ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Διπλωματική Εργασία :

Ασφάλεια Υλικού σε κυκλώματα FPGA και Ανάλυση και Ενδυνάμωση της Ασφάλειας του Υλικού σε συστήματα τεχνητής νοημοσύνης : Εξέλιξη και Προηγμένες επιθέσεις

Εργασία των:

Ανδρέα Χριστοφόρου ΑΕΜ 2885 & Ανδρέα Κάσινου ΑΕΜ 2884

Επιβλέπων καθηγητής:

Σταμούλης Γεώργιος

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

UNIVERSITY OF THESSALY

SCHOOL OF ENGINEERING DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

Diploma Thesis :

Hardware Safety in FPGA Circuits and Analyzing and Enhancing Hardware Security in Artificial Intelligence Systems: Evolution and Advanced Attacks

Subject of:

Andrea Christoforou AEM 2885 & Andrea Kasinou AEM 2884

Supervisor :

George Stamoulis

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

Εγκρίνεται από την Επιτροπή Εξέτασης:

Επιβλέπων	**Γεώργιος Σταμούλης** Καθηγητής, Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, Πανεπιστήμιο Θεσσαλίας
Μέλος	**Μούντανος Ιωάννης** Αναπληρωτής Καθηγητής, Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, Πανεπιστήμιο Θεσσαλίας
Μέλος	**Ευμορφόπουλος Νέστωρ** Αναπληρωτής Καθηγητής, Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, Πανεπιστήμιο Θεσσαλίας

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ ΠΕΡΙ ΑΚΑΔΗΜΑΪΚΗΣ ΔΕΟΝΤΟΛΟΓΙΑΣ ΚΑΙ ΠΝΕΥΜΑΤΙΚΩΝ ΔΙΚΑΙΩΜΑΤΩΝ

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, δηλώνω ρητά ότι η παρούσα διπλωματική εργασία, καθώς και τα ηλεκτρονικά αρχεία και πηγαίοι κώδικες που αναπτύχθηκαν ή τροποποιήθηκαν στα πλαίσια αυτής της εργασίας, αποτελούν αποκλειστικά προϊόν προσωπικής μου εργασίας, δεν προσβάλλουν οποιασδήποτε μορφής δικαιώματα διανοητικής ιδιοκτησίας, προσωπικότητας και προσωπικών δεδομένων τρίτων, δεν περιέχουν έργα/εισφορές τρίτων για τα οποία απαιτείται άδεια των δημιουργών/δικαιούχων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής, οι πηγές δε που χρησιμοποιήθηκαν περιορίζονται στις βιβλιογραφικές αναφορές και μόνον και πληρούν τους κανόνες της επιστημονικής παράθεσης. Τα σημεία όπου έχω χρησιμοποιήσει ιδέες, κείμενο, αρχεία ή/και πηγές άλλων συγγραφέων αναφέρονται ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή. Δηλώνω επίσης ότι τα αποτελέσματα της εργασίας δεν έχουν χρησιμοποιηθεί για την απόκτηση άλλου πτυχίου. Αναλαμβάνω πλήρως, ατομικά και προσωπικά, όλες τις νομικές και διοικητικές συνέπειες που δύναται να προκύψουν στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής.

Οι Δηλών

Ανδρέας Χριστοφόρου & Ανδρέας Κάσινος

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

DISCLAIMER ON ACADEMIC ETHICS AND INTELLECTUAL PROPERTY RIGHTS

Being fully aware of the implications of copyright laws, I expressly state that this diploma thesis, as well as the electronic files and source codes developed or modified in the course of this thesis, are solely the product of my personal work and do not infringe any rights of intellectual property, personality and personal data of third parties, do not contain work / contributions of third parties for which the permission of the authors / beneficiaries is required and are not a product of partial or complete plagiarism, while the sources used are limited to the bibliographic references only and meet the rules of scientific citing. The points where I have used ideas, text, files and / or sources of other authors are clearly mentioned in the text with the appropriate citation and the relevant complete reference is included in the bibliographic references section. I also declare that the results of the work have not been used to obtain another degree. I fully, individually and personally undertake all legal and administrative consequences that may arise in the event that it is proven, in the course of time, that this thesis or part of it does not belong to me because it is a product of plagiarism.

The Declarant

Andreas Christoforou & Andreas Kasinos

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

Εργασία : Ασφάλεια Υλικού σε κυκλώματα FPGA και Ανάλυση και Ενδυνάμωση της Ασφάλειας του Υλικού σε συστήματα τεχνητής νοημοσύνης : Εξέλιξη και Προηγμένες επιθέσεις

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

Πίνακας περιεχομένων

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

ΠΕΡΙΛΗΨΗ

Η ασφάλεια υλικού σε συστήματα προγραμματιζόμενων πυλών πεδίου (FPGA) και συστήματα Τεχνητής Νοημοσύνης (AI) είναι ένας κρίσιμος τομέας έρευνας λόγω της αυξανόμενης εξάρτησης από αυτές τις τεχνολογίες σε διάφορες εφαρμογές. Τα συστήματα FPGA, γνωστά για την ευελιξία και τη δυνατότητα επαναδιαμόρφωσής τους, είναι λόγο αυτής ιδιότητας τους, επιρρεπή σε διάφορες απειλές ασφαλείας, όπως επιθέσεις πλευρικού καναλιού, αντίστροφη μηχανική και Trojans υλικού. Αυτά τα τρωτά σημεία πηγάζουν σε μεγάλο βαθμό από το λειτουργικό τους περιβάλλον και την ανοιχτή φύση της αρχιτεκτονικής τους, γεγονός που τα καθιστά στόχους για εκμετάλλευση τόσο σε στρατιωτικές όσο και σε εμπορικές εφαρμογές. Παράλληλα, η εργασία εξετάζει την εστίαση στην ασφάλεια υλικού, που μέχρι πρόσφατα δεν δινόταν τόσο μεγάλη σημασία αλλά και στα συστήματα τεχνητής νοημοσύνης, όπου η ταχεία εξέλιξη των μοντέλων μηχανικής μάθησης και η ανάπτυξή τους σε διάφορες πλατφόρμες απαιτούν ισχυρά μέτρα ασφαλείας. Για την ενίσχυση της ασφάλειας, προτείνεται από τη διεθνή βιβλιογραφία και την εμπειρία από την εφαρμογή, μια υβριδική προσέγγιση που συνδυάζει αρχές συν-σχεδιασμού υλικού-λογισμικού για FPGA και την εφαρμογή προηγμένων τεχνικών κρυπτογράφησης σε συστήματα τεχνητής νοημοσύνης. Υποστηρίζεται η ανάπτυξη ενός ενιαίου πλαισίου ασφαλείας που αντιμετωπίζει τόσο εγγενείς ευπάθειες όσο και αναδυόμενες απειλές, ενώ υπογραμμίζεται η σημασία της συνεχούς έρευνας και της προσαρμογής των μέτρων ασφαλείας ώστε να συμβαδίζει με το εξελισσόμενο τοπίο των επιθέσεων που βασίζονται σε υλικό και την αυξανόμενη πολυπλοκότητα των συστημάτων.

Λέξεις κλειδιά: *Ασφάλεια υλικού, μοντέλα απειλών, ολοκληρωμένα κυκλώματα, Πίνακες προγραμματιζόμενων πυλών πεδίου, Ολοκληρωμένα κυκλώματα για συγκεκριμένες εφαρμογές, Σύνθετες Προγραμματιζόμενες Λογικές Συσκευές, αρχιτεκτονική FPGA, Ασφάλεια κυκλωμάτων FPGA, Τεχνητή νοημοσύνη, λογισμικό.*

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

ABSTRACT

Hardware security in field programmable gate arrays (FPGAs) and Artificial Intelligence (AI) systems is a critical area of research due to the increasing reliance on these technologies in various applications. FPGA systems, known for their flexibility and reconfiguration, are therefore prone to various security threats, such as Side-channel attacks, reverse engineering, and hardware Trojans. These vulnerabilities stem largely from their operating environment and the open nature of their architecture, which makes them targets for exploitation in both military and commercial applications. At the same time, the paper examines the focus on hardware security, which until recently has not been given so much importance, but also on artificial intelligence systems, where the rapid evolution of machine learning models and their deployment on various platforms require strong security measures. To enhance security, a hybrid approach combining hardware-software co-design principles for FPGAs and the application of advanced encryption techniques in artificial intelligence systems is suggested by international literature and application experience. It advocates the development of a unified security framework that addresses both inherent vulnerabilities and emerging threats, while underlining the importance of continuous research and adaptation of security measures to keep pace with the evolving landscape of hardware-based attacks and increasing complexity of systems.

Keywords: *Hardware security, threat models, integrated circuits, Field Programmable Gate Arrays, Application Specific Integrated Circuits, Complex Programmable Logic Devices, FPGA architecture, FPGA Circuit Security, Artificial Intelligence, software.*

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ – ΣΧΗΜΑΤΩΝ

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

Εισαγωγή στην εκπόνηση της εργασίας

Πρόλογος

Η ασφάλεια των συστημάτων πληροφορικής με την ευρεία έννοια έχει καταστεί η πιο σημαντική απαίτηση για κάθε έργο ή εγκατάσταση πληροφοριακού συστήματος. Η ευρεία διασύνδεση, διαφόρων ψηφιακών συστημάτων, μέσω του διαδικτύου των πραγμάτων (IoT), και της χρήσης τεχνητής νοημοσύνης, έχει αυξήσει την προκλήσεις και τις απειλές από κυβερνοεπιθέσεις.

Μέχρι και πρόσφατα, είχε δοθεί μεγάλη προσοχή στην ασφάλεια στον κυβερνοχώρο με έμφαση στο λογισμικό. Γρήγορα, ωστόσο, έγινε αντιληπτό ότι η επίθεση στο υλικό ήταν πολύ πιο αποδοτική και κατά συνέπεια, η συνολική και ολοκληρωμένη ασφάλεια δεν μπορεί να επιτευχθεί χωρίς την προστασία του υλικού.

Τις τελευταίες δεκαετίες, η βιομηχανία ημιαγωγών γνώρισε σημαντική ανάπτυξη. Οι κρίσιμες σύγχρονες υποδομές όπως τα δίκτυα ηλεκτρικής ενέργειας, οι δημόσιες συγκοινωνίες και τα εθνικά αμυντικά συστήματα εξαρτώνται σε μεγάλο βαθμό από πολυάριθμα ολοκληρωμένα κυκλώματα (IC). Κατά συνέπεια, η ασφάλεια, η ποιότητα και η αξιοπιστία αυτών των υποδομών συνδέονται άμεσα με την αξιοπιστία των IC.

Ωστόσο, αυτή η αξιοπιστία απειλείται για διάφορους λόγους όπως το ότι πολλές νέες τεχνολογίες υλικού ενσωματώνονται σε υπολογιστικούς πόρους για επιτάχυνση χωρίς να τηρούνται οι αρχές σχεδιασμού ασφάλειας. Οι ακατάλληλες πρακτικές ασφαλείας, οι ελλιπείς έλεγχοι ασφαλείας και οι επιταχυνόμενοι κύκλοι παραγωγής μπορούν να οδηγήσουν στην αγνόηση της ευπάθειες υλικού. Ταυτόχρονα η ευρεία χρήση κινητών συσκευών, αισθητήρων και συσκευών ενεργοποίησης, οι οποίες είτε λόγου κόστους, είτε λόγω μεγέθους και δυνατοτήτων, δεν μπορούν να έχουν υψηλά επίπεδα ασφάλειας, σημαίνει ότι ακόμη και λίγες συσκευές που θα έχουν επηρεαστεί από απειλές ασφάλειας, θα μπορούν να διαταράξουν σοβαρά το ευρύ δίκτυο που αποτελούν μέρος του, δημιουργώντας προβλήματα σε επιχειρήσεις, κυβερνητικές λειτουργίες και στην εθνική άμυνα κρατών.

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

Ταυτόχρονα η παγκοσμιοποίηση της κατασκευής ημιαγωγών, η οποία είναι συγκεντρωμένη σε μερικές εταιρείες, εγκυμονεί κινδύνους από αναξιόπιστη κατασκευή και διανομή, συμπεριλαμβανομένης της πιθανότητας για εισαγωγές Trojan, κλωνοποίηση IP και προϊόντα απομίμησης. Καθώς τα τρωτά σημεία υλικού ανακαλύπτονται και αναφέρονται όλο και περισσότερο, η ανάγκη για αξιόπιστες συσκευές υλικού κερδίζει ολοένα και περισσότερη προσοχή. Σε αυτό το επίπεδο η ανάπτυξη αλγορίθμων μηχανικής μάθησης (ML) έχουν καταστεί ζωτικής σημασίας για την ασφάλεια του υλικού. Οι τεχνικές ML έχουν προσφέρει καινοτόμες λύσεις σε πολύπλοκα προβλήματα σε αυτόν τον τομέα, αλλά έχουν επίσης εισαγάγει νέα μοντέλα απειλών και ευπάθειες.

Αυτές οι διαδικασίες περιλαμβάνουν τη μάθηση (την απόκτηση πληροφοριών και τους κανόνες για τη χρήση της πληροφορίας), τη συλλογιστική (χρήση κανόνων για την εξαγωγή κατά προσέγγιση ή οριστικών συμπερασμάτων) και την αυτό-επιδιόρθωση. Το υλικό που χρησιμοποιείται στα συστήματα που λειτουργούν οι εφαρμογές της τεχνητής νοημοσύνης και της μηχανικής μάθησης, είναι εξίσου σημαντικό μέρος της διαδικασίας εφαρμογής.

Οι τρεις κύριες λύσεις υλικού για λειτουργίες τεχνητής νοημοσύνης είναι οι προγραμματιζόμενες συστοιχίες πύλης πεδίου (FPGA), οι μονάδες επεξεργασίας γραφικών (GPU) και οι κεντρικές μονάδες επεξεργασίας (CPU). Οι προγραμματιζόμενες συστοιχίες πύλης πεδίου (FPGA) είναι τύποι ολοκληρωμένων κυκλωμάτων. Η επαναπρογραμματιζόμενη και επαναδιαμορφώσιμη αρχιτεκτονική των FPGA, προσφέρει οφέλη στο διαρκώς μεταβαλλόμενο τοπίο της τεχνητής νοημοσύνης, επιτρέποντας στους σχεδιαστές να δοκιμάζουν γρήγορα νέους και ενημερωμένους αλγόριθμους. Αυτό προσφέρει ισχυρά ανταγωνιστικά πλεονεκτήματα όσον αφορά την επιτάχυνση του χρόνου στην αγορά και εξοικονόμηση κόστους, καθώς δεν απαιτεί την ανάπτυξη και την κυκλοφορία νέου υλικού.

Οι Προγραμματιζόμενες Συστοιχίες Πυλών Πεδίου (FPGA) είναι συσκευές ημιαγωγών που μπορούν να προγραμματιστούν ή να διαμορφωθούν εκ νέου από τον χρήστη μετά την κατασκευή. Σε αντίθεση με τους παραδοσιακούς μικροεπεξεργαστές, οι οποίοι έχουν σχεδιαστεί για να εκτελούν ένα συγκεκριμένο σύνολο εργασιών, τα FPGA

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

παρέχουν μια προσαρμόσιμη πλατφόρμα υλικού που μπορεί να προσαρμοστεί σε ένα ευρύ φάσμα εφαρμογών. Αυτή η ευελιξία τα καθιστά ιδιαίτερα πολύτιμα σε τομείς που απαιτούν εξειδικευμένες υπολογιστικές εργασίες.

Σκοπός της εργασίας

Ο σκοπός αυτής της εργασίας είναι να διεξαγάγει παρουσίαση της αρχιτεκτονικής των ολοκληρωμένων κυκλωμάτων και ειδικά των προγραμματιζόμενων πυλών πεδίου και μια ανάλυση των μέτρων ασφαλείας υλικού σε (FPGAs) καθώς και σε συστήματα Τεχνητής Νοημοσύνης (AI), εστιάζοντας στην κατανόηση της εξέλιξης των προκλήσεων ασφαλείας και των μηχανισμών αντιμετώπισης επιθέσεων με βάση προηγμένο υλικό και λογισμικό. Καθώς τα συστήματα FPGA και AI γίνονται ολοένα και πιο απαραίτητα και ευρέως χρησιμοποιούμενα σε ένα ευρύ φάσμα κρίσιμων εφαρμογών, από τις τηλεπικοινωνίες έως τα αυτόνομα συστήματα, οι ευπάθειες ασφαλείας τους αποτελούν σημαντικό κίνδυνο που πρέπει να αντιμετωπιστεί για την αποτροπή κακόβουλων εκμεταλλεύσεων που θα μπορούσαν να έχουν εκτεταμένες συνέπειες.

Η παρούσα εργασία έχει επίσης σαν στόχους:

- Παρουσίαση της αρχιτεκτονικής των ολοκληρωμένων κυκλωμάτων και ειδικά των προγραμματιζόμενων πυλών πεδίου
- Προσδιορισμός και ανάλυση τρωτών σημείων από την χρήση τους
- Ιστορική εξέλιξη και τις προοδευτικές βελτιώσεις στην ασφάλεια υλικού τόσο για συστήματα FPGA όσο και για συστήματα AI.
- Αντίκτυπος των προηγμένων επιθέσεων
- Μελλοντικές κατευθύνσεις και εφαρμογές

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

Δομή της εργασίας

Κεφάλαιο 1: Αυτό το κεφάλαιο διερευνά τις κρίσιμες παραμέτρους της ασφάλειας υλικού στα συστήματα πληροφοριών, τη σημασία της προστασίας των φυσικών στοιχείων αυτών των συστημάτων για τη διασφάλιση της συνολικής ακεραιότητας του συστήματος και της προστασίας των δεδομένων.

Κεφάλαιο 2: Το Κεφάλαιο 2 παρουσιάζει την εξέλιξη των ολοκληρωμένων κυκλωμάτων (ICs), παρακολουθώντας την ανάπτυξή τους από την αρχή έως τη σύγχρονη χρήση. Εξετάζει διαφορετικούς τύπους IC, όπως Field Programmable Gate Arrays (FPGAs), Application Specific Integrated Circuits (ASIC) και Complex Programmable Logic Devices (CPLDs), δίνοντας έμφαση στις μοναδικές αρχιτεκτονικές και τις λειτουργικές τους διαφορές.

Κεφάλαιο 3: Σε αυτό το κεφάλαιο παρουσιάζονται οι Προγραμματιζόμενες Συστοιχίες Πυλών Πεδίου, εξετάζει την εξέλιξη, την αρχιτεκτονική και τη σημασία της τεχνολογίας FPGA.

Κεφάλαιο 4: Το τέταρτο κεφάλαιο αναλύει συγκεκριμένες προκλήσεις ασφαλείας που σχετίζονται με τα κυκλώματα FPGA. Διερευνά διάφορες αρχές ασφάλειας, απειλές και φορείς επιθέσεων που επηρεάζουν τα FPGA. Επιπλέον, το κεφάλαιο εξετάζει μεθόδους και τεχνικές για τη βελτίωση της ασφάλειας των κυκλωμάτων FPGA, συμπεριλαμβανομένης της ενσωμάτωσης συστημάτων τεχνητής νοημοσύνης για την ενίσχυση της ασφάλειας υλικού έναντι προηγμένων απειλών και επιθέσεων.

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

ΚΕΦΑΛΑΙΟ 1. Ασφάλεια Υλικού

1.1 Εισαγωγή

Στον τομέα της κυβερνοασφάλειας, η ασφάλεια υλικού είναι ζωτικής σημασίας για την προστασία των συστημάτων πληροφοριών από μη εξουσιοδοτημένη πρόσβαση και ζημιά. Τα τρωτά σημεία υλικού μπορούν να χρησιμεύσουν ως πύλες για εκτεταμένες παραβιάσεις ασφάλειας, επηρεάζοντας όχι μόνο μεμονωμένους χρήστες αλλά και μεγάλες επιχειρήσεις και κυβερνητικούς φορείς. Οι ευπάθειες υλικού είναι εγγενείς αδυναμίες στα φυσικά στοιχεία ενός πληροφοριακού συστήματος που μπορούν να χρησιμοποιηθούν για να αποκτηθεί μη εξουσιοδοτημένη πρόσβαση ή να προκληθεί σκόπιμη βλάβη (Tehranipoor & Bhunia, 2019).

1.2 Σημασία της ασφάλειας υλικού στα πληροφοριακά συστήματα

Στο συνεχώς εξελισσόμενο τοπίο των πληροφοριακών συστημάτων και στην ψηφιακή επανάσταση, η διασύνδεση των πάντων έχει αναγάγει την ασφάλεια των συστημάτων πρωταρχικό μέλημα, καθώς πλέον όλοι οι τομείς των ανθρωπίνων δραστηριοτήτων, των καθημερινών εργασιών και αναγκών αλλά και των συστημάτων άμυνας και προστασίας, εξαρτώνται όλο και περισσότερο από διασυνδεμένα ψηφιακά συστήματα μέσω του διαδικτύου, που έχει αποδοθεί ο όρος το **διαδίκτυο των πάντων - internet of everything.** (DeNardis, 2020).

Ενώ η ασφάλεια λογισμικού συχνά βρίσκεται στο επίκεντρο, η ασφάλεια υλικού είναι εξίσου κρίσιμη και ασχολούνται με αυτή οι κατασκευαστές. Η ασφάλεια υλικού αναφέρεται στην προστασία των φυσικών συσκευών από απειλές που θα μπορούσαν να θέσουν σε κίνδυνο την ακεραιότητα, την εμπιστευτικότητα και τη διαθεσιμότητα των δεδομένων και των λειτουργιών που υποστηρίζουν (Guha, et al, 2021)

Ο πολλαπλασιασμός των συνδεδεμένων συσκευών, από προσωπικούς υπολογιστές έως συσκευές Internet of Things (IoT), έχει αυξήσει εκθετικά την επιφάνεια επίθεσης για κακόβουλους παράγοντες. Η ασφάλεια υλικού περιλαμβάνει διάφορα μέτρα που έχουν σχεδιαστεί για την προστασία των φυσικών στοιχείων αυτών των συστημάτων από

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

παραβιάσεις, κλοπές και άλλες μορφές φυσικής επίθεσης. Σε αντίθεση με την ασφάλεια λογισμικού, η οποία μπορεί συχνά να ενημερωθεί ή να διορθωθεί, τα τρωτά σημεία στο υλικό μπορεί να είναι πιο δύσκολο να αντιμετωπιστούν λόγω της εγγενούς μονιμότητάς τους μόλις κατασκευαστούν και τοποθετηθούν σε άλλες συσκευές ή μηχανήματα (Koylu, et al, 2023).

