειτουργίες του ομαλά και αποδοτικά. Το γεγονός αυτό παραπέμπει στην σπουδαιότητα που έχει η ανάπτυξη του λογισμικού μέρους μιας κατασκευής για την λειτουργία της και για αυτό θα πρέπει να του δίνεται η ανάλογη προσοχή προκειμένου να σχηματιστεί και να λειτουργήσει όσο το δυνατόν καλύτερα και βέλτιστα γίνεται. Κρίσιμο παράγοντα στην ποιότητα της ανάπτυξης του λογισμικού αποτελεί το πρώτο στάδιο σχεδιασμού του που πραγματοποιείται με τον σχεδιασμό του αλγόριθμου του κάνοντας χρήση των διαγραμμάτων ροής.

Όταν πρόκειται για ανάπτυξη λογισμικού που πρόκειται να λειτουργήσει στα πλαίσια ενός συστήματος μικροελεγκτή τότε είναι καλή πρακτική από πλευράς μηχανικού να αναπτύξει τα κύρια μέρη του λογισμικού έτσι ώστε να λειτουργήσουν όσο πιο απλά γίνεται προτού να προσαρμοστούν στις απαιτήσεις του λογισμικού. Η ανάπτυξη λογισμικού που πρόκειται να εφαρμοστεί σε σύστημα μικροελεγκτή αποτελεί μία ξεχωριστή κατηγορία λογισμικού που ονομάζεται υλικολογισμικό το οποίο πρέπει να προσαρμοστεί συγκεκριμένα στο σύστημα μικροελεγκτή που θα εφαρμοστεί και εκτελεστεί.

Η εφαρμογή συστήματος κρυπτογράφησης στα πλαίσια ενός συστήματος μικροελεγκτή προσφέρει κάποια σημαντικά οφέλη κυρίως στο χαμηλό κόστος καθώς πραγματοποιείται στα πλαίσια προσθήκης και αναβάθμισης λογισμικού όπου από υλικής άποψης η πολυπλοκότητα και το κόστος είναι σχετικά χαμηλό.

Η αποδοτικότητα μιας αυτόνομης συσκευής GPS παρέχει μία ευελιξία στον σχεδιασμό του συστήματος καθώς είναι μία συσκευή συγκεκριμένου σκοπού και είναι εύκολο να προσαρμοστεί σε ένα σύστημα μικροελεγκτή και σαν υλικό αλλά και σαν μέρος του υλικολογισμικού.

Τα συστήματα μικροελεγκτών αποτελούν πραγματικό παράγοντα αναβάθμισης ενός συστήματος ή μιας συσκευής χάρη στο γεγονός ότι είναι ένα πλήρες ηλεκτρονικό υπολογιστικό σύστημα. Επομένως παρέχει ένα σύνολο δυνατοτήτων αν και σαφώς περιορισμένο σε σύγκριση με ένα τυπικό οικιακό ηλεκτρονικό υπολογιστικό σύστημα οι οποίες επιτρέπουν την ενσωμάτωση ενός συστήματος εντοπισμού συντεταγμένων και κατ’ επέκταση την ενσωμάτωση οποιουδήποτε άλλου συστήματος που είναι δυνατόν να σχηματιστεί.

3.3 Συμπεράσματα Κατασκευής

Η εφαρμογή ενός χαοτικού χάρτη για την παραγωγή ενός κλειδιού κρυπτογράφησης προσφέρει μία μέθοδο παραγωγής του κλειδιού κρυπτογράφησης με παράγοντα τυχαιότητας τόσο υψηλό που είναι πρακτικά αδύνατο να παραβιαστεί.

Προκειμένου να αναπτυχθεί ένα λογισμικό είναι απαραίτητη για τον μηχανικό η ελάχιστη γνώση μίας γλώσσας προγραμματισμού. Η γλώσσα C παρέχει δυνατότητες ανάπτυξης λογισμικού σε επίπεδο κοντά σε αυτό της μηχανής επιτρέποντας έναν υψηλό παράγοντα αποδοτικότητας και βελτιστοποίησης του αναπτυσσόμενου προγράμματος κάνοντας την κατάλληλη επιλογή για την ανάπτυξη κάποιου προγράμματος, αλλά όχι και την πιο γρήγορη σε χρόνο ανάπτυξης καθώς αυτό είναι το κόστος για την ακρίβεια στην λεπτομέρεια που παρέχει.

