ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΗΛΕΚΤΡΙΚΗΣ ΙΣΧΥΟΣ

Μέθοδοι Αντίστροφης Ανάλυσης Συσκευών Προσομοιώσεων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Δημήτριος Α. Δήμου

Καθηγητής : Νικόλαος Κ. Ουζούνογλου
Καθηγητής ΕΜΠ

Αθήνα, Ιούνιος 2012

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΗΛΕΚΤΡΙΚΗΣ ΙΣΧΥΟΣ

Μέθοδοι Αντίστροφης Ανάλυσης Συσκευών Προσομοιώσεων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Δημήτριος Α. Δήμου

Καθηγητής : Νικόλαος Κ. Ουζούνογλου
Καθηγητής ΕΜΠ

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 18η Ιουνίου του 2012.

.....	.....	.....
Νικόλαος Κ. Ουζούνογλου	Δήμητρα-Θεοδώρα Ι. Κακλαμάνη	Γεώργιος Ματσόπουλος
Καθηγητής	Καθηγήτρια	Επίκουρος Καθηγητής

Αθήνα, Ιούνιος 2012

……

Δημήτριος Α. Δήμου

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

Copyright © Δημήτριος Δήμου, 2012

Με επιφύλαξη παντός δικαιώματος. All rights reserved.

Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας εργασίας, εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Ερωτήματα που αφορούν τη χρήση της εργασίας για κερδοσκοπικό σκοπό πρέπει να απευθύνονται προς τον συγγραφέα.

Οι απόψεις και τα συμπεράσματα που περιέχονται σε αυτό το έγγραφο εκφράζουν τον συγγραφέα και δεν πρέπει να ερμηνευθεί ότι αντιπροσωπεύουν τις επίσημες θέσεις του Εθνικού Μετσόβιου Πολυτεχνείου.

Περίληψη

Στην παρούσα διπλωματική εργασία αναπτύσσεται η τεχνική μεθοδολογία της διαδικασίας της αντίστροφης μηχανικής συσκευών και κυρίως ηλεκτρονικών συσκευών. Παρατίθεται η διαδικασία από την θεωρητική πλευρά, περιγράφοντας γενικά τους τομείς στους οποίους μπορεί να εφαρμοστεί. Η διαδικασία αυτή πέρα από την ευθεία εφαρμογή της για την αντιγραφή του υλικού, μπορεί να χρησιμοποιηθεί κατά την σχεδίαση του υλικού ως μεθοδολογία για την ασφάλιση και προστασία του. Επίσης αναπτύσσεται η ηθική και νομική πλευρά του θέματος ώστε να εξασφαλίζεται η νομιμότητα σε κάθε προσπάθεια εφαρμογής της αντίστροφης μηχανικής.

Τέλος αναπτύσσεται αναλυτικά η μεθοδολογία που μπορεί να εφαρμοστεί κατά την αντιγραφή μιας ηλεκτρονικής συσκευής όπου: γίνεται η συλλογή πληροφοριών, η αποσυναρμολόγηση του υλικού, η αντίστροφη μηχανική του μόνιμου προγράμματος του λογισμικού (όπου υπάρχει), η ανάλυση των εξωτερικών διεπαφών και η ανάλυση του υλικού σε επίπεδο στοιχείου πυριτίου.

Λέξεις κλειδιά

Αντίστροφη μηχανική , Ολοκληρωμένο κύκλωμα, Τυπωμένο κύκλωμα, Τεχνική ì αύρου κουτιού, Ψηφίδα πυριτίου, Φύλλο δεδομένων.

Abstract

The subject of the current thesis is the technical methodology of the process of reverse engineering (RE) in devices and electronic devices in particular. This process is approached from a theoretical standpoint, offering a description of the fields in which it can be applied. This process, in addition to its direct implementation for duplication of the material, can also be used during its design as a method of insurance and protection. There is also reference to the legal and moral side of the subject so as to ensure legality in every application of reverse engineering.

Finally a detailed methodology of the replication of an electronic device is provided in this thesis consisting of the following stages: gathering of information, deconstruction of the material, reverse engineering of the permanent part of the software (where available), the analysis of the external interface and the analysis of the material to an item-level silicon die.

Key Words

Reverse Engineering (RE), Integrated Circuit (IC), Printed Circuit Board (PCB), Black Box Technique, Silicon Die, Data Sheet.

Πρόλογος

Η εργασία αυτή πραγματοποιήθηκε με σκοπό την διευκόλυνση του μελετητή μηχανικού για την απόκτηση βασικών γνώσεων επάνω στην διαδικασία εφαρμογής της αντίστροφης μηχανικής σε ηλεκτρονικές συσκευές, καθώς και για να πληροφορήσει τους σχεδιαστές ηλεκτρονικών συσκευών για την εξασφάλιση των πνευματικών τους δικαιωμάτων στα προϊόντα τους όπως και την αντιμετώπιση των επιθέσεων για αντιγραφή που μπορεί να δεχθούν.

Στο σημείο αυτό θα ήθελα να ευχαριστήσω τον καθηγητή μου κ. Νικόλαο Ουζούνογλου, μετά από παρότρυνση του οποίου κινήθηκα για την ανάληψη της διπλωματικής εργασίας, την εμπιστοσύνη που μου έδειξε και τις πολύτιμες συμβουλές που μου προσέφερε, καθ' όλη τη διάρκεια της άψογης συνεργασίας μας.

Τέλος, θα ήθελα να ευχαριστήσω τους γονείς μου και τα δύο αδέλφια μου για την αγάπη, εμπιστοσύνη και υποστήριξή που μου έδειξαν καθ'όλη τη διάρκεια αυτής της διαδικασίας και της συμπαράστασης που επέδειξαν, όλα αυτά τα χρόνια, στην δύσκολη και συνεχή προσπάθεια για την επίτευξη των στόχων μου.

Η εργασία αυτή αφιερώνεται στους γονείς μου.

Περιεχόμενα

1 ΕΙΣΑΓΩΓΗ 8

2 ΔΙΑΔΙΚΑΣΙΑ ΤΕΣΣΑΡΩΝ ΣΤΑΔΙΩΝ 14

2.1 ΕΙΣΑΓΩΓΗ 14

2.2 ΔΙΑΔΙΚΑΣΙΑ ΣΤΑΔΙΩΝ 15

2.3 ΑΝΤΙΣΤΡΟΦΗ ΜΗΧΑΝΙΚΗ ΣΥΝΑΡΤΗΣΕΙ ΤΗΣ ΠΟΙΟΤΗΤΑΣ ΚΑΙ ΤΟΥ ΚΟΣΤΟΥΣ 17

2.4 ΗΘΙΚΕΣ ΚΑΙ ΝΟΜΙΚΕΣ ΠΤΥΧΕΣ 19

2.4.1 Γενικά 19

2.4.2 Νόμιμες χρήσεις αντίστροφης μηχανικής 19

2.4.3 Παράνομες δραστηριότητες αντίστροφης μηχανικής 20

3 ΜΕΘΟΔΟΙ ΔΙΑΔΙΚΑΣΙΑΣ ΑΝΤΙΣΤΡΟΦΗΣ ΜΗΧΑΝΙΚΗΣ 21

3.1 ΕΙΣΑΓΩΓΗ 21

3.2 ΜΕΘΟΔΟΛΟΓΙΑ ΔΙΑΔΙΚΑΣΙΑΣ 22

3.2.1 Γενικά 22

3.2.2 Επισκόπιση διαδικασίας-Συλλογή πληροφοριών 23

3.2.3 Αποσυναρμολόγηση του υλικού-Χαρτογράφηση κυκλωμάτων 23

3.2.4 Αντιστροφή του λογισμικού 24

3.2.5 Ανάλυση διασυνδέσεων 24

3.2.6 Ανάλυση σε επίπεδο Πυριτίου 25

4 ΑΝΟΙΓΜΑ ΤΟΥ ΥΛΙΚΟΥ ΚΑΙ ΑΝΤΙΣΤΡΟΦΗ ΜΗΧΑΝΙΚΗ 26

4.1 ΕΙΣΑΓΩΓΗ 26

4.2 ΜΗΧΑΝΙΣΜΟΙ ΠΡΟΣΤΑΣΙΑΣ ΤΟΥ ΥΛΙΚΟΥ 27

4.3 ΑΝΟΙΓΜΑ ΤΟΥ ΠΕΡΙΒΛΗΜΑΤΟΣ 27

4.4 ΑΝΤΣΤΡΟΦΗ ΜΗΧΑΝΙΚΗ ΤΟΥ ΥΛΙΚΟΥ 29

4.5 ΣΧΕΔΙΑΣΗ ΓΙΑ ΕΛΕΓΧΟ 32

4.6 ΣΗΜΕΙΑ ΕΛΕΓΧΟΥ 32

4.7 ΜΝΗΜΗ-ΠΡΟΓΡΑΜΜΑΤΙΖΟΜΕΝΗ ΛΟΓΙΚΗ 35

4.8 ΔΙΑΣΥΝΔΕΣΕΙΣ ΜΕ ΕΞΩΤΕΡΙΚΕΣ ΣΥΣΚΕΥΕΣ 37
4.9 JTAG 38
4.10 ΕΜΜΕΣΑ ΚΑΝΑΛΙΑ ΕΠΙΘΕΣΗΣ 40
4.11 ΑΝΑΛΥΣΗ ΣΤΟΙΧΕΙΟΥ ΠΥΡΙΤΙΟΥ 41
ΒΙΒΛΙΟΓΡΑΦΙΑ 48

ΚΕΦΑΛΑΙΟ 1

1 ΕΙΣΑΓΩΓΗ

Πολλά ηλεκτρονικά συστήματα περιέχουν πλακέτες τυπωμένων κυκλωμάτων (PCBs) που έχουν κατασκευαστεί από εταιρίες που δεν υπάρχουν πια και είναι αδύνατον να βρεθούν τα ηλεκτρονικά τους σχέδια. Ακόμα και αν είναι εφικτός ο σχεδιασμός του ηλεκτρονικού κυκλώματος, πολλές φορές τα PCBs περιέχουν ολοκληρωμένα κυκλώματα (ICs) και άλλα στοιχεία, τα οποία ή δεν αναγράφεται κάποιο χαρακτηριστικό τους ή αν αναγράφεται δεν μπορεί να ταυτοποιηθεί η λειτουργία τους. Στην περίπτωση βλάβης μιας τέτοιας πλακέτας δεν θα μπορεί να αντικατασταθεί με άλλη, αφού θα έχει πάψει η παραγωγή της και δεν θα υπάρχουν τα ηλεκτρονικά της σχέδια ώστε να αντικατασταθεί κάποιο απάρτιο της. Για να λυθούν τέτοιου είδους προβλήματα θα πρέπει να μελετηθεί το ήδη υπάρχον PCB και να παραχθεί ένα υποκατάστατό του ή να βρεθεί το βεβλαμένο απάρτιό του και απλά να αντικατασταθεί. Η διαδικασία αυτή επιτυγχάνεται με μία μέθοδο που ονομάζεται ‘’Αντίστροφη Μηχανική’’ (Reverse Engineering RE).

Η αντίστροφη μηχανική εφαρμόζεται σε ένα μέρος του συστήματος, προκειμένου να διακρίνει τα στοιχεία σχεδιασμού του, της κατασκευής του, και την χρήση του, συχνά με στόχο την παραγωγή ενός υποκατάστατου. Η διαδικασία αυτή υλοποιείται με την έρευνα του συστήματος, την παρατήρηση και την αποσυναρμολόγηση του. Στο κεφάλαιο αυτό θα εξηγηθεί το πλαίσιο του προβλήματος, οι στόχοι της μελέτης, η σημασία του και οι υποθέσεις και περιορισμοί που θα ληφθούν υπόψη.

Ένας ορισμός που μπορεί να δοθεί για την αντίστροφη μηχανική είναι η διαδικασία της παραγωγής γνώσης μέσω της έρευνας, της παρατήρησης και της αποσυναρμολόγησης των τμημάτων ενός συστήματος, προκειμένου να διακριθούν τα στοιχεία του σχεδιασμού του, της κατασκευής και της χρήσης του, συχνά με στόχο την παραγωγή ενός υποκατάστατό του [1].

Η αντίστροφη μηχανική έχει μεγάλο εύρος εφαρμογής. Σε οποιοδήποτε αντικείμενο ή κατασκευή, ο μηχανικός μπορεί να χρησιμοποιήσει την αντίστροφη μηχανική για να εξαγάγει τα αποτελέσματα που του χρειάζονται.

Στη μηχανολογία ο μηχανικός χρειάζεται πολλές φορές από το πραγματικό αντικείμενο ή από το πρότυπο που έχει υποστεί επεμβάσεις και αλλαγές, να μεταβεί στα ηλεκτρονικά μοντέλα του ή στα κατασκευαστικά του σχέδια. Με τον αντίστροφο μηχανολογικό σχεδιασμό επιτυγχάνεται η ταχεία και με υψηλή ακρίβεια αποτύπωση της γεωμετρίας και των διαστάσεων μιας δεδομένης υπαρκτής κατασκευής καθώς και του προσδιορισμού των διαστασιολογικών και γεωμετρικών ανοχών της. Χρησιμοποιώντας ως βασικά εργαλεία τις Μηχανές Μέτρησης Διαστάσεων και τα συναφή άλλα συστήματα, ο αντίστροφος μηχανολογικός σχεδιασμός είναι στην πραγματικότητα η δημιουργία του συνόλου των τεχνολογικών δεδομένων που περιγράφουν πλήρως γεωμετρικά ένα αντικείμενο, όταν τα δεδομένα αυτά είναι, για διάφορους λόγους, ελλειπή, ανύπαρκτα ή απλά δεν είναι διαθέσιμα.

Τυπικές περιπτώσεις όπου βρίσκει εφαρμογή ο αντίστροφος μηχανολογικός σχεδιασμός είναι ο σχεδιασμός νέων μηχανολογικών προϊόντων όπου το αρχικό φυσικό μοντέλο είναι χειροποίητο ή έχουν χρησιμοποιηθεί συμβατικά μέσα και εργαλεία. Άλλη εφαρμογή είναι η αλλαγή ή ο εκσυγχρονισμός των μεθόδων και των εργαλείων παραγωγής όταν το ίδιο προϊόν σχεδιάζεται ξανά με βάση τις προδιαγραφές και τις απαιτήσεις μιας διαφορετικής μεθόδου παραγωγής. Επίσης η τροποποίηση της κατασκευαστικής διαμόρφωσης εξαρτημάτων κατά την παραγωγή όταν κομμάτια υφίστανται αλλαγές από την αρχική τους σχεδίαση κατά την διάρκεια της παραγωγής, χωρίς να υπάρχει η δυνατότητα έγκαιρης και λεπτομερούς καταγραφής αυτών των αλλαγών. Ακόμα μια εφαρμογή είναι στην αστοχία κατά την λειτουργία στοιχείων μηχανής, όταν τα κατασκευαστικά σχέδια δεν είναι διαθέσιμα και υπάρχει η ανάγκη δημιουργίας τους προκειμένου να γίνει εκ νέου η κατασκευή του στοιχείου. Τέλος εφαρμόζεται στην φάση του ποιοτικού ελέγχου, όταν στην γραμμή παραγωγής λαμβάνεται τυχαίο δείγμα και συγκρίνεται με το ηλεκτρονικό του μοντέλο όσον αφορά την γεωμετρία, τις διαστάσεις και τις ανοχές του.

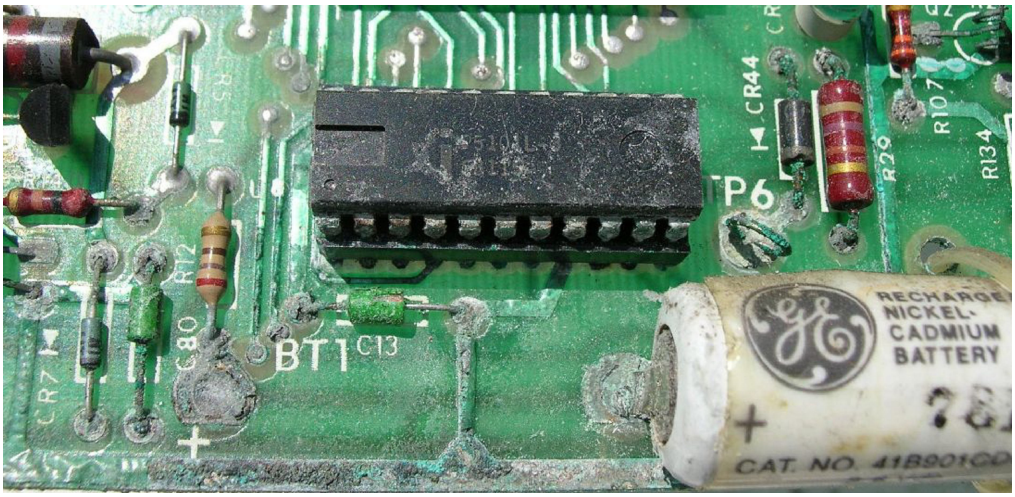
Επίσης, στην αρχαιολογία, η αντίστροφη μηχανική είναι χρήσιμη σε διάφορες περιπτώσεις. Για την δημιουργία αντιγράφων των διαφόρων ευρημάτων, χρησιμοποιούνται μέθοδοι και μέσα ώστε να γίνει πιστή αποτύπωση του πρωτοτύπου. Σε ευρήματα όπου έχει καταστραφεί τμήμα του πρωτοτύπου, με κατάλληλη διαδικασία, μπορεί να παραχθεί αντίγραφο όπως αρχικά είχε κατασκευαστεί.

Χαρακτηριστικό παράδειγμα που συνδυάζει αντίστροφη μηχανική στην αρχαιολογία και την μηχανολογία είναι η μελέτη του “Μηχανισμού των Αντικυθήρων” (εικόνα 1.1). Επιστήμονες χρησιμοποιώντας συσκευές τελευταίας τεχνολογίας κατάφεραν να σχεδιάσουν

και να κατασκευάσουν με μεγάλη ακρίβεια αντίγραφο του μηχανισμού και να αποδείξουν ότι λειτουργεί ως ένας αναλογικός υπολογιστής με σύνθετη λειτουργία ο οποίος είχε κατασκευαστεί με απίστευτη λεπτότητα και ακρίβεια, κάτι αδιανόητο για τα μέσα της εποχής που κατασκευάστηκε.