1.3 Μοντέλα απειλών

Physical Attacks - Φυσικές επιθέσεις: Αυτές περιλαμβάνουν άμεσες αλληλεπιδράσεις με τα στοιχεία υλικού, όπως κλοπή, παραβίαση ή καταστροφή και στα τρωτά σημεία του υλικού.

Τα τρωτά σημεία υλικού αναφέρονται σε αδυναμίες στα φυσικά στοιχεία ενός συστήματος υπολογιστή που μπορούν να αξιοποιηθούν για να θέσουν σε κίνδυνο την ασφάλεια. Αυτά τα τρωτά σημεία μπορεί να προέρχονται από ελαττώματα σχεδιασμού, κατασκευαστικά ελαττώματα ή ακατάλληλη εφαρμογή. Σε αντίθεση με τα τρωτά σημεία λογισμικού, τα οποία συχνά μπορούν να επιδιορθωθούν, οι ευπάθειες υλικού είναι πιο δύσκολο να αντιμετωπιστούν όταν η συσκευή χρησιμοποιείται (Tehranipoor & Bhunia, 2019).

Firmware Attacks - Επιθέσεις υλικολογισμικού: Το υλικολογισμικό, το οποίο ελέγχει τα στοιχεία υλικού πριν από την εκκίνηση του λειτουργικού συστήματος, μπορεί να στοχευτεί με κακόβουλη μορφή κώδικα (Qureshi & Newe, 2024).

Side-channel Attacks - Επιθέσεις πλευρικού καναλιού: Αυτές εκμεταλλεύονται τη φυσική υλοποίηση ενός κρυπτοσυστήματος, με στόχο την εξαγωγή ευαίσθητων δεδομένων αναλύοντας την κατανάλωση ενέργειας, τις ηλεκτρομαγνητικές διαρροές ή ακόμα και τον ήχο (Xu & Zhang 2020).

Supply Chain Attacks - Επιθέσεις εφοδιαστικής αλυσίδας: Τα εξαρτήματα μπορεί να τεθούν σε κίνδυνο κατά την κατασκευή ή τη μεταφορά, επιτρέποντας την εισαγωγή κερκόπορτων ή τρωτών σημείων στο σύστημα (Tehranipoor & Bhunia, 2019).

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

1.4 Σχεδίαση ασφάλειας υλικού

Οι σύγχρονοι επεξεργαστές και τα εξαρτήματα υλικού είναι συχνά εξοπλισμένα με ενσωματωμένα χαρακτηριστικά ασφαλείας. Αυτές μπορεί να περιλαμβάνουν μονάδες αξιόπιστης πλατφόρμας - Trusted Platform Modules (TPMs), μονάδες ασφαλείας υλικού - Hardware Security Modules (HSMs), και διαδικασίες ασφαλούς εκκίνησης - Secure boot processes.

Οι **μονάδες αξιόπιστης πλατφόρμας - Trusted Platform Modules TPMs**, παρέχουν ένα ασφαλές κρυπτογραφικό περιβάλλον, προστατεύοντας κλειδιά, κωδικούς πρόσβασης και άλλα κρίσιμα δεδομένα (Qureshi & Newe, 2024).

Βασικές λειτουργίες των TPMs είναι:

- Hardware-based Security - Ασφάλεια βασισμένη σε υλικό: Τα TPMs βασίζονται σε μηχανισμούς υλικού για να διασφαλίσουν την ακεραιότητα του συστήματος (Kim & Solomon, 2018).
- Cryptographic Operations - Κρυπτογραφικές λειτουργίες: Εκτελούν κρυπτογραφικές λειτουργίες όπως δημιουργία κλειδιού, κρυπτογράφηση, αποκρυπτογράφηση, ψηφιακές υπογραφές και ασφαλής αποθήκευση κλειδιών (Guha, et al, 2021)
- Platform Integrity - Ακεραιότητα πλατφόρμας: Τα TPMs μετρούν και επαληθεύουν την ακεραιότητα της πλατφόρμας αποθηκεύοντας τιμές κατακερματισμού των διαμορφώσεων συστήματος και επαληθεύοντάς τις κατά τη διάρκεια των διαδικασιών εκκίνησης (π.χ. Ασφαλής εκκίνηση).
- Secure Storage - Ασφαλής αποθήκευση: Αποθηκεύουν με ασφάλεια ευαίσθητα δεδομένα όπως κλειδιά κρυπτογράφησης, κωδικούς πρόσβασης και πιστοποιητικά (Qureshi & Newe, 2024).
- Remote Attestation - Απομακρυσμένη βεβαίωση: Τα TPMs μπορούν να δημιουργήσουν αναφορές που αποδεικνύουν την κατάσταση της πλατφόρμας σε απομακρυσμένες οντότητες, ενισχύοντας την εμπιστοσύνη στην απομακρυσμένη πρόσβαση και στις συναλλαγές.

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

Οι μονάδες ασφαλείας υλικού - Hardware Security Modules (HSMs) είναι εξειδικευμένες συσκευές σχεδιασμένες να διαχειρίζονται και να προστατεύουν κρυπτογραφικά κλειδιά σε ένα εξαιρετικά ασφαλές περιβάλλον (Maglaras & Kantzavelou, 2021).

Βασικές λειτουργίες των (HSMs) είναι:

- Security - Ασφάλεια: Τα HSMs παρέχουν ένα εξαιρετικά ασφαλές περιβάλλον για κρυπτογραφικές λειτουργίες, προστατεύοντας τόσο από φυσικές όσο και από λογικές επιθέσεις. Είναι συνήθως συσκευές ανθεκτικές σε παραβιάσεις που μπορούν να διαχειρίζονται, να επεξεργάζονται και να αποθηκεύουν με ασφάλεια κρυπτογραφικά κλειδιά.
- Compliance - Συμμόρφωση: Η χρήση HSMs βοηθά τις επιχειρήσεις και τους οργανισμούς, να πληρούν διάφορες απαιτήσεις συμμόρφωσης για το χειρισμό ευαίσθητων δεδομένων, όπως PCI-DSS, GDPR και HIPAA. Αυτές οι συσκευές διασφαλίζουν ότι τα κρυπτογραφικά κλειδιά δεν αφήνουν τα φυσικά όρια του υλικού σε μια χρησιμοποιήσιμη μορφή (Tehranipoor & Bhunia, 2019).
- Types - Τύποι: Υπάρχουν διάφοροι τύποι HSMs, συμπεριλαμβανομένων συσκευών συνδεδεμένων με USB, καρτών PCI και μονάδων συνδεδεμένων στο δίκτυο. Η επιλογή εξαρτάται από τις συγκεκριμένες ανάγκες της εφαρμογής και το περιβάλλον στο οποίο αναπτύσσονται (Kim & Solomon, 2018).
- Applications - Εφαρμογές: Τα HSMs χρησιμοποιούνται σε διάφορα σενάρια, όπως κρυπτογράφηση δεδομένων, ψηφιακή υπογραφή και ως βάση εμπιστοσύνης για διάφορες εφαρμογές ασφαλείας. Είναι εξαιρετικής σημασίας σε κλάδους όπως η χρηματοδότηση, η υγειονομική περίθαλψη και η δημόσια διακυβέρνηση, όπου η προστασία της ακεραιότητας και της εμπιστευτικότητας των δεδομένων είναι πρωταρχικής σημασίας.
- Key Management - Διαχείριση κλειδιών: Τα HSMs παρέχουν έναν ασφαλή τρόπο δημιουργίας, διαχείρισης και προστασίας κρυπτογραφικών κλειδιών σε όλο τον κύκλο ζωής τους. Υποστηρίζουν διάφορους τύπους κλειδιών και

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

κρυπτογραφικούς αλγόριθμους, ανάλογα με το μοντέλο HSM και τον κατασκευαστή (Qureshi & Newe, 2024).

Διαδικασίες ασφαλούς εκκίνησης - Secure boot processes. Η ασφαλής εκκίνηση είναι ένα πρότυπο ασφαλείας που αναπτύχθηκε για να διασφαλίσει ότι μια συσκευή εκκινείται χρησιμοποιώντας μόνο λογισμικό που είναι αξιόπιστο από τον Κατασκευαστή Γνήσιου Εξοπλισμού - Original Equipment Manufacturer (OEM). διασφαλίζει ότι μια συσκευή εκκινείται χρησιμοποιώντας μόνο λογισμικό που είναι αξιόπιστο από τον κατασκευαστή του υλικού, αποτρέποντας την εκτέλεση μη εξουσιοδοτημένου λογισμικού κατά τη διαδικασία εκκίνησης (Ross, 2020).

- Fundamentals level of Trust - θεμελιώδες επίπεδο εμπιστοσύνης: Η ασφαλής εκκίνηση δημιουργεί ένα θεμελιώδες επίπεδο εμπιστοσύνης σε επίπεδο υλικού, διασφαλίζοντας ότι μόνο αξιόπιστο λογισμικό μπορεί να εκτελεστεί κατά την εκκίνηση μιας συσκευής.
- Υλικολογισμικό - Firmware UEFI: Είναι ενσωματωμένο στο υλικολογισμικό - Unified Extensible Firmware Interface (UEFI), το οποίο είναι μια σύγχρονη έκδοση του BIOS. Το UEFI ελέγχει τις υπογραφές κάθε τμήματος λογισμικού εκκίνησης, συμπεριλαμβανομένων των προγραμμάτων οδήγησης υλικολογισμικού και του λειτουργικού συστήματος (Δρόσος, 2015).
- Key Management - Διαχείριση κλειδιών: Το Secure Boot χρησιμοποιεί κρυπτογραφικά κλειδιά για την επαλήθευση της γνησιότητας και της ακεραιότητας του λογισμικού εκκίνησης.
    - Platform Key - Κλειδί πλατφόρμας (PK) : Ελέγχει τα επιτρεπόμενα κλειδιά και μπορεί να εγγράψει ή να αντικαταστήσει το κλειδί ανταλλαγής κλειδιών (KEK).
    - Key Exchange Key - Κλειδί ανταλλαγής κλειδιών (KEK) : Χρησιμοποιείται για την εξουσιοδότηση κλειδιών και υπογραφών βάσης δεδομένων (Kim & Solomon, 2018).
    - Signature Database - Βάση δεδομένων υπογραφών (db) : Περιέχει τις υπογραφές εξουσιοδοτημένου λογισμικού.

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

- Forbidden Signatures Database (dbx) - Βάση δεδομένων απαγορευμένων υπογραφών (dbx) : Περιέχει υπογραφές γνωστού κακόβουλου λογισμικού ή μη εξουσιοδοτημένου λογισμικού.

- Verification Process - Διαδικασία επαλήθευσης: Κατά την εκκίνηση, το υλικολογισμικό UEFI ελέγχει κάθε τμήμα λογισμικού εκκίνησης σε σχέση με τις υπογραφές στα «db» και «dbx». Εάν η υπογραφή του λογισμικού ταιριάζει με μια υπογραφή στο «dbx», αποκλείεται. Εάν ταιριάζει με μια υπογραφή στο «db», επιτρέπεται να εκτελεστεί (Smith, 2020).

- Ασφάλεια Boot Loader: Μετά τη φάση UEFI, ο μηχανισμός ασφαλούς εκκίνησης ελέγχει το boot Loader, το οποίο είναι το πρώτο σημαντικό κομμάτι λογισμικού που φορτώνεται. Ο boot Loader, με τη σειρά του, θα επαληθεύσει την ακεραιότητα του φορτωτή του λειτουργικού συστήματος (Vacca, 2017).

- OS Protection - Προστασία λειτουργικού συστήματος: Μόλις επαληθευτεί και φορτωθεί ο bootloader, στη συνέχεια φορτώνει το λειτουργικό σύστημα με ασφαλή τρόπο, διασφαλίζοντας ότι το ίδιο το λειτουργικό σύστημα είναι η σωστή, αξιόπιστη έκδοση πριν από την εκτέλεση περαιτέρω διεργασιών.

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

ΚΕΦΑΛΑΙΟ 2. Ολοκληρωμένα κυκλώματα

2.1 Εισαγωγή στα ολοκληρωμένα κυκλώματα

Τα ολοκληρωμένα κυκλώματα - Integrated circuits (ICs), που συχνά αναφέρονται ως μικροτσίπ, είναι τα θεμελιώδη δομικά στοιχεία της σύγχρονης ηλεκτρονικής. Αυτά τα μικροσκοπικά στοιχεία φιλοξενούν μια σειρά ηλεκτρονικών εξαρτημάτων, συμπεριλαμβανομένων τρανζίστορ, αντιστάσεων και πυκνωτών, όλα κατασκευασμένα σε ένα μόνο κομμάτι ημιαγωγού υλικού, συνήθως πυριτίου. Αυτή η μικρογραφία επιτρέπει στα IC να εκτελούν πολύπλοκες ηλεκτρονικές λειτουργίες με αποτελεσματικότητα, καθώς είναι τοποθετημένα στις περισσότερες συσκευές που χρησιμοποιούνται καθημερινά (Tehranipoor & Bhunia, 2019).

2.2 Ιστορικό των ολοκληρωμένων κυκλωμάτων

Η εφεύρεση του τρανζίστορ το 1947 σηματοδότησε μια αλλαγή στα ηλεκτρονικά. Ωστόσο, η γέννηση του IC μπορεί να εντοπιστεί στα τέλη της δεκαετίας του 1950, όπου το όραμα επιστημόνων όπως του Jack Kilby στην Texas Instruments και του Robert Noyce στην Fairchild Semiconductor, δημιούργησε την ιδέα, ανεξάρτητα ο ένας από τον άλλο, την ενσωμάτωση πολλαπλών τρανζίστορ σε ένα μόνο τσιπ. Αυτά τα πρώτα IC, που χρησιμοποιούν τεχνολογία διπολικών τρανζίστορ, περιείχαν περιορισμένο αριθμό τρανζίστορ. Παρόλα αυτά, έθεσαν τις βάσεις για τις επαναστατικές προόδους που ακολούθησαν (Γκορίλας, 2022).

Η ανάπτυξη της φωτολιθογραφίας και των τεχνικών κλιμάκωσης αποδείχθηκε καθοριστική στην εξέλιξη των IC. Η φωτολιθογραφία επέτρεψε την ακριβή διαμόρφωση των κυκλωμάτων στο υπόστρωμα πυριτίου, ενώ η κλιμάκωση επέτρεψε τη συνεχή μείωση του μεγέθους του τρανζίστορ. Αυτό το φαινόμενο σμίκρυνσης, που συχνά αναφέρεται ως Νόμος του Μουρ, έχει οδηγήσει στην ενσωμάτωση δισεκατομμυρίων τρανζίστορ σε ένα μόνο τσιπ, επιτρέποντας τη δημιουργία όλο και πιο εξελιγμένων και ισχυρών συσκευών (Ryan, 2010).

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

2.3 Τύποι ολοκληρωμένων κυκλωμάτων

Οι βασικές κατηγορίες των ολοκληρωμένων κυκλωμάτων είναι:

Ψηφιακά Ολοκληρωμένα Κυκλώματα - Digital Integrated Circuits (IC): Αυτά τα κυκλώματα επεξεργάζονται πληροφορίες με τη μορφή δυαδικών ψηφίων (0 και 1). Παραδείγματα περιλαμβάνουν μικροεπεξεργαστές, τσιπ μνήμης και λογικές πύλες, που αποτελούν τον πυρήνα ψηφιακών συσκευών όπως οι υπολογιστές, ψηφιακά συστήματα, smartphones και τα τελευταία χρόνια κάθε συσκευής που έχει μετατραπεί σε «ψηφιακή», από απλές κάμερες και αισθητήρες, οικιακές συσκευές, μέχρι εξελιγμένες βιομηχανικές συσκευές, αυτοκίνητα, αεροπλάνα κ.λπ. (Δρόσος, 2015).

Αναλογικά ολοκληρωμένα κυκλώματα - (IC): Λειτουργώντας με συνεχή αναλογικά σήματα που αντιπροσωπεύουν φυσικά μεγέθη όπως τάση ή ρεύμα, αυτά τα IC είναι ζωτικής σημασίας για τη διασύνδεση με τον πραγματικό κόσμο. Παραδείγματα περιλαμβάνουν λειτουργικούς ενισχυτές, μετατροπείς αναλογικού σε ψηφιακό (ADC) και μετατροπείς ψηφιακού σε αναλογικό (DAC), που χρησιμοποιούνται ευρέως σε εφαρμογές αισθητήρων και επεξεργασία σήματος.

Ολοκληρωμένα κυκλώματα μικτού σήματος (IC): Γεφυρώνοντας το χάσμα μεταξύ του ψηφιακού και αναλογικού τομέα, τα IC μικτού σήματος συνδυάζουν και τις δύο λειτουργίες σε ένα μόνο τσιπ. Αυτή η ενοποίηση επιτρέπει την αποτελεσματική αλληλεπίδραση μεταξύ των δύο κόσμων, την εύρεση εφαρμογών σε τηλεπικοινωνιακές συσκευές και στις διεπαφές αισθητήρων (Martin, 2018).

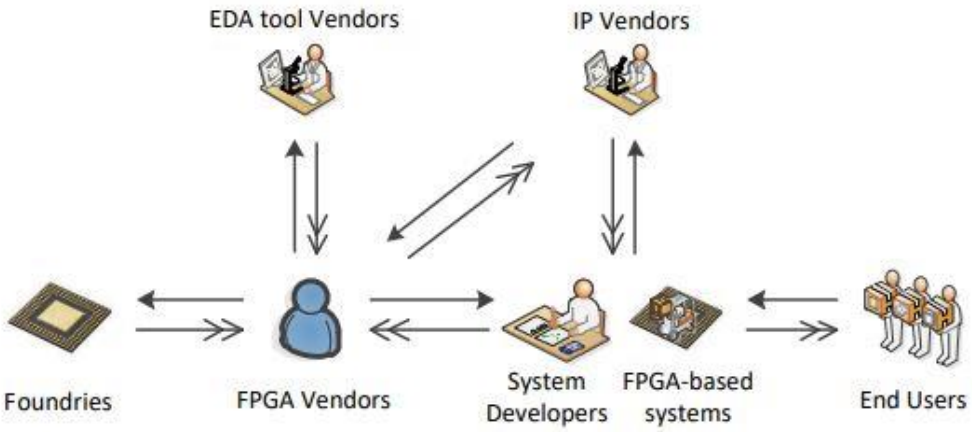
2.4 Αρχιτεκτονικές ολοκληρωμένων κυκλωμάτων

2.4.1 Πίνακες προγραμματιζόμενων πυλών πεδίου (FPGA)

Η συστοιχία πύλης με δυνατότητα προγραμματισμού πεδίου - Field-programmable gate array (FPGA), είναι ένας ευέλικτος τύπος τσιπ που μπορεί να διαμορφωθεί μετά την κατασκευή τους. Αυτή η ευελιξία τα καθιστά δημοφιλή σε διάφορες βιομηχανίες, από τις αυτοκινητοβιομηχανίες, την κατασκευή ιατρικών συσκευών, στρατιωτικό

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

εξοπλισμό και ηλεκτρονικά είδη ευρείας κατανάλωσης. Ο επαναπρογραμματισμός τους τα διαφοροποιεί από τα Ενσωματωμένα Κυκλώματα Ειδικής Εφαρμογής (ASIC), τα οποία είναι ειδικά κατασκευασμένα για έναν και μόνο σκοπό. Ωστόσο, αυτό ακριβώς το πλεονέκτημα εισάγει μοναδικές προκλήσεις όσον αφορά την ασφάλεια και την εμπιστοσύνη εντός της αλυσίδας εφοδιασμού και της διαδικασίας σχεδιασμού του FPGA (Zhang & Qu, 2019).



Σχήμα 1. Οι ροές προσφοράς και ζήτησης στην αγορά συστημάτων που βασίζονται σε FPGA. (Zhang & Qu, 2019).

Ένα FPGA αποτελείται από ένα σύνολο προγραμματιζόμενων λογικών μπλοκ και μια ιεραρχία αναδιαμορφώσιμων διασυνδέσεων. Τα λογικά μπλοκ συνδέονται μέσω των αναδιαμορφώσιμων διασυνδέσεων για να διαμορφωθούν για διαφορετικές λειτουργίες (Zhang & Qu, 2019).

2.4.2 Ολοκληρωμένα κυκλώματα για συγκεκριμένες εφαρμογές (ASIC)

Τα ASIC είναι ειδικά σχεδιασμένα για μια συγκεκριμένη εφαρμογή ή προϊόν. Σε αντίθεση με τα FPGA, τα οποία είναι επαναπρογραμματιζόμενα, τα ASIC είναι συσκευές σταθερής λειτουργίας που έχουν σχεδιαστεί για να εκτελούν συγκεκριμένες εργασίες.

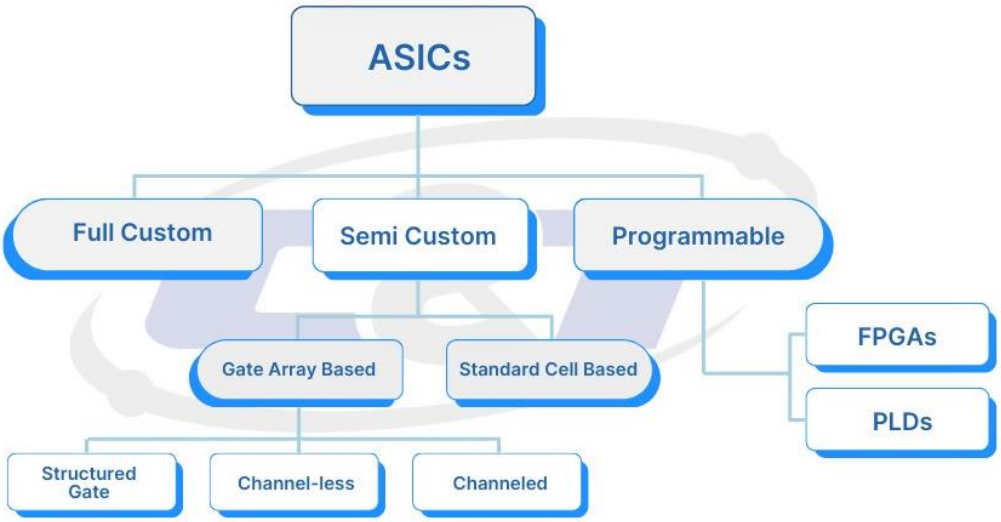
Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

Ένα Ενσωματωμένο Κύκλωμα Ειδικής Εφαρμογής Application-Specific Integrated Circuit (ASIC), είναι ακριβώς αυτό που υποδηλώνει το όνομά του: ένα τσιπ που έχει σχεδιαστεί και κατασκευαστεί για μια συγκεκριμένη χρήση και όχι για μια γενική. Αυτά τα ειδικά κατασκευασμένα κυκλώματα μπορούν να χειριστούν λειτουργίες που είναι αναλογικές, ψηφιακές ή ακόμα και συνδυασμός και των δύο, καθιστώντας τα ιδανικά για εφαρμογές μεγάλου όγκου και υψηλής απόδοσης. Παραδοσιακά, οι μηχανικοί βασίζονταν σε διαγράμματα κυκλωμάτων για να περιγράψουν τη λειτουργικότητα ενός ASIC. Ωστόσο, με τη διαρκώς αυξανόμενη πολυπλοκότητα αυτών των κυκλωμάτων, οι γλώσσες περιγραφής υλικού (HDL) όπως η Verilog και η VHDL έχουν γίνει η προτιμώμενη μέθοδος (Tehranipoor & Bhunia, 2019).