Η προσαρμογή ενός ανεπτυγμένου και λειτουργικού λογισμικού σε ένα υλικολογισμικό που θα λειτουργεί σε συγκεκριμένο σύστημα μικροελεγκτή είναι μία διαδικασία που απαιτεί ιδιαίτερες και εξειδικευμένες γνώσεις προκειμένου να λειτουργήσει μέσα στα επιθυμητά πλαίσια και να αποδίδει τα ελάχιστα αναμενόμενα αποτελέσματα.

Ο συνδυασμός μεταξύ υλικού και λογισμικού για την ανάπτυξη ενός αυτόνομου συστήματος είναι μία διαδικασία που απαιτεί από τον μηχανικό να έχει ένα μεγάλο εύρος γνώσεων προκειμένου να προκύψει ένα λειτουργικό προϊόν που να εκτελεί τις αναμενόμενες λειτουργίες του αλλά προσφέρει ένα σημαντικό βαθμό πλεονεκτημάτων ιδιαίτερα στον τομέα της αυτονομίας και των εκτελέσιμων ενεργειών σε σχέση με το κόστος ανάπτυξης τους.

Η επικοινωνία μεταξύ δύο συστημάτων μικροελεγκτών με το πρωτόκολλο επικοινωνίας Wi-Fi επιτρέπει την επικοινωνία μέσα σε μία σχετικά μικρή ακτίνα από τον επίγειο χειριστή που σημαίνει πως επιτρέπει την εφαρμογή του σε καταστάσεις που η μεγάλη εμβέλεια δεν το επιτρέπει. Το μειονέκτημα είναι ο βαθμός περιπλοκότητας καθώς απαιτείται να οριστεί οπωσδήποτε ένας διακομιστής στον οποίο να μπορούν να συνδεθούν οι πελάτες του προκειμένου να δουλέψει όλο το σύστημα.

Η αυτόνομη συσκευή του δέκτη GPS αφού έχει γίνει μέρος του συστήματος μικροελεγκτή ως περιφερειακή του συσκευή προκειμένου να μπορέσει να ανιχνευτεί από το δορυφορικό δίκτυο απαιτεί κατά την διαδικασία εκκίνησης λειτουργίας και μέχρι τον εντοπισμό της θέσης της να βρίσκεται σε ανοιχτό χώρο με καθαρό οπτικό πεδίο μεταξύ αυτής και του δορυφορικού δικτύου. Αν κατά την διάρκεια λειτουργίας της και αφού εντοπιστεί από το δίκτυο βρεθεί εντός κλειστού χώρου είναι σχεδόν σίγουρο ότι θα χαθεί το στίγμα της. Όταν αυτή γνωρίζει την τοποθεσία της τότε θα έχει ακρίβεια μικρότερη των δύο μέτρων.

3.4 Προτάσεις Βελτίωσης και Συνέχισης

Στα πλαίσια της βελτίωσης είναι υπαρκτή η δυνατότητα της συνέχισης της ανάπτυξης του περιεχομένου αυτής της εργασίας αρκεί ο μηχανικός που την ανέπτυξε να επισημάνει ενδεικτικά κάποια σημεία της ώστε να διευκολύνει την αναγνώριση τους.

Συγκεκριμένα στην εργασία αυτή θα μπορούσε να βελτιωθεί στο κομμάτι της μεθόδου κρυπτογράφησης ως προς τον τρόπο με τον οποίο πραγματοποιείται η κρυπτογράφηση των δεδομένων με το κλειδί κρυπτογράφησης επιχειρώντας την αύξηση του συντελεστή περιπλοκότητας της μεθόδου είτε προσθέτοντας περισσότερες αριθμητικές ή μαθηματικές πράξεις.

Στα πλαίσια της βελτίωσης της παραγωγής του κλειδιού κρυπτογράφησης να προστεθεί μέσα στην συνάρτηση ένα σύνολο εντολών για την τακτική παραγωγή κλειδιών σε μεταξύ τους χρονικό συσχετισμό.

Μία σημαντική αναβάθμιση του συστήματος θα μπορούσε να γίνει στην εμβέλεια της ασύρματης επικοινωνίας μεταξύ του ζεύγους των συστημάτων μικροελεγκτών οι οποίοι έχουν μεταξύ τους εμβέλεια 50-60 μέτρα.

Η αναβάθμιση της παροχής ενέργειας του μη επανδρωμένου εναέριου οχήματος για την αύξηση της αυτονομίας της λειτουργίας του θα ήταν ένας σημαντικός παράγοντας αναβάθμισης του συνολικού συστήματος.