Εικόνα 1.1*Ο μηχανισμός των Αντικυθήρων*

Το κομμάτι της αντίστροφης μηχανικής που εφαρμόζεται στην ηλεκτρονική, αντιμετωπίζει προβλήματα που παρουσιάζονται εξαιτίας κάποιας βλάβης ενός απάρτιου του συστήματος λόγο φθοράς του από πολυετή χρήση ή λόγο κάποιου εξωγενούς παράγοντα, όπως η καταστροφή μιας πλακέτας λόγο της υγρασίας ή η διάβρωση της από διαρροή κάποιας μπαταρίας [2] (εικόνα 1.2).



Εικόνα 1.2 *Κατεστραμμένη πλακέτα λόγω διάβρωσης και υγρασίας*

Οι αιτίες βλάβης ενός ηλεκτρονικού κυκλώματος μπορεί να είναι ποικίλες, δεν θα γίνει όμως αναφορά σε αυτές στην συγκεκριμένη εργασία. Αυτό στο οποίο θα γίνει αναφορά στο παρόν είναι οι τρόποι επίλυσης προβλημάτων που παρουσιάζονται σε βλάβες ηλεκτρονικών συστημάτων. Η εύκολη και κλασική λύση που μπορεί να δοθεί σε ένα τέτοιο πρόβλημα είναι

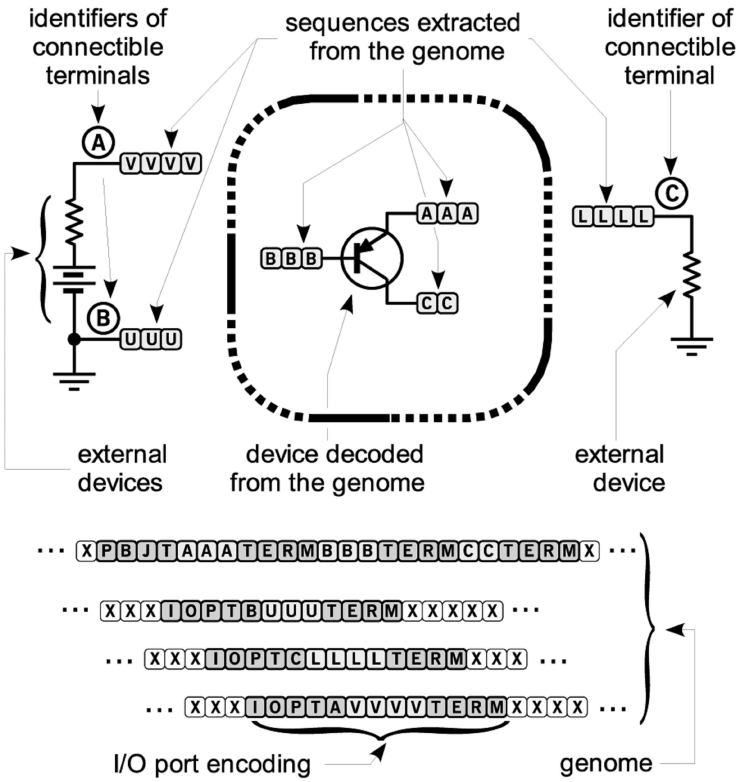
ή να δοθεί η συσκευή για συντήρηση στο εξουσιοδοτημένο, από τον αντιπρόσωπο, συνεργείο ή εάν δεν υπάρχει αυτό, να γίνει η αντικατάσταση και επισκευή της βλάβης από ηλεκτρονικό, ο οποίος θα έχει προμηθευτεί το απάρτιο του συστήματος που είχε την βλάβη, μέσο του αντιπροσώπου, έχοντας τους αριθμούς ονομαστικού και μερίδας του ανταλλακτικού. Υπάρχουν όμως και περιπτώσεις όπου η κατασκευάστρια εταιρία έχει πάψει πλέον να λειτουργεί και η συντήρηση της συσκευής να μην είναι εφικτό να υποστηριχτεί από εξουσιοδοτημένο τεχνικό. Σε αυτές τις περιπτώσεις και με την προϋπόθεση ότι δεν είναι εύκολη η αντικατάσταση της συσκευής, θα πρέπει να πραγματοποιηθεί η επισκευή της από κάποιον ηλεκτρονικό. Όταν όμως δεν είναι γνωστό που ακριβώς είναι η βλάβη και η συσκευή αποτελείται από πολλά πολύπλοκα ηλεκτρονικά κυκλώματα είναι αδύνατο να βρούμε το βεβλαμένο απάρτιο με μια ματιά. Ακόμα και αν είναι εμφανές το στοιχείο που παρουσιάζει την βλάβη είναι πολύ πιθανό να μην αναγράφεται κάποιο χαρακτηριστικό του, με αποτέλεσμα να μην είναι δυνατό να βρεθεί το αντίστοιχο ανταλλακτικό στην αγορά ή ακόμα και να μην είναι πλέον διαθέσιμο. Άρα θα πρέπει με κάποιο τρόπο το στοιχείο αυτό να κατασκευαστεί από την αρχή. Σε αυτές τις περιπτώσεις χρησιμοποιούμε την μέθοδο της αντίστροφης μηχανικής ώστε να επιλυθούν τέτοιου είδους προβλήματα.

Ένα εύλογο ερώτημα που θα μπορούσε να διατυπωθεί είναι γιατί να μην αγοραστεί μια καινούργια συσκευή με την ίδια λειτουργία για την επίλυση του προβλήματος; Η απάντηση μπορεί εύκολα να δοθεί αν αναλογιστεί κανείς πόσο περισσότερο δαπανηρό είναι να αγοραστεί μια ολόκληρη συσκευή από το να κατασκευαστεί απλά ένα απάρτιο ή ακόμα και ένα μόνο στοιχείο του συστήματος. Επίσης, η συγκεκριμένη συσκευή ενδέχεται να είναι μέρος ενός μεγαλύτερου συστήματος, αποτελούμενο από περισσότερες συσκευές και η αντικατάσταση της να μην είναι συμβατή στη λειτουργία του όλου συστήματος.

Επίσης στον χώρο της πληροφορικής, οι μηχανικοί ηλεκτρονικών υπολογιστών χρησιμοποιούν την αντίστροφη μηχανική σε προγραμματισμένα ηλεκτρονικά κυκλώματα, ώστε να πετύχουν τροποποίηση του κώδικα η και αλλαγή του γιατί οι συνθήκες το επιβάλουν. Στον συγκεκριμένο χώρο η χρήση της αντίστροφης μηχανικής πρέπει να είναι πολύ προσεκτική ώστε να μην παραβιάζονται τα δικαιώματα του σχεδιαστή του κώδικα.

Μια ποιο πρωτοποριακή εφαρμογή της αντίστροφης μηχανικής είναι στον χώρο της γενετικής [3]. Για την αποκωδικοποίηση των γονιδιωμάτων, εφαρμόζεται μια μέθοδος αντιστοίχησης τους με αναλογικά ηλεκτρονικά κυκλώματα και νευρωνικά δίκτυα. Έτσι όπως ένα ηλεκτρικό κύκλωμα αποτυπώνεται σε ηλεκτρονικό σχέδιο και μελετάται ανάλογα με την

βοήθεια της αντίστροφης μηχανικής, έτσι και το γονιδίωμα αποτυπώνεται σε σχέδιο για περαιτέρω μελέτη των επιμέρους γονιδίων, με τον ίδιο τρόπο (εικόνα 1.3).



Εικόνα 1.3 *Αντιστοίχηση γονιδιώματος με ηλεκτρονικά στοιχεία*

Σχετικά με την ηθική πλευρά του θέματος, η συνεχώς αυξανόμενη αίσθηση περιβαλλοντολογικής συνείδησης αναγνωρίζει "τα απόβλητα υψηλής τεχνολογίας" ως ένα παγκόσμιο πρόβλημα. Πλέον, η πολιτική των εταιρειών στον σχεδιασμό των προϊόντων, κατευθύνεται στην ελαχιστοποίηση των μελλοντικών αποβλήτων. Στην ίδια πολιτική θα πρέπει να προστεθεί και η παροχή κινήτρων για την χρηματοδότηση της έρευνας, ώστε να διατηρηθούν κατηγορίες προϊόντων, που μέχρι σήμερα δεν κρινόταν αναγκαίο λόγο της δαπανηρής επιδιόρθωσής τους. Η περιβαλλοντολογική πολιτική που ασκείται πλέον παντού, έχει σαν αρχή της την οικονομία στην κατανάλωση πόρων. Με την χρήση της αντίστροφης μηχανικής στην επιδιόρθωση βεβλαμένων συσκευών επιτυγχάνεται η μείωση αποβλήτων που προέρχονται από της συσκευές και πολλές φορές μπορεί να είναι αρκετά βλαβερά για το περιβάλλον. Επίσης με την επιδιόρθωση των συσκευών επιτυγχάνεται εξοικονόμηση χρημάτων, μιας και η επισκευή μιας συσκευής είναι οικονομικότερη από την αγορά της και πολλές φορές βλάβη ενός υποσυστήματος μπορεί να προκαλέσει την αντικατάσταση ολόκληρου του συστήματος λόγω έλλειψης συμβατότητας. Όμως η λύση της αντίστροφης μηχανικής, συμπεριλαμβανομένων και των μεθόδων και μέσων που χρειάζονται για να

παραχθεί αυτή, δεν πρέπει παρανόμως να παραβιάζει αναγνωρισμένα πνευματικά δικαιώματα υλικών και ευρεσιτεχνιών, καθώς επίσης και οποιαδήποτε παραβίαση νομοθεσιών που διέπουν την αντίστροφη μηχανική.

Περαιτέρω πρακτική σπουδαιότητα θα μπορεί να παραχθεί, όταν η μέθοδος αυτή εδραιωθεί στους τομείς που εφαρμόζεται και να επεκταθεί με επιτυχία και σε άλλες κατηγορίες, πάντα ακλουθώντας αυστηρούς κανόνες. Έτσι η αντίστροφη μηχανική μπορεί να χρησιμεύσει ως μια εκπαιδευτική μέθοδος σε ακαδημαϊκό επίπεδο, καθώς και ένα πρακτικό εργαλείο στα χέρια των μηχανικών.

ΚΕΦΑΛΑΙΟ 2

2 ΔΙΑΔΙΚΑΣΙΑ ΤΕΣΣΑΡΩΝ ΣΤΑΔΙΩΝ

2.1 Εισαγωγή

Μια πρωτοποριακή εργασία από την Kathryn Ingle που εκδόθηκε στο βιβλίο της με τίτλο Reverse Engineering το 1994, περιγράφει στην γενικότερη μορφή της την αντίστροφη μηχανική, μια διαδικασία που ακολουθείται από τέσσερεις φάσεις [1]. Το επιθυμητό αποτέλεσμα απορρέει μέσω των σταδίων της αξιολόγησης και επαλήθευσης, δημιουργίας τεχνικών δεδομένων, επαλήθευση των τεχνικών δεδομένων και τέλος της εφαρμογής των αποτελεσμάτων.

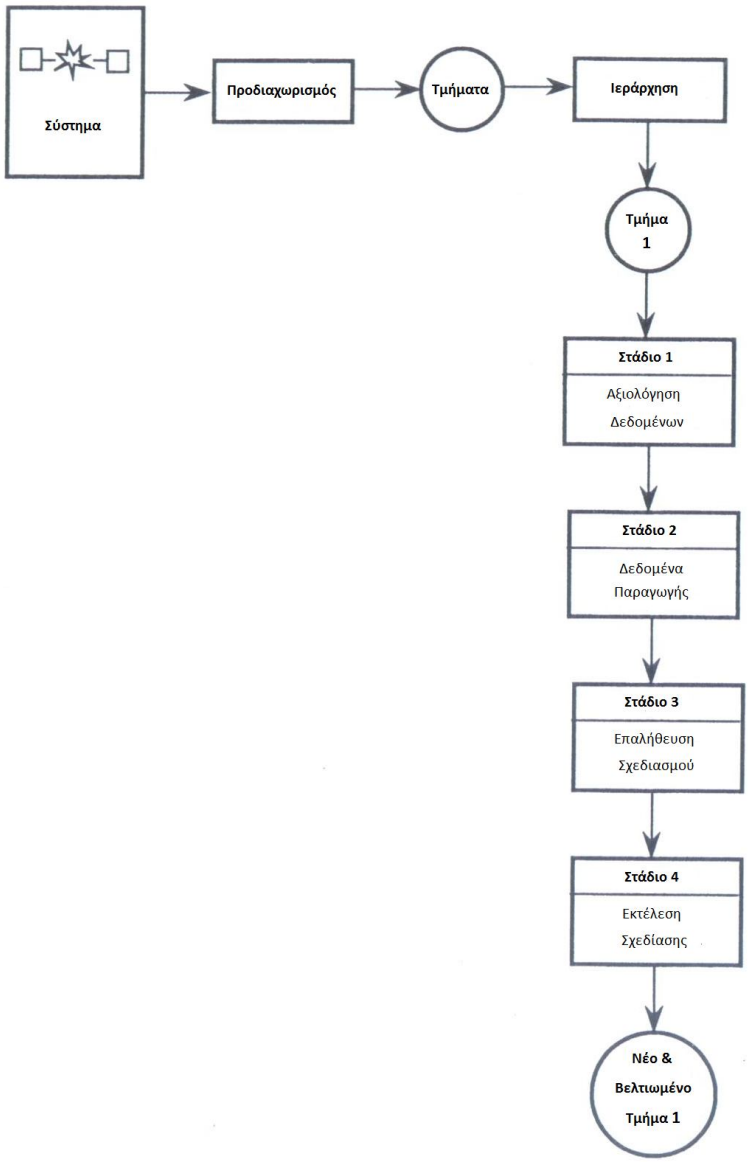
Ο όρος Reverse Engineering εμφανίζεται για πρώτη φορά περίπου το 1985, σε επίσημο δημόσιο έγγραφο της κυβέρνησης των Ηνωμένων Πολιτειών, στο αμυντικό ομοσπονδιακό τμήμα ρύθμισης εξαγορών (217.7202).

Η αντίστροφη μηχανική βασίζεται στην τεχνική του μαύρου κουτιού (Black Box Technique) μια τεχνική που εφαρμόζει μια επαναληπτική μέθοδο. Αξιοποιεί τα δεδομένα για να αναλύσει το στοιχείο που ερευνάται όσον αφορά μια διαδικασία ελέγχου, με ένα μοντέλο κλειστού βρόχου. Με αυτή την τεχνική αντιμετωπίζεται το στοιχείο σαν ένα μαύρο κουτί και αδιαφορώντας για το περιεχόμενο του, διεγείρονται εξωτερικά οι είσοδοι του ώστε να ληφθούν αντίστοιχα δεδομένα από τις εξόδους του. Επαναλαμβάνοντας την ίδια διαδικασία μπορείς να συλλέξεις τα αποτελέσματα που θα σε βοηθήσουν να περιγράψεις την λειτουργία του στοιχείου και να σχεδιάσεις την εσωτερική του διάταξη. Ακλουθώντας αυτή την διαδικασία γίνεται κατ' ουσία η ανάπτυξη τεχνικών δεδομένων, απαραίτητων για να υποστηρίξουν ένα υπάρχον στοιχείο του συστήματος, για μελλοντική χρήση, όπως εφαρμόζεται στο σύστημα αυτό. Τα τεχνικά δεδομένα είναι κρίσιμα για την ομαλή και συνεχή λειτουργία, για κάθε σύστημα ή παραγωγική εγκατάσταση. Έτσι ο σκοπός της αντίστροφης μηχανικής είναι να αυξήσει την παραγωγικότητα με την επίλυση κατασκευαστικών και λειτουργικών προβλημάτων.

2.2 Διαδικασία σταδίων

Η αντίστροφη μηχανική είναι μια διαδικασία τεσσάρων σταδίων (σχήμα 2.1) που επιφέρουν την εξαγωγή των τεχνικών δεδομένων για την υποστήριξη της αποτελεσματικής χρήσης των κεφαλαιακών πόρων και την αύξηση της παραγωγικότητας. Τα στάδια αυτά είναι:

- Στάδιο 1: Αξιολόγηση των δεδομένων
- Στάδιο 2: Δεδομένα παραγωγής
- Στάδιο 3: Επαλήθευση του σχεδιασμού
- Στάδιο 4: Εκτέλεση της σχεδίασης



Σχήμα 2.1 *Επισκόπηση των διαδικασιών της αντίστροφης μηχανικής*

Όλα τα στάδια διεξάγονται με αυστηρό προδιαχωρισμό μεταξύ τους για τα πιθανά προς μελέτη υποψήφια στοιχεία. Αυτή η διαδικασία τυπικά απευθύνεται στη βελτίωση της γραμμής παραγωγής και των βιομηχανικών δυνατοτήτων. Ιδανικά, η ομαδοποίηση των τμημάτων του συστήματος ή του υποσυστήματος παρέχουν το φάσμα των προς αντίστροφη μηχανική υποψηφίων.

Παραδοσιακή διαδικασία σχεδίασης	**Διαδικασία σχεδίασης αντίστροφης μηχανικής**
Ανάγκη ↓ Σχεδιαστική ιδέα ↓ Πρωτότυπο και δοκιμή ↓ Προϊόν	Προϊόν ↓ Αποσυναρμολόγηση ↓ Μετρήσεις και δοκιμή ↓ Ανάκτηση σχεδιασμού ↓ Πρωτότυπο και δοκιμή ↓ Προϊόν αντίστροφης μηχανικής

Σχήμα 2.2 *Παραδοσιακή διαδικασία σχεδίασης έναντι διαδικασία αντίστροφης μηχανικής*

Ο ακριβής σχεδιασμός των δεδομένων για την μακροπρόθεσμη συντήρηση και υποστήριξη μιας τεχνικής δυνατότητας, είναι ο ακρογωνιαίος λίθος της αντίστροφης μηχανικής. Αυτή η διαδικασία παρέχει ένα επίπεδο τεχνικής υποστήριξης. Όποτε η αντίστροφη μηχανική απαιτεί την επένδυση κεφαλαίων τα σχέδια της οποίας θα πρέπει εύκολα να προδιαχωρίζονται για να εξασφαλίσουν μεγάλη πιθανότητα επιτυχίας. Εκείνα τα

σχέδια τα οποία δεν πληρούν κριτήρια προδιαχωρισμού τυπικά, δεν εξετάζονται. Αυτό γίνεται επειδή η επιτυχία στην αντίστροφη μηχανική μετριέται κατά κύριο λόγο από την απόδοση των επενδύσεων. Επίσης η επιτυχία της μετριέται και από την συνολική αποτελεσματικότητα των μακροπρόθεσμων και βραχυπρόθεσμων στόχων. Το σχήμα 2.2 απεικονίζει τις διαφορές μεταξύ της παραδοσιακής διαδικασίας σχεδίασης και της διαδικασίας της αντίστροφης μηχανικής.