Η διαδικασία σχεδιασμού και κατασκευής ενός ASIC περιλαμβάνει διάφορα στάδια, συμπεριλαμβανομένου του ορισμού προδιαγραφών, του αρχιτεκτονικού σχεδιασμού, του λειτουργικού σχεδιασμού και της φυσικής υλοποίησης. Κάθε ASIC είναι μοναδικά κατασκευασμένο για να εκτελεί τη συγκεκριμένη λειτουργία του πιο αποτελεσματικά από ότι μια συσκευή γενικής χρήσης.

- Design Flow - Ροή σχεδίασης: Η ροή σχεδίασης των ASIC ξεκινά με τη δημιουργία μιας προδιαγραφής που περιγράφει τις επιθυμητές παραμέτρους λειτουργικότητας και απόδοσης. Ακολουθεί η ανάπτυξη της αρχιτεκτονικής τσιπ, η οποία χαρτογραφεί τη δομή και την ολοκλήρωση του κυκλώματος.
- Fabrication Techniques - Τεχνικές Κατασκευής: Η κατασκευή ASIC χρησιμοποιεί φωτολιθογραφία για να χαράξει σχέδια κυκλωμάτων σε τσιπ πυριτίου. Αυτή η διαδικασία έχει εξελιχθεί από διεργασίες μαζικής CMOS σε προηγμένα σχέδια FinFET, τα οποία είναι απαραίτητα για την ανάπτυξη εξαιρετικά μικρών ASIC υψηλής απόδοσης.

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250



Σχήμα 2. Τύποι Ολοκληρωμένων Κυκλωμάτων Ειδικής Εφαρμογής (ASIC).

Η δομή περιλαμβάνει κατηγορίες[1] όπως Full Custom, Semi Custom και Programmable. Η κατηγορία Semi Custom χωρίζεται περαιτέρω σε Gate Array Based και Standard Cell Based.

Η κατηγορία Προγραμματιζόμενα περιλαμβάνει FPGA (Προγραμματιζόμενοι Πυλώνες Πυλώνων Πεδίου) και PLD (Προγραμματιζόμενες Λογικές Συσκευές).

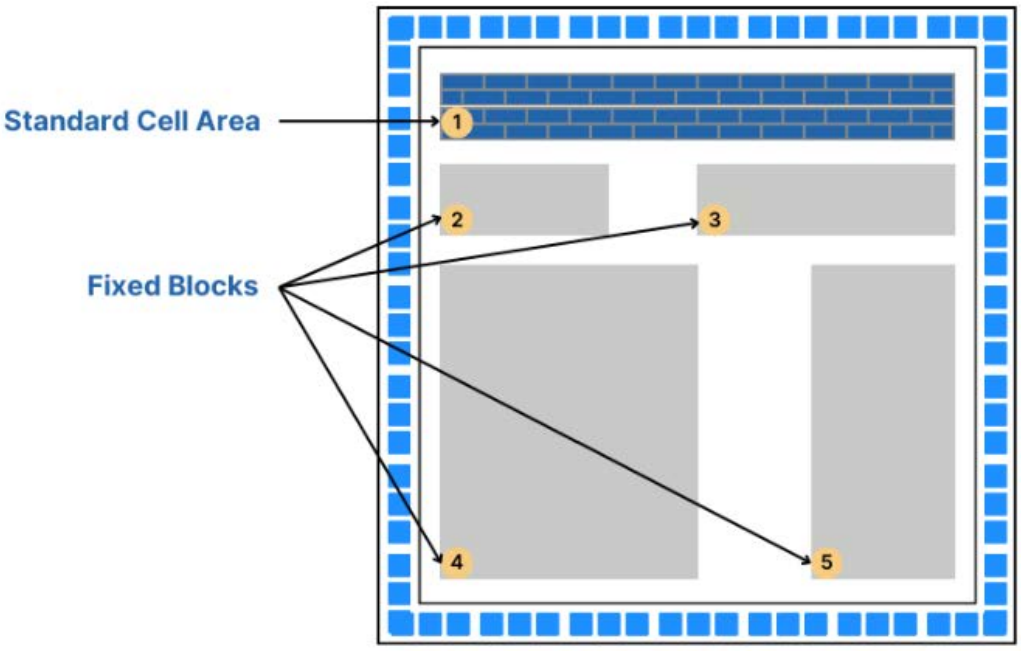
Πλήρως προσαρμοσμένα - Full Custom ASICs: Αυτά τα ASIC έχουν σχεδιαστεί από την αρχή για μια συγκεκριμένη εφαρμογή. Κάθε πτυχή του τσιπ, από τις λογικές πύλες έως τη διάταξη του κυκλώματος, είναι προσαρμοσμένη για να πληροί τις ακριβείς απαιτήσεις της προβλεπόμενης εφαρμογής. Τα πλήρως προσαρμοσμένα ASIC προσφέρουν την υψηλότερη απόδοση και τη χαμηλότερη κατανάλωση ενέργειας, αλλά είναι επίσης τα πιο ακριβά και χρονοβόρα στη σχεδίαση και την κατασκευή τους. Συνήθως χρησιμοποιούνται σε εφαρμογές όπου ο όγκος είναι αρκετά υψηλός ή οι απαιτήσεις απόδοσης είναι αρκετά αυστηρές ώστε να δικαιολογούν το πρόσθετο κόστος και προσπάθεια.

[1] https://www.candtsolution.com/news_events-detail/what-is-asic-application-specific-integrated-circuits/ what is ASIC? Application Specific Integrated Circuits. (Ανάκτηση 10.6.2024)

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

Ημι-προσαρμοσμένα - Semi-Custom ASICs: Τα ημι-προσαρμοσμένα ASIC, συμπεριλαμβανομένων των ASIC τυπικών κυψελών και των ASIC συστοιχιών πύλης, προσφέρουν μια ισορροπία μεταξύ προσαρμογής και κόστους.

- **Τυπικά ASIC κυψελών - Standard Cell ASICs:** Στον τυπικό σχεδιασμό ASIC που βασίζεται σε κυψέλες, μια τυπική βιβλιοθήκη κυψελών περιέχει προσχεδιασμένα λογικά κελιά όπως πύλες AND, πύλες OR, πολυπλέκτης και flip-flops. Αυτά τα κύτταρα είναι τυποποιημένα και αποθηκεύονται για χρήση σε σχέδια τσιπ ASIC. Το τσιπ ASIC[2] τυπικά περιλαμβάνει μια τυπική περιοχή κυψέλης ή ένα ευέλικτο μπλοκ, που αποτελείται από αυτά τα κελιά διατεταγμένα σε σειρές και μπορεί επίσης να ενσωματώνει μέγα κελιά όπως μικροελεγκτές ή μικροεπεξεργαστές, που αναφέρονται ως μέγα συναρτήσεις, μακροεντολές σε επίπεδο συστήματος ή σταθερά μπλοκ/λειτουργικά τυπικά μπλοκ. Τα στρώματα μάσκας της τυπικής κυψέλης της ASIC είναι προσαρμόσιμα, επιτρέποντας στους σχεδιαστές να τοποθετούν τα τυπικά κελιά στρατηγικά κατά μήκος της μήτρας, οδηγώντας σε αποτελεσματική χρήση και βελτιστοποιημένη απόδοση, μια σχεδιαστική προσέγγιση γνωστή και ως C-BIC.

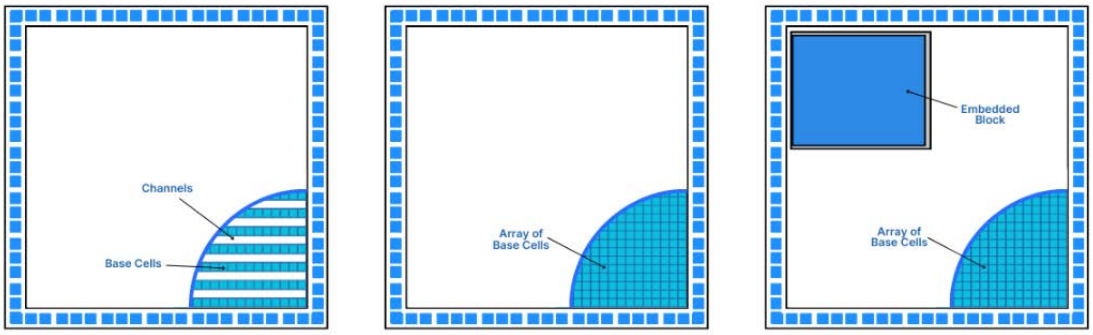


Σχήμα 3. Standard Cell ASICs

[2] https://www.candtsolution.com/news_events-detail/what-is-asic-application-specific-integrated-circuits/ what is ASIC? Application Specific Integrated Circuits. (Ανάκτηση 10.6.2024)

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

- **Συστοιχία πύλης ASIC - Gate Array ASIC:** Τα ASIC Gate Array είναι ένας τύπος ημι-προσαρμοσμένου ASIC με προκαθορισμένα τρανζίστορ στη γκοφρέτα πυριτίου, όπου ο σχεδιαστής δεν μπορεί να αλλάξει την τοποθέτηση του τρανζίστορ, αλλά μπορεί να αλλάξει τις διασυνδέσεις μεταξύ τους χρησιμοποιώντας τα αρχικά μεταλλικά στρώματα της μήτρας. Ο σχεδιασμός χρησιμοποιεί μια βιβλιοθήκη πίνακα πυλών για διαμόρφωση, που συνήθως καταλήγει σε Channeled - Συστοιχίες πυλών με κανάλια, Channel-less - χωρίς κανάλια, ή Structured Gate Arrays - δομημένες πύλες.



Σχήμα 4. Διαμόρφωση - Channeled, Channel-less, or Structured Gate Arrays

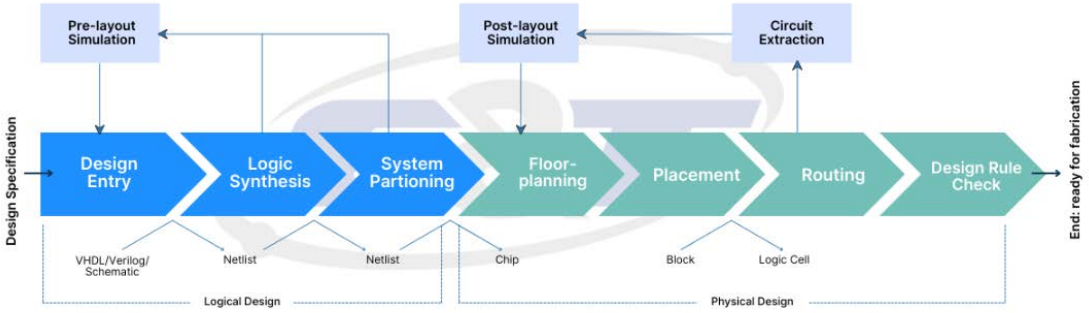
Συστοιχίες πύλης καναλιών - Channeled Gate Arrays: Χρησιμοποιεί προκαθορισμένα κανάλια δρομολόγησης μεταξύ λογικών κυψελών για συνδέσεις καλωδίων, κατάλληλα για τυποποιημένα σχέδια που χρειάζονται ευέλικτες διαδρομές διασύνδεσης.

Συστοιχίες πύλης χωρίς κανάλια - Channel-less Gate Arrays: Δεν έχουν προκαθορισμένα κανάλια δρομολόγησης, επιτρέποντας πιο συμπαγή σχέδια τοποθετώντας διασυνδέσεις απευθείας πάνω από κυψέλες, βελτιώνοντας την πυκνότητα του τσιπ.

Δομημένες πύλες - Structured Gate Arrays: Συνδυασμός με προκαθορισμένα λογικά μπλοκ και με προσαρμόσιμα επίπεδα διασύνδεσης, προσφέροντας ισορροπία μεταξύ ευελιξίας σχεδιασμού και ταχείας ανάπτυξης.

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

Προγραμματιζόμενα - Programmable ASICs: Προγραμματιζόμενες λογικές συσκευές (PLD): ένας τύπος ψηφιακού ολοκληρωμένου κυκλώματος που μπορεί να προγραμματιστεί για να εκτελεί ένα ευρύ φάσμα λογικών λειτουργιών. Χρησιμοποιούνται σε διάφορες εφαρμογές για την υλοποίηση προσαρμοσμένων λογικών κυκλωμάτων χωρίς την ανάγκη προσαρμοσμένης κατασκευής ημιαγωγών.



Σχήμα 5. Ροή σχεδίασης ολοκληρωμένου κυκλώματος ειδικών εφαρμογών (ASIC). (https://www.candtsolution.com/news_events-detail/what-is-asic-application-specific-integrated-circuits/)

Πλεονεκτήματα των ASIC

Υψηλή απόδοση : Τα ASIC έχουν σχεδιαστεί ειδικά για μια συγκεκριμένη εφαρμογή, γεγονός που τους επιτρέπει να υπερέχουν σε απόδοση για τη συγκεκριμένη περίπτωση χρήσης. Αυτός ο εστιασμένος σχεδιασμός οδηγεί συχνά σε μεγαλύτερες ταχύτητες επεξεργασίας και πιο αποτελεσματική εκτέλεση εργασιών σε σύγκριση με τα ολοκληρωμένα κυκλώματα πολλαπλών χρήσεων.

Χαμηλότερη κατανάλωση ενέργειας : Λόγω της βελτιστοποίησης για συγκεκριμένες εφαρμογές, τα ASIC συνήθως απαιτούν λιγότερη ισχύ από τα αντίστοιχα γενικής χρήσης όταν εκτελούν τις ίδιες εργασίες. Αυτό τα καθιστά ιδανική επιλογή για εφαρμογές ευαίσθητες στην ενέργεια, όπως κινητές συσκευές και ενσωματωμένα συστήματα (Tehranipoor & Bhunia, 2019).

Μικρότερο μέγεθος : Τα ASIC μπορούν να ενοποιήσουν πολλαπλές λειτουργίες και στοιχεία σε ένα ενιαίο τσιπ. Αυτή η ενσωμάτωση επιτρέπει πολύ μικρότερες και πιο

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

συμπαγείς συσκευές, κάτι που είναι ζωτικής σημασίας σε βιομηχανίες όπου ο χώρος είναι κορυφαίος, όπως στην τεχνολογία φορητών συσκευών ή στα smartphones.

Μειωμένο κόστος ανά μονάδα : Αν και το αρχικό κόστος για το σχεδιασμό και την ανάπτυξη ενός ASIC μπορεί να είναι αρκετά υψηλό, το κόστος ανά μονάδα κατά τη μαζική παραγωγή είναι συχνά χαμηλότερο σε σύγκριση με τα IC γενικής χρήσης. Αυτό καθιστά τα ASIC οικονομικά αποδοτικά για κατασκευή μεγάλης κλίμακας, αφού το κόστος ανάπτυξης αποσβεστεί σε πολλές μονάδες (Zhang & Qu, 2019).

Υψηλότερη ασφάλεια : Η προσαρμοσμένη φύση των ASIC προσθέτει ένα επίπεδο ασφάλειας, επειδή είναι πιο δύσκολο για κακόβουλες οντότητες να αναστρέψει το υλικό. Αυτό το χαρακτηριστικό είναι ιδιαίτερα πολύτιμο σε τομείς όπως οι τράπεζες και οι τηλεπικοινωνίες, όπου η ασφάλεια είναι πρωταρχικής σημασίας.

Λιγότερα εξαρτήματα : Με την ενσωμάτωση πολλαπλών λειτουργιών σε ένα ενιαίο τσιπ, τα ASIC μειώνουν την ανάγκη για πρόσθετα εξαρτήματα. Αυτή η απλοποίηση όχι μόνο μειώνει το κόστος αλλά αυξάνει και την αξιοπιστία της συσκευής μειώνοντας τα σημεία αστοχίας (Tu, et al, 2024).

Τα ASIC είναι διαδεδομένα σε διάφορες εφαρμογές όπου συγκεκριμένες, επαναλαμβανόμενες εργασίες πρέπει να εκτελούνται με βέλτιστη απόδοση.

- Τηλεπικοινωνίες: Στις τηλεπικοινωνίες, τα ASIC χρησιμοποιούνται για επεξεργασία σήματος, δρομολόγηση δικτύου και κρυπτογράφηση δεδομένων. Ενισχύουν την ταχύτητα και την ασφάλεια της μετάδοσης δεδομένων στα δίκτυα.
- Καταναλωτικά Ηλεκτρονικά: Οι καταναλωτικές συσκευές όπως smartphones, κάμερες και συστήματα οικιακής ψυχαγωγίας χρησιμοποιούν ASIC για επεξεργασία εικόνας, επεξεργασία ήχου και βελτίωση συνδεσιμότητας (Zhang & Qu, 2019).
- Εξόρυξη κρυπτονομισμάτων: Τα ASIC χρησιμοποιούνται στην εξόρυξη κρυπτονομισμάτων για να χειρίζονται τον αλγόριθμο κατακερματισμού SHA-

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

256 πολύ πιο γρήγορα από οποιονδήποτε επεξεργαστή γενικής χρήσης. Η εξόρυξη Bitcoin είναι η διαδικασία με την οποία τίθενται σε κυκλοφορία νέα Bitcoin και είναι επίσης ένα κρίσιμο στοιχείο της συντήρησης και ανάπτυξης του καθολικού blockchain. Ισχυρά ASIC (Application Specific Integrated Circuits) χρησιμοποιούνται για εξόρυξη bitcoin. Για παράδειγμα, το WhatsMiner M30S++ παρέχει 112 TH/s (λειτουργίες κατακερματισμού Tera ανά δευτερόλεπτο) (Marinescu, 2022).

Η ανάπτυξη της τεχνολογίας ASIC οφείλεται στην ανάγκη για μεγαλύτερη λειτουργικότητα, μικρότερο μέγεθος και υψηλότερη υπολογιστική ισχύ.

- Ενσωμάτωση δυνατοτήτων AI: Τα σύγχρονα ASIC ενσωματώνουν λειτουργίες τεχνητής νοημοσύνης για να βελτιώσουν τις διαδικασίες λήψης αποφάσεων και τις εργασίες μηχανικής μάθησης απευθείας στο τσιπ.
- Quantum-dot Cellular Automata (QCA): Αυτή η αναδυόμενη τεχνολογία υπόσχεται να μειώσει την κατανάλωση ενέργειας και το φυσικό αποτύπωμα των ASIC χρησιμοποιώντας κβαντικές κουκκίδες για την εκτέλεση δυαδικών υπολογισμών (Qadir, et al, 2013).

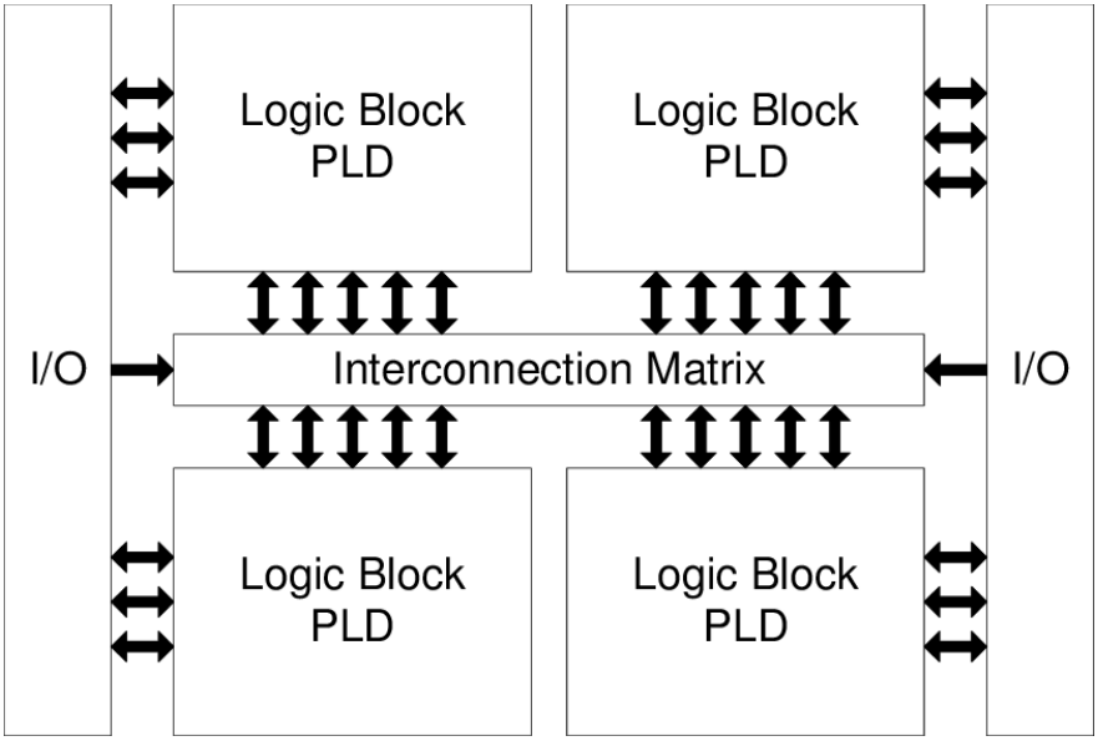
Το 2015, η Google ανέπτυξε το πρώτο προσαρμοσμένο ολοκληρωμένο κύκλωμα συγκεκριμένης εφαρμογής (ASIC) για την υποδομή cloud computing, μια μονάδα επεξεργασίας - Tensor Processing Unit[3] (TPU). Τα TPUs σχεδιάστηκαν για εφαρμογές μηχανικής μάθησης (ML), ιδίως για στάδια συμπερασμάτων βαθιών νευρωνικών δικτύων (DNNs). Τα TPU ακολουθήθηκαν από το Microsoft Catapult, ένα Field-Programable Gate Array (FPGS), το ASIC της Nervana που ονομάζεται CREST και το Pixel Visual Core της Google (Marinescu, 2022).