3.5 Περίληψη κεφαλαίου

- Το τέλος μιας εργασίας πρέπει απαραίτητα να συνοδεύεται από τα συμπεράσματα της και τις προτάσεις βελτίωσης και/ή συνέχισης της.
- Τα συμπεράσματα εξυπηρετούν στην σύνοψη των κυρίων αποτελεσμάτων και ευρημάτων από το σύνολο της εργασίας.
- Οι προτάσεις βελτίωσης αποσκοπούν στην ενθάρρυνση της έρευνας αλλά και τις τεχνολογικής προόδου τόσο στο γενικό και αόριστο όσο και στο στοχευμένο σκέλος που έχει ως σημείο αναφοράς μία συγκεκριμένη εργασία.
- Η συνέχιση του έργου μιας εργασίας αφορά είτε την ολοκληρωτική της συνέχεια αυτούσια είτε κάποιων επιλεγμένων από αυτή τμημάτων της στον σχηματισμό μιας νέας εργασίας εμπνευσμένης από αυτήν με στόχο την περαιτέρω ανάπτυξης της είτε για ακαδημαϊκό σκοπό είτε για οποιονδήποτε άλλο.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Data Sheet

[8] GlobalTop Technology Corporation, “GPS Standalone Module,” FGPMMOPA6H datasheet, 2011.

[9] Espressif Systems, “ESP32 Wroom Module,” ESP32-WROOM-MODULE datasheet, 2021.

Internet Site

[1] Wikipedia, “Unmanned aerial vehicle,” Wikipedia. [Online]. Available:

https://en.wikipedia.org/wiki/Unmanned_aerial_vehicle

[2] Cloudflare, “What is encryption,” Cloudflare. [Online]. Available:

https://www.cloudflare.com/learning/ssl/what-is-encryption/

[3] Wikipedia, “List of chaotic maps,” Wikipedia. [Online]. Available:

https://en.wikipedia.org/wiki/List_of_chaotic_maps

[4] The fast code, “Τι είναι το υλικολογισμικό ή μικροκώδικας και πως μπορώ να ενημερώσω το υλικό μου,” thefastcode. [Online]. Available: https://www.thefastcode.com/el-eur/article/what-is-firmware-or-microcode-and-how-can-i-update-my-hardware

[5] Tech target, “Embedded system,” Techtarget. [Online]. Available:

https://internetofthingsagenda.techtarget.com/definition/embedded-system

[7] Wikipedia, “Global Pointing System,” Wikipedia. [Online]. Available:

https://el.wikipedia.org/wiki/Global_Positioning_System

[10] Wikipedia, “Wi-Fi,” Wikipedia. [Online]. Available:

https://en.wikipedia.org/wiki/Wi-Fi

[11] Geeks for geeks, “C Programming Language,” Geeksforgeeks. [Online]. Available:

https://www.geeksforgeeks.org/c-programming-language/

Paper in Conference Proceedings

[6] A. Iatropoulos, L. Moysis, A. Giakoumis, C. Volos, A. Ouannas and S. Goudos, “Medical Data Encryption based on a Modified Sinusoidal 1D Chaotic Map and Its Microcontroller Implementation,” In MOCAST International Conference on Modern Circuits And System Technologies ’21, 2021, pp. 44.