Η απευθείας μηχανική είναι η παραδοσιακή διαδικασία της μετάβασης από τις υψηλού επιπέδου έννοιες και αφηρημένες λογικές στην υλοποίηση τους. Όταν όμως η εφαρμογή ανεξάρτητης σχεδίασης είναι αναγκαία σε ένα φυσικό σύστημα , τότε με την αντίστροφη μηχανική θα γίνει η ανάλυση σχεδίασης των εξαρτημάτων του συστήματος και η αλληλεξάρτησή τους με το υψηλότερου επιπέδου διακριτό σύστημα.

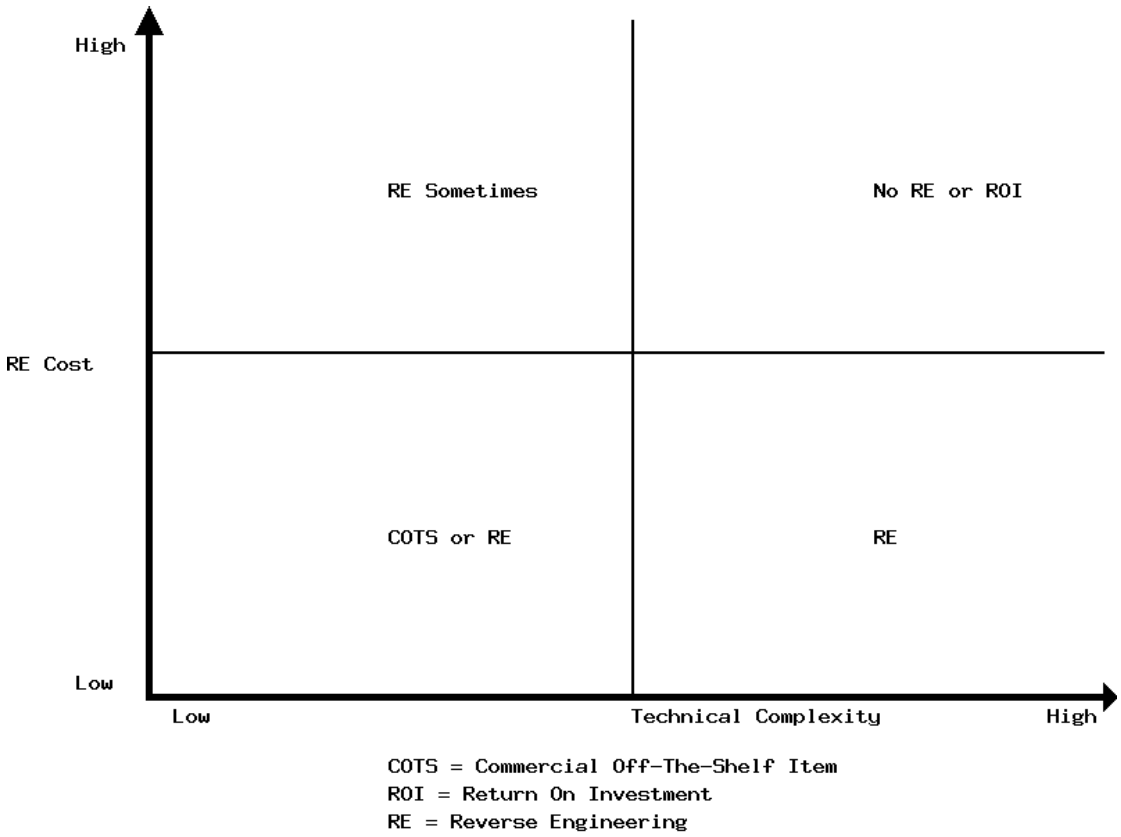
2.3 Αντίστροφη μηχανική συναρτήσει της ποιότητας και του κόστους

Η ποιότητα στην κατασκευή επιτυγχάνεται με προσοχή στη λεπτομέρεια σε κάθε βήμα του σχεδιασμού, στην προπαραγωγή, την παραγωγή και μεταπαραγωγή, περιλαμβανομένων των βελτιώσεις του προϊόντος. Επειδή η ποιότητα στην διαδικασία της αντίστροφης μηχανικής επιτυγχάνεται με τη χρησιμοποίηση κάθε εργαζόμενου, από χειριστές μηχανημάτων μέχρι στελέχη της εταιρείας σε υψηλές θέσεις. Όλοι οι εργαζόμενοι μπορούν να προσφέρουν στην ποιότητα μέσω της επάρκειας στους αντίστοιχους ρόλους σε αυτή την διαδικασία.

Όταν η αντίστροφη μηχανική οδηγείται από την οικονομία, ο κοινός στόχος της εφαρμογής της είναι η εξοικονόμηση του 25% του κόστους του προϊόντος της εμπορικής του αξίας και η απόδοση της επένδυσης 25:1. Το κόστος και οι κίνδυνοι ενός έργου σχετίζονται θετικά στην πολυπλοκότητα του συστήματος. Αυτή η σχέση έχει καταγραφεί σε ένα Go/No-Go διάγραμμα απόφασης (σχήμα 2.3) το οποίο παρουσιάζει τις σχέσεις μεταξύ τεχνικής πολυπλοκότητας, κόστους αντίστροφης μηχανικής. Η σχέση αυτή συνδέεται με τον κίνδυνο και την απόφαση για χρήση ή όχι της αντίστροφης μηχανικής και συνοψίζονται ως εξής:

Περισσότερα στοιχεία, μικρότερος κίνδυνος και χαμηλότερο κόστος είναι μια καλή ένδειξη για χρήση της αντίστροφης μηχανικής. Όταν τα τεχνικά στοιχεία του προϊόντος φαίνονται πλήρη αλλά υπάρχει κάποια αμφιβολία ως προς την χρησιμότητα του τότε δεν μπορεί να ελεγχθεί το προϊόν για αντίστροφη μηχανική. Αν υπάρχουν κάποια τεχνικά

στοιχεία που είναι διαθέσιμα τότε το έργο απαιτεί την ενίσχυση των δεδομένων. Ενίσχυση δεδομένων γίνεται κάθε φορά που υπάρχει έλλειψη οποιασδήποτε ποσότητας δεδομένων. Εάν δεν υπάρχουν διαθέσιμα τεχνικά στοιχεία, τότε το έργο απαιτεί την πλήρη ανάπτυξη των δεδομένων [1].



Σχήμα 2.3 *Go/No-Go διάγραμμα απόφασης*

Η διαθεσιμότητα δεδομένων καθορίζει τον τύπο του έργου, που κυμαίνονται στην επαλήθευση των προϊόντων από την βελτίωση δεδομένων ως την ανάπτυξη δεδομένων. Το κόστος και οι κίνδυνοι τείνουν να κλιμακωθούν αρκετά όταν τα δεδομένα πρέπει να αναπτυχθούν με αντίστροφη μηχανική γιατί συχνά απαιτούν εργασία και συσκευές που κοστίζουν αρκετά. Είναι επίσης δυνατό να υπάρχουν έργα με υψηλό κόστος και χαμηλή πολυπλοκότητα, δηλαδή, να λαμβάνονται άλλοι παράγοντες εκτός από την πολυπλοκότητα για το υψηλό κόστος. Η ανάπτυξη των δεδομένων μπορεί να γίνει ένας εφιάλτης όταν η σύνθεση των υλικών δεν είναι εύκολο να προσδιοριστεί, θα πρέπει να γίνει μάντεμα των ανοχών , ή το στοιχείο μπορεί να παράξει μια δυσάρεστη έκπληξη με την ενδεχόμενη ύπαρξη μιας εσωτερικής κοιλότητας γεμάτη με άγνωστο λιπαντικό ή μια κάρτα κυκλώματος που μπορεί να έχει τρία επιπλέον στρώματα που δεν είχαν αναφέρθηκαν προηγουμένως.

Επίσης, τα έργα που σχετίζονται με το υλικό και το λογισμικό συχνά παρουσιάζουν μέτρια έως υψηλή πολυπλοκότητα που οφείλεται σε όλες τις λεπτομέρειες που μπορεί να κρύβονται στα ηλεκτρονικά κυκλώματα. Θα πρέπει να είναι προφανές ότι τα δεδομένα της ανάπτυξης συνεπάγονται το υψηλότερο κόστος και κίνδυνο. Ωστόσο, μπορεί να υπάρχουν σημαντικοί παράγοντες που μπορεί να αναγκάσει την "πάση θυσία" διακοπή της εργασίας. Σύνηθες φαινόμενο είναι η απαξίωση και η έλλειψη παροχής υποστήριξης σε συστήματα που ωστόσο θεωρούνται κρίσιμα.

2.4 Ηθικές και Νομικές Πτυχές

2.4.1 Γενικά

Βασικά, η νομιμότητα της αντίστροφης μηχανικής διέπεται από νόμους περί πνευματικής ιδιοκτησίας. Οι νόμοι περί πνευματικής ιδιοκτησίας δεν είναι ίδιοι παντού, αλλά διαφέρουν από χώρα σε χώρα. Η διαδικασία της αντίστροφης μηχανικής είναι νόμιμη μόνο σε λίγες ειδικές περιπτώσεις οι οποίες θα πρέπει να είναι ξεκάθαρο πως δεν περιέχουν κάποια παράνομη διαδικασία. Θα πρέπει να γίνει ξεκάθαρο πως η διαδικασία δοκιμής και ελέγχου "Μαύρου Κουτιού" δεν αποτελεί διαδικασία αντίστροφης μηχανικής. Επίσης η εφαρμογή αντίστροφης μηχανικής για επιδιορθώσεις συμβατότητας σε ένα υλικό είναι ξεκάθαρα νόμιμη. Αντίθετα, ξεκάθαρα παράνομη διαδικασία είναι η εφαρμογή αντίστροφης μηχανικής για οποιαδήποτε μορφή υποκλοπής του υλικού ή τμήματός του, στις περισσότερες χώρες. Όταν για ένα μηχανικό υπάρχει αμφιβολία για την εργασία που εκτελεί αν είναι νόμιμη ή παράνομη δεν θα πρέπει να την εκτελέσει μέχρι να εξακριβωθεί η νομιμότητα της [4].

2.4.2 Νόμιμες χρήσεις αντίστροφης μηχανικής

- Ανάκτηση του δικού μας πηγαίου κώδικα μιας συσκευής.
- Ανάκτηση αποθηκευμένων δεδομένων λόγω format.
- Ανάλυση και έρευνα για κακόβουλο λογισμικό.
- Ασφάλεια και ευπάθεια έρευνας.
- Έρευνα παραβίασης πνευματικών δικαιωμάτων.
- Ανακαλύπτοντας αλλού το περιεχόμενο της βάσης δεδομένων που έχετε τα δικαιώματα να το πωλείται νόμιμα.
- Ανάλυση για συμβατότητα υλικού.

- Σε περιπτώσεις διακοπής παροχής υποστήριξης και παραγωγής του προϊόντος από τον κατασκευαστή του και μετά από την παροχή της κατάλληλης άδειας από τον ίδιο ή όποιον κατέχει τα δικαιώματα του προϊόντος εφόσον υπάρχει.
- Γενικά μετά από την παροχή άδειας από τον ιδιοκτήτη των πνευματικών δικαιωμάτων του προϊόντος.

2.4.3 Παράνομες δραστηριότητες αντίστροφης μηχανικής

- Παράνομη αντιγραφή και πώληση ενός ανταγωνιστικού προϊόντος.
- Παράνομο "σπάσιμο" της προστασίας αντιγραφής ενός προϊόντος.
- Παράνομη διανομή "σπασμένου" πιστοποιητικού εγγραφής πνευματικών δικαιωμάτων λογισμικού.
- Παράνομη απόκτηση μη εξουσιοδοτημένης πρόσβασης σε οποιοδήποτε ηλεκτρονικό σύστημα.
- Τα προστατευμένα πνευματικά δικαιώματα λογισμικού στις περισσότερες περιπτώσεις είναι εκτός ορίων.
- Κακόβουλο λογισμικό (Spyware) ή λογισμικό εγκατάστασης αυτόματων διαφημίσεων (Adware) με τις εταιρίες που βρίσκονται πίσω από αυτές.

ΚΕΦΑΛΑΙΟ 3

3 ΜΕΘΟΔΟΙ ΔΙΑΔΙΚΑΣΙΑΣ ΑΝΤΙΣΤΡΟΦΗΣ ΜΗΧΑΝΙΚΗΣ

3.1 Εισαγωγή

Η ραγδαία ανάπτυξη της τεχνολογίας έχει μπει στην ζωή μας σε τέτοιο βαθμό που εξαρτόμαστε από αυτή και φτάνει στο σημείο να μας ελέγχει. Τα ηλεκτρονικά συστήματα έχουν ενσωματωθεί σχεδόν σε όλες τις συσκευές που χρησιμοποιεί ο άνθρωπος σε καθημερινή βάση. Η χρήση των συστημάτων αυτών προϋποθέτει ιδιαίτερη εξειδίκευση τόσο στην σχεδίαση και την λειτουργία τους όσο και στην συντήρηση και επισκευή τους. Τα ηλεκτρονικά συστήματα τα οποία περιέχουν οποιοδήποτε είδος επεξεργαστή και μνήμη αποτελούνται από το hardware και το software. Το hardware είναι ουσιαστικά τα ηλεκτρονικά στοιχεία, τα κυκλώματα, οι πλακέτες, τα μέσα αποθήκευσης πληροφορίας και τα μέσα διασύνδεσης, δηλαδή γενικά τα υλικά από τα οποία είναι κατασκευασμένο το ηλεκτρονικό σύστημα. Το software είναι το λογισμικό δηλαδή ο κώδικας του προγράμματος που έχει χρησιμοποιηθεί ώστε να λειτουργήσει το υλικό. Η ύπαρξη του software δεν είναι πάντα αναγκαία, αλλά εξαρτάται από την κατασκευή και την χρήση του ίδιου του ηλεκτρονικού συστήματος [5].

Το hardware δεν είναι κάτι το ασύλληπτο που δεν μπορούμε να το αντιληφθούμε. Συνήθως όμως οι άνθρωποι το αντιμετωπίζουν με αυτόν τον τρόπο. Εφόσον κάποιος άνθρωπος έχει κάνει την σχεδίαση του συστήματος είναι εφικτό να την κατανοήσουμε. Το πρόβλημα όμως, που μπορεί να παρουσιαστεί είναι κατά πόσο ασφαλισμένο από τον σχεδιαστή του είναι αυτό το σύστημα, τόσο για την κατανόηση της σχεδίασης του όσο και για την λειτουργία του. Το υλικό, σε μεγάλο βαθμό έχει αγνοηθεί στο πεδίο της ασφάλειας. Πολλά προϊόντα είναι ευπαθή στο να εκτίθενται σε απλές και πρακτικές τακτικές επίθεσης. Οι επιθέσεις αυτές έχουν σαν σκοπό την αντιγραφή του ηλεκτρονικού συστήματος για διάφορους λόγους.

Πώς όμως το υλικό είναι δυνατόν να αντιγραφεί;

Ποιοι είναι οι στόχοι μιας επίθεσης; Ένας λόγος που γίνονται επιθέσεις για αντιγραφή είναι η απόκτηση μιας υπηρεσίας δωρεάν, που κανονικά θα κόστιζε πολλά χρήματα. Επίσης ο ανταγωνισμός μεταξύ κατασκευαστών είναι αιτία επίθεσης ώστε να παραχθεί κλώνος

κάποιου προϊόντος. Έτσι παρατηρούνται ειδικές αντιγραφές πληροφοριών και δεδομένων ώστε τελικά να κερδηθεί από κάποιους, το πλεονέκτημα στην αγορά. Στόχος επίθεσης γίνεται και ο τρόπος πρόσβασης στο σύστημα στο οποίο αναζητούνται αυτές οι πληροφορίες και τα δεδομένα. Έτσι με την αντιγραφή της ταυτότητας κάποιου χρήστη ή την παράκαμψη των χαρακτηριστικών ασφαλείας του συστήματος επιτυγχάνεται η πρόσβαση σε ένα σύστημα ή ακόμα αποκτάται και ο αυξημένος έλεγχος του.

Τα περισσότερα ηλεκτρονικά προϊόντα είναι σχεδιασμένα από τους μηχανικούς χωρίς να εξασφαλίζεται η ασφάλεια τους. Πολλά από τα προϊόντα αυτά σχεδιάζονται και παράγονται από τους κατασκευαστές τους βασιζόμενα σε διαθέσιμα σχεδιαστικά πρότυπα και αρχές, οι οποίες είναι κοινές για όλους, έτσι ώστε να επιτυγχάνεται συμβατότητα στη λειτουργία τους με άλλα προϊόντα. Οι σχεδιαστικές αρχές με τις οποίες σχεδιάζονται τα εξαρτήματα, τα οποία θα χρησιμοποιηθούν ως απάρτια μεγαλύτερων συγκροτημάτων είναι η ευκολία στην πρόσβαση, στον εντοπισμό και την διασύνδεση τους. Η εύκολη πρόσβαση στο προϊόν επιτρέπει στους μηχανικούς να ελέγχουν και να εντοπίζουν τυχόν σφάλματα που μπορεί να εμφανιστούν.

3.2 Μεθοδολογία διαδικασίας

3.2.1 Γενικά

Η μεθοδολογία που ακολουθείται για την επίτευξη της αντιγραφής του υλικού στο επίπεδο των πιο σημαντικών υποσυστημάτων μιας ηλεκτρονικής συσκευής είναι η εξής:

- Επισκόπηση διαδικασίας- Συλλογή πληροφοριών
- Αποσυναρμολόγηση του υλικού-Αντιστροφή κυκλωμάτων
- Αντίστροφη μηχανική του μόνιμου προγράμματος του λογισμικού (όπου υπάρχει)
- Ανάλυση των εξωτερικών διεπαφών
- Ανάλυση του υλικού σε επίπεδο στοιχείου πυριτίου
- Εργαστηριακός έλεγχος

Για την επίτευξη του αντικειμενικού σκοπού, που είναι η επιτυχείς αντιγραφή του υλικού, βασική προϋπόθεση είναι η συλλογή αξιόπιστων πληροφοριών. Με

αποφασιστικότητα και επιμονή, που είναι το κλειδί της επιτυχίας, θα πρέπει να συνεχιστεί η εργασία μέχρι την ολοκλήρωσή της. Ακόμα και όταν η μέθοδος που ακολουθείται δεν βγάζει αποτέλεσμα θα πρέπει να συνεχίζεται η προσπάθεια ακλουθώντας εναλλακτικές λύσεις. Η αποτυχία στο επίπεδο αντιγραφής του υλικού δημιουργεί αίσθημα απογοήτευσης, όμως ακόμα και σε αυτή την περίπτωση το όφελος είναι εκπαιδευτικό. Γι'αυτό δεν πρέπει ποτέ να τα παρατήσει κάποιος αν πρώτα δεν εξαντλήσει κάθε περίπτωση εξεύρεσης λύσης.