[3] Τα Tensor Processing Units (TPU) είναι τα προσαρμοσμένα ανεπτυγμένα ολοκληρωμένα κυκλώματα (ASIC) της Google για συγκεκριμένες εφαρμογές που χρησιμοποιούνται για την επιτάχυνση του φόρτου εργασίας μηχανικής εκμάθησης. Το Cloud TPU είναι μια υπηρεσία ιστού που καθιστά διαθέσιμες τις TPU ως κλιμακωτούς υπολογιστικούς πόρους στο Google Cloud. (Ανάκτηση 12.6.2024 από https://cloud.google.com/tpu/docs/intro-to-tpu).

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

2.4.3 Σύνθετες Προγραμματιζόμενες Λογικές Συσκευές (CPLD)

Complex Programmable Logic Devices (CPLD) είναι εξαιρετικά ευέλικτα εργαλεία σχεδιασμού ψηφιακών κυκλωμάτων που διευκολύνουν την ταχεία δημιουργία πρωτοτύπων και επιτρέπουν την υλοποίηση λογικών λειτουργιών σε υψηλές ταχύτητες. Προσφέρουν ένα μείγμα της προγραμματισιμότητας των Προγραμματιζόμενων Λογικών Συσκευών (PLD) με την υψηλότερη πολυπλοκότητα και ικανότητα των Προγραμματιζόμενων Συστοιχιών Πυλών Πεδίου (FPGA). Τα CPLD αποτελούνται από πολλαπλά προγραμματιζόμενα λογικά στοιχεία που διασυνδέονται με μια ευέλικτη αρχιτεκτονική, καθιστώντας τα ιδανικά για ψηφιακές εφαρμογές υψηλής ταχύτητας (Guha, et al, 2021)



Σχήμα 6. Complex Programmable Logic Device-CPLD.

Αρχιτεκτονική CPLD

Τα CPLD διαθέτουν μια μοναδική αρχιτεκτονική που περιλαμβάνει ένα σύνολο προγραμματιζόμενων λογικών μπλοκ, πόρων διασύνδεσης και μια σειρά μπλοκ εισόδου/εξόδου - input/output blocks (IOBs). Κάθε λογικό μπλοκ μπορεί να

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

διαμορφωθεί για να εκτελεί μια ποικιλία λογικών λειτουργιών, ενώ οι διασυνδέσεις επιτρέπουν σε αυτά τα μπλοκ να συνδέονται σε πολλές διαμορφώσεις, προσαρμοσμένες σε διαφορετικές απαιτήσεις σχεδιασμού (Tehranipoor & Bhunia, 2019).

Logic Blocks - Λογικά μπλοκ: Τα λογικά μπλοκ στα CPLD περιέχουν έναν σταθερό αριθμό μακροκυψελών, τα οποία περιλαμβάνουν λογικές πύλες και στοιχεία μνήμης. Κάθε macrocell μπορεί να προγραμματιστεί ξεχωριστά για να εκτελεί σύνθετες συνδυαστικές και διαδοχικές λογικές λειτουργίες (Brown & Rose, 2012).

Interconnection Resources - Πόροι διασύνδεσης: Η ευελιξία των CPLD προέρχεται από τους εκτεταμένους πόρους διασύνδεσής τους, οι οποίοι μπορούν να προγραμματιστούν για να δημιουργήσουν σχεδόν οποιοδήποτε επιθυμητό δίκτυο λογικών μπλοκ, επιτρέποντας την προσαρμογή των λογικών οδών σύμφωνα με συγκεκριμένες ανάγκες εφαρμογής (Farooq & Mehrez, 2015).

Input/Output Blocks (IOBs) - Μπλοκ εισόδου/εξόδου: Τα IOB χρησιμεύουν ως διεπαφή επικοινωνίας μεταξύ του CPLD και του εξωτερικού κυκλώματος. Είναι ζωτικής σημασίας για την παροχή της ευελιξίας και της απόδοσης που αναμένεται από ένα CPLD, που φιλοξενεί ένα ευρύ φάσμα προτύπων σήματος.

Εφαρμογές CPLD

Τα CPLD προσφέρουν έναν συνδυασμό υψηλής ταχύτητας και λογικής πυκνότητας, καθιστώντας τα κατάλληλα για ένα ευρύ φάσμα ψηφιακών εφαρμογών. Η ανάπτυξή τους προήλθε από την ανάγκη να ενοποιηθούν πολύπλοκα κυκλώματα, που προηγουμένως είχαν εφαρμοστεί με χρήση πολλαπλών απλών προγραμματιζόμενων λογικών συσκευών (SPLD), σε ένα ενιαίο, πιο αποτελεσματικό CPLD.

Τα CPLD επιδεικνύουν εξαιρετική ικανότητα στην υλοποίηση περίπλοκων σχεδίων όπως κυκλώματα επεξεργασίας γραφικών, ελεγκτές δικτύου και ελεγκτές κρυφής μνήμης. Είναι ιδιαίτερα ικανοί στο χειρισμό κυκλωμάτων με υψηλή συγκέντρωση AND/OR gates, ενώ απαιτούν μικρότερο αριθμό flip-flops (Guha, et al, 2021)

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

Ένα σημαντικό πλεονέκτημα των CPLD έγκειται στην εγγενή επαναπρογραμματισμό τους. Αυτή η δυνατότητα επιτρέπει την πραγματοποίηση τροποποιήσεων σχεδίασης χωρίς την ανάγκη αντικατάστασης υλικού. Επιπλέον, ορισμένα CPLD διαθέτουν δυνατότητα προγραμματισμού εντός του συστήματος, επιτρέποντας προσαρμογές υλικού σε πραγματικό χρόνο χωρίς αποσυναρμολόγηση του συστήματος. Αυτή η ευελιξία καθιστά τα CPLD μια εξαιρετικά ελκυστική επιλογή για σχεδιαστές που αναζητούν προσαρμοστικότητα και προστασία στο μέλλον στις ψηφιακές τους δημιουργίες (Tehranipoor & Bhunia, 2019).

Χρησιμοποιούνται σε διάφορους τομείς λόγω των δυνατοτήτων γρήγορης διαμόρφωσης και της αντοχής στο χειρισμό ψηφιακών λειτουργιών υψηλής ταχύτητας:

- Καταναλωτικά Ηλεκτρονικά: Τα CPLD χρησιμοποιούνται συνήθως στα ηλεκτρονικά είδη ευρείας κατανάλωσης για τη διαχείριση αλληλουχιών ισχύος, τη γεφύρωση διεπαφής και τη βελτίωση των χαρακτηριστικών του προϊόντος μέσω πρόσθετης λογικής χωρίς εκτεταμένες αλλαγές υλικού.
- Συστήματα Αυτοκινήτων: Σε εφαρμογές αυτοκινήτων, τα CPLD είναι αναπόσπαστα για την υλοποίηση λειτουργιών διαχείρισης συστήματος σε πραγματικό χρόνο, όπως ο έλεγχος του κινητήρα και η παρακολούθηση του συστήματος, όπου η αξιοπιστία και η ταχύτητα είναι ζωτικής σημασίας (Brown & Rose, 2012).
- Τηλεπικοινωνίες: Τα CPLD διευκολύνουν την τηλεπικοινωνιακή υποδομή παρέχοντας αποτελεσματικές λύσεις για την επεξεργασία σήματος, τη δρομολόγηση δικτύου και τη μετατροπή πρωτοκόλλων.

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

2.5 Διαφορές μεταξύ αρχιτεκτονικών ολοκληρωμένων κυκλωμάτων

2.5.1 Σύγκριση CPLD και FPGA

Η αυξανόμενη βελτιστοποίηση των Προγραμματιζόμενων Συστοιχιών Πυλών Πεδίου (FPGA) εγείρει ένα σχετικό ερώτημα: οι σύνθετες προγραμματιζόμενες λογικές συσκευές (CPLD) εξακολουθούν να έχουν αξία στο σύγχρονο τοπίο σχεδιασμού; Αυτή η έρευνα μπορεί να αντιμετωπιστεί με την εξέταση των βασικών διαφοροποιήσεων μεταξύ αυτών των δύο τεχνολογιών.

Ένα καθοριστικό χαρακτηριστικό έγκειται στη λογική ικανότητα. Τα CPLD προσφέρουν συνήθως δεκάδες χιλιάδες λογικές πύλες, ενώ τα FPGA διαθέτουν σημαντικά υψηλότερες δυνατότητες. Αν και η διαφορά κόστους μεταξύ των δύο μπορεί να μην είναι σημαντική, ο τεράστιος αριθμός των πυλών που διατίθενται στα FPGA τα καθιστά την προτιμώμενη επιλογή για έργα που απαιτούν εκτεταμένους λογικούς πόρους.

Πέρα από την ικανότητα, οι αρχιτεκτονικές διακρίσεις διαδραματίζουν ρόλο. Τα CPLD διαθέτουν μια σχετικά απλή αρχιτεκτονική, που αποτελείται από λογικά μπλοκ που τροφοδοτούνται σε καταχωρητές. Αυτή η απλότητα μεταφράζεται σε μειωμένη ευελιξία σε σύγκριση με τα FPGA. Κατά συνέπεια, τα FPGA υπερέχουν σε εφαρμογές που εξαρτώνται σε μεγάλο βαθμό από τη διαδοχική λογική (μεγάλη χρήση καταχωρητή) και τους αγωγούς παράλληλης επεξεργασίας. Ωστόσο, αυτή η ίδια η αρχιτεκτονική παρέχει επίσης στα CPLD ένα κρίσιμο πλεονέκτημα: προβλέψιμες καθυστερήσεις σήματος. Η ακριβής πρόβλεψη καθυστέρησης στα FPGA δεν μπορεί να γίνει εύκολα. Σε σενάρια όπου ο απόλυτος έλεγχος του χρονισμού είναι πρωταρχικής σημασίας, τα CPLD γίνονται η πιο ευνοϊκή επιλογή λόγω της εγγενούς προβλεψιμότητας τους. Η συνεχής εξέλιξη των FPGA δεν αναιρεί τη διαρκή πρόταση αξίας των CPLD. Οι προβλέψιμες καθυστερήσεις και η βελτιωμένη αρχιτεκτονική τους εξασφαλίζουν τη συνεχή συνάφειά τους σε συγκεκριμένες εφαρμογές, ακόμη και εν μέσω προόδου στην τεχνολογία FPGA.

Τα FPGA διαθέτουν πολλά χαρακτηριστικά που ενισχύουν την ευελιξία τους σε σύγκριση με τα CPLD. Τα περισσότερα FPGA επιτρέπουν την πλήρη ή μερική

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

αναδιαμόρφωση ενώ η συσκευή είναι ακόμα σε λειτουργία, επιτρέποντας γρήγορες και αποτελεσματικές ενημερώσεις στα σχέδια κυκλωμάτων. Αυτό το πλεονέκτημα ενισχύεται περαιτέρω με τη δυναμική μερική αναδιαμόρφωση, όπου συγκεκριμένα τμήματα μπορούν να τροποποιηθούν χωρίς να διακόπτονται οι συνεχείς διαδικασίες.

Επιπλέον, τα FPGA συχνά χρησιμοποιούν τεχνολογία SRAM σε σύγκριση με το EPROM ή το EEPROM που βρίσκεται στα CPLD. Αυτό μεταφράζεται σε ταχύτερους χρόνους επαναπρογραμματισμού και δυνητικά χαμηλότερη κατανάλωση ενέργειας λόγω της χαμηλότερης τάσης λειτουργίας των FPGA (συνήθως 3.3V σε σύγκριση με 5V για CPLD). Ωστόσο, είναι σημαντικό να σημειωθεί ότι τα FPGA απαιτούν επαναπρογραμματισμό κάθε φορά που φορτώνονται από εξωτερική πηγή, σε αντίθεση με ορισμένα CPLD.

Η απόφαση μεταξύ CPLD και FPGA εξαρτάται από τις ανάγκες της συγκεκριμένης εφαρμογής. Παράγοντες όπως η πολυπλοκότητα, οι απαιτήσεις ταχύτητας και το κόστος θα πρέπει να λαμβάνονται υπόψη κατά τη διαδικασία επιλογής.

2.5.2 Σύγκριση ASIC και FPGA

Δεδομένου ότι τα ASIC είναι ημι- ή πλήρως προσαρμοσμένα σχέδια, απαιτούν υψηλότερο κόστος ανάπτυξης και συχνά φτάνουν τα εκατομμύρια κατά τη διάρκεια των σταδίων σχεδιασμού και υλοποίησης. Επιπλέον, τα ASIC είναι μη επαναπρογραμματιζόμενα μόλις παραχθούν. Για το λόγο αυτό, οι αλλαγές στο σχεδιασμό συνεπάγονται πρόσθετο κόστος (Tehranipoor & Bhunia, 2019). Παρόλο που τα ASIC έχουν σχετικά υψηλότερο μη επαναλαμβανόμενο κόστος, δικαιολογείται λόγω των ακόλουθων γεγονότων:

- Τα ASIC έχουν συχνά μεγαλύτερη πυκνότητα και μπορούν να ενσωματώσουν πολύπλοκες λειτουργίες σε ένα τσιπ, παρέχοντας έτσι περιορισμένο μέγεθος, χαμηλή ισχύ, καθώς και σχεδιασμό χαμηλού κόστους.

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

- Λόγω του προσαρμοσμένου χαρακτηριστικού τους, ο αριθμός των τρανζίστορ εξετάζεται πολύ προσεκτικά και ελάχιστοι πόροι θα σπαταληθούν σε σχεδιασμό ASIC.
- Κατά την εκπόνηση μεγάλων ποσοτήτων σχεδίων για συγκεκριμένη χρήση, τα ASIC θα ήταν η βέλτιστη επιλογή.

Το πλεονέκτημα των FPGA έγκειται στην ευελιξία τους, την ικανότητά τους να επαναπρογραμματίζονται στο πεδίο και την οικονομική αποδοτικότητα. Για παράδειγμα, η επαναπρογραμματιζόμενη φύση επιτρέπει στους σχεδιαστές και τους κατασκευαστές να αλλάξουν το σχέδιο ή να στείλουν τις αλλαγές ακόμη και μετά την πώληση των προϊόντων.

Οι πελάτες χρησιμοποιούν συχνά αυτήν τη δυνατότητα για να δημιουργήσουν τα πρωτότυπά τους με βάση FPGA, έτσι ώστε τα σχέδιά τους να μπορούν να διορθωθούν πλήρως, να δοκιμαστούν και να ενημερωθούν στο πραγματικό σενάριο πριν από την κατασκευή.

Παρόλο που το μη επαναλαμβανόμενο κόστος είναι πολύ περιορισμένο και αυτό έχει σαν αποτέλεσμα, ο χρόνος διάθεσης τους στην αγορά να είναι γρήγορος, ορισμένοι πόροι σε ένα FPGA ξοδεύονται, καθώς το πακέτο και οι πόροι για έναν συγκεκριμένο τύπο FPGA είναι στάνταρ. Επιπλέον, κατά την ανάλυση του κόστους παραγωγής σε σχέση με τον όγκο παραγωγής, η χρήση FPGA γίνεται δαπανηρή σε σύγκριση με τα ASIC καθώς αυξάνεται ο όγκος. Επίσης, δεδομένου ότι τα FPGA δεν μπορούν να προσαρμοστούν πλήρως, ορισμένα συγκεκριμένα αναλογικά μπλοκ πρέπει να προστεθούν στις πλατφόρμες FPGA (Tehranipoor & Bhunia, 2019). Αυτές οι λειτουργίες-στοιχεία συνήθως απαιτούν να υλοποιηθούν από εξωτερικά IC, αυξάνοντας έτσι περαιτέρω το μέγεθος και το κόστος του τελικού προϊόντος. Η διαφορά[4] μεταξύ ASIC και FPGA συνοψίζεται στον Πίνακα 1.

[4] https://anysilicon.com/fpga-vs-asic-choose/ FPGA vs ASIC, What to Choose? (Ανάκτηση 10.6.2024)

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

Πίνακας 1. Η διαφορά μεταξύ FPGA και ASIC

Χαρακτηριστικό	**FPGA**	**ASIC**
Ευκαμψία	Υψηλό (επαναπρογραμματιζόμενο)	Χαμηλό (δεν επαναπρογραμματίζεται)
Εκτέλεση	Χαμηλότερο από το ASIC	Υψηλότερη απόδοση για συγκεκριμένες εργασίες
Κατανάλωση ενέργειας	Υψηλότερο σε σύγκριση με το ASIC	Χαμηλότερο (βελτιστοποιημένο για αποτελεσματικότητα)
Κόστος Ανάπτυξης	Χαμηλό (χωρίς κόστος NRE)	Υψηλό (υψηλό κόστος NRE)
Κόστος Παραγωγής ανά Μονάδα	Υψηλότερο σε σύγκριση με το ASIC	Χαμηλότερο (βελτιστοποιημένο για αποτελεσματικότητα)
Ώρα για Αγορά	Κοντύτερο (επαναπρογραμματιζόμενο, προσαρμόσιμο)	Μεγαλύτερο (λόγω σχεδιασμού και κατασκευής)
Επαναπρογραμματισμός	Ναι (μπορεί να αλλάξει αλγόριθμους μετά την παραγωγή)	Όχι (σταθερή σχεδίαση)
Κατάλληλος κύκλος παραγωγής	Μικρή έως μεσαία κλίμακα	Υψηλός όγκος (για αντιστάθμιση κόστους NRE)
Κύκλος σχεδίασης	Κοντύτερος	Μακρύτερος

(πηγή: https://anysilicon.com/fpga-vs-asic-choose/)

Τα ολοκληρωμένα κυκλώματα ειδικών εφαρμογών (ASIC) και οι προγραμματιζόμενες συστοιχίες πυλών πεδίου (FPGA) είναι ολοκληρωμένα κυκλώματα, τα οποία εξυπηρετούν διαφορετικά άκρα στο φάσμα των εφαρμογών για σύγχρονα ολοκληρωμένα κυκλώματα. Λόγω της δικής τους σχεδιαστικής φιλοσοφίας και χαρακτηριστικών, οι διαφορές τους περιλαμβάνουν μη επαναλαμβανόμενη μηχανική (NRE), κόστος, ευελιξία και απόδοση.

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

ΚΕΦΑΛΑΙΟ 3. Πίνακες προγραμματιζόμενων πυλών πεδίου - FPGA

3.1 Εισαγωγή

Η τεχνητή νοημοσύνη (AI) ήδη χρησιμοποιείται σε όλο και περισσότερα συστήματα σε κάθε δραστηριότητα, μεταμορφώνοντας την ψηφιακή επανάσταση με αλγόριθμους ικανούς να μιμούνται την ανθρώπινη μάθηση και τη λήψη αποφάσεων. Ωστόσο, αυτοί οι αλγόριθμοι απαιτούν ισχυρή υποδομή υλικού για να μεταφράσουν τις δυνατότητές τους σε εφαρμογές πραγματικού κόσμου. Ενώ οι κεντρικές μονάδες επεξεργασίας (CPU) και οι μονάδες επεξεργασίας γραφικών (GPU) είναι οι παραδοσιακοί πόροι εργασίας του υπολογισμού της τεχνητής νοημοσύνης, οι προγραμματιζόμενες στο πεδίο συστοιχίες πύλης (FPGA) συμπληρώνουν το υλικό που απαιτείται για την εκθετική απαίτηση των εφαρμογών της τεχνητής νοημοσύνης για ταχύτητα και ασφάλεια.

Σε αντίθεση με τις CPU και τις GPU, οι οποίες είναι προσχεδιασμένες για ένα ευρύ φάσμα εργασιών, οι FPGA είναι ουσιαστικά κενές πλάκες πυριτίου. Μπορούν να προσαρμοστούν για να εκτελούν συγκεκριμένες λειτουργίες διαμορφώνοντας τα εσωτερικά λογικά τους κυκλώματα. Αυτή η δυνατότητα προσαρμογής παρέχει στα FPGA αρκετά πλεονεκτήματα στον τομέα της τεχνητής νοημοσύνης. Για παράδειγμα, τα FPGA μπορούν να προσαρμοστούν ώστε να ταιριάζουν με ακρίβεια στις μοναδικές υπολογιστικές ανάγκες ενός συγκεκριμένου αλγορίθμου AI, οδηγώντας ενδεχομένως σε σημαντικές βελτιώσεις απόδοσης. Επιπλέον, τα FPGA συχνά διαθέτουν χαμηλότερη κατανάλωση ενέργειας σε σύγκριση με τους CPU και τις GPU, καθιστώντας τα ιδανικά για εφαρμογές όπου η ενεργειακή απόδοση αποτελεί κρίσιμο πρόβλημα.