ΠΑΡΑΡΤΗΜΑ Α : Κώδικας συστήματος μικροελεγκτή που λειτουργεί ως server στην γλώσσα προγραμματισμού C

```
// Necessary libraries for the use of certain functions
#include "WiFi.h"
#include "ESPAsyncWebServer.h"
#include <HardwareSerial.h>
#include <Wire.h>
#include <TinyGPSPlus.h>

/*Set access point network credentials*/
const char* ssid = "ESP32-Access-Point";
const char* password = "123456789";

//Make a place to store the key
static char* encBits;
TinyGPSPlus gps;

// Create AsyncWebServer object on port 80
AsyncWebServer server(80);

HardwareSerial SerialGPS(2);

String dtGPS;
/*function that generates a chaotic bitstream.*/
char* GenrateChaoticBitsream() {

  /*Initialize buffers.*/
  bool Chaotic_Bitsream[32];
  static char c[4] ;

  /*Initialize equation variables.*/
  float X = 0.1;
```

```
 int A = 8, B = 15, C = 100;


 /*Loop that executes 32 iterations of the chaotic equation and stores 32 bits into an array.*/
 for (int i = 0; i < 32; i++) {
  X = A * sin(C / (X - 1)) + B * (tanh(X - 1) * tanh(X - 1));

  Chaotic_Bitsream[i] = (int(X) % 2); //convert to binary

 }



 //Convert from bool[32] to char [4]
 for (int x = 0; x < 4; x++) {
  for (int i = 0; i < 8; i++) {
   if (Chaotic_Bitsream[x * i + i]) {
    c [x] |= 1 << i;
   }
  }
 }


 return  c;

}



//Encryption function
char* encrypt (char data[], int dataSize, char key[]) {
 static char dataOut[10000]; // Ouput buffer (length must be bigger than data)
 for (int i = 0; i < dataSize; i++) {
```

```
    dataOut [i] = data[i] ^ key [i % 4]; // Do the actual Xor op. key[i%4] in order to have an index 0-3 every 4 iterations;
  }

  return dataOut;

}

/*This is the part where the code will set the standard parameters*/
void setup() {
  Serial.begin(115200); // initialization of serial communication
  Serial2.begin(115200);

  WiFi.begin(ssid, password); // initialization of  Wi-Fi communication protocol and ask for user and password information
  Serial.println("Connecting"); // after correct information are given print on screen the “Connecting” status
  while (WiFi.status() != WL_CONNECTED) { // Prints dots until connection is established
    delay(100);
    Serial.print(".");
  }
/*a series of screen messages*/
  Serial.println("");
  Serial.print("Connected to WiFi network with IP Address: ");
  Serial.println(WiFi.localIP());
  encBits = GenrateChaoticBitsream(); //creation of encryption key
  SerialGPS.begin(9600, SERIAL_8N1, 16, 17); //initialization of gps device serial communication
  SerialGPS.setTimeout(10);

  server.on("/test", HTTP_GET, [](AsyncWebServerRequest * request) {
    char dt[dtGPS.length()]; // setting a testing request to check server functionality

    dtGPS.toCharArray(dt,dtGPS.length());
    dtGPS=""; // assign the length of gps information to a variable
```

```
    request->send_P(200, "text/plain", encrypt(dt, sizeof(dt), encBits) );
   });
  server.begin(); //execution of server
}
/*declaration of time variables*/
unsigned long previousMillis = 0;
const long interval = 200;



void loop() { // This is the part of the code that will be executed repeatedly
  while (SerialGPS.available() > 0) {dtGPS+=SerialGPS.readString();} // continuous reception of gps information


  unsigned long currentMillis = millis();

/*statement check for getting gps information in regular time indexes*/
  if (currentMillis - previousMillis >= interval) {
    int i=0;
   while (dtGPS.length()>i){
   i++;
    if (gps.encode(dtGPS[i])){
      displayInfo();}
      }
      previousMillis = currentMillis;
  }
  }



/*A statement check regarding screen information about gps status*/
void displayInfo(){
  Serial.print(F("Location: "));
  if (gps.location.isValid())
  {
```

```
  Serial.print(gps.location.lat(), 6);
  Serial.print(F(","));
  Serial.print(gps.location.lng(), 6);
}
else
{
  Serial.print(F("INVALID"));
}

Serial.print(F("  Date/Time: "));
if (gps.date.isValid())
{
  Serial.print(gps.date.month());
  Serial.print(F("/"));
  Serial.print(gps.date.day());
  Serial.print(F("/"));
  Serial.print(gps.date.year());
}
else
{
  Serial.print(F("INVALID"));
}

Serial.print(F(" "));
if (gps.time.isValid())
{
  if (gps.time.hour() < 10) Serial.print(F("0"));
  Serial.print(gps.time.hour());
  Serial.print(F(":"));
  if (gps.time.minute() < 10) Serial.print(F("0"));
  Serial.print(gps.time.minute());
  Serial.print(F(":"));
  if (gps.time.second() < 10) Serial.print(F("0"));
```

```
    Serial.print(gps.time.second());
    Serial.print(F("."));
    if (gps.time.centisecond() < 10) Serial.print(F("0"));
    Serial.print(gps.time.centisecond());
  }
  else
  {
    Serial.print(F("INVALID"));
  }

  Serial.println();
}
```