3.2.2 Επισκόπηση διαδικασίας-Συλλογή πληροφοριών

Αρχικά γίνεται μια έρευνα στο διαδίκτυο για την εξαγωγή συγκεκριμένων πληροφοριών, τόσο για το προϊόν όσο και για τον κατασκευαστή του. Πληροφορίες που συλλέγονται είναι οι προδιαγραφές του προϊόντος, έντυπα σχεδίασης, οδηγίες λειτουργίας, οδηγίες διασύνδεσής του με άλλα υλικά καθώς και πληροφορίες για τον κατασκευαστή και τους τρόπους προώθησης των προϊόντων του. Η έρευνα για τν συλλογή αυτών των πληροφοριών γίνεται σε διάφορα forums, blogs, στο Google, Twitter, Facebook κλπ.

Μετά την συλλογή των πληροφοριών, εφόσον το υλικό δεν βρίσκεται στην κατοχή μας ή αν βρίσκεται είναι καταστραμμένο και δεν μπορούμε να το μελετήσουμε τότε θα πρέπει να το αποκτήσουμε. Η απόκτηση του γίνεται με πολλούς τρόπους. Το υλικό μπορεί να αγοραστεί από καταστήματα και δικτυακούς τόπους πώλησης όπως το eBay. Μπορεί να δανειστεί ή να ενοικιαστεί από προμηθευτές, ερευνητικά εργαστήρια ή χώρους μελετών, εφόσον υπάρχει. Ακόμα μπορεί και να ζητηθεί από τον ίδιο τον κατασκευαστή στην περίπτωση που το προϊόν έχει πάψει να πωλείτε και να υποστηρίζεται αλλά ο κατασκευαστής έχει ακόμα ποσότητες από αυτό. Γενικά το προς μελέτη υλικό θα πρέπει να βρίσκεται στα χέρια μας όσον το δυνατό σε καλύτερη κατάσταση ώστε να πάρουμε και τα καλύτερα αποτελέσματα.

3.2.3 Αποσυναρμολόγηση του υλικού-Χαρτογράφηση κυκλωμάτων

Στη συνέχεια, αφού έχουμε εξασφαλίσει στην κατοχή μας το υλικό θα πρέπει να ξεκινήσει η διαδικασία αποσυναρμολόγησής του. Η αποσυναρμολόγηση θα γίνει σε στάδια έτσι ώστε να εξάγονται από κάθε επίπεδο οι αντίστοιχες πληροφορίες στο υλικό και τα ηλεκτρονικά συστήματα. Αρχικά θα ανοιχτεί το υλικό μέχρι να αποκτήσουμε πρόσβαση στο ηλεκτρονικό κύκλωμα. Αφού γίνει η ταυτοποίηση των στοιχείων και η αναγνώριση των υποσυστημάτων θα ακολουθήσει η ανάλυση τους έως την μικρότερη δομική μονάδα του υλικού. Τέλος θα γίνει η σχεδίαση όλου του συστήματος του υλικού με κάθε λεπτομέρεια.

Γενικά με την αποσυναρμολόγηση του υλικού εξάγονται πληροφορίες σχετικά με την τεχνικές σχεδίασης του, τους τρόπους και τα σημεία στα οποία μπορεί να δεχθεί επίθεση και την λειτουργικότητα του συστήματος. Τυπικά υπάρχουν ομοιότητες μεταξύ παλαιότερων και νεότερων σχεδιασμών, ακόμα και μεταξύ ανταγωνιστικών προϊόντων, έτσι μπορούμε να βγάλουμε πολλά συμπεράσματα κατά την αποσυναρμολόγηση του υλικού.

3.2.4 Αντιστροφή του λογισμικού

Έχοντας ταυτοποιήσει όλα τα δομικά στοιχεία των κυκλωματικών διατάξεων μπορούμε να αναγνωρίσουμε ποια από αυτά είναι στοιχεία μνήμης (εάν υπάρχουν). Τα στοιχεία μνήμης περιέχουν κώδικα ή δεδομένα κάποιου προγράμματος που είναι απαραίτητα για την λειτουργία της συσκευής. Τέτοια στοιχεία μνήμης μπορεί να είναι μνήμες Flash, ROM, RAM, EEPROM ή FPGA. Σκοπός μας πλέον είναι να εξαγάγουμε και να διαβάσουμε αυτό το πρόγραμμα. Για να επιτευχθεί κάτι τέτοιο θα χρησιμοποιήσουμε μια off-the-self συσκευή προγραμματισμού ή κάποιο ειδικό εργαλείο το οποίο βρίσκεται στην ίδια την συσκευή μας. Χρησιμοποιώντας αυτά τα μέσα θα καταλήξουμε να έχουμε το δυαδικό ή εξαδικό αποτύπωμα του κώδικα του προγράμματος. Σε αυτό το κομμάτι της αντιγραφής, στην διαδικασία υπεισέρχονται καθαροί αντιγραφείς λογισμικού, ώστε χρησιμοποιώντας τα εργαλεία και τις τεχνικές στα οποία είναι ήδη εξοικειωμένοι θα μπορέσουν να επεξεργαστούν τα δεδομένα. Γενικά τα ηλεκτρονικά ή ενσωματωμένα συστήματα που περιέχονται στην συσκευή για αντιστροφή δεν είναι τίποτα περισσότερο από προγραμματιζόμενους υπολογιστές, γενικής χρήσεως για την εκτέλεση μιας συγκεκριμένης εργασίας. Πραγματοποιώντας ένα γρήγορο τρέξιμο διαμέσο των w διαδρομών και της εξαδικής σύνθεσης μπορεί να επιλεγεί η ποιο ενδιαφέρουσα περιοχή για την έναρξη της αντιγραφής. Έτσι βρίσκονται οι ενδείξεις της πιθανής εισόδου ή του σημείου πρόσβασης στο μενού διαχείρισης του λογισμικού και ενδεχομένως σκέψεις για επιπλέων επιθέσεις αντιγραφής. Εφόσον είναι επιθυμητό μπορούμε να αποσυναρμολογήσουμε, να τροποποιήσουμε, να επαναμεταγλωττίσουμε και να αναπρογραμματίσουμε την συσκευή δίνοντας μας επιπλέον δυνατότητες στην χρήση της.

3.2.5 Ανάλυση διασυνδέσεων

Ένα πολύ σημαντικό σημείο στην ανάλυσή μας είναι η εύρεση και η μελέτη των μέσων και των τρόπων διασύνδεσης του υλικού τόσο εσωτερικά μεταξύ των υποσυστημάτων του όσο και με το εξωτερικό περιβάλλον. Έχοντας σχεδιάσει τα διάφορα υποσυστήματα του υλικού μας, θα πρέπει να εντοπιστούν τα σημεία εκείνα στα οποία παίρνοντας μετρήσεις με

κατάλληλα όργανα, να διευκολυνθούμε στην μελέτη των κυκλωμάτων και υποσυστημάτων. Οι διασυνδέσεις ολόκληρου του υλικού με το εξωτερικό περιβάλλον θα δώσουν την δυνατότητα στον μηχανικό να μελετήσει την λειτουργία της συσκευής δίνοντας κατάλληλες διεγέρσεις και λαμβάνοντας τα αντίστοιχα σήματα στις εξόδους του υλικού. Για τις διασυνδέσεις χρησιμοποιούνται συγκεκριμένα πρωτόκολλα αποκωδικοποίησης ή προσομοίωσης. Τέτοια μπορεί να είναι Smartcard, Serial, USB, JTAG, I2C, SPI, Ethernet, CAN. Κάθε διασύνδεση με το εξωτερικό περιβάλλον μπορεί να είναι και σημείο επίθεσης για τον επίδοξο αντιγραφέα. Εάν ο κατασκευαστής, ο οποίος σχεδίασε το υλικό έχει πρόσβαση στο περιβάλλον εργασίας του, τότε θα μπορεί να έχει πρόσβαση και ο οποιοσδήποτε. Χρησιμοποιώντας ειδικά προγράμματα και μέσα σύνδεσης θα είναι εφικτό να επιτευχθεί η σύνδεση με τα σημεία εκείνα του υλικού από τα οποία θα πάρουμε τα δεδομένα που μας χρειάζονται για την ανάλυση της λειτουργίας του. Τα δεδομένα αυτά μπορούμε να τα εξαγάγουμε με την χρήση κατάλληλων οργάνων και μέσων παλμογράφους, λογικούς αναλυτές, εργαλεία λογισμικού κ.α.

3.2.6 Ανάλυση σε επίπεδο πυριτίου

Αφού έχει γίνει η κυκλωματική ανάλυση του υλικού, γίνεται έλεγχος για την ύπαρξη τυπωμένων ολοκληρωμένων κυκλωμάτων. Όταν δεν γνωρίζουμε την ταυτότητα των ICs τότε θα πρέπει να μπούμε στην διαδικασία ανάλυσης τους σε μικρότερο επίπεδο κατασκευής τους, δηλαδή σε επίπεδο πυριτίου. Αρχικά, κατά την ανάλυση θα πρέπει να γίνει μια απλή απεικόνιση του IC ώστε να συλλέξουμε κάθε στοιχείο που θα μας είναι χρήσιμο για την ταυτοποίηση του. Θα πρέπει να εξαγάγουμε κλειδιά ή αλγόριθμους εφόσον υπάρχουν στο ολοκληρωμένο κύκλωμα. Για τις περιπτώσεις κυκλωμάτων όπως Flash, ROM, FPGAs ή άλλων μη ασταθών τυπωμένων κυκλωμάτων θα πρέπει να γίνει ανάκτηση και καταγραφή του περιεχομένου τους. Τέλος αφού κοπεί το περίβλημα του τυπωμένου ολοκληρωμένου κυκλώματος θα πρέπει να γίνει μελέτη των δομών πυριτίου ώστε να παρακαμφθούν οι ασφάλειες προστασίας και να γίνει η αποτύπωση των κυκλωματικών σχεδίων του. Η όλη διαδικασία θα μπορούσε να περιγραφεί ως η αντίστοιχη κλασική κυκλωματική ανάλυση για αντιγραφή αλλά σε μικροσκοπικό επίπεδο.

ΚΕΦΑΛΑΙΟ 4

4 ΑΝΟΙΓΜΑ ΤΟΥ ΥΛΙΚΟΥ ΚΑΙ ΑΝΤΙΣΤΡΟΦΗ ΜΗΧΑΝΙΚΗ

4.1 Εισαγωγή

Ο στόχος του ανοίγματος του υλικού είναι να αποκτηθεί από τον μηχανικό η πρόσβαση στα εσωτερικά κυκλώματα. Ο μηχανικός θα πρέπει να είναι προετοιμασμένος να θυσιάσει κάτι από το υλικό κατά την απόπειρα του ανοίγματος του, για τις αρχικές δοκιμές, όπως το να υπάρχει φθορά σε κάποιο τμήμα του. Η διαδικασία θα αρχίσει με τον εντοπισμό των σημείων στήριξης και σύνδεσης του περιβλήματος του υλικού. Τα υλικά σύνδεσης μπορεί να είναι βίδες, πλαστικές ασφάλειες κατάλληλα διαμορφωμένες για κάθε περίπτωση, κόλλες σύνδεσης (που μαλακώνουν με θερμικά πιστόλια), ταινίες κόλλησης διπλής όψεως κ.α. Οι βίδες μερικές φορές είναι κρυμμένες από την οπτική επαφή του χρήστη σε διάφορα σημεία του υλικού όπως στο κάτω μέρος του υλικού, κάτω από διάφορες ετικέτες ή κάτω από κομμάτια συγκράτησης από καουτσούκ.

Βήμα προς βήμα η διαδικασία είναι η εξής. Προετοιμάζουμε τον χώρο που θα εργαστούμε. Ο χώρος αυτός πρέπει να είναι καθαρός και να περιέχει ένα καλά φωτισμένο πάγκο. Αφαιρούμε κάθε είδους τροφοδοσία από την συσκευή αποσυνδέοντας το καλώδιο τροφοδοσίας και αφαιρώντας τους συσσωρευτές εφόσον υπάρχουν. Στην συνέχεια εντοπίζονται οι βίδες και αφαιρούνται με την σειρά. Εάν υπάρχουν βίδες με διαφορετικό ὶ έγεθος τότε θα πρέπει να καθοριστεί η θέση τους επί τού υλικού ώστε όταν χρειαστεί να ξανά τοποθετηθεί το περίβλημα ή οτιδήποτε άλλο είναι βιδωμένο να γίνει σωστά η σύνδεση του. Οι βίδες θα πρέπει να φυλάσσονται σε μαγνητικό δοχείο ή εάν δεν υπάρχει αυτό σε κάποιο ασφαλές χώρο. Έπειτα ελέγχονται οι ραφές στις οποίες είναι ενωμένα τα διάφορα τμήματα του υλικού και τα τραβάμε απαλά σε αυτές. Δεν πρέπει να ασκηθεί μεγάλη πίεση γιατί υπάρχει περίπτωση κάποια τμήματα να συνδέονται με πλαστικά κλιπ και να προκληθεί φθορά του υλικού. Σωστό είναι να εξεταστεί η ραφή κατά μήκος της με ένα μικρό, μακρύ, ίσιο κατσαβίδι ή ένα λεπτό έλασμα ώστε να εξασφαλιστεί ότι δεν υπάρχει κάποιο επιπλέον μέσο ασφάλισης και μπορούν να τραβηχτούν τα τμήματα χωρίς κίνδυνο.

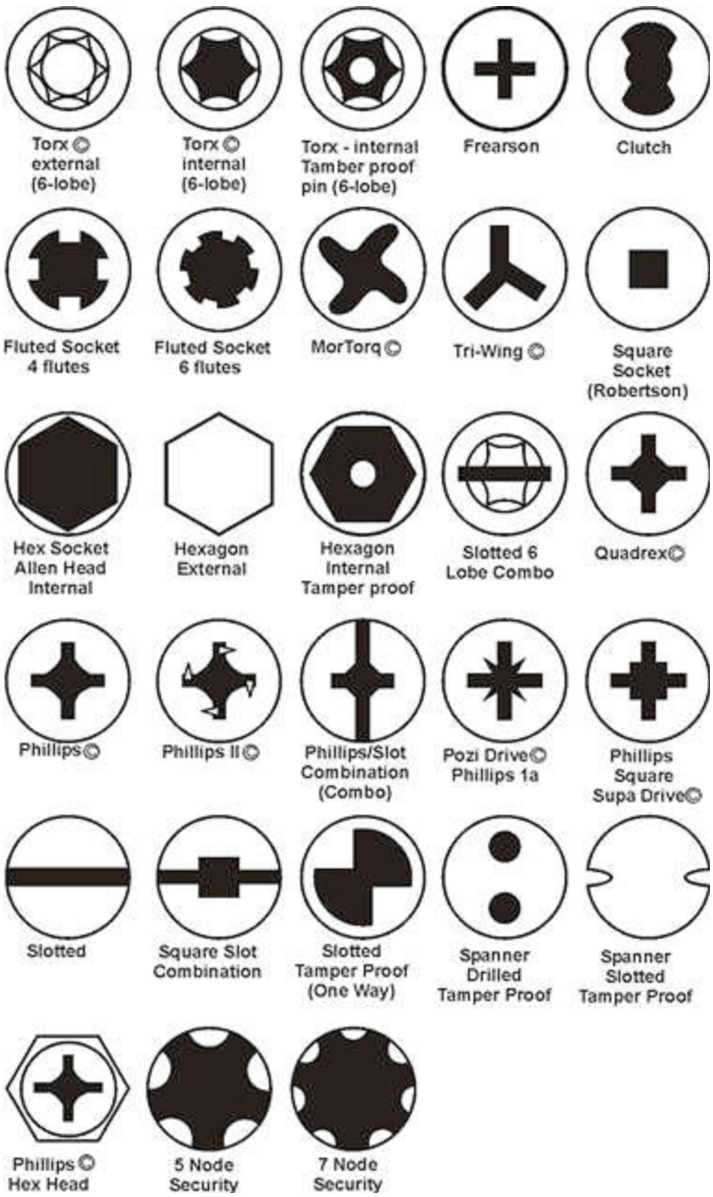
4.2 Μηχανισμοί προστασίας του υλικού

Ο κατασκευαστής του υλικού για την αποφυγή της παραβίασής του από τρίτους το θωρακίζει με κάποια είδη ασφάλειας. Για τα ενσωματωμένα συστήματα παρέχεται φυσική ασφάλεια. Κατά την σχεδίαση και κατασκευή του υλικού γίνεται προσπάθεια για την αποτροπή μη εξουσιοδοτημένης φυσικής ή ηλεκτρονικής επέμβασης στην μετέπειτα χρήση του. Για μεγαλύτερη αποτελεσματικότητα στην ασφάλεια του υλικού, που μπορεί να δεχθεί επίθεση για αντιγραφή, η σχεδίαση του γίνεται με τέτοιο τρόπο ώστε η χρήση του να γίνεται σε επίπεδα. Έτσι οι διαδικασίες της λειτουργίας της συσκευής γίνονται πιο πολύπλοκες και δύσκολο να διαβαστούν και να αντιγραφούν. Γενικά μπορεί να παρακαμφθεί οποιοδήποτε είδος ασφάλειας αναγνωρίζοντας την μέθοδο σχεδίασής του. Για να προσδιοριστεί ο μηχανισμός ασφάλειας μιας συσκευής, μπορεί ο επιτιθέμενος, σκόπιμα, να φτάσει στο σημείο ακόμα και να την καταστρέψει. Ο κατασκευαστής θα πρέπει να εστιάσει την προσοχή στα παρακάτω σημεία ώστε να έχει εξασφαλίσει κάποιου είδους ασφάλεια στην συσκευή του. Θα πρέπει να χρησιμοποιήσει εξειδικευμένα υλικά, ανθεκτικά στην παραβίαση. Το υλικό θα πρέπει να είναι έτσι σχεδιασμένο ώστε σε απόπειρα επίθεσης να γίνονται εμφανή τα σημάδια της παραβίασης και τα σημεία που ενδεχομένως μπορούν να παραβιαστούν να είναι και σημεία ελέγχου της συσκευής από τον χρήστη. Τέλος με την ενεργοποίηση της συσκευής από τον χρήστη, να γίνεται αντιληπτή η παραβίαση όπου αυτό είναι δυνατόν. Το μόνο θετικό σημείο σε μια παραβίαση είναι ότι με την ανίχνευσή της, θα μπορεί ο κατασκευαστής να αναβαθμίσει τα συστήματα ασφαλείας του υλικού και η σχεδίαση νέων συστημάτων να γίνεται με περισσότερες δικλίδες ασφαλείας. Στην πράξη όμως οι μηχανισμοί προστασίας δεν παρέχουν πραγματική ασφάλεια και οι περισσότερες σφραγίδες ασφαλείας μπορούν να παρακαμφθούν από τους επιτήδειους αντιγραφείς με συνήθη εργαλεία. Μια αξιολόγηση της ευπάθειας των σφραγίδων ασφαλείας έχει γίνει από τον R.G. Johnston σύμφωνα με το [6].