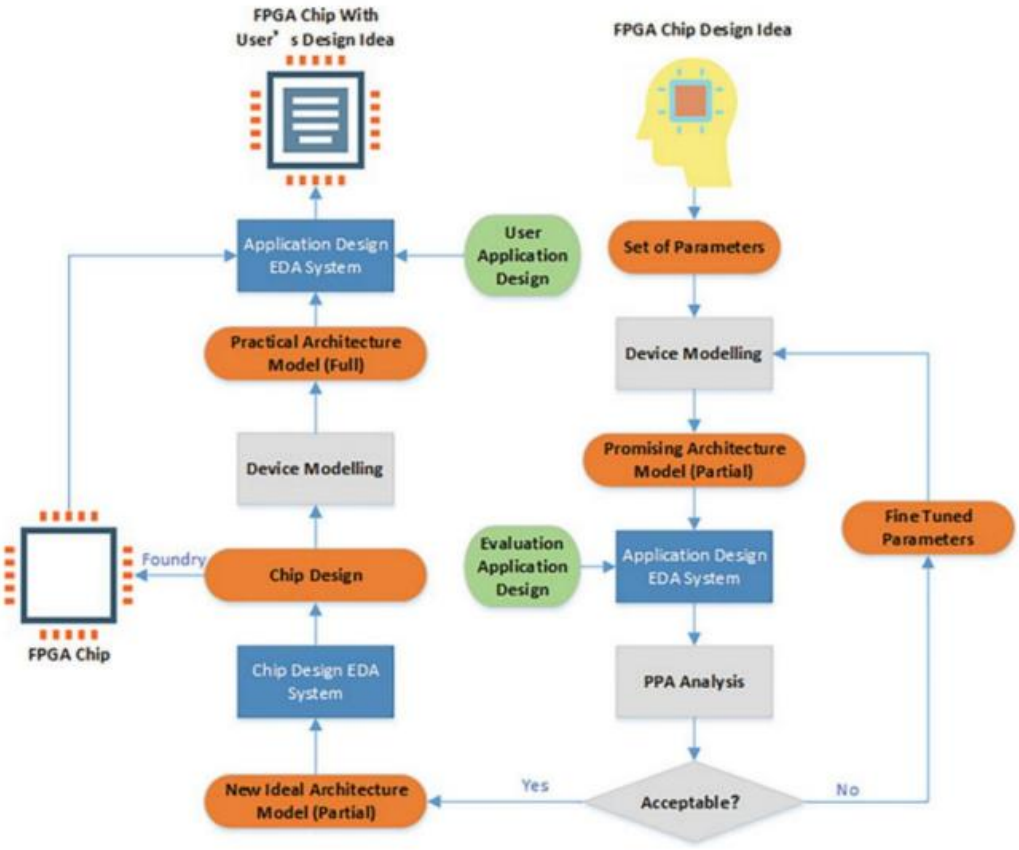
3.2 Πίνακες προγραμματιζόμενων πυλών πεδίου – FPGA

Το FPGA είναι ένα ημι-προσαρμοσμένο ολοκληρωμένο κύκλωμα, δηλαδή προγραμματιζόμενες μονάδες μέσα σε αυτό είναι προ-προσαρμοσμένες από τους

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

προμηθευτές στο σπίτι σχεδιασμού, αφού η συσκευή κατασκευαστεί και παραδοθεί στους τελικούς χρήστες, μπορεί να προσαρμοστεί σε επίπεδο πεδίου για δεύτερη φορά για να εφαρμόσει πλήρως την επιθυμητή λειτουργικότητα. Αυτό το χαρακτηριστικό κάνει τα FPGA να μπορούν να μπορούν να συναρμολογηθούν και να προγραμματιστούν σε προσχεδιασμένα μπλοκ (προγραμματιζόμενες μονάδες) και σχήματα (λειτουργίες κυκλώματος). Ωστόσο, αυτές οι εργασίες «προσχεδιασμού» και «συναρμολόγησης» για FPGA είναι πολύ περίπλοκες για να πραγματοποιηθούν χωρίς τη βοήθεια υπολογιστή (Tu, et al, 2024).

Ακριβώς όπως πολλοί άλλοι ημιαγωγοί, η διαδικασία σχεδιασμού του FPGA εξαρτάται σε μεγάλο βαθμό από τα εργαλεία αυτοματισμού ηλεκτρονικού σχεδιασμού - Electronic Design Automation (EDA). Λόγω των ημι-προσαρμοσμένων χαρακτηριστικών του FPGA, το FPGA EDA είναι πολύ διακριτικό και μπορεί να κατηγοριοποιηθεί ανάλογα σε δύο διαφορετικά πεδία: σχεδιασμός τσιπ EDA και σχεδιασμός εφαρμογών EDA (Tehranipoor & Bhunia, 2019).

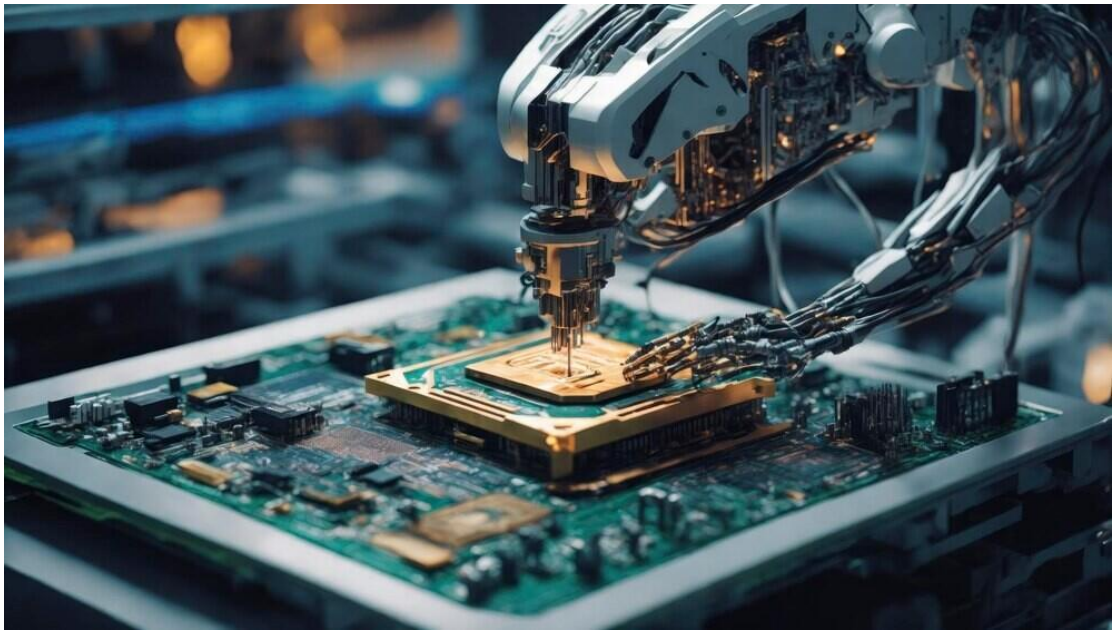


Σχήμα 7. Πλήρης ροή FPGA EDA: από τους προμηθευτές στους χρήστες

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

Τα σχέδια FPGA εξαρτώνται σε μεγάλο βαθμό από το EDA. Η πλήρης διαδικασία σχεδιασμού του FPGA χωρίζεται σε δύο στάδια: το στάδιο σχεδιασμού τσιπ και το στάδιο σχεδιασμού εφαρμογής. Το πρώτο συμπληρώνεται από τους προμηθευτές FPGA και το τελευταίο παραδίδεται στους χρήστες FPGA. Κατά τη διάρκεια του σχεδιασμού του τσιπ υιοθετούνται και οι πλήρεις προσαρμοσμένες και ημι-προσαρμοσμένες μέθοδοι σχεδίασης. Ο πλήρως προσαρμοσμένος σχεδιασμός απαιτεί από τους σχεδιαστές να ολοκληρώσουν τη σχεδίαση κυκλώματος από το κάτω επίπεδο, ενώ μια άλλη σχεδιαστική προσέγγιση, η ημιπροσαρμοσμένη σχεδίαση, χρησιμοποιεί προσχεδιασμένες μακροεντολές για να απλοποιήσει την προσπάθεια (Tu, et al, 2024).

Αντίστοιχα, το FPGA EDA μπορεί επίσης να χωριστεί σε δύο μέρη: Σχεδιασμός τσιπ FPGA EDA (για να βοηθήσει τους προμηθευτές στο στάδιο σχεδιασμού τσιπ) και σχεδιασμός εφαρμογής FPGA EDA (για να βοηθήσει τους τελικούς χρήστες στο στάδιο του σχεδιασμού της εφαρμογής (Tu, et al, 2024).



Εικόνα 1. Electronic Design Automation (EDA)

Τα βασικά πλεονεκτήματα που προσφέρουν τα FPGA περιλαμβάνουν:

Εξαιρετική απόδοση με μειωμένα πλεονεκτήματα καθυστέρησης : Τα FPGA παρέχουν χαμηλό λανθάνοντα χρόνο καθώς και ντετερμινιστικό λανθάνοντα χρόνο (DL). Το DL

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

ως μοντέλο θα παράγει συνεχώς την ίδια έξοδο από μια αρχική κατάσταση ή δεδομένη συνθήκη εκκίνησης. Το DL παρέχει έναν γνωστό χρόνο απόκρισης που είναι κρίσιμος για πολλές εφαρμογές με σκληρές προθεσμίες. Αυτό επιτρέπει την ταχύτερη εκτέλεση εφαρμογών σε πραγματικό χρόνο όπως η αναγνώριση ομιλίας, η ροή βίντεο και η αναγνώριση κίνησης.

Αποτελεσματικότητα κόστους: Τα FPGA μπορούν να επαναπρογραμματιστούν μετά την κατασκευή για διαφορετικούς τύπους δεδομένων και δυνατότητες, αποδίδοντας πραγματική αξία από την ανάγκη αντικατάστασης της εφαρμογής με νέο υλικό. Ενσωματώνοντας πρόσθετες δυνατότητες —όπως ένας αγωγός επεξεργασίας εικόνας στο ίδιο τσιπ, οι σχεδιαστές μπορούν να μειώσουν το κόστος και να εξοικονομήσουν χώρο στην πλακέτα χρησιμοποιώντας το FPGA για κάτι περισσότερο από τεχνητή νοημοσύνη. Ο μακρύς κύκλος ζωής του προϊόντος των FPGA μπορεί να προσφέρει αυξημένη χρησιμότητα για μια εφαρμογή που μπορεί να μετρηθεί σε χρόνια ή και δεκαετίες. Αυτό το χαρακτηριστικό τα καθιστά ιδανικά για χρήση σε βιομηχανικές, αεροδιαστημικές, αμυντικές, ιατρικές αγορές και αγορές μεταφορών.

Ενεργειακή απόδοση: Τα FPGA δίνουν στους σχεδιαστές τη δυνατότητα να προσαρμόσουν με ακρίβεια το υλικό στις ανάγκες της εφαρμογής. Η σωστή χρήση μπορεί να μειώσει τις απαιτήσεις μνήμης και υπολογιστών, γεγονός που μπορεί να συρρικνώσει τη χρήση της μνήμης και του εύρους ζώνης έως και 75%. Αυτό μπορεί να αποδειχθεί κρίσιμο για την ικανοποίηση των απαιτήσεων απόδοσης ισχύος σε απαιτητικές εφαρμογές.

Τα FPGA μπορούν να φιλοξενήσουν πολλαπλές λειτουργίες παράλληλα και μπορούν ακόμη και να εκχωρήσουν τμήματα του τσιπ για συγκεκριμένες λειτουργίες, γεγονός που βελτιώνει σημαντικά τη λειτουργική και ενεργειακή απόδοση. Η μοναδική αρχιτεκτονική των FPGA τοποθετεί μικρές ποσότητες κατανεμημένης μνήμης, φέρνοντάς το πιο κοντά στην επεξεργασία. Αυτό μειώνει την καθυστέρηση και το πιο σημαντικό, μπορεί να μειώσει την κατανάλωση ενέργειας σε σύγκριση με μια σχεδίαση GPU.

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

3.3 Εξέλιξη του υλικού FPGA

Στα σύγχρονα FPGA, τα μπλοκ λογικής περιλαμβάνουν στοιχεία μνήμης, ή πλήρη μπλοκ μνήμης. Παραδείγματα FPGAs παρουσιάζονται στο Σχήμα 2, όπου το αριστερό είναι ένα Stratix IV FPGA που αναπτύχθηκε από την Altera, και το δεξί είναι ένα Spartan FPGA που αναπτύχθηκε από την Xilinx

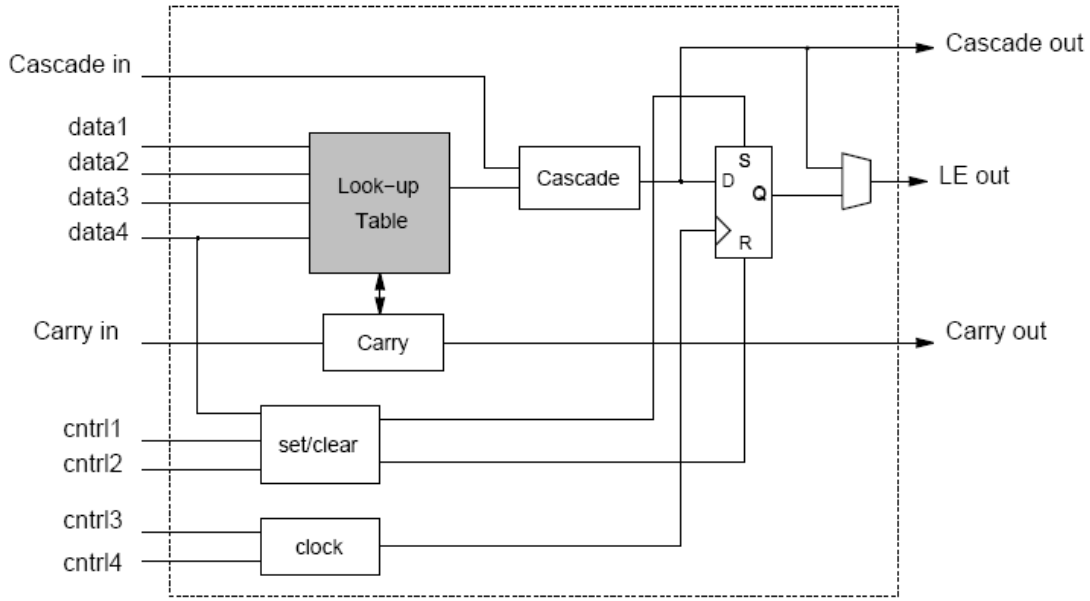
Σχήμα 8. FPGAs from Altera (αριστερά) and Xilinx (δεξιά).

Η σειρά Flex 8000 της Altera κατέχει μια μοναδική θέση στο προγραμματιζόμενο λογικό τοπίο, παρουσιάζοντας χαρακτηριστικά τόσο των Προγραμματιζόμενων Συστοιχιών Πυλών Πεδίου (FPGAs) όσο και των Πολύπλοκων Προγραμματιζόμενων Λογικών Συσκευών (CPLD). Ενώ η αρχιτεκτονική τριών επιπέδων του παρουσιάζει ομοιότητες με τα CPLD, το θεμελιώδες δομικό στοιχείο, το λογικό στοιχείο (LE), ενσωματώνει βασικά χαρακτηριστικά FPGA. Πιο συγκεκριμένα, τα LE χρησιμοποιούν πίνακες αναζήτησης (LUT) στο βασικό επίπεδο, ένα καθοριστικό χαρακτηριστικό των FPGA. Επιπλέον, η σειρά Flex 8000 αξιοποιεί τον προγραμματισμό που βασίζεται σε SRAM, ενισχύοντας περαιτέρω την ταξινόμησή της ως FPGA. Με λογική χωρητικότητα που κυμαίνεται από 4.000 έως 15.000 πύλες, αυτή η σειρά προσφέρει μια ευέλικτη λύση για έργα με διαφορετικές απαιτήσεις πολυπλοκότητας.

Ερευνώντας βαθύτερα την αρχιτεκτονική LE, βρίσκουμε μια ολοκληρωμένη σειρά λειτουργιών. Κάθε LE στεγάζει ένα LUT τεσσάρων εισόδων ικανό να εφαρμόσει ένα

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

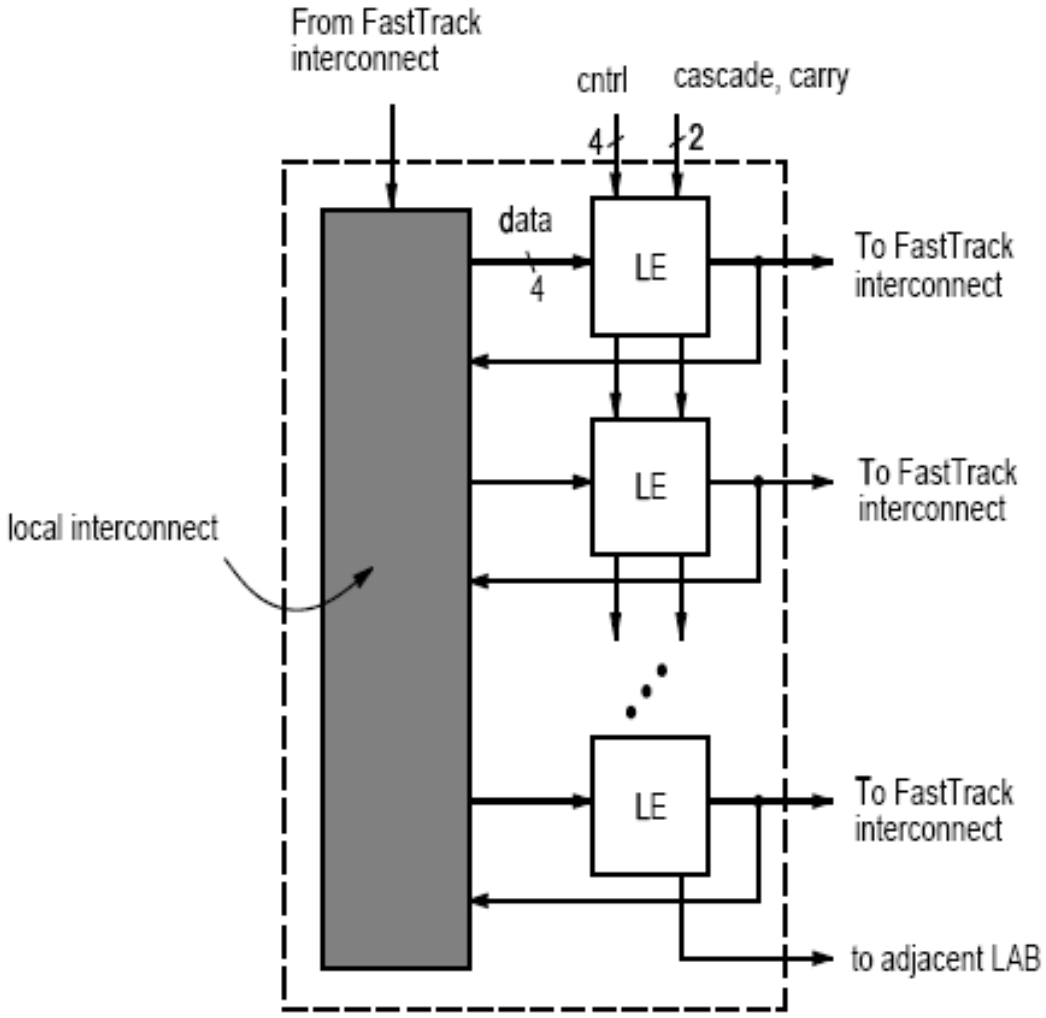
ευρύ φάσμα λογικών συναρτήσεων. Επιπλέον, ένα flip-flop παρέχει δυνατότητες αποθήκευσης δεδομένων, ενώ ένα αποκλειστικό κύκλωμα κλειδώματος διευκολύνει τις αριθμητικές λειτουργίες, επιδεικνύοντας μια σχεδιαστική φιλοσοφία παρόμοια με τη σειρά XC4000 της Xilinx. Ένα πρόσθετο κύκλωμα καταρράκτη εντός του LE ενισχύει την κατασκευή λειτουργιών AND πολλαπλών εισόδων. Ενώ μια λεπτομερής απεικόνιση της αρχιτεκτονικής LE παρέχεται στο Σχήμα 9, είναι η εγγενής ευελιξία του LE που δικαιολογεί την έμφαση, καθώς επιτρέπει στη σειρά Flex 8000 να αντιμετωπίσει ένα πλήθος προκλήσεων λογικού σχεδιασμού.



Σχήμα 9. Λογικό στοιχείο της σειράς Flex 8000

Η σειρά Flex 8000 οργανώνει τα λογικά της στοιχεία (LEs) σε συμπλέγματα γνωστά ως Logic Array Blocks (LAB). Κάθε LAB ενοποιεί οκτώ LE, παρέχοντας ένα δομημένο πλαίσιο επικοινωνίας και συνεργασίας. Αυτό το εσωτερικό δίκτυο διευκολύνει την επικοινωνία μεταξύ οποιωνδήποτε δύο LE μέσα στο ίδιο LAB. Επιπλέον, κάθε LAB είναι εξοπλισμένο με μια αποκλειστική γραμμή ελέγχου. Αυτή η γραμμή προφανώς φέρει κρίσιμα σήματα ελέγχου που διέπουν τη λειτουργία των LEs εντός του LAB.

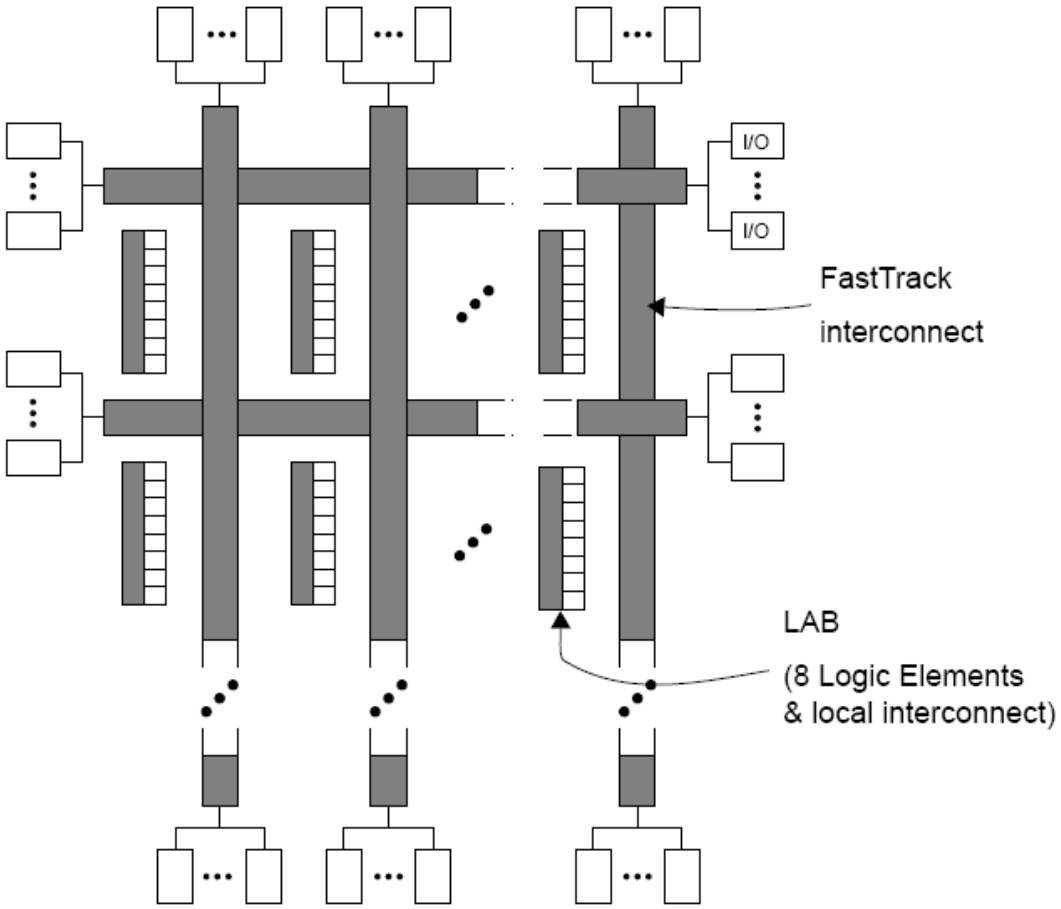
Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250



Σχήμα 10. Πίνακας λογικών στοιχείων (Logic array block)

Κάθε πλακέτα λογικού μπλοκ συνδέεται με το εξωτερικό δίκτυο διασύνδεσης που ονομάζεται FastTrack, όπως φαίνεται στο σχήμα 10. Οι γραμμές FastTrack εκτείνονται σε όλο το μήκος και το πλάτος του τσιπ, παρόμοια με τη σειρά XC της Xilinx. Ωστόσο, μια βασική διάκριση είναι ότι οι γραμμές διασύνδεσης του FastTrack είναι μεγάλες, ενώ τα τσιπ Xilinx έχουν διασυνδέσεις που αποτελούνται από γραμμές διαφορετικού μήκους. Οι μεγαλύτερες γραμμές στο FastTrack απαιτούν λιγότερους προγραμματιζόμενους διακόπτες, γεγονός που απλοποιεί την πρόβλεψη της καθυστέρησης διάδοσης στις συσκευές Altera και διευκολύνει το σχεδιασμό κυκλωμάτων χρησιμοποιώντας εργαλεία CAD.