ΠΑΡΑΡΤΗΜΑ Β : Κώδικας συστήματος μικροελεγκτή που λειτουργεί ως client στην γλώσσα προγραμματισμού C

```
// Necessary libraries for the use of certain functions
#include <TinyGPSPlus.h>
#include "WiFi.h"
#include <HTTPClient.h>
#include <Wire.h>

/*Set access point network credentials*/
const char* ssid = "ESP32-Access-Point";
const char* password = "123456789";

//Make a place to store the key
static char* encBits;

TinyGPSPlus gps;


/*declaration of global functions.*/
/*function that generates a chaotic bitstream.*/
```

```
char* GenrateChaoticBitsream() {

 /*Initialize buffers.*/
 bool Chaotic_Bitsream[32];
 static char c[4] ;

 /*Initialize equation variables.*/
 float X = 0.1;
 int A = 8, B = 15, C = 100;


 /*Loop that executes 32 iterations of the chaotic equation and stores 32 bits into an array.*/
 for (int i = 0; i < 32; i++) {
  X = A * sin(C / (X - 1)) + B * (tanh(X - 1) * tanh(X - 1));

  Chaotic_Bitsream[i] = (int(X) % 2); //convert to binary

 }



 //Convert from bool[32] to char [4]
 for (int x = 0; x < 4; x++) {
  for (int i = 0; i < 8; i++) {
   if (Chaotic_Bitsream[x * i + i]) {
    c [x] |= 1 << i;
   }
  }
 }


 return  c;
```

```
}



//Encryption function
char* encrypt (char data[], int dataSize, char key[]) {
  static char dataOut[10000]; // Ouput buffer (length must be bigger than data)
  for (int i = 0; i < dataSize; i++) {
    dataOut [i] = data[i] ^ key [i % 4]; // Do the actual Xor op. key[i%4] in order to have an index 0-3 every 4 iterations;
  }

  return dataOut;

}

/*Declaration of time variables*/
unsigned long previousMillis = 0;
const long interval = 200;

void setup() {
  // This is where the code will initialize the standard settings
  /*Serial port for debugging*/
  Serial.begin(115200);
  Serial.println();

  /*Setting the ESP as an Access Point*/
  Serial.print("Setting AP (Access Point)...");
  WiFi.softAP(ssid, password);

  IPAddress IP = WiFi.softAPIP();
  Serial.print("AP IP Address: ");
  Serial.println(IP);
```

```
  encBits = GenrateChaoticBitsream();

}



void loop() {
  // This is where the code will be executed repeatedly

  unsigned long currentMillis = millis();

  if (currentMillis - previousMillis >= interval) {
    //Check WiFi connection status
    char *gpsStream;
    String indt = httpGETRequest("http://192.168.4.2/test");
    char  dt[indt.length()];
    indt.toCharArray(dt,sizeof(dt));
    char* decrypted = gpsStream;  encrypt(dt,sizeof(dt),encBits);
    Serial.print(decrypted);
   while (*gpsStream){
    if (gps.encode(*gpsStream++)){
      displayInfo();}}


    previousMillis = currentMillis;
  }

}


String httpGETRequest(const char* serverName) {
  WiFiClient client;
  HTTPClient http;
```

```
  // Your Domain name with URL path or IP address with path
  http.begin(client, serverName);

  // Send HTTP POST request
  int httpResponseCode = http.GET();

  String payload = "--";

  if (httpResponseCode > 0) {
    Serial.print("HTTP Response code: ");
    Serial.println(httpResponseCode);
    payload = http.getString();
  }
  else {
    Serial.print("Error code: ");
    Serial.println(httpResponseCode);
  }
  // Free resources
  http.end();

  return payload;
}


void displayInfo() //A series of screen information about gps status in statement check
{
  Serial.print(F("Location: "));
  if (gps.location.isValid())
  {
    Serial.print(gps.location.lat(), 6);
    Serial.print(F(","));
    Serial.print(gps.location.lng(), 6);
```

```
}
else
{
  Serial.print(F("INVALID")); //A series of screen information about gps status in statement check
}

Serial.print(F("  Date/Time: "));
if (gps.date.isValid())
{
  Serial.print(gps.date.month());
  Serial.print(F("/"));
  Serial.print(gps.date.day());
  Serial.print(F("/"));
  Serial.print(gps.date.year());
}
else
{
  Serial.print(F("INVALID")); //A series of screen information about gps status in statement check
}

Serial.print(F(" "));
if (gps.time.isValid())
{
  if (gps.time.hour() < 10) Serial.print(F("0"));
  Serial.print(gps.time.hour());
  Serial.print(F(":"));
  if (gps.time.minute() < 10) Serial.print(F("0"));
  Serial.print(gps.time.minute());
  Serial.print(F(":"));
  if (gps.time.second() < 10) Serial.print(F("0"));
  Serial.print(gps.time.second());
  Serial.print(F("."));
  if (gps.time.centisecond() < 10) Serial.print(F("0"));
```

```
    Serial.print(gps.time.centisecond());
  }
  else
  {
    Serial.print(F("INVALID"));
  }

  Serial.println();
}
```