4.3 Άνοιγμα του περιβλήματος

Στη συνέχεια, αφού έχουν εντοπιστεί τα σημεία ανοίγματος του περιβλήματος θα πρέπει να χρησιμοποιηθούν οι κατάλληλες μύτες ασφαλείας για κατσαβίδι ή εξειδικευμένα κατσαβίδια μιας λειτουργίας ώστε να αφαιρεθούν οι αντίστοιχες βίδες συγκράτησης του περιβλήματος. Τα κατσαβίδια αυτά θα μπορούσαν να χρησιμοποιηθούν ως ένας μηχανισμός αποτροπής παραβίασης. Όμως παρόλο που ονομάζονται μύτες "ασφαλείας" ή "εξειδικευμένα" κατσαβίδια μπορεί ο καθένας να τα αγοράσει σχεδόν οπουδήποτε όπως

καταστήματα ηλεκτρονικών, καταστήματα εργαλείων και στο διαδίκτυο. Επίσης μπορεί κάποιος με κατάλληλα εργαλεία ακόμα και να τα κατασκευάσει. Ουσιαστικά η χρήση αυτών των κατσαβιδιών μπορεί να εμποδίσει μόνο τις απλές επιθέσεις. Για τον εντοπισμό ενός συγκεκριμένου τύπου μύτης μπορεί να γίνει χρήση του πίνακα της εικόνας 4.1 ή μέσω διαδικτύου από την ιστοσελίδα [7].



Εικόνα 4.1 *Τύποι από μύτες ασφαλείας*

Αφού ανοιχτεί το περίβλημα της συσκευής αλλά και οποιαδήποτε ασφάλεια της, φτάνουμε στο επίπεδο των πλακετών των ηλεκτρονικών κυκλωμάτων. Οι πλακέτες τις περισσότερες φορές είναι κατασκευασμένες με μια εποξειδική επικάλυψη. Η επικάλυψη αυτή χρησιμοποιείται συνήθως για την προστασία των κυκλωμάτων από υγρασία, σκόνη,

μούχλα, διάβρωση ή δημιουργία ηλεκτρονικού τόξου. Η επίστρωση από εποξειδικό υλικό ή υλικό ουρεθάνης αφήνει ένα σκληρό φιλμ στο ηλεκτρονικό υλικό που είναι δύσκολο να αφαιρεθεί. Οι περισσότερες εποξειδικές επιστρώσεις δεν έχουν σχεδιαστεί ειδικά για την ασφάλεια του υλικού σε ενδεχόμενες επιθέσεις αντιγραφής, αν και μερικές φορές χρησιμοποιούνται και για αυτό τον λόγο. Για την αφαίρεση τους μπορούν να χρησιμοποιηθούν φυσικές ή χημικές μέθοδοι. Με φυσικές μεθόδους μπορεί να χρησιμοποιηθεί πιστόλι θερμού αέρα, ώστε να λιώσει η επικάλυψη και με κατάλληλο απορροφητήρα να αφαιρεθεί. Επίσης μπορεί να χρησιμοποιηθεί εργαλείο ξυσίματος ή σουβλί ξύλου ως αιχμή ξυσίματος και με προσοχή για να μην καταστραφούν τα στοιχεία κάτω από την επίστρωση να αφαιρεθεί το προστατευτικό φιλμ. Κατά την διαδικασία υπάρχει κίνδυνος να αφαιρεθεί η μάσκα από την κόλληση (καλάι), αλλά κάτι τέτοιο δεν θα ήταν κάτι σοβαρό αφού μπορεί να διορθωθεί σχετικά εύκολα. Με χημικές μεθόδους μπορεί να χρησιμοποιηθεί κάποιο κατάλληλο χημικό υλικό ανάλογο με το φιλμ επικάλυψης, ώστε να αντιδράσει με αυτό και να αφαιρεθεί. Τέτοιο μπορεί να είναι το "MG Chemicals' 8310" σύμφωνα με την ιστοσελίδα [8].

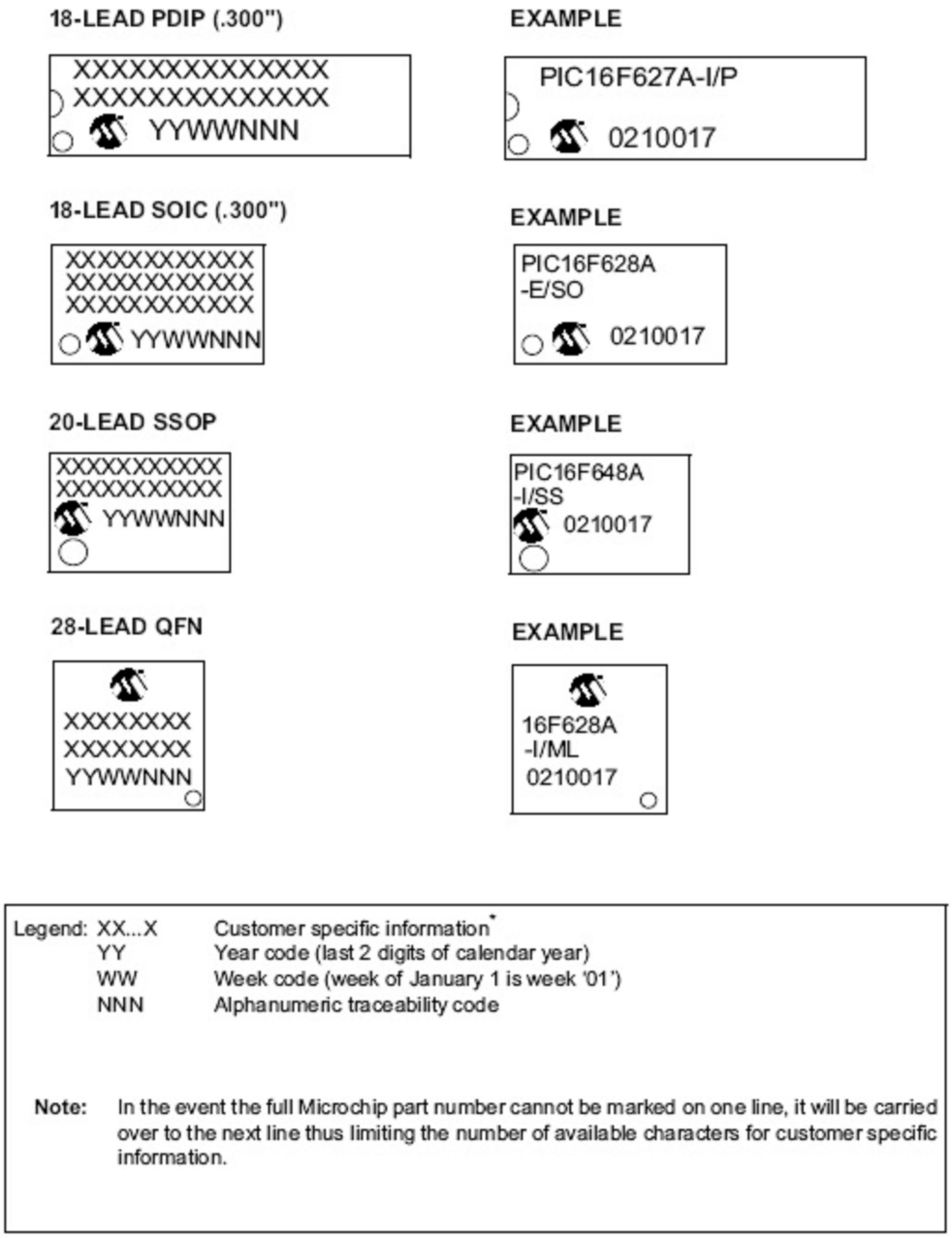
4.4 Αντίστροφη μηχανική του υλικού

Αφού έχει καθαριστεί η επιφάνεια της πλακέτας από τις διάφορες επικαλύψεις, στην συνέχεια θα πρέπει να γίνει η αναγνώριση των στοιχείων τα οποία περιέχονται στα κυκλώματα ώστε να μπορέσουμε να σχεδιάσουμε την κυκλωματική διάταξη. Οι περισσότερες επωνυμίες των κατασκευαστών και αριθμοί περιγραφής τυπώνονται απευθείας στα μεγαλύτερα στοιχεία. Αυτά τα στοιχεία βρίσκονται σε πλαίσια στην επιφάνεια του τυπωμένου κυκλώματος (IC). Υπάρχουν και μικρότερα ICs στα οποία δεν υπάρχει αρκετός χώρος στο περίβλημά τους για να τυπωθεί ολόκληρη η πληροφορία, γι'αυτό σε αυτά υπάρχουν μόνο κάποιες συντμήσεις. Έχοντας όποια στοιχεία είναι τυπωμένα επάνω στο IC αναγνωρίζεται το στοιχείο και από τα φύλλα δεδομένων του κατασκευαστή μπορούν να ανεβρεθούν περισσότερες λεπτομέρειες. Ένα καλά εκπαιδευμένος μηχανικός ή μια τυχερή εικασία θα βοηθήσει σε μια γρήγορη συνέχιση της διαδικασίας. Τα βασικά στάδια για την αναγνώριση των στοιχείων είναι τα εξής:

- Αναζήτηση του λογότυπου του κατασκευαστή
- Έλεγχος για την αλφαριθμητική συμβολοσειρά της παρτίδας του IC (αριθμητικός τύπος υλικού, κωδικός υλικού, ημερομηνία παραγωγής, εκτιμώμενη ταχύτητα, μέγεθος)

- Ανεύρεση των φύλλων δεδομένων

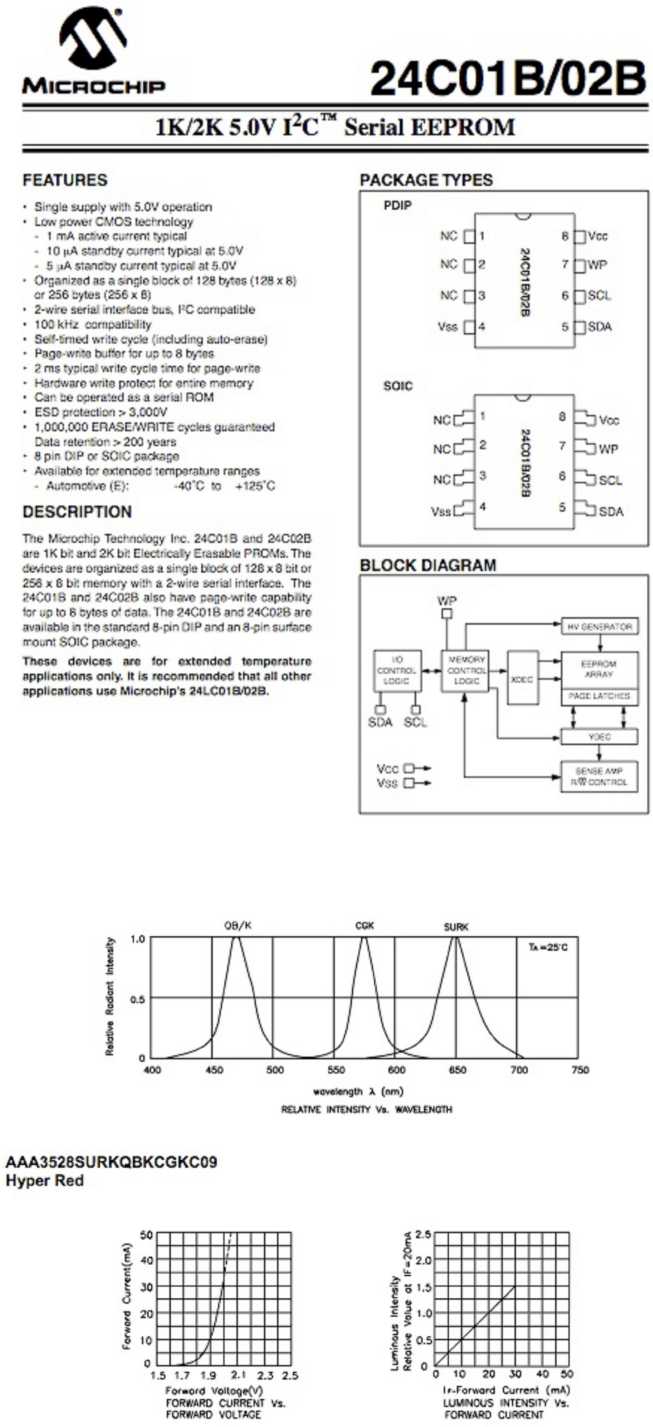
Για τον εντοπισμό του λογότυπου του κατασκευαστή μπορεί να χρησιμοποιηθεί η παρακάτω ιστοσελίδα [9]. Παραδείγματα μεγέθους και στοιχείων σε διάφορα ICs παρουσιάζονται στην εικόνα 4.2.



Εικόνα 4.2 *Μέγεθος και στοιχεία ICs*

Πολλές φορές ειδικής παραγγελίας ή αποκλειστικά ICs κατασκευάζονται με τέτοιο τρόπο ώστε εσκεμμένα να γίνεται δύσκολη η πρόσβαση στα στοιχεία τους. Οι κατασκευαστές ή οι προμηθευτές αφαιρούν τα διακριτικά και τις ενδείξεις ή μέρος αυτών από τα ICs. Αυτή η διαδικασία γίνεται με βουρτσάκια από ανοξείδωτο χάλυβα, μικροτριβεία, προσβολείς μικρό-

σφαιριδίων, χαράκτες λέιζερ ή με άλλες μεθόδους. Παρόλο της έλλειψης στοιχείων από τα ICs είναι δυνατόν να προσδιοριστεί η λειτουργία τους χρησιμοποιώντας κατάλληλα probes και ψάχνοντας με κατάλληλα όργανα τα σήματα εξόδου σε ανάλογη διέγερση η αποτυπώνοντας το ίχνος που αφήνουν.



Εικόνα 4.3 *Παράδειγμα Data Sheet*

Αφού γίνει γνωστή η ταυτότητα του IC στη συνέχεια θα πρέπει να βρεθεί το αντίστοιχο φύλλο δεδομένων (Data Sheet). Τα φύλλα δεδομένων περιέχουν εξαιρετικά χρήσιμες τεχνικές πληροφορίες για το στοιχείο, όπως παρακάτω:

- Περιληπτική σύνοψη του προϊόντος
- Λειτουργία ακροδεκτών εισόδου και εξόδου
- Ηλεκτρικές παραμέτρους και όρια λειτουργίας
- Εφαρμογές των δεδομένων
- Σχέδιο πακεταρίσματος του στοιχείου

Παράδειγμα μέρους ενός φύλλου δεδομένων δίνεται στην εικόνα 4.3. Για την εύρεση των φύλλων δεδομένων υπάρχουν πολλές δωρεάν ή με πληρωμή διαδικτυακές υπηρεσίες αναζήτησης και εντοπισμού τους. Μερικές σημειώνονται στα [10],[11],[12],[13] και [14].

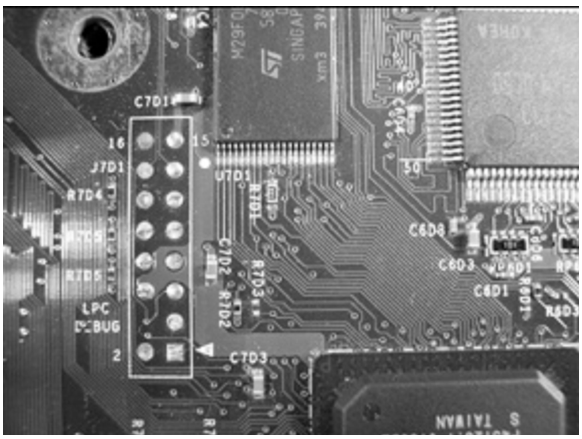
4.5 Σχεδίαση για έλεγχο

Κατά την σχεδίαση του υλικού για την παραγωγή του, ο κατασκευαστής επιθυμεί για να μπορεί να ελέγξει το υλικό, να έχει μια πλήρη εικόνα σχετικά με την κατάσταση των συστημάτων και κυκλωμάτων του. Επίσης θα πρέπει να έχει μια απρόσκοπτη πρόσβαση στα θεμελιώδη σήματα λειτουργίας του υλικού και τέλος να έχει οπτική δυνατότητα ελέγχου. Αυτό θα βοηθήσει κατά τον ποιοτικό έλεγχο και τον έλεγχο καλής λειτουργίας του προϊόντος, να αναγνωριστούν άμεσα τυχόν σφάλματα, να επισκευαστούν εύκολα και με χαμηλό κόστος και να ξανακάνουν το υλικό να δουλέψει με υψηλή απόδοση και εξασφαλίζοντας την επιτυχημένη μελλοντική λειτουργία του. Αυτή όμως η διαδικασία από τον σχεδιαστή, πέρα από την βοήθεια που παρέχει στον κατασκευαστή βοηθάει επίσης και τους επίδοξους αντιγραφείς να την χρησιμοποιήσουν για την διευκόλυνσή τους στην περιγραφή της λειτουργίας του υλικού. Η σχεδίαση για δοκιμή γίνεται σε δομές ελέγχου του υλικού που να επιτρέπουν μια γρήγορη διάγνωση της κατάστασης ενός συστήματος ή ενός κυκλώματος. Έτσι η σχεδίαση γίνεται με τέτοιο τρόπο ώστε να παρέχεται εύκολη πρόσβαση στα σημεία δοκιμής και λειτουργίας, να υπάρχουν εργοστασιακά τυπωμένες διεπαφές δοκιμής και η δοκιμή να είναι αποκλειστική από τον κατασκευαστή σε θύρες εντοπισμού σφαλμάτων (π.χ. Microchip PIC ICD2, Freescale BDM, Texas Instruments Spy-by-Wire).