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250



Σχήμα 11. Αρχιτεκτονική Altera Flex 8000

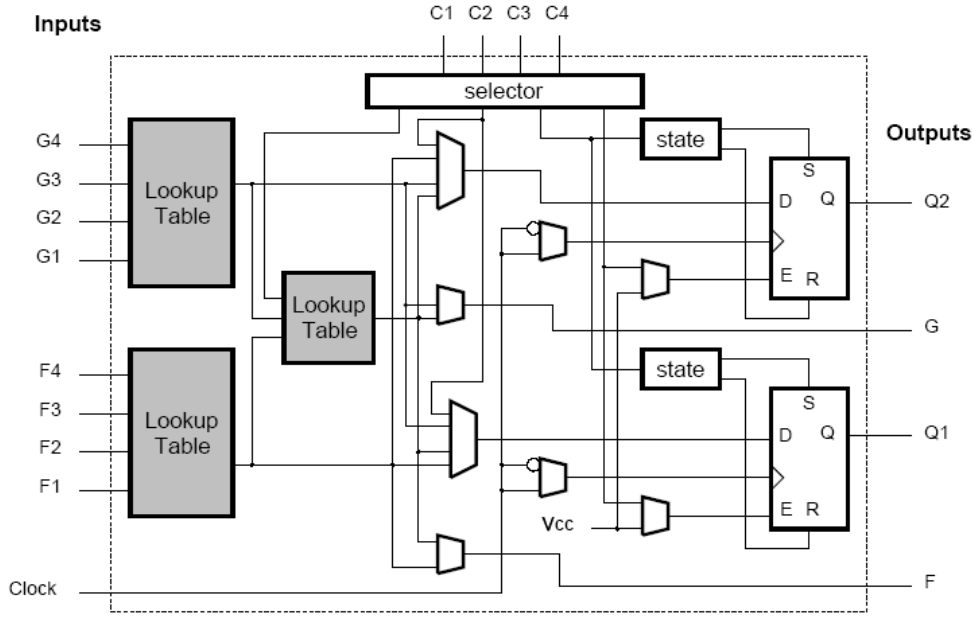
Από το 1985, η Xilinx καθιερώθηκε ως κορυφαίος πάροχος Field-Programmable Gate Arrays (FPGAs) με την εισαγωγή της σειράς XC2000. Αυτές οι συσκευές αξιοποιούν την τεχνολογία SRAM για διαμόρφωση. Επί του παρόντος, η Xilinx προσφέρει δύο ξεχωριστές οικογένειες FPGA – Spartan και Virtex, που καλύπτουν ένα ευρύ φάσμα εφαρμογών. Αυτές οι οικογένειες διαθέτουν λογικές ικανότητες που κυμαίνονται από 1.700 έως 55.000 μπλοκ και προσφέρουν δυνατότητες επεξεργασίας υψηλής απόδοσης.

Εσωτερικά, τα Xilinx FPGA χρησιμοποιούν μια δισδιάστατη αρχιτεκτονική από Configurable Logic Blocks (CLBs) που είναι διατεταγμένα σε ένα πλέγμα. Αυτά τα CLB διασυνδέονται μέσω ενός δικτύου οριζόντιων και κατακόρυφων καναλιών. Ως θεμελιώδες δομικό στοιχείο, το CLB μπορεί να προγραμματιστεί ώστε να πραγματοποιεί διάφορες λογικές συναρτήσεις. Κάθε CLB χρησιμοποιεί πίνακες

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

αναζήτησης (LUT). Ένας πίνακας αναζήτησης με K εισόδους αντιστοιχεί σε μνήμη εύρους 2^K x1-bit. Οι είσοδοι του λογικού μπλοκ χρησιμεύουν ως γραμμές διεύθυνσης για το LUT, ενώ οι έξοδοι LUT αντιστοιχούν στις εξόδους δεδομένων μνήμης. Προγραμματίζοντας τον σχετικό πίνακα αλήθειας απευθείας σε αυτή τη μνήμη, οι χρήστες έχουν την ευελιξία να εφαρμόσουν οποιαδήποτε λογική συνάρτηση K-bit.

Στο **σχήμα 12.** διακρίνεται η εσωτερική δομή ενός λογικού μπλοκ XC4000. Αποτελείται από δύο πίνακες αναζήτησης (LUT), και τέσσερις εισόδους. Αυτά συμπληρώνονται από ένα τρίτο LUT που παίρνει τις εξόδους των δύο πρώτων ως εισόδους του. Αυτή η διαμόρφωση επιτρέπει το CLB να εφαρμόσει ένα ευρύ φάσμα λογικών συναρτήσεων, με μία μόνο είσοδο 8-bit, δύο εισόδων 4-bit και πολλών άλλων συνδυασμών. Επιπλέον, τα CLB ενσωματώνουν ειδικό κύκλωμα για να διευκολύνουν τις αριθμητικές πράξεις και ενσωματώνουν δύο flip-flops για την αποθήκευση της λογικής κατάστασης.

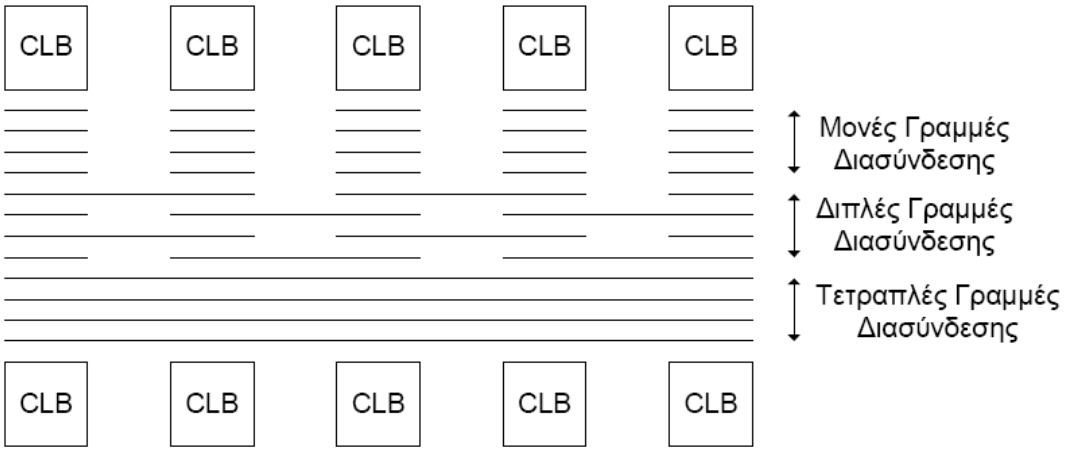


Σχήμα 12. XC4000- Configurable Logic Block

Πέρα από τα θεμελιώδη λογικά στοιχεία, μια κρίσιμη πτυχή της λειτουργικότητας του FPGA έγκειται στην εσωτερική αρχιτεκτονική δρομολόγησης. Η σειρά XC4000 χρησιμοποιεί ένα δίκτυο που βασίζεται σε κανάλια ενσωματωμένο στα Configurable Logic Blocks (CLB). Αυτό το δίκτυο περιλαμβάνει τρεις διαφορετικούς τύπους

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

γραμμών: σύντομες γραμμές που εκτείνονται σε ένα μόνο CLB, μεσαίες γραμμές που διασχίζουν δύο CLB και μεγάλες γραμμές που εκτείνονται σε ολόκληρο το τσιπ. Οι προγραμματιζόμενοι διακόπτες, που υλοποιούνται με χρήση τεχνολογίας SRAM, διευκολύνουν τη διασύνδεση μεταξύ αυτών των γραμμών. Μια λεπτομερής απεικόνιση ενός οριζόντιου τμήματος καναλιού μέσα σε μια συσκευή XC4000 παρέχεται στο Σχήμα 13.



Σχήμα 13. Εσωτερική διασύνδεση-σειρά XC4000

Η μετάδοση ενός σήματος από ένα Configurable Logic Block (CLB) σε ένα άλλο περιλαμβάνει την πλοήγηση μέσω πολλαπλών διακοπτών, ο αριθμός των οποίων καθορίζεται από τα τμήματα του καλωδίου που χρησιμοποιούνται. Κατά συνέπεια, η καθυστέρηση διάδοσης εντός του ολοκληρωμένου κυκλώματος εξαρτάται κυρίως από τη διάταξη των εσωτερικών συνδέσεων και την ποσότητα των διακοπτών που χρησιμοποιούνται.

2.4 Αρχιτεκτονική FPGA

Στα σύγχρονα υπολογιστικά συστήματα, οι FPGA χρησιμοποιούνται ως ειδικοί προγραμματιζόμενοι επιταχυντές (Zhang & Qu, 2019). Τα FPGA γενικής χρήσης είναι καλά βελτιστοποιημένα για να ταιριάζουν σε ένα ευρύ φάσμα εφαρμογών με λογικό

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

συμβιβασμό στην απόδοση, την ισχύ και την περιοχή, αλλά είναι σοβαρά μη βέλτιστα σε συγκεκριμένα πλαίσια εφαρμογών. Σε αυτή την περίπτωση, οι προσαρμοσμένες αρχιτεκτονικές FPGA, οι οποίες είναι ιδιαίτερα προσαρμοσμένες για ένα συγκεκριμένο σύνολο εφαρμογών, καθώς και η απρόσκοπτη ενσωμάτωση σε άλλους υπολογιστικούς πόρους στο σύστημα, αποτελούν την κατάλληλη λύση. Ωστόσο, η ανάπτυξη μιας διάταξης FPGA μέσω πλήρων προσαρμοσμένων προσεγγίσεων είναι μια χρονοβόρα διαδικασία ακόμη και για τη βιομηχανία κατασκευής, των οποίων μπορεί να χρειαστούν χρόνια για να οριστικοποιηθούν (Tang, et al, 2016).

Επιπλέον, εργαλεία σχεδιασμού όπως οι αλγόριθμοι χαρτογράφησης και η παραγωγή bitstream πρέπει να προσαρμοστούν για διαφορετικές αρχιτεκτονικές FPGA, γεγονός που οδηγεί σε μια άλλη χρονοβόρα εργασία ανάπτυξης. Για το λόγο αυτό, οι κύκλοι ανάπτυξης προσαρμοσμένων FPGA μπορούν να συγκριθούν με τους σύγχρονους ASIC, γεγονός που ανοίγει την πόρτα για τη στενή ενσωμάτωση FPGA σε SoCs[5]. Σε αυτήν την ενότητα, θα εξετάσουμε πρώτα τα υπάρχοντα εργαλεία EDA και στη συνέχεια θα επικεντρωθούμε σε κρίσιμες τεχνικές EDA που επιτρέπουν ημι-προσαρμοσμένα σχεδιασμένα FPGA (Tu, et al, 2024).

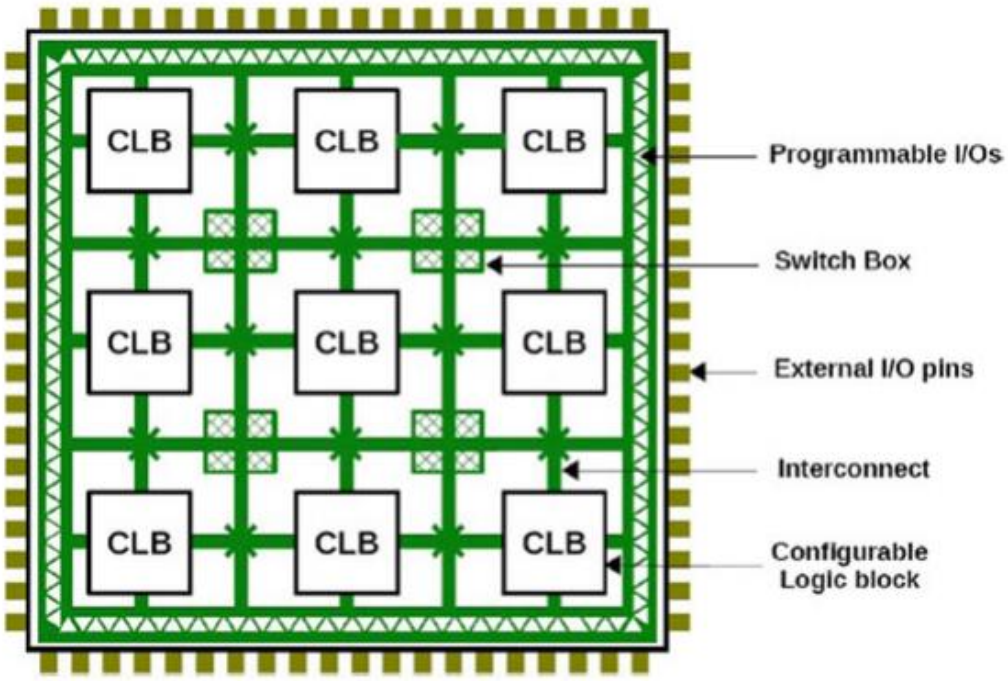
Καθώς η αρχιτεκτονική των FPGA μπορεί να είναι πραγματικά διαφορετική ανάλογα με το πλαίσιο εφαρμογής τους, μια βασική αξία των γεννητριών FPGA είναι η υποστήριξη ευέλικτων αρχιτεκτονικών FPGA. Αυτό έχει σαν αποτέλεσμα, οι γλώσσες περιγραφής αρχιτεκτονικής FPGA να είναι απαραίτητες για τη μοντελοποίηση περίπλοκων και μεγάλης κλίμακας συσκευών FPGA σε συμπαγείς και αναγνώσιμες από τον άνθρωπο αναπαραστάσεις. Αξιοποιώντας τη γλώσσα αρχιτεκτονικής FPGA του Πανεπιστημίου του Τορόντο (UTFAL), οι γεννήτριες FPGA μπορούν να μετατρέψουν μια περιγραφή FPGA υψηλού επιπέδου σε συνθετικές λίστες netl HDL και, στη συνέχεια, να υλοποιήσουν διατάξεις μέσω εργαλείων σχεδίασης ASIC. Χάρη στην εμπλουτισμένη σύνταξη του UTFAL, οι γεννήτριες FPGA μπορούν να υποστηρίξουν ένα ευρύ φάσμα αρχιτεκτονικών FPGA (Tang, et al, 2020).

[5] Ένα σύστημα σε ένα τσιπ είναι ένα ολοκληρωμένο κύκλωμα που συμπιέζει όλα τα απαιτούμενα εξαρτήματα ενός συστήματος σε ένα κομμάτι πυριτίου . Εξαλείφοντας την ανάγκη για ξεχωριστά και μεγάλα εξαρτήματα συστήματος, τα SoCs βοηθούν στην απλούστευση του σχεδιασμού της πλακέτας κυκλώματος, με αποτέλεσμα βελτιωμένη ισχύ και ταχύτητα χωρίς συμβιβασμούς στη λειτουργικότητα του συστήματος. (Ανάκτηση 12.6.2024 από https://www.ansys.com/blog/what-is-system-on-a-chip)

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

Ένα βασικό FPGA αποτελείται από τρία κύρια στοιχεία όπως φαίνεται στο Σχήμα 14.

1. Συνδυαστικά λογικά μπλοκ
2. Προγραμματιζόμενες διασυνδέσεις
3. Προγραμματιζόμενες ακίδες εισόδου/εξόδου.



Σχήμα 14. Λεπτομερής εσωτερική αρχιτεκτονική FPGA

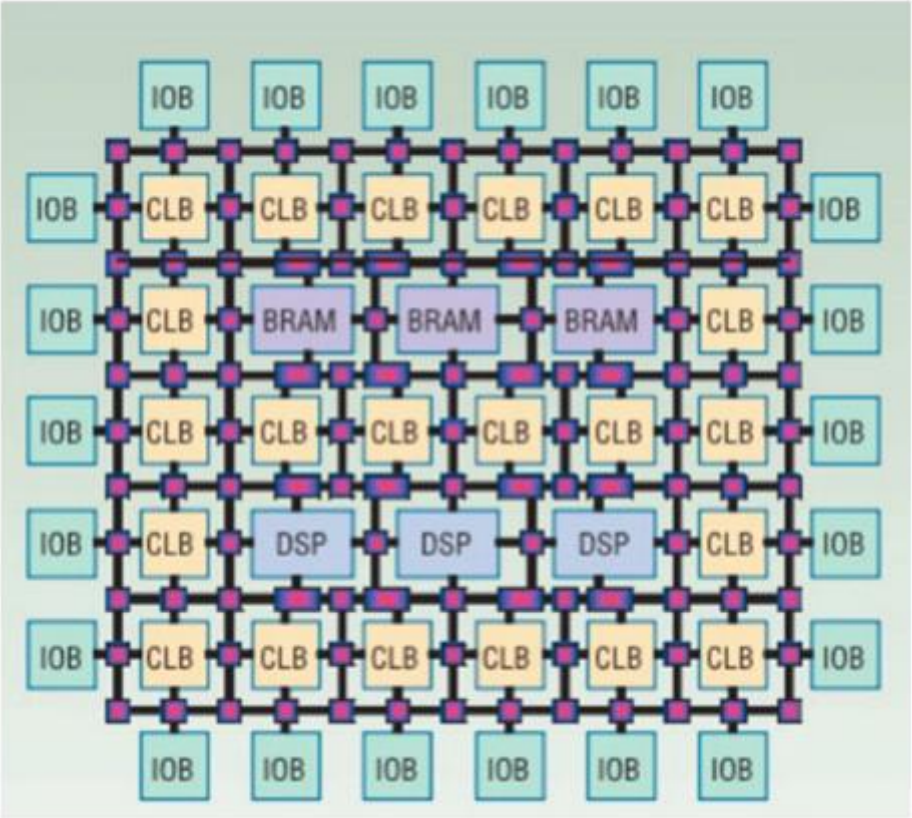
Τα μπλοκ συνδυαστικής λογικής είναι διαμορφώσιμα μπλοκ που χρησιμοποιούνται για την υλοποίηση προσαρμοσμένων λογικών συναρτήσεων. Συμβολίζονται ως λογικά στοιχεία - logic Elements (LEs) ή διαμορφώσιμα συνδυαστικά λογικά μπλοκ - configurable combinational logic blocks (CLBs) (Guha, et al, 2021)

Αυτά τα μπλοκ είναι γενικά διατεταγμένα ως δισδιάστατη δομή και περιβάλλονται από προγραμματιζόμενες διασυνδέσεις. Ο σχεδιασμός που θα υλοποιηθεί χωρίζεται σε μικρές ενότητες, καθεμία από τις οποίες εντάσσεται σε ένα λογικό μπλοκ. Στη συνέχεια, αρκετά μπλοκ διασυνδέονται χρησιμοποιώντας προγραμματιζόμενες διασυνδέσεις προκειμένου να υλοποιηθεί ολόκληρο το κύκλωμα (σχεδιασμός). Καθώς το FPGA είναι επαναπρογραμματιζόμενο, η υλοποιημένη λειτουργία θα μπορούσε να αλλάξει ενημερώνοντας το περιεχόμενο των μνημών διαμόρφωσης.