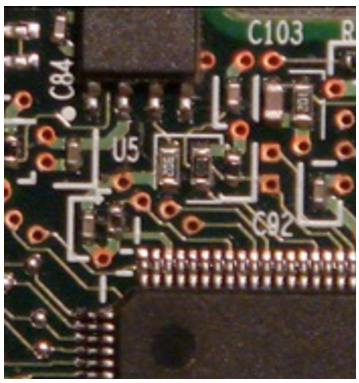
4.6 Σημεία ελέγχου

Τα σημεία ελέγχου είναι σημεία επάνω στο κύκλωμα όπου κατάλληλα όργανα συνδέονται σε αυτά με probes και είτε διεγείρουν το κύκλωμα είτε λαμβάνουν σήματα

εξόδου, τα οποία επεξεργάζονται και μπορούν να βγουν πληροφορίες για την λειτουργία των κυκλωμάτων. Αυτά τα σημεία μπορεί να είναι μικροί κύκλοι με ή χωρίς τρύπα εσωτερικά, μικρές ακίδες κάθετες στην πλακέτα ή επαφές χαλκού στην άκρη της πλακέτας. Για την εύρεση τους επάνω στην πλακέτα, μερικές φορές είναι εύκολα αναγνωρίσιμα από το μεταξότυπο περίγραμμά τους, την διαφορετικότητά τους σε σχέση με τα υπόλοιπα σημεία και την εύκολη πρόσβαση που έχουν. Χαρακτηριστικά σημεία ελέγχου φαίνονται στις εικόνες 4.4 και 4.5.



Εικόνα 4.4 *Σημεία ελέγχου σε πλακέτα*

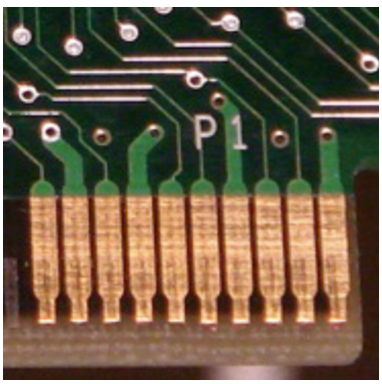


Εικόνα 4.5 *Χαρακτηριστικά σημεία ελέγχου*

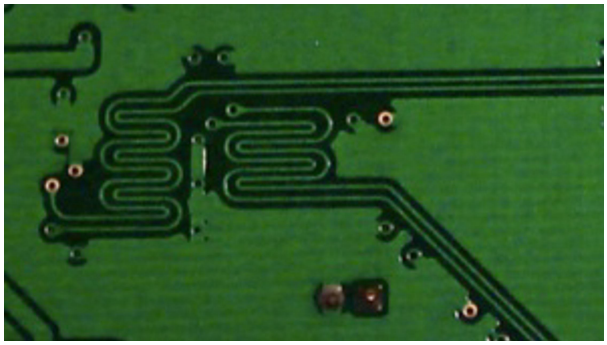
Αν δεν είναι εύκολα αναγνωρίσιμα τότε θα πρέπει να εντοπιστούν. Αυτό γίνεται ακλουθώντας τις διαδρομές που ενώνουν τα στοιχεία του κυκλώματος επάνω στην πλακέτα, δηλαδή "ακολουθώντας τον χαλκό", θα βρεθεί το σημείο εκείνο που θέλουμε να ελέγξουμε. Αν οι διαδρομές του χαλκού είναι καλυμμένες ή έχουμε πλακέτες πολλαπλών όψεων, τότε

με ένα πολύμετρο σε λειτουργία για εντοπισμό βραχυκυκλώματος, σαρώνοντας τις άκρες των στοιχείων μπορούμε να βρούμε τις συνδέσεις των διαδρομών. Επειδή τα δεδομένα μπορεί να μεταφέρονται παντού επάνω στο κύκλωμα, είναι δυνατόν να είναι εκτεθειμένα διευθύνσεις, δεδομένα και διαδρομές ελέγχου. Για την ασφάλεια των κυκλωμάτων σχεδιάζονται έτσι ώστε να μπλέκουν τα ίχνη των μονοπατιών ή να είναι κρυμμένα κρίσιμα ίχνη σε εσωτερικά στρώματα της πλακέτας. Οι υπόγειες διαδρομές χρησιμοποιούνται για την σύνδεση μεταξύ δυο ή περισσοτέρων εσωτερικών στρώσεων και όχι για εξωτερικές συνδέσεις. Επίσης οι υπόγειες διαδρομές δεν μπορούν να φαίνονται και από τις δυο πλευρές τις επιφάνειας. Γενικά ο προσδιορισμός των ιχνών είναι μια πολύ σημαντική διαδικασία για την ανάλυση των ηλεκτρονικών κυκλωμάτων, γιατί αναγνωρίζοντας τα θα οδηγηθούμε άμεσα στο σημείο ελέγχου, είναι όμως επίσης και χρονοβόρα. Θα πρέπει κατά την ανάλυση με μια ματιά, χωρίς ιδιαίτερη σκέψη να εντοπιστεί η λειτουργία του κάθε ίχνους. Έτσι ανάλογα την λειτουργία τους τα ίχνη κατηγοριοποιούνται ως εξής:

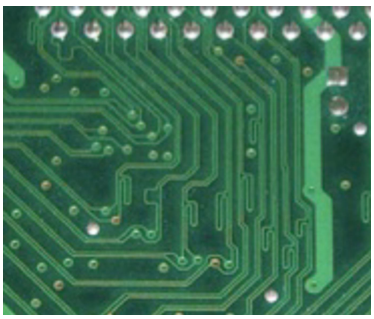
- Ίχνη ισχύος (ρεύματος) είναι παχιά και συνήθως μικρού μήκους (εικόνα 4.6)
- Ίχνη ελεγχόμενων σημάτων από σύνθετες αντιστάσεις είναι παχιά και συνήθως μεγάλου μήκους. Τέτοια σήματα μπορεί να είναι παλμοί ρολογιού, δεδομένα υψηλής ταχύτητας κ.α.
- Ζεύγη ιχνών καταδεικνύουν διαφορικά σήματα (εικόνα 4.7)
- Ίχνη σε μορφή "Zig Zag" καταδεικνύουν γραμμές συνδυασμένου μήκους (τυπικά για δεδομένα υψηλής ταχύτητας) (εικόνα 4.7)
- Παράλληλα ίχνη ή ομαδοποιημένα ίχνη καταδεικνύουν σήματα με παρόμοια λειτουργία (εικόνες 4.8 και 4.9)



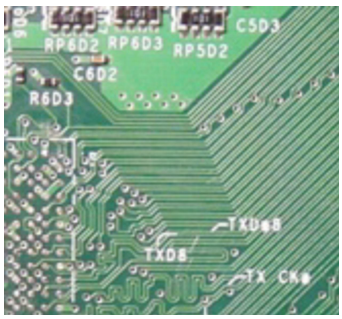
Εικόνα 4.6 *Ίχνη ισχύος*



Εικόνα 4.7 *Ζεύγη ιχνών σε μορφή "Zig Zag"*



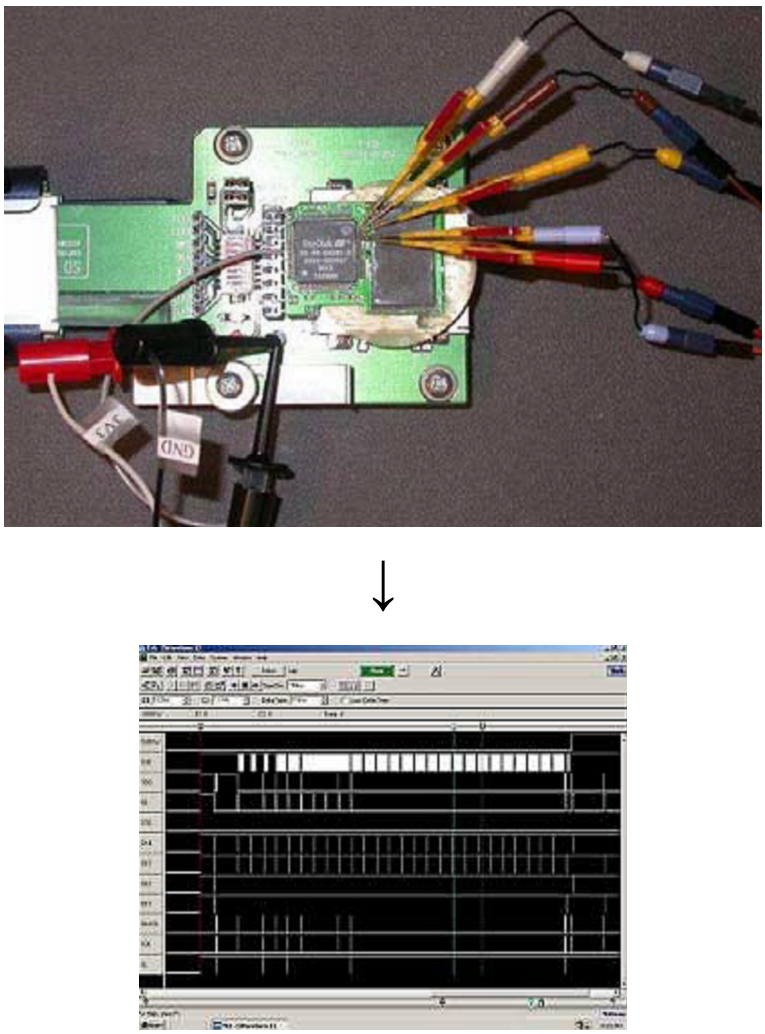
Εικόνα 4.8 *Παράλληλα ίχνη*



Εικόνα 4.9 *Παράλληλα ομαδοποιημένα ίχνη*

4.7 Μνήμη-Προγραμματιζόμενη λογική

Στα περισσότερα κυκλώματα κατά την σχεδίαση τους περιέχουν διαφόρων ειδών μνήμες. Οι περισσότερες μνήμες δεν έχουν σχεδιαστεί με γνώμονα την ασφάλεια, έτσι θα μπορούσαν να διαβαστούν εύκολα με μια off-the-shelf συσκευή προγραμματισμού γενικού σκοπού (εικόνα 4.10). Επίσης οι σειριακές EEPROMs μπορούν συνήθως να διαβάσουν εσωτερικά κυκλώματα. Η SRAM-βάση των FPGAs είναι ευάλωτη σε επιθέσεις εφόσον η πληροφορία πρέπει να φορτωθεί από εξωτερική μνήμη. Η ροή των bits, για ασφάλεια, μπορεί να κρυπτογραφηθεί και θα πρέπει να ελέγχεται για να μπορεί να γίνει ανάκτηση στο σύνολο της διαμόρφωσης.



Εικόνα 4.10 *Χρήση probe σε SanDisk SD Memory Card για λειτουργική ανάλυση*

Κατάλοιπα μπορεί να συνεχίσουν να υπάρχουν λίγο μετά την αφαίρεση της τροφοδοσίας και να είναι ανακτήσιμα από κατάλληλες συσκευές [15]. Αυτά τα κατάλοιπα θα μπορούν να είναι χρήσιμα για την λήψη κώδικα προγράμματος, προσωρινά δεδομένα ή κλειδιά crypto. Σε συσκευές ημιαγωγών λόγω της παραμένουσας μαγνήτισης μπορεί να γίνει ανάκτηση δεδομένων. Μια ολοκληρωμένη προσέγγιση για την ανάκτηση των διαγραμμένων αρχείων από μια NAND Flash δεδομένων δίνεται στο [16]. Η προστασία στις μνήμες παρέχεται με ασφαλιστικές δικλίδες και Boot-Block προστασία. Οι διάφορες προστασίες θα πρέπει να καθιστούν ικανές τις μνήμες για πρόσβαση στην περιοχή της μνήμης με μονή εγγραφή ή να παρεμποδίζεται κάποιος να διαβάσει πίσω την εγγραφή, πλήρως. Μία μνήμη μπορεί να παρακαμφθεί με επιθέσεις μπλοκ ανάλυσης ή ηλεκτρικών σφαλμάτων. Αρχές σχεδίασης παραβιάσεων ανθεκτικότητας των επεξεργαστών για έξυπνες κάρτες και προστασία αντιγραφής στους σύγχρονους μικροελεγκτές παραθέτονται στα [17] και [18]. Όταν ο

μηχανικός ανακτήσει τα δεδομένα από την μνήμη τότε χρησιμοποιώντας τυπικές τεχνικές λογισμικού μπορεί να τροποποιήσει, να ξανά μεταγλωττίσει, να αναπρογραμματίσει, να αποσυναρμολογήσει και να επανασυνδέσει μια συσκευή εάν το επιθυμεί. Για παράδειγμα μπορεί να χρησιμοποιηθούν IDA Pro [19] ή PICDisasm [20]

4.8 Διασυνδέσεις με εξωτερικές συσκευές

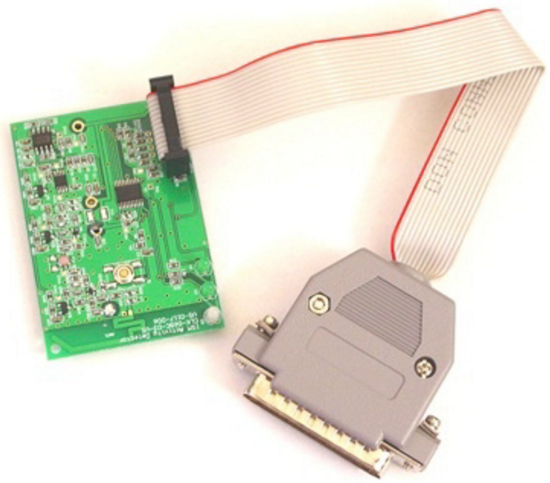
Κάθε συσκευή έχει τουλάχιστον ένα δίαυλο επικοινωνίας με τον έξω κόσμο και αυτό υλοποιείται με τις διάφορες διασυνδέσεις. Μέσω των διασυνδέσεων αυτών πραγματοποιούνται διάφορες βιομηχανικές δοκιμές, αναβαθμίσεις ή άλλες εργασίες στον τομέα του προγραμματισμού, διορθώσεις σφαλμάτων ή διάφορες περιφερειακές συνδέσεις. Οι διασυνδέσεις αυτές μπορεί να είναι είτε ενσύρματες είτε ασύρματες. Ενσύρματες διασυνδέσεις μπορεί να είναι RS 232, USB, Firewire, Ethernet κ.α. Επίσης θύρες εσωτερικών ελέγχων ή διόρθωσης σφαλμάτων όπως Microchip PIC ICD2, Freescale BDM, Texas Instruments Spy-by-Wire, Nokia F-Bus/M Bus. Ασύρματες διασυνδέσεις μπορεί να είναι 802.11, Bluetooth, ZigBee, ANT+. Κάθε διεπαφή η οποία συνδέει μια συσκευή με μια άλλη μπορεί να μεταφέρει πληροφορίες που να είναι χρήσιμες για μια επίθεση. Εκτός από τις διεπαφές που βρίσκονται σε εμφανή σημεία επάνω στην συσκευή, υπάρχουν και αυτές που δεν είναι συνήθεις και είναι για ειδική χρήση. Πολλές από αυτές είναι κρυμμένες και ο επίδοξος αντιγραφέας θα πρέπει να ψάξει για να τις βρει. Σημεία στα οποία μπορεί να είναι κρυμμένη μια διεπαφή είναι κάτω από την μπαταρία του κατασκευαστή ή κάτω από ένα αυτοκόλλητο (εικόνα 4.11). Αφού εντοπιστεί η διεπαφή μπορεί να χρησιμοποιηθεί ένα πολύμετρο ή ένας παλμογράφος για την εξέτασή του και τον καθορισμό της λειτουργικότητας του.

Εικόνα 4.11 *Διεπαφές σε κινητό τηλέφωνο*

Η λογική κατάσταση των ακίδων της διεπαφής μπορεί να βοηθήσει αρχικά σε ένα γρήγορο προσδιορισμό της λειτουργίας της συσκευής. Επικοινωνίες παρακολούθησης χρησιμοποιούν πρωτόκολλα ανάλυσης με βάση H/W ή S/W όπως RS232 και παράλληλη θύρα (PortMon), USB (SnoopyPro, SourceUSB), Bus Pirate. Σαν επίθεση μπορεί να σταλεί σκοπίμως κακόβουλο πακέτο για την πρόκληση κάποιου σφάλματος. Εάν το λογισμικό δεν μπορεί να χειριστεί αυτό το δικαίωμα, τότε η συσκευή θα μπορούσε να προκαλέσει ακούσια λειτουργία, που να είναι χρήσιμη σε μια επίθεση που θα δεχθεί.

4.9 JTAG

Αρχικά για τον έλεγχο τυπωμένων κυκλωμάτων με οριακή σάρωση σχεδιάστηκε το πρότυπο JTAG (Joint Test Action Group) που αργότερα εφαρμόστηκε το πρότυπο IEEE 1149.1. Σήμερα το πρότυπο JTAG χρησιμοποιείται ευρέως για τον εντοπισμό σφαλμάτων σε ICs, επίσης χρησιμοποιείται για δοκιμή και εντοπισμό σφαλμάτων σε τυποποιημένες-βιομηχανικές διασυνδέσεις. Παραδείγματα ελέγχων των οποίων κάνει είναι για το συστηματικό επίπεδο δοκιμής, σειριακό όριο-σάρωσης, χαμηλού επιπέδου δοκιμή για ολοκληρωμένα κυκλώματα και στοιχεία, εντοπισμό σφαλμάτων λογισμικού [21]. Επίσης μπορεί να προσφέρει μια άμεση διασύνδεση με το υλικό όπως να αναπρογραμματίσει μια μνήμη Flash.