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

Ετερογενή – Heterogeneous FPGA

Σήμερα, τα FPGA χρησιμοποιούνται όλο και περισσότερο σε πολλές υπολογιστικά εντατικές εφαρμογές με αυστηρές απαιτήσεις απόδοσης. Προκειμένου να ικανοποιηθούν οι απαιτήσεις απόδοσης, αυτά τα FPGA περιλαμβάνουν συχνά εξειδικευμένα ενσωματωμένα σκληρά μπλοκ - embedded Hard Blocks (HBs) όπως μπλοκ μνήμης και μονάδες DSP εντός της ομοιόμορφης μήτρας ομοιογενών CLB, όπως φαίνεται στο Σχήμα 15. Η συμπερίληψη αυτών των HB επιτρέπει στις τρέχουσες πλατφόρμες FPGA να είναι πιο ετερογενείς στη φύση τους (Guha, et al, 2021)



Σχήμα 15. Ετερογενή FPGA: ένα διάγραμμα εννοιολογικού μπλοκ

Τα πιο κοινά ενσωματωμένα HB είναι:

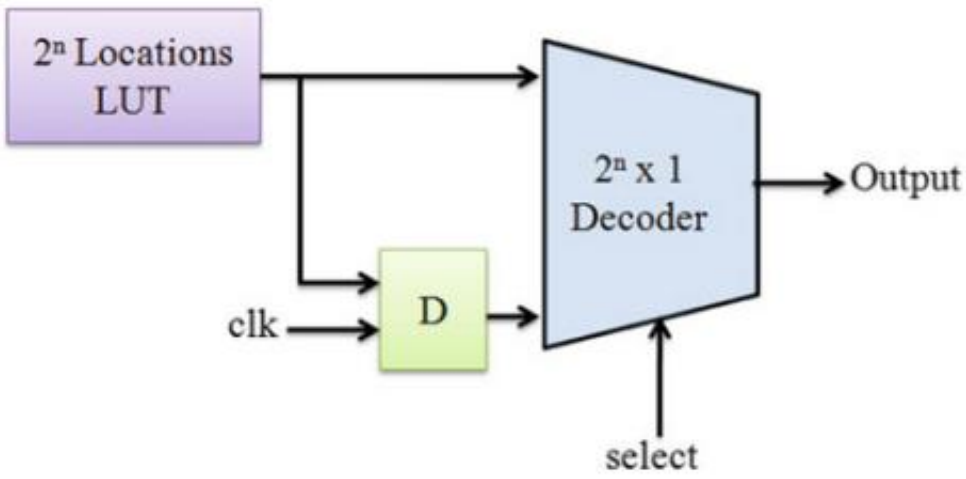
Μπλοκ μνήμης: Σε εφαρμογές όπως η επεξεργασία εικόνας, τεράστιες ποσότητες ενδιάμεσων δεδομένων πρέπει να αποθηκεύονται συχνά και προσωρινά κατά την επεξεργασία τους. Η χρήση ενσωματωμένων μπλοκ μνήμης σε FPGA έχει καταστεί κρίσιμη για την αποτελεσματική εφαρμογή αυτών των εφαρμογών με μειωμένες

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

καθυστερήσεις πρόσβασης στη μνήμη. Αυτά τα μπλοκ μνήμης, που συχνά ονομάζονται Block RAM (BRAM) παρέχουν αποκλειστική χωρητικότητα αποθήκευσης έως περίπου ≈1 MB σε πολλά σύγχρονα FPGA

Ενσωματωμένα μπλοκ DSP: Τα ενσωματωμένα μπλοκ DSP σε FPGA παρέχουν συνήθως πολλές μονάδες MAC (Πολλαπλασιασμός και Συσσώρευση). Σε συνδυασμό με τις προαναφερθείσες μονάδες ενσωματωμένης μνήμης BRAM, μπορούν να χρησιμοποιηθούν για την εύκολη εφαρμογή λειτουργιών ψηφιακής επεξεργασίας, όπως φίλτρα (Guha, et al, 2021).

Ένα CLB, το οποίο μπορεί να θεωρηθεί ως δομικό στοιχείο μονάδας ενός FPGA, αποτελείται ουσιαστικά από έναν πίνακα αναζήτησης (LUT), έναν καταχωρητή και έναν αποκωδικοποιητή όπως φαίνεται στο Σχήμα 16. Ο καταχωρητής που φαίνεται στο σχήμα χρησιμοποιείται για το συγχρονισμό της εξόδου LUT με ένα ρολόι, εάν είναι απαραίτητο. Ένα LUT με θέσεις 2^n μαζί με έναν αποκωδικοποιητή $2^n \times 1$ είναι ικανό να υλοποιήσει οποιαδήποτε λειτουργία n-input. (Guha, et al, 2021).



Σχήμα 16. Διαμορφώσιμο μπλοκ λογικής

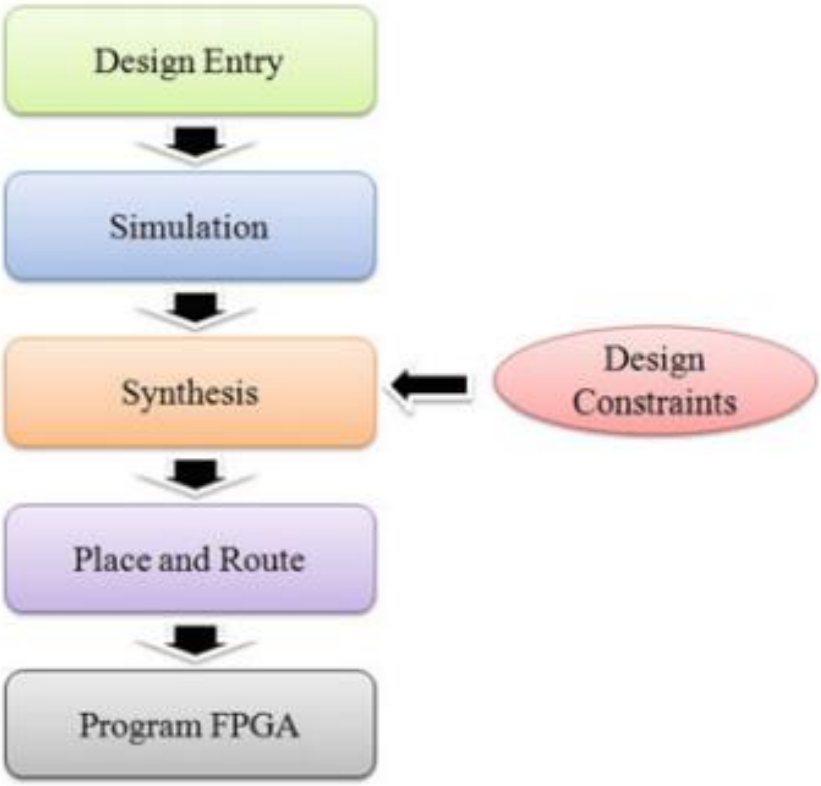
Τα FPGA δυναμικής και μερικής αναδιαμόρφωσης συνήθως κατηγοριοποιούνται ως πλήρως επαναδιαμορφώσιμες ή μερικώς αναδιαμορφώσιμες πλατφόρμες. Αρχικά, τα FPGAs ήρθαν μόνο ως πλήρως επαναδιαμορφώσιμες πλατφόρμες όπου όλοι οι λογικοί πόροι σε ολόκληρο το πλαίσιο FPGA σε μια δεδομένη στιγμή πρέπει να

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

αναδιαμορφωθούν ως μία ατομική λειτουργία. Έτσι, όλες οι εφαρμογές που εκτελούνται ταυτόχρονα σε διαφορετικές υποπεριοχές ή εικονικά τμήματα (VPs) του δαπέδου ή του ιστού FPGA και πρέπει ταυτόχρονα να σταματούν σε κάθε συμβάν αναδιαμόρφωσης. Ένας τέτοιος περιορισμός περιόριζε τη δυναμική εκτέλεση ανεξάρτητων εφαρμογών που εκτελούνται σε διαφορετικούς VP εντός της περιοχής του δαπέδου (Guha, et al, 2021).

Ωστόσο, ένας τέτοιος περιορισμός καταργήθηκε με την έλευση των εμπορικών πλατφορμών που διαθέτουν επίσης δυναμική μερική αναδιαμόρφωση που επιτρέπει την αναδιαμόρφωση μιας δημιουργίας υλικού που εκτελείται σε VP, επιτρέποντας παράλληλα στις δημιουργίες σε άλλες υποπεριοχές να συνεχίσουν να εκτελούνται αδιάκοπα. Τα FPGA της Xilinx συνήθως υιοθετούν το στυλ που βασίζεται σε λειτουργικές μονάδες για μερική αναδιαμόρφωση. Μια λειτουργική μονάδα σε μια αναδιαμόρφωση που βασίζεται σε λειτουργική μονάδα καθορίζεται από ένα ξεχωριστό μερικό bitstream, που ονομάζεται επίσης «εργασία». Ένα τέτοιο άρθρωμα σε μια συγκεκριμένη υποπεριοχή FPGA ή VP μπορεί να αναδιαμορφωθεί χωρίς διακοπή της εκτέλεσης άλλων μονάδων, κατεβάζοντας το bitstream του αρθρώματος μέσω του ICAP στη μνήμη διαμόρφωσης της υποπεριοχής ή του VP (Σχήμα 17.).

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250



Σχήμα 17. Προγραμματιζόμενη διαδικασία σχεδιασμού λογικής (Guha, et al, 2021).

Υπάρχει μια νέα τάση στο σχεδιασμό των FPGA (Προγραμματιζόμενες σε Πεδίο Συστοιχίες Πυλών) που διαφέρει από τον τρόπο κατασκευής τους. Αυτή η προσέγγιση, που ονομάζεται ημι-προσαρμοσμένη σχεδίαση, χρησιμοποιεί ειδικά εργαλεία για την αυτοματοποίηση τμημάτων της διαδικασίας, καθιστώντας ταχύτερη και ευκολότερη τη δημιουργία νέων διατάξεων FPGA. Ενώ είναι ακόμη νωρίς για ημι-προσαρμοσμένο σχεδιασμό, έχει τη δυνατότητα να βελτιώσει σημαντικά την απόδοση του FPGA.

Ένα πλεονέκτημα είναι ότι αυτά τα εργαλεία είναι συχνά ανοιχτού κώδικα, επιτρέποντας στους ερευνητές να επικεντρωθούν στο να κάνουν τα FPGA πιο γρήγορα και πιο αποτελεσματικά. Επιπλέον, αυτά τα εργαλεία μπορούν να συνεργαστούν με εργαλεία εξερεύνησης αρχιτεκτονικής για να δοκιμάσουν γρήγορα νέα σχέδια FPGA και να επικυρώσουν την αποτελεσματικότητά τους. Αυτό είναι πολύ πιο γρήγορο από τις παραδοσιακές μεθόδους. Ένα άλλο πλεονέκτημα είναι η δυνατότητα ανάπτυξης νέων αλγορίθμων για FPGA, όπως η συσκευασία, η τοποθέτηση και η δρομολόγηση.

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

Προηγουμένως, αυτοί οι αλγόριθμοι δοκιμάστηκαν σε υποθετικά μοντέλα, τα οποία δεν ήταν πολύ ακριβή. Με ημι-προσαρμοσμένο σχεδιασμό, οι ερευνητές μπορούν να τα επικυρώσουν σε πραγματικά υφάσματα FPGA (Tu, et al, 2024).

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

ΚΕΦΑΛΑΙΟ 4. Ασφάλεια κυκλωμάτων FPGA

4.1 Εισαγωγή

Η σημασία της ασφάλειας των κυκλωμάτων FPGA αλλά και γενικά του υλικού έχει πολύ μεγάλη σημασία λόγω των εξειδικευμένων απειλών στην ασφάλεια καίριων συστημάτων.

Ένα χαρακτηριστικό παράδειγμα έγινε το 2007, αλλά έγινε γνωστό το 2012. Ισραηλινά αεροσκάφη βομβάρδισαν μια ύποπτη πυρηνική εγκατάσταση στη βορειοανατολική Συρία. Μεταξύ των πολλών μυστηρίων που εξακολουθούσαν να περιβάλλουν αυτό το χτύπημα ήταν η αποτυχία ενός συριακού ραντάρ, υποτίθεται υπερσύγχρονου, να προειδοποιήσει τον συριακό σύστημα αεράμυνας για την επερχόμενη επίθεση. Ειδικοί που έλεγξαν το θέμα κατέληξαν στο συμπέρασμα ότι επρόκειτο για περιστατικό ηλεκτρονικού πολέμου και όχι οποιουδήποτε είδους. Εικάστηκε ότι οι εμπορικοί μικροεπεξεργαστές στο συριακό ραντάρ μπορεί να είχαν κατασκευαστεί σκόπιμα με μια κρυφή «πίσω πόρτα - back door μέσα». Με την αποστολή ενός προ-προγραμματισμένου κώδικα σε αυτά τα τσιπ, ένας άγνωστος αντίπαλος είχε διακόψει τη λειτουργία των τσιπ και είχε μπλοκάρει προσωρινά το ραντάρ (Adee, 2008).

Σε 2014, για την υπόθεση που εκδικάστηκε από το Ανώτατο Δικαστήριο του Χονγκ Κονγκ, η VIA Technologies Inc. παραδέχτηκε την ύπαρξη κερκόπορτας στο τσιπ VT3421. Οι πελάτες δεν γνωρίζουν την κερκόπορτα και δεν μπορούν να την απενεργοποιήσουν μόνοι τους. Ωστόσο, η VIA Technologies μπορεί εύκολα να χρησιμοποιήσει την κερκόπορτα για να αποκτήσει ορισμένα ευαίσθητα δεδομένα, συμπεριλαμβανομένων πληροφοριών συνομιλίας, βιβλίου διευθύνσεων, πιστωτικής κάρτας και τοποθεσίας από τελικές συσκευές (π.χ. κινητό τηλέφωνο, αποκωδικοποιητή), χωρίς να γίνεται αντιληπτή αυτή η παραβίαση ασφάλειας (Zhang & Qu, 2019).

Οι αιτίες των ζητημάτων ασφάλειας υλικού είναι πολλαπλές και πολύπλοκες, στις οποίες, οι κύριες αιτίες είναι η εξωτερική ανάθεση της κατασκευής ολοκληρωμένου κυκλώματος και η επαναχρησιμοποίηση IP.

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

4.2 Προκλήσεις και ασφάλεια των κυκλωμάτων FPGA

4.2.1 Προκλήσεις ασφάλειας στα κυκλώματα FPGA

Η δυνατότητα διαμόρφωσης που επιτρέπει στα FPGA να προγραμματίζονται και να εκτελούν συγκεκριμένες εργασίες γρηγορότερα ή με λιγότερη ισχύ από περισσότερους επεξεργαστές γενικής χρήσης, όπως CPU ή GPU, δημιουργούν ταυτόχρονα σημαντικές προκλήσεις ασφαλείας. Η επαναπρογραμματιζόμενη φύση των FPGA, οι πολύπλοκες διαδικασίες διαμόρφωσης τους και η εφαρμογή τους σε ευαίσθητες περιοχές απαιτούν ολοκληρωμένα μέτρα ασφαλείας για τον μετριασμό των κινδύνων όπως παραβίαση υλικού και κακόβουλες επιθέσεις.

Οι ευπάθειες ασφαλείας των FPGA επικεντρώνονται σε:

Επιθέσεις χρόνου διαμόρφωσης - Configuration Time Attacks: Κατά τη στιγμή της διαμόρφωσης, τα FPGA είναι ιδιαίτερα ευάλωτα. Καθώς τα δεδομένα φορτώνονται στο FPGA, η διαδικασία διαμόρφωσης μπορεί να υποκλαπεί ή να τροποποιηθεί, οδηγώντας σε πιθανές παραβιάσεις. Αυτό μπορεί να προκύψει από φυσικές επιθέσεις, όπου ένας εισβολέας αποκτά άμεση πρόσβαση στο FPGA ή μέσω απομακρυσμένων επιθέσεων στα δεδομένα διαμόρφωσης καθώς αυτά μεταβαίνουν από τη μνήμη ή τις πηγές δικτύου.

Οι Trojans επιθέσεις υλικού - Hardware Trojans: είναι κακόβουλες τροποποιήσεις στο υλικό του FPGA, που εισάγονται είτε κατά τη διαδικασία κατασκευής είτε κατά την ανάπτυξη μέσω παραβίασης της διαμόρφωσής του. Αυτοί οι Trojans μπορούν να αλλάξουν τις κανονικές λειτουργίες του FPGA, να διαρρεύσουν δεδομένα ή να απενεργοποιήσουν το σύστημα υπό συγκεκριμένες συνθήκες. Ο εντοπισμός αυτών των αλλαγών είναι δύσκολος, καθώς μπορεί να είναι αδρανείς μέχρι να ενεργοποιηθούν. (Εικάζεται ότι τέτοια ήταν η επίθεση στην περίπτωση των Συριακών Ραντάρ του παραδείγματος). Το κακόβουλο λογισμικό και μάλιστα σε επίπεδο υλικού, μπορεί να παραμένει απενεργοποιημένο και με ένα κώδικα, να ενεργοποιείται για ελάχιστο χρόνο, κάνοντας δύσκολο τον εντοπισμό του (Adee, 2008).

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

Επιθέσεις πλευρικού καναλιού - Side-channel Attacks: Οι επιθέσεις πλευρικού καναλιού περιλαμβάνουν την ανάλυση παραλλαγών στις φυσικές εξόδους από το FPGA, όπως η κατανάλωση ενέργειας, οι ηλεκτρομαγνητικές εκπομπές ή ακόμα και οι χρόνοι επεξεργασίας, για την εξαγωγή εμπιστευτικών πληροφοριών. Αυτές οι επιθέσεις είναι πολύπλοκες και δεν παραβιάζουν άμεσα τη λειτουργία του FPGA, γεγονός που καθιστά ιδιαίτερα δύσκολη την προστασία τους (Tu, et al, 2024).

4.2.2 Αρχές ασφαλείας και επιθέσεις κατά των FPGA

Οι αρχές ασφαλείας και οι επιθέσεις κατά των Field-Programmable Gate Arrays (FPGAs) αποτελούν κρίσιμα ζητήματα για τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων που υποβάλλονται σε επεξεργασία από αυτές τις επαναδιαμορφώσιμες συσκευές (Wanderley, et al, 2011).

Βασικές αρχές ασφαλείας και πιθανές επιθέσεις που σχετίζονται με τα FPGA:

- Εμπιστευτικότητα - Confidentiality: Διασφάλιση ότι μόνο εξουσιοδοτημένες οντότητες έχουν πρόσβαση σε ευαίσθητα δεδομένα που επεξεργάζονται το FPGA.
    - Τα σύγχρονα FPGA περιλαμβάνουν συχνά ενσωματωμένα μπλοκ ελέγχου ταυτότητας, όπως κωδικούς ελέγχου ταυτότητας μηνυμάτων με κλειδί κατακερματισμού (HMAC), που δημιουργούν κωδικούς ελέγχου ταυτότητας μηνυμάτων σταθερού μήκους από ροές bit αυθαίρετου μήκους. Επιπλέον, πολλά FPGA διαθέτουν μπλοκ αποκρυπτογράφησης bitstream (π.χ. AES) για την υποστήριξη κρυπτογραφημένων ροών bit που είναι αποθηκευμένα στη μνήμη flash διαμόρφωσης. Κατά την ενεργοποίηση, το κρυπτογραφημένο bitstream, το κλειδί ελέγχου ταυτότητας και ο κατακερματισμός αποκρυπτογραφούνται χρησιμοποιώντας ένα αποθηκευμένο κλειδί. Το ενσωματωμένο μπλοκ ελέγχου ταυτότητας του FPGA δημιουργεί μια σύνοψη της αποκρυπτογραφημένης ροής bit, η οποία συγκρίνεται με μια προηγουμένως αποκρυπτογραφημένη σύνοψη. Εάν ταιριάζουν, η ροή

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

bit παραμένει ανέπαφη. Ωστόσο, οι επιτυχημένες επιθέσεις στο κλειδί μπορούν να θέσουν σε κίνδυνο τόσο την εμπιστευτικότητα όσο και την ακεραιότητα. Οι επιθέσεις πλευρικού καναλιού, όπως η ανάλυση διαφορικής ισχύος (DPA), μπορούν να ανακτήσουν το κλειδί. Μπορεί επίσης να προκύψουν διαρροές κατά τη διάρκεια αποθήκευσης κλειδιών ή απομακρυσμένων αναβαθμίσεων (Tehranipoor & Bhunia, 2019).

- Ακεραιότητα - Integrity: Εγγύηση ότι τα δεδομένα παραμένουν αναλλοίωτα κατά τη μεταφορά και ότι η διαμόρφωση του FPGA δεν έχει παραβιαστεί.
- Διαθεσιμότητα - Availability: Διασφάλιση ότι τα δεδομένα και οι υπηρεσίες που παρέχονται από το FPGA είναι διαθέσιμα όταν χρειάζεται.
- Αυθεντικότητα - Authenticity: Επαλήθευση της ταυτότητας οντοτήτων που αλληλοεπιδρούν με το FPGA και διασφάλιση της νομιμότητας των πηγών δεδομένων (Tu, et al, 2024).
- Μη απόρριψη - Non-Repudiation: Αποτροπή οντοτήτων από το να αρνηθούν τις ενέργειες ή τις συναλλαγές τους που πραγματοποιούνται μέσω του FPGA.

4.3 Τεχνικές και μέθοδοι ασφάλειας σε κυκλώματα FPGA

Τα περισσότερα σύγχρονα FPGA υποστηρίζουν κρυπτογραφημένα δεδομένα διαμόρφωσης και τη χρήση πρωτοκόλλων ελέγχου ταυτότητας για να διασφαλιστεί ότι φορτώνονται μόνο τα νόμιμα δεδομένα διαμόρφωσης (Wanderley, et al, 2011). Ωστόσο, οι ίδιοι οι αλγόριθμοι κρυπτογράφησης μπορεί να είναι ευάλωτοι σε επιθέσεις και τα κλειδιά πρέπει να τυγχάνουν ασφαλούς διαχείρισης για την αποτροπή μη εξουσιοδοτημένης πρόσβασης.

Μέτρα φυσικής ασφάλειας: Τα φυσικά αντίμετρα περιλαμβάνουν πακέτα και αισθητήρες που εντοπίζουν και ανταποκρίνονται σε μη εξουσιοδοτημένες απόπειρες πρόσβασης. Αν και είναι αποτελεσματικά σε κάποιο βαθμό, αυτά τα μέτρα αυξάνουν το κόστος και την πολυπλοκότητα των αναπτύξεων FPGA και δεν είναι αλάνθαστα (Rangarajan, et al, 2021; Guha, et al, 2021).

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

Ασφαλής Διαμόρφωση και Τεχνικές Προστασίας IP: Τεχνικές όπως η κρυπτογράφηση bitstream και η χρήση εσωτερικής ασφαλούς αποθήκευσης για κρυπτογραφικά κλειδιά χρησιμοποιούνται για την προστασία της IP και των δεδομένων διαμόρφωσης. Ωστόσο, αυτές οι προστασίες είναι συχνά αποκλειστικές και δεν είναι τυποποιημένες σε διαφορετικούς κατασκευαστές FPGA, οδηγώντας σε πιθανές ευπάθειες. Προκειμένου να ενσωματώσουν διακριτικά αναγνωριστικά στα σχέδιά τους, οι σχεδιαστές FPGA χρησιμοποιούν τεχνικές υδατογράφησης[6]. Αυτά τα υδατογραφήματα μπορούν να χρησιμοποιηθούν για τον εντοπισμό του πραγματικού κατόχου της πνευματικής ιδιοκτησίας και τον εντοπισμό τυχόν μη εξουσιοδοτημένης χρήσης ή διανομής. Αλλά η δημιουργία αξιόπιστων μεθόδων υδατογράφησης που να αντέχουν σε χειρισμούς και εξαγωγή είναι δύσκολη (Guha, et al, 2021)

Ο μετριασμός των κινδύνων στον κύκλο ζωής ανάπτυξης του FPGA απαιτεί μια πολύπλευρη προσέγγιση. Πρώτον, η διατήρηση μιας ασφαλούς αλυσίδας εφοδιασμού είναι απαραίτητη για τη διασφάλιση της ακεραιότητας των στοιχείων FPGA από την αρχή. Δεύτερον, η συνεχής επαγρύπνηση και η επίγνωση των εξελισσόμενων απειλών για την ασφάλεια είναι ζωτικής σημασίας για την προληπτική διαχείριση κινδύνων. Οι αυστηρές πρακτικές δοκιμών ασφαλείας, συμπεριλαμβανομένων των τακτικών ελέγχων και των δοκιμών διείσδυσης, ενισχύουν περαιτέρω τη στάση ασφαλείας των FPGA. Υιοθετώντας μια ολοκληρωμένη στρατηγική ασφαλείας που περιλαμβάνει αυτά τα μέτρα, οι σχεδιαστές και οι αρχιτέκτονες συστημάτων FPGA μπορούν να δημιουργήσουν ανθεκτικά συστήματα που προστατεύουν την πνευματική ιδιοκτησία, προστατεύουν πολύτιμα περιουσιακά στοιχεία και εγγυώνται την ακλόνητη αξιοπιστία των εφαρμογών που τροφοδοτούνται από FPGA ενόψει ενός δυναμικού τοπίου απειλής (Tu, et al, 2024).

Το σεμινάριο FPGA Hardware Security for Datacenters and Beyond, που παρουσιάστηκε στο 28ο ACM/SIGDA International Symposium on Field-Programmable Gate Arrays (FPGA), αντιμετωπίζει τις αυξανόμενες ανησυχίες ασφαλείας που σχετίζονται με την ενσωμάτωση των Field-Programmable Gate Arrays (FPGAs) στα κέντρα δεδομένων. Καθώς τα FPGA χρησιμοποιούνται όλο και

[6] https://fpgainsights.com/fpga/fpga-security-challenges-and-best-practices/ FPGAs security: challenges and best practices. (Ανάκτηση 22.6.2024)

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

περισσότερο για την επιτάχυνση των εφαρμογών, ειδικά στο πλαίσιο του FPGA-as-a-Service (FaaS), η διασφάλιση της ασφάλειάς τους έχει καταστεί υψίστης σημασίας. Αυτό το σεμινάριο υπογραμμίζει τις πιθανές απειλές και τους προτεινόμενους μετριασμούς για την προστασία του υλικού FPGA σε αυτά τα περιβάλλοντα (Kaspar, et al, 2020)

Αρχικά, η ασφάλεια FPGA επικεντρώθηκε στην προστασία της πνευματικής ιδιοκτησίας (IP) που είναι ενσωματωμένη στα δεδομένα διαμόρφωσης (bitstreams) από κλωνοποίηση, αντίστροφη μηχανική και παραβίαση. Ωστόσο, η στροφή προς την ενσωμάτωση των FPGA σε κέντρα δεδομένων και υποδομές cloud έχει διευρύνει την εστίαση στην ασφάλεια. Το σεμινάριο τονίζει ότι, ενώ δεν έχουν σημειωθεί ακόμη εμπορικές επιθέσεις, η πιθανότητα μελλοντικών απειλών είναι σημαντική, προκαλώντας μια προληπτική προσέγγιση για την ασφάλεια FPGA.

Έρευνα Απειλών Υλικού

Το σεμινάριο κατηγοριοποιεί τις απειλές ασφαλείας FPGA σε δύο βασικούς τύπους: επιθέσεις στη διαθεσιμότητα του συστήματος και επιθέσεις στο απόρρητο των χρηστών.

Βραχυκυκλώματα: Τα σύγχρονα FPGA μπορούν να αντιμετωπίσουν προβλήματα από τη δημιουργία βραχυκυκλωμάτων μέσω της ροής δυαδικών ψηφίων διαμόρφωσης, οδηγώντας σε αυξημένες παροχές ρεύματος και πιθανά σφάλματα συστήματος.

Power Hammering: Αυτό περιλαμβάνει τη χρήση κυκλωμάτων όπως ταλαντωτές δακτυλίου για την άντληση υπερβολικής ισχύος, προκαλώντας πτώσεις τάσης και πιθανή συντριβή του FPGA. Το σεμινάριο καταδεικνύει ότι η ενεργοποίηση ενός μικρού κλάσματος των πόρων ενός FPGA μπορεί να οδηγήσει σε σημαντική κατανάλωση ενέργειας, αρκετή για να υπερβεί τα θερμικά και ηλεκτρικά όρια του υλικού.

Επιθέσεις στο απόρρητο των χρηστών (επιθέσεις πλευρικού καναλιού):

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

Έγχυση σφαλμάτων χρονισμού: Αυτή η μέθοδος περιλαμβάνει την πρόκληση πτώσεων τάσης μέσω κυκλωμάτων ταχείας εναλλαγής, τα οποία στη συνέχεια μπορούν να αναλυθούν για να αποκαλυφθούν μυστικά κλειδιά κρυπτογραφικών αλγορίθμων.

Επιθέσεις ανάλυσης ισχύος: Αυτές οι επιθέσεις μετρούν τις διακυμάνσεις της τάσης για την εξαγωγή ευαίσθητων πληροφοριών όπως κρυπτογραφικά κλειδιά. Μπορούν να εκτελεστούν στο ίδιο FPGA, σε μια CPU ενσωματωμένη στο FPGA ή ακόμα και σε άλλο FPGA στην ίδια πλακέτα.

Στρατηγικές Μετριασμού που προτάθηκαν:

- Απόκρυψη: Μετασχηματισμός κρυπτογραφικών αλγορίθμων για να γίνουν ανθεκτικοί σε επιθέσεις ανάλυσης ισχύος και προσθήκη θορύβου για μείωση της αναλογίας σήματος προς θόρυβο.

- Χρήση ταλαντωτών δακτυλίου για παρακολούθηση: Εφαρμογή ταλαντωτών δακτυλίου για την ανίχνευση πτώσεων τάσης και άλλες επιθέσεις που σχετίζονται με την ισχύ.

- Σάρωση ιών FPGA με FPGA Defender: Ένα εργαλείο ανοιχτού κώδικα σχεδιασμένο για να ανιχνεύει κακόβουλες κατασκευές σε ροές bit FPGA πριν από την ανάπτυξη. Σαρώνει για συνδυαστικούς κύκλους, ασύγχρονα στοιχεία, απαγορευμένες θύρες, διαδρομές και βραχυκυκλώματα και αναφέρει τυχόν πιθανά ζητήματα.

Η εργασία των Miyazakin, et al (2009), περιγράφει την ανάπτυξη, την εφαρμογή και τα πλεονεκτήματα της χρήσης της τεχνολογίας FPGA σε συστήματα πυρηνικής ασφάλειας στην Ιαπωνία.

Ιστορικά, τα συστήματα I&C των πυρηνικών σταθμών μεταπήδησαν από τα αναλογικά σε συστήματα που βασίζονται σε υπολογιστές τη δεκαετία του 1980, με σημαντικές προόδους στην ψηφιακή τεχνολογία που ενισχύουν τη λειτουργική ασφάλεια. Η τελευταία εξέλιξη της Toshiba χρησιμοποιεί τεχνολογία FPGA, η οποία είναι εγγενώς

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

πιο σταθερή και λιγότερο επιρρεπής σε λειτουργική μετατόπιση από τις προηγούμενες τεχνολογίες. Σε αντίθεση με τους συμβατικούς μικροεπεξεργαστές, οι FPGA είναι προγραμματιζόμενες συσκευές μίας χρήσης, εξαλείφοντας τους κινδύνους που σχετίζονται με ακούσιο επαναπρογραμματισμό κατά τη συντήρηση.

Πλεονεκτήματα των συστημάτων που χρησιμοποιούνται στην πυρηνική ασφάλεια και που βασίζονται σε FPGA

- Μακροζωία της προμήθειας : Εξασφαλίζουν μεγαλύτερο κύκλο ζωής προϊόντος που είναι ζωτικής σημασίας στην πυρηνική βιομηχανία όπου τα συστήματα πρέπει να παραμείνουν λειτουργικά και συνεπή για εκτεταμένες περιόδους.

- Βελτιωμένη δυνατότητα δοκιμής: Η απλούστερη αρχιτεκτονική των FPGA σε σύγκριση με συστήματα που βασίζονται σε CPU καθιστά τις διαδικασίες επαλήθευσης και επικύρωσης (V&V) λιγότερο επαχθή και πιο οικονομικά.

- Σταθερότητα : Από τη σχεδίασή τους, τα FPGA εξαλείφουν τα προβλήματα μετατόπισης που είναι κοινά στα αναλογικά συστήματα και μειώνουν την πολυπλοκότητα που παρατηρείται στα συστήματα που βασίζονται σε CPU.

Σχεδιασμός και Υλοποίηση

Η διαδικασία σχεδιασμού της Toshiba για αυτά τα συστήματα που βασίζονται σε FPGA συμμορφώνεται στενά με τους κανονισμούς και τα πρότυπα της βιομηχανίας, στοχεύοντας συγκεκριμένα στις ανάγκες των εφαρμογών πυρηνικής ασφάλειας. Αυτή η διαδικασία περιλαμβάνει τον καθορισμό των προδιαγραφών του συστήματος, τη λεπτομέρεια των απαιτήσεων στοιχείων και το σχεδιασμό της λογικής που θα ενσωματωθεί στο FPGA. Κάθε στάδιο ανάπτυξης από τον προγραμματισμό FPGA έως τη συναρμολόγηση του συστήματος υποβάλλεται σε αυστηρούς ελέγχους για να διασφαλιστεί η συμμόρφωση με τα πρότυπα ασφαλείας.

Σύστημα PRM που βασίζεται σε FPGA

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

Η συγκεκριμένη εφαρμογή σε συστήματα PRM περιλαμβάνει την ενσωμάτωση του FPGA για την παρακολούθηση των επιπέδων νετρονίων στον πυρήνα του αντιδραστήρα, μια κρίσιμη παράμετρος για την ασφάλεια του αντιδραστήρα. Ο σχεδιασμός του συστήματος διασφαλίζει ότι η παρακολούθηση νετρονίων είναι αξιόπιστη, ακριβής και ασφαλής από εξωτερικές παραβιάσεις ή εσωτερικές αστοχίες.

Εκτεταμένες δοκιμές πιστοποίησης επιβεβαιώνουν την ευρωστία του συστήματος PRM που βασίζεται σε FPGA έναντι περιβαλλοντικών προκλήσεων, σεισμικών συμβάντων, ηλεκτρομαγνητικών παρεμβολών και άλλων πιθανών λειτουργικών κινδύνων. Αυτές οι δοκιμές είναι ζωτικής σημασίας για να αποδειχθεί ότι το σύστημα μπορεί να αντέξει τις αυστηρές συνθήκες λειτουργίας των πυρηνικών σταθμών ηλεκτροπαραγωγής.

Τα συστήματα I&C της Toshiba που βασίζονται σε FPGA όχι μόνο πληρούν τα τρέχοντα πρότυπα ασφάλειας και λειτουργίας, αλλά αποτελούν επίσης προηγούμενο για τη μελλοντική τεχνολογία πυρηνικής ασφάλειας. Η εταιρεία σχεδιάζει να επεκτείνει αυτήν την τεχνολογία σε άλλους τύπους πυρηνικών εγκαταστάσεων, αξιοποιώντας την επιτυχημένη ανάπτυξη σε BWR για να βελτιώσει την ασφάλεια και την αποτελεσματικότητα των επιχειρήσεων πυρηνικής ενέργειας παγκοσμίως.

Οι βασικοί κανονισμοί ασφαλείας υλικού που πρέπει να γνωρίζουν οι εταιρείες περιλαμβάνουν σύμφωνα με την Cycuity και τον οδηγό ασφάλειας Guide-to-HW-Security-Requirements, είναι:

Common Weakness Enumeration (CWE): Αυτό το πρότυπο αντιμετωπίζει την ανάγκη για μια τυποποιημένη ονοματολογία και ταξινόμηση για αδυναμίες ασφάλειας υλικού. Στοχεύει στην καταγραφή και περιγραφή των αδυναμιών ασφάλειας υλικού με δομημένο τρόπο, διευκολύνοντας τον εντοπισμό, την κατανόηση και την αποκατάσταση κοινών τρωτών σημείων υλικού.

EU Cyber Resilience Act (CRA): Αυτός ο κανονισμός στοχεύει στην ενίσχυση της ασφάλειας ψηφιακών προϊόντων, υπηρεσιών και συσκευών. Θεσπίζει αυστηρές

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

απαιτήσεις κυβερνοασφάλειας για τους κατασκευαστές ψηφιακών προϊόντων προκειμένου να διασφαλιστεί υψηλό κοινό επίπεδο ασφάλειας στον κυβερνοχώρο σε ολόκληρη την ΕΕ. Η συμμόρφωση με τα πρότυπα κυβερνοασφάλειας είναι υποχρεωτική για όλα τα ψηφιακά προϊόντα που εισέρχονται στην αγορά της Ε.Ε.

Κανονισμός UNECE Αρ. 155: Θεσμοθετημένος από την UNECE για την καταπολέμηση των αυξανόμενων κινδύνων κυβερνοασφάλειας στη συνδεσιμότητα και την αυτοματοποίηση οχημάτων, αυτός ο κανονισμός περιγράφει τις απαιτήσεις για συστήματα αυτοκινήτων, συμπεριλαμβανομένων των στοιχείων υλικού. Επιβάλλει εκτενείς ελέγχους κυβερνοασφάλειας και την εφαρμογή ενός Συστήματος Διαχείρισης Κυβερνοασφάλειας (CSMS) από τους κατασκευαστές οχημάτων.

Αυτοί οι κανονισμοί διαδραματίζουν κρίσιμο ρόλο στην προώθηση ασφαλών πρακτικών σχεδιασμού υλικού, στην εξασφάλιση της ασφάλειας στον κυβερνοχώρο σε διαφορετικούς κλάδους και στην προστασία από μη εξουσιοδοτημένη πρόσβαση και επιθέσεις στον κυβερνοχώρο. Οι εταιρείες πρέπει να ενημερώνονται για αυτούς τους κανονισμούς για να συμμορφώνονται με τα πρότυπα και να βελτιώνουν την ασφάλεια των προϊόντων και των υπηρεσιών τους.

4.4 Ενδυνάμωση της Ασφάλειας του Υλικού με συστήματα τεχνητής νοημοσύνης

Η αξιοποίηση της τεχνητής νοημοσύνης (AI) για τη βελτίωση της ασφάλειας FPGA παρουσιάζει τόσο προκλήσεις όσο και ευκαιρίες στον τομέα της ασφάλειας υλικού (Qureshi & Newe, 2024). Οι προκλήσεις που αντιμετωπίζει το υλικό, που χρησιμοποιείται σε ολοκληρωμένα συστήματα τεχνητής νοημοσύνης είναι:

- Πολυπλοκότητα: Οι συσκευές FPGA γίνονται πιο περίπλοκες με μεγαλύτερα μεγέθη και υψηλότερα επίπεδα ενοποίησης, γεγονός που καθιστά δύσκολο τον αποτελεσματικό εντοπισμό και τον μετριασμό των τρωτών σημείων ασφαλείας.

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

- Multi-Tenancy: Η ανάπτυξη FPGA σε περιβάλλοντα cloud εισάγει νέες απειλές ασφαλείας, όπως επιθέσεις σε κοινές πλατφόρμες χρήσης, όπου κακόβουλοι χρήστες στο ίδιο τσιπ FPGA μπορούν να έχουν πρόσβαση σε ευαίσθητες πληροφορίες άλλων χρηστών (Mavromoustakis, et al, 2017).
- Επιθέσεις πλευρικού καναλιού: Οι τεχνικές τεχνητής νοημοσύνης μπορούν να χρησιμοποιηθούν για τη διεξαγωγή επιθέσεων πλευρικού καναλιού σε FPGA, εκμεταλλευόμενες τη διαρροή πληροφοριών μέσω χωρητικής συνομιλίας και άλλων καναλιών.
- Επιθέσεις εισαγωγής σφαλμάτων: Η συνδιαμονή πολλών ενοικιαστών συστημάτων μέσω cloud, δίνει δυνατότητες πρόσβασης σε τσιπ FPGA και μπορεί να οδηγήσει σε ευπάθειες κοινών πόρων που μπορούν να χρησιμοποιηθούν για κακόβουλους σκοπούς, όπως η εξαγωγή μυστικών κλειδιών μέσω επιθέσεων ανάλυσης ισχύος.

Αντιμετώπιση με τη χρήση τεχνητής νοημοσύνης

Στην μελέτη τους οι Xu & Zhang (2020) και σύμφωνα με τα ευρήματα και τις συστάσεις που παρουσιάζονται στην εργασία τους με τίτλο «Επανεξετάζοντας την ασφάλεια FPGA στη Νέα Εποχή της Τεχνητής Νοημοσύνης» μπορούν να εφαρμοστούν σε σενάρια πραγματικού κόσμου για την ενίσχυση της ασφάλειας των ηλεκτρονικών συσκευών, ιδιαίτερα των συσκευών FPGA, με τους ακόλουθους τρόπους:

Εφαρμογή λύσεων ασφάλειας που βασίζονται στη μηχανική μάθηση: Οι επιχειρήσεις μπορούν να εφαρμόσουν λύσεις που βασίζονται στη μηχανική μάθηση για τον εντοπισμό και τον μετριασμό των Trojans υλικού, επιθέσεων πλευρικού καναλιού και επιθέσεων έγχυσης σφαλμάτων σε συσκευές FPGA. Με την αξιοποίηση αλγορίθμων τεχνητής νοημοσύνης για τον εντοπισμό ανωμαλιών και την αναγνώριση προτύπων, η παρακολούθηση σε πραγματικό χρόνο των συσκευών FPGA μπορεί να βελτιωθεί για τον εντοπισμό και την άμεση απόκριση σε απειλές ασφαλείας (Xu & Zhang 2020).

Ενισχυμένα μέτρα ασφαλείας για αναπτύξεις FPGA που βασίζονται σε Cloud: Οι πάροχοι υπηρεσιών cloud μπορούν να ενισχύσουν τα μέτρα ασφαλείας για υπηρεσίες

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

cloud που βασίζονται σε FPGA για να μετριάσουν τους κινδύνους που σχετίζονται με ευπάθειες πολλαπλών μισθώσεων και κοινών πόρων. Η εφαρμογή ελέγχων πρόσβασης, μηχανισμών κρυπτογράφησης και συστημάτων ανίχνευσης εισβολής μπορεί να βοηθήσει στην αποτροπή μη εξουσιοδοτημένης πρόσβασης και κακόβουλων δραστηριοτήτων σε τσιπ FPGA που μοιράζονται πολλοί χρήστες.

Ανάπτυξη Μηχανισμών Αντίπαλης Άμυνας: Οι ερευνητές και οι προγραμματιστές μπορούν να επικεντρωθούν στην ανάπτυξη άμυνας έναντι επιθέσεων αντιπάλου σε επιταχυντές Deep Neural Network (DNN) που βασίζονται σε FPGA. Με την ενσωμάτωση τεχνικών τεχνητής νοημοσύνης για άμυνα, οι συσκευές FPGA μπορούν να προστατεύονται από χειραγώγηση και εκμετάλλευση από κακόβουλους παράγοντες που στοχεύουν να διακυβεύσουν τους αλγόριθμους μηχανικής μάθησης (Xu & Zhang 2020).

Συνεχής Έρευνα και Καινοτομία: Η συνεχής έρευνα στη διασταύρωση της ασφάλειας υλικού και της τεχνητής νοημοσύνης μπορεί να οδηγήσει στην ανακάλυψη νέων τρωτών σημείων και στην ανάπτυξη προληπτικών μέτρων ασφαλείας για συσκευές FPGA.

Συμπερασματικά οι Xu & Zhang (2020), θεωρούν ότι ενώ η μόχλευση της τεχνητής νοημοσύνης για τη βελτίωση της ασφάλειας FPGA θέτει προκλήσεις που σχετίζονται με την πολυπλοκότητα, την πολλαπλή μίσθωση και τους διάφορους φορείς επιθέσεων, προσφέρει επίσης ευκαιρίες για ενίσχυση των δυνατοτήτων ανίχνευσης, ανάπτυξη ισχυρών άμυνες και προώθηση μελλοντικής έρευνας για την ασφάλεια των συσκευών FPGA από εξελισσόμενες απειλές. την εποχή της τεχνητής νοημοσύνης.

4.5 Ανάλυση και Ενδυνάμωση της Ασφάλειας του Υλικού σε συστήματα τεχνητής νοημοσύνης: Εξέλιξη και Προηγμένες επιθέσεις

Η ανάπτυξη εξειδικευμένου υλικού τεχνητής νοημοσύνης, συμπεριλαμβανομένων των FPGAs (Field-Programmable Gate Arrays) και ASIC (Application-Specific Integrated Circuits), σηματοδότησε μια σημαντική εξέλιξη στον σχεδιασμό υλικού AI. Αυτές οι

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

συσκευές πρόσφεραν βελτιωμένη απόδοση και ενεργειακή απόδοση, αλλά εισήγαγαν νέες προκλήσεις ασφαλείας, όπως Trojans υλικού και ευπάθειες στην εφοδιαστική αλυσίδα.

Οι τελευταίες εξελίξεις στο υλικό τεχνητής νοημοσύνης περιλαμβάνουν την ενσωμάτωση της ασφάλειας σε επίπεδο σχεδιασμού. Τεχνικές όπως οι Physical Unclonable Functions (PUF) και η κρυπτογράφηση που βασίζεται σε υλικό χρησιμοποιούνται τώρα για τη βελτίωση της ασφάλειας. Επιπλέον, η υιοθέτηση ασφαλών θύλακων, όπως το SGX της Intel για υπολογισμούς τεχνητής νοημοσύνης, παρέχει ένα απομονωμένο περιβάλλον εκτέλεσης που μετριάζει πολλές απειλές που βασίζονται σε υλικό (Tehranipoor & Bhunia, 2019).

Το Υπουργείο Άμυνας των Ηνωμένων Πολιτειών εισήγαγε διάφορα χρηματοδοτούμενα ερευνητικά προγράμματα για να διευκολύνει την ανάπτυξη λύσεων ασφάλειας υλικού. Το