Εικόνα 4.12 *Πλαστική φύσσα για έλεγχο JTAG*

Στην εικόνα 4.12 παρουσιάζεται ένας έλεγχος με JTAG με πλαστική βάση φύσσας των ακίδων εξόδου. Η JTAG αποτελείται από πέντε συνδέσεις, τέσσερις είναι απαραίτητες και μια προαιρετική (εικόνα 4.13). Οι συνδέσεις είναι όπως παρακάτω:

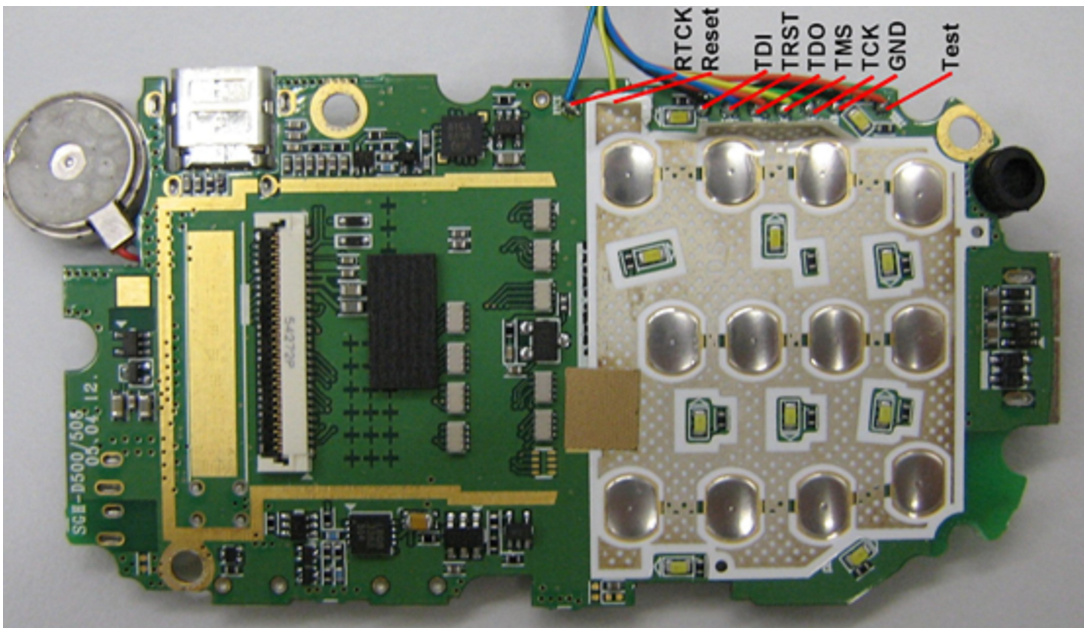
← TDO = Data Out (από την συσκευή)

→ TDI = Data In (προς την συσκευή)

→ TMS = Test Mode Select

→ TCK = Test Clock

→ /TRST = Test Reset (προαιρετικό)



Εικόνα 4.13 *Συνδέσεις πρόσβασης ελέγχου JTAG σε Samsung SGH-D500*

Γενικά, χαμηλού κόστους διασυνδέσεις JTAG είναι διαθέσιμες, συνήθως για ειδικές συσκευές και εργαλεία [22]. Παλιότερης τεχνολογίας παράλληλες θύρες διασύνδεσης είναι σχετικά εύκολο και οικονομικό να κατασκευαστούν. Παραδείγματα σχεδίασης JTAG συστημάτων ελέγχου δίνονται στα [23] και [24]. Στο περιβάλλον ανάπτυξης είναι δυνατόν να παρέχεται υποστήριξη για διασυνδέσεις JTAG, ειδικά οι χαμηλού επιπέδου λειτουργίες μπορούν να αντληθούν από τον ίδιο τον χρήστη. Υπάρχουν αρκετά εργαλεία λογισμικού ανοιχτού κώδικα όπως Open On-Chip Debugger (OpenOCD) [25] ή UrJTAG (Universal JTAG Library) [26].

Το να αφαιρεθεί μια διασύνδεση λειτουργίας JTAG από μια συσκευή είναι αρκετά δύσκολο. Οι σχεδιαστές συνήθως συγχέουν τα ίχνη ή τα κόβουν διακριτικά και χτυπούν τις ασφάλειες από εκείνα τα τμήματα μιας συσκευής που θα μπορούσαν να επισκευαστούν από

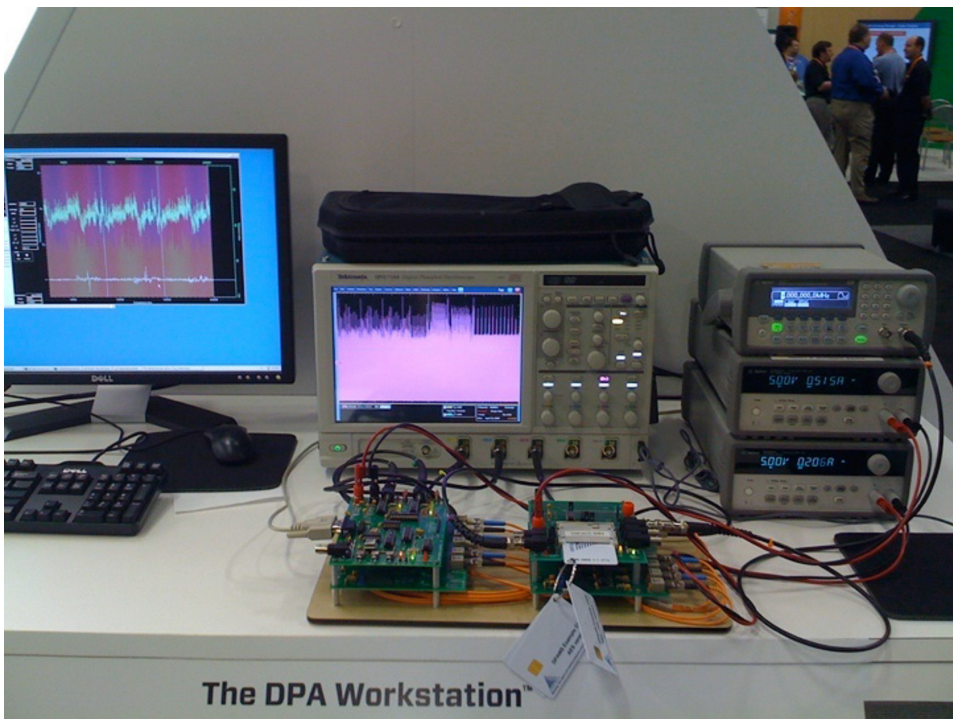
κάποιον εισβολέα. Κάτι τέτοιο θα ήταν ενοχλητικό για τους νόμιμους χρήστες γιατί δεν θα μπορούσαν να εξάγουν το πρόγραμμα, να κάνουν έλεγχο εντοπισμού σφαλμάτων ή δοκιμή δυνατοτήτων. Τέλος μια διασύνδεση μπορεί να προστατεύεται και με κωδικό πρόσβασης. Πάντως οι διασυνδέσεις για μια συσκευή είναι η "Αχίλλειος Πτέρνα" της.

4.10 Έμμεσα κανάλια επίθεσης

Όλες οι συσκευές μπορεί να έχουν διαρροή πληροφορίας οποιασδήποτε μορφής. Τέτοιες διαρροές μπορούν να είναι:

- Χρόνος.
- Κατανάλωση ισχύος.
- Ηλεκτρομαγνητική παρεμβολή EMI (Electromagnetic Interference) π.χ. Ηλεκτρομαγνητική ακτινοβολία από μονάδες προβολής βίντεο [27].
- Εικόνα και Ήχος π.χ. διαρροή πληροφοριών από οπτική πηγή ή κίνδυνος οπτικής υποκλοπής στο πεδίο του χρόνου στις οθόνες CRT.

Τα έμμεσα κανάλια επίθεσης μπορούν να χρησιμοποιηθούν για την ανάκτηση μυστικών πλήκτρων, PIN ή για αντίστροφη μηχανική λογισμικού όπως program flow ή crypto π.χ. ανάλυση έμμεσων καναλιών σε ενσωματωμένα συστήματα [28]. Εργαστηριακή ανάλυση έμμεσων καναλιών παρουσιάζεται στην εικόνα 4.14.



Εικόνα 4.14 *Εργαστηριακή ανάλυση*

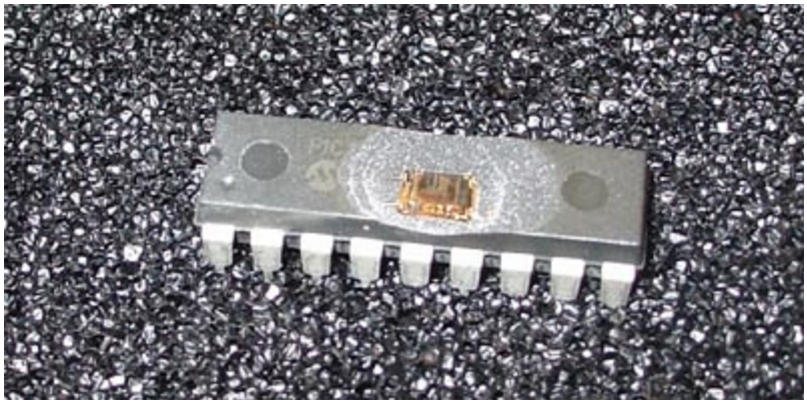
Χρησιμοποιώντας τα έμμεσα κανάλια επίθεσης μπορεί αναλύοντας την κατανάλωση της ισχύος της συσκευής να καταγραφούν χρήσιμα συμπεράσματα. Αυτό μπορεί να συμβεί γιατί βάση την κατανάλωση ισχύος μπορεί να σημειωθεί ακούσια φυσική διαρροή πληροφορίας. Έτσι υπάρχει η απλή ανάλυση ισχύος SPA (Simple Power Analysis) και διαφορική ανάλυση ισχύος DPA (Differential Power Analysis). Στην απλή ανάλυση ισχύος ο επιτιθέμενος παρατηρεί την κατανάλωση ισχύος η οποία διαφέρει ανάλογα την λειτουργία του εκάστοτε επεξεργαστή. Είναι επίσης εύκολο να εντοπιστούν οι εντατικές λειτουργίας όπως η κρυπτογράφηση. Στην διαφορική ανάλυση ισχύος χρησιμοποιούνται στατιστικές μέθοδοι για τον προσδιορισμό των κρυφών πληροφοριών σε μια συσκευή [29], [30] και [31].

Τέλος χρήσιμα συμπεράσματα μπορούν να καταγραφούν και με την χρήση έμμεσων καναλιών επίθεσης των ρολογιών και του χρονισμού της συσκευής. Οι επιθέσεις αυτές βασίζονται στην αλλαγή των χαρακτηριστικών του χρόνου μέτρησης του συστήματος. Οι επιθέσεις ενεργητικού χρονισμού (επεμβατικές) ενεργοποίησης διαφορετικών ρολογιών (επιτάχυνσης ή επιβράδυνσης) ώστε να προκληθεί βλάβη στην συσκευή ή ακούσια λειτουργία σε αυτή. Οι επιθέσεις παθητικού χρονισμού είναι μη επεμβατικές μετρήσεις του χρόνου υπολογισμού και σαν αρχή έχουν ότι διαφορετικές εργασίες λειτουργίας πραγματοποιούνται σε διαφορετικά χρονικά διαστήματα.

4.11 Ανάλυση στοιχείου Πυριτίου

Η ανάλυση σε επίπεδο στοιχείου πυριτίου είναι εξαιρετικά χρήσιμη ανάλογα με τους στόχους της επίθεσης. Η ανάλυση αυτή θα περιλαμβάνει απλή απεικόνιση του IC για την συλλογή στοιχείων, εξαγωγή κλειδιών ασφαλείας και αλγορίθμων από το IC, ανάκτηση περιεχομένου από στοιχεία Flash, ROM, FPGA και άλλων μη ασταθών στοιχείων, κοπή ή επισκευή δομών πυριτίου (ασφάλειες προστασίες, ίχνη κλπ) και τέλος εφαρμογή αντίστροφης μηχανικής όπως της κυκλωματικής αντιστροφής, αλλά σε μικροσκοπικό επίπεδο.

Η επεμβατική επιθέσεις ξεκινάει με την απομάκρυνση του περιβλήματος από το IC. Για την εργασία αυτή χρησιμοποιούνται μηχανικά ή χημικά μέσα (ή και τα δυο). Θερμαίνεται το περίβλημα μέχρι να μαλακώσει και χρησιμοποιώντας εργαλεία τομής κόβεται και ανοίγει η κορυφή του περιβλήματος (εικόνα. 4.15). Με προσοχή, αφαιρείται η ψηφίδα πυριτίου από το περίβλημα αφού κοπούν οι διασυνδέσεις της με τους ακροδέκτες. Καλύπτεται η ψηφίδα με 20-50 ml νιτρικού οξέος και θερμαίνεται στους 60 ^{o}C έως η εποξική ρητίνη, που περιβάλει την ψηφίδα διαλυθεί πλήρως (εικόνα. 4.16).

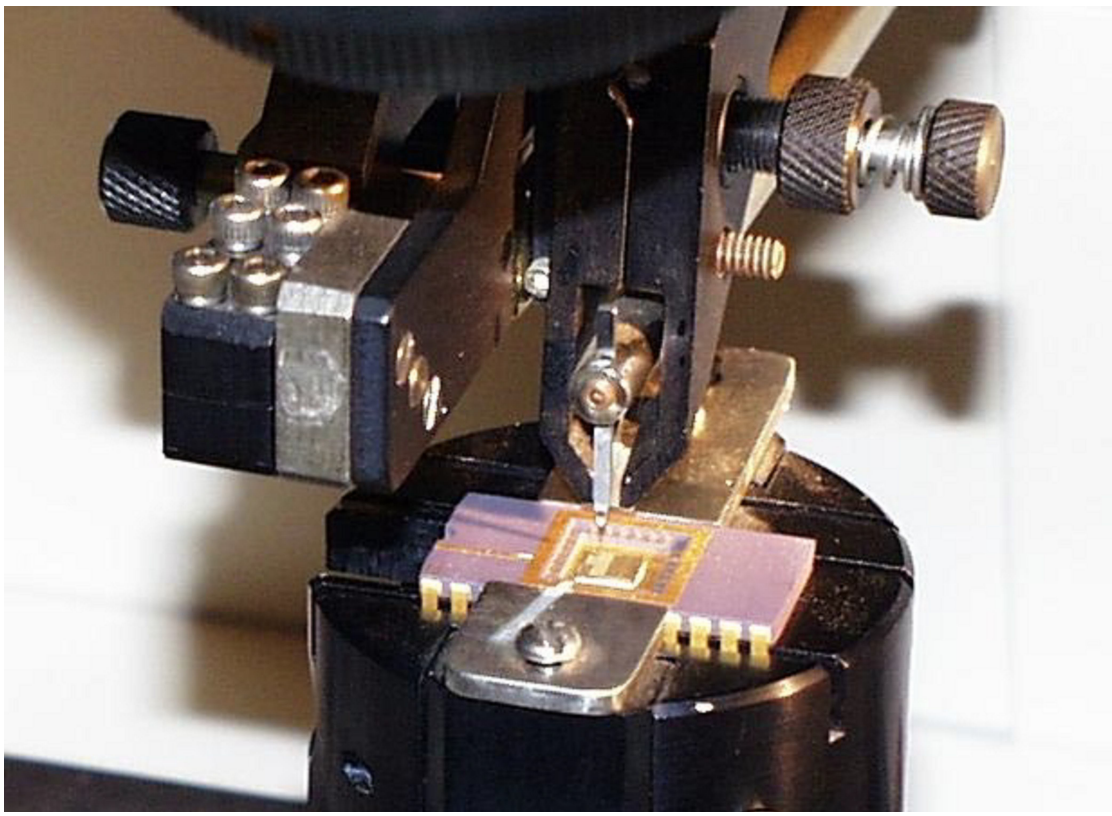


Εικόνα 4.15 *Άνοιγμα περιβλήματος IC*

Εικόνα 4.16 *Καθαρισμός ψηφίδας από το περίβλημα*

Η διαδικασία αυτή θα πρέπει κατά προτίμηση να πραγματοποιούνται κάτω από πολύ ξηρές συνθήκες, διότι η παρουσία του νερού θα μπορούσε να διαβρώσει τις εκτεθειμένες διασυνδέσεις αλουμινίου. Η ψηφίδα πυριτίου στη συνέχεια πλένεται με ακετόνη σε λουτρό υπερήχων, που ακολουθείται προαιρετικά από ένα μικρό λουτρό σε απιονισμένο νερό και ισοπροπανόλη. Βγαίνουν τα εναπομείναντα καλώδια συγκόλλησης με τσιμπιδάκια, τοποθετείται η ψηφίδα σε μια πλακέτα δοκιμής και συνδέονται οι ακίδες εισόδου-εξόδου της ψηφίδας με την πλακέτα (εικόνα 4.16). Γενική αρχή είναι ότι θα πρέπει να διατηρήσουμε την

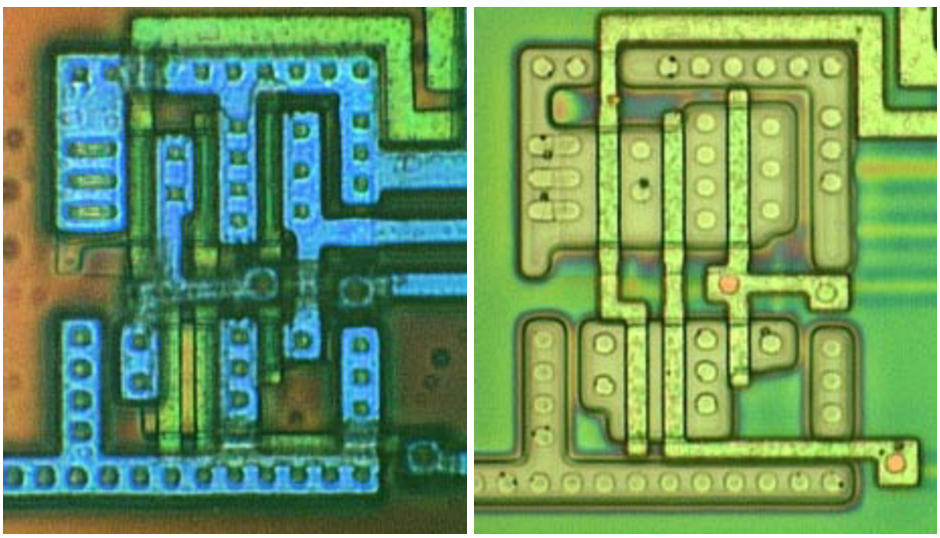
ψηφίδα πυριτίου κατά την αφαίρεσή της άθικτη και λειτουργική. Πλέον η ψηφίδα πυριτίου ενός IC είναι έτοιμη προς μελέτη.



Εικόνα 4.16 *Αφαίρεση διασυνδέσεων ψηφίδας*

Το επόμενο βήμα μιας επεμβατικής επίθεσης σε ένα IC είναι να χαρτογραφηθεί η κυκλωματική του διάταξη. Χρησιμοποιείται ένα οπτικό μικροσκόπιο με μια κάμερα CCD για να ληφθούν αρκετά μεγάλου μήκους ψηφιδωτά υψηλής φωτογραφικής ανάλυσης από την επιφάνεια της ψηφίδας. Βασικές αρχιτεκτονικές δομές, όπως είναι τα στοιχεία και τα ίχνη των διαδρομών, μπορεί να προσδιοριστούν πολύ γρήγορα από τη μελέτη των μοντέλων συνδεσιμότητας και με τον εντοπισμό μεταλλικών γραμμών που καθιστούν ορατά τα όρια κάθε μονάδας (ROM, RAM, EEPROM, ALU, αποκωδικοποιητές, κλπ.). Όλες οι μονάδες επεξεργασίας συνήθως συνδέονται με το κεντρικό σημείο διασύνδεσης ιχνών μέσω εύκολα αναγνωρίσιμων μανδαλωτών και οδηγούς διαδρομών. Ο επιτιθέμενος πρέπει προφανώς να είναι καλά εξοικειωμένοι με τεχνικές σχεδιασμού CMOS και αρχιτεκτονικές μικροελεγκτή VLSI, αλλά η απαραίτητη γνώση είναι εύκολα διαθέσιμα από τα πολυάριθμα βιβλία [32,33,34,35].

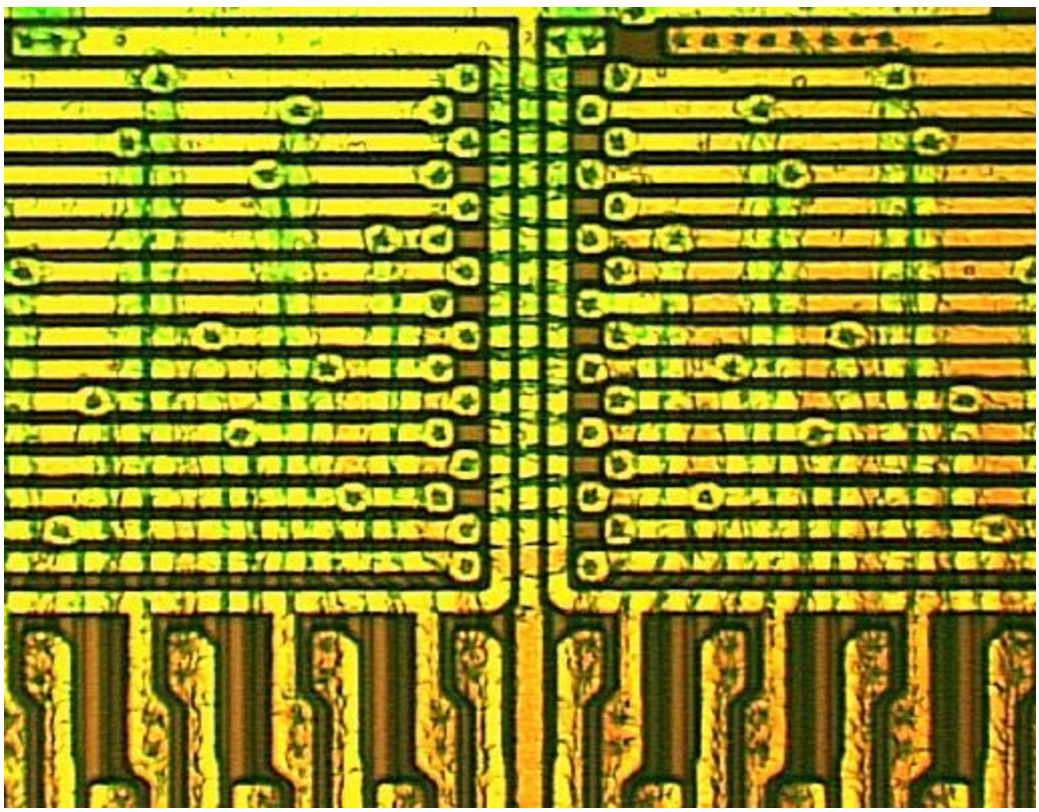
Φωτογραφίες από την επιφάνεια της ψηφίδας δείχνουν το ανώτερο στρώμα μετάλλου, το οποίο δεν είναι διαφανές και ως εκ τούτου κρύβει τη θέα σε πολλές δομές παρακάτω από αυτό. Εκτός και αν τα στρώματα του οξειδίου έχουν γίνει επίπεδα, τότε τα κατώτερα στρώματα μπορεί να αναγνωριστούν μέσα από τις υψομετρικές διαφορές που προκαλούν τα στρώματα που τα καλύπτουν. Τα βαθύτερα στρώματα μπορεί να αναγνωριστούν μόνο σε μια δεύτερης σειράς λήψη φωτογραφιών αφού τα μεταλλικά στρώματα έχουν αποκολληθεί, εργασία η οποία θα επιτευχθεί με την εμβάπτιση της ψηφίδας για λίγα δευτερόλεπτα σε υδροφθορικό οξύ (HF) ì ε λουτρό υπερήχων [36]. Το HF διαλύει γρήγορα το οξείδιο πυριτίου γύρω από τα κομμάτια του μετάλλου και στην συνέχεια τα απομακρύνει από την επιφάνεια της ψηφίδας. Το HF είναι μια εξαιρετικά επικίνδυνη ουσία και κατά το χειρισμό πρέπει να ακολουθούνται προσεκτικά οι κανόνες προφύλαξης και ασφάλειας. Η εικόνα 4.17 δείχνει μια οπτική διάταξη ανοικοδόμηση μιας πύλης NAND που ακολουθείται από έναν αντιστροφέα. Αυτές οι εικόνες έχουν ληφθεί με ένα ομοεστιακό μικροσκόπιο (Zeiss Axiotron-2 CSM), το οποίο εκχωρεί διαφορετικά χρώματα σε διαφορετικά εστιακά επίπεδα (π.χ., μετάλλου = μπλε, πολυπυριτίου = πράσινο) και ως εκ τούτου διαφυλάσσει το βάθος της πληροφορίας [38].



Εικόνα 4.17 *Εικόνες πύλης NAND με αντιστροφέα από ομοεστιακό μικροσκόπιο*

Εικόνες πολλαπλών επιφανειών, όπως αυτές που παρουσιάζονται στην εικόνα 4.17, μπορούν να διαβαστούν με κάποια εμπειρία σχεδόν το ίδιο εύκολα όπως και τα κυκλωματικά διαγράμματα. Αυτά τα κύκλωμα θα βοηθήσουν στην κατανόηση των τμημάτων του κυκλώματος που έχουν σημασία για τη σχεδιαζόμενη επίθεση.

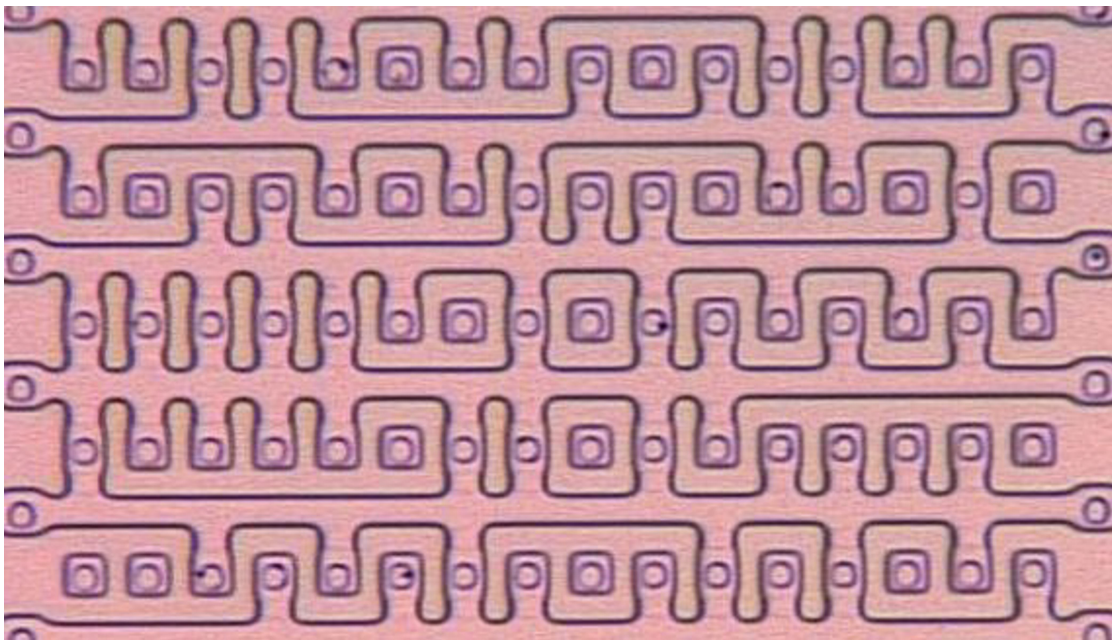
Εάν το ολοκληρωμένο τυπωμένο κύκλωμα έχει μια κοινά προσβάσιμη πρότυπη αρχιτεκτονική, τότε θα πρέπει να ανακατασκευάσει τη διάταξη μόνο μέχρι να έχουμε εντοπίσει αυτές τις διαδρομές και λειτουργικές ενότητες που θα πρέπει να χειριστούμε ώστε να έχουμε πρόσβαση σε όλες τις τιμές μνήμης. Πιο πρόσφατα, οι σχεδιαστές έχουν αρχίσει να προσθέτουν ειδικές λειτουργίες κρυπτογράφησης υλικού και αναγκάζουν τους επιτιθέμενους να επανακτήσουν πιο περίπλοκη κύκλωμα όπου εμπλέκονται σε αυτά πολλές χιλιάδες τρανζίστορ, πριν να καταφέρουν να παραβιάσουν πλήρως το σύστημα. Ωστόσο, η χρήση των τυποποιημένων σχεδίων ASIC, επιτρέπει να αναγνωριστούν με ευκολία οι λογικές πύλες από την περιοχή διάχυσης της διάταξης, γεγονός που καθιστά το έργο σημαντικά ευκολότερο από την επανάκτηση της διασύνδεσης του ηλεκτρονικού σχεδιού σε επίπεδο τρανζίστορ. Μερικοί κατασκευαστές χρησιμοποιούν μη-τυπικές διαδικασίες κρυπτογράφησης για την ασφάλεια των επεξεργαστών. Στην περίπτωση αυτή, όλη η διαδρομή από τα κύτταρα μνήμης EEPROM έως τις εντολές του αποκωδικοποιητή και την ALU θα πρέπει να εξετάζονται προσεκτικά πριν να επιτευχθεί επιτυχώς η αποσυναρμολόγηση για την εξαγωγή του κώδικα μηχανής. Παράλληλες διαδρομές οι οποίες είναι εύκολο να εντοπιστούν φαίνονται στην εικόνα 4.18.



Εικόνα 4.18 *Φωτογραφία παράλληλων διαδρομών*

Κάθε καλό μικροσκόπιο μπορεί να χρησιμοποιηθεί για την οπτική ανασυγκρότηση μιας διάταξης VLSI, όμως τα ομοεστιακά μικροσκόπια έχουν μια σειρά από ιδιότητες που τα καθιστούν πιο κατάλληλο για το έργο αυτό. Ενώ τα κανονικά μικροσκόπια παράγουν μια θολή εικόνα για κάθε πλάνο που είναι εκτός εστίασης, τα οπτικά μικροσκόπια ομοεστιακής σάρωσης, παρουσιάζουν τα πάντα έξω από το εστιακό πλάνο ακριβώς σαν σκοτάδι [37]. Τα ομοεστιακή μικροσκόπια προσφέρουν επίσης την καλύτερη ανάλυση και αντίθεση. Ένας χρωματικός φακός στο σύστημα μπορεί να κάνει τη θέση του εστιακού πλάνου να εξαρτάται από το μήκος κύματος, έτσι ώστε κάτω από λευκό φως τα διαφορετικά στρώματα της ψηφίδας να εμφανίζονται ταυτόχρονα, αλλά με διαφορετικά χρώματα.

Αυτόματη ανασχηματισμός μιας διάταξης έχει υλοποιηθεί με σάρωση με ηλεκτρονικό μικροσκόπιο [38]. Μπορεί να θεωρηθεί το ομοεστιακό μικροσκόπιο ως μία ελκυστική εναλλακτική λύση, επειδή δεν χρειαζόμαστε ένα περιβάλλον κενού, το βάθος πληροφοριών διατηρείται, και η επιλογή του ελαιοκαταδυτικού φακού επιτρέπει την απόκρυψη τής ανομοιόμορφης αφαίρεσης των στρωμάτων οξειδίου. Με μικροσκοπία UV, μπορούν να διαβαστούν ψηφίδες δομής μεγέθους ακόμη και της τάξης των 0,1μm. Με ημιαυτόματες μεθόδους επεξεργασίας εικόνας, σημαντικά τμήματα ενός επεξεργαστή μπορούν να αντιγραφούν μέσα σε λίγες ημέρες. Τα δεδομένα που θα προκύψουν μπορούν στη συνέχεια να χρησιμοποιηθούν για να δημιουργηθεί αυτόματα διαγραμματική διάταξη των τρανζίστορ σε επίπεδο πύλης για την προσομοίωση του κυκλώματος. Οπτικές τεχνικές ανακατασκευής μπορούν επίσης να χρησιμοποιηθούν για να διαβαστεί μια ROM άμεσα. Το μοτίβο μιας ROM σε επίπεδο bit αποθηκεύεται στο στρώμα διάχυσης, που αφήνει ελάχιστα κάθε οπτική ένδειξη των στοιχείων στην επιφάνεια της ψηφίδας. Θα πρέπει να αρθούν όλα τα στρώματα που καλύπτουν τη χρήση HF υγρής χάραξης, μετά την οποία μπορούμε εύκολα να αναγνωρίσουμε τις ζάντες των περιοχών διάχυσης που αποκαλύπτουν το αποθηκευμένο σχέδιο σε επίπεδο bit (εικόνα 4.19).



Εικόνα 4.19 *Η εικόνα παραθέτει 16x10bits σε ένα ST16xyz*

Η ανάλυση των στοιχείων πυριτίου αποτελεί μια αρκετά δύσκολη διαδικασία αντιγραφής και ο εξοπλισμός που απαιτείται για την εφαρμογή της είναι ειδικός και αρκετά ακριβός. Μπορεί όμως ο εξοπλισμός να βρεθεί σε ακαδημαϊκό επίπεδο ή σε επίπεδο έρευνας ή ο μηχανικός να κινηθεί σε χαμηλότερου επιπέδου τεχνολογία που όμως θα έχει χειρότερα αποτελέσματα.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Ingle Kathryn A., 1994, Reverse Engineering, McGraw-Hill, Inc.

[2] John R. Bork, August 2005, Reverse Engineering a Microcomputer-Based Control Unit

[3] Claudio Mattiussi and Dario Floreano, October 2007, Analog Genetic Encoding for the Evolution of Circuits and Networks, IEEE Transactions on Evolutionary Computation, Vol. 11, No. 5

[4] Gergely Erdelyi, February 2002, Introduction to Reverse Engineering

[5] Joe Grand, 2011, Hardware Reverse Engineering: Access, Analyze, & Defeat, Black Hat DC 2011 Workshop

[6] Author R.G. Johnston,Vulnerability Assessment of Security Seals, http://www.securitymanagement.com/archive/library/lanl_00418796.pdf

[7] http://www.instructables.com/id/When-a-Phillips-is-not-a-Phillips/

[8] www.mgchemicals.com

[9] http://www.engineering.uiowa.edu/~eshop/mflogo.dir/ic-id.html

[10] www.alldatasheet.com/

[11] http://www.datasheet4u.net/

[12] http://www.datasheetarchive.com/

[13] http://www.datasheetdirect.com/

[14] http://www.datasheetdir.com/

[15] http://citp.princeton.edu/memory/

[16] An Integrated Approach to Recovering Deleted Files from NAND Flash Data, June 2008, James Luck & Mark Stokes

[17] www.cl.cam.ac.uk/~mgk25/sc99-tamper.pdf

[18] www.cl.cam.ac.uk/~sps32/mcu_lock.html

[19] http://www.hex-rays.com/

[20] http://hagi-online.org/picmicro/ picdisasm_en.html

[21] http://en.wikipedia.org/wiki/Joint_Test_Action_Group

[22] www.sparkfun.com

[23] http://jtag-arm9.sourceforge.net/circuit.txt

[24] ftp://www.keith-koep.com/pub/arm-tools/jtag/jtag05_sch.pdf

[25] http://openocd.sourceforge.net/supported-jtag-interfaces/

[26] http://urjtag.org/

[27] Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?, Wim van Eck.
[28] http://conference.hitb.org/hitbsecconf2009kl/materials/D2T1%20-%20Job%20De%20Haas%20-%20Side%20Channel%20Analysis.pdf
[29] Differential Power Analysis, Paul Kocher, Joshua Jane, and Benjamin Jun.
[30] http://www.dpabook.org/
[31] http://opensca.sourceforge.net/
[32] N.H.E. Weste, K. Eshraghian: Principles of CMOS VLSI Design. Addison-Wesley, 1993.
[33] S.-M. Kang, Y. Leblebici: CMOS Digital Integrated Circuits: Analysis and Design. McGraw-Hill, 1996.
[34] J. Carter: Microprocessor Architecture and Microprogramming { A State-Machine Approach. Prentice-Hall, 1996.
[35] S.M. Sze: Semiconductor Devices { Physics and Technology. John Wiley & Sons, 1985.
[36] F. Beck: Integrated Circuit Failure Analysis A Guide to Preparation Techniques. JohnWiley & Sons, 1998.
[37] T.R. Corle, G.S. Kino: Confocal Scanning Optical Microscopy and Related Imaging Systems. Academic Press, 1996.
[38] S. Blythe, et al.: Layout Reconstruction of Complex Silicon Chips. IEEE Journal of Solid-State Circuits, 28(2):138{145, February 1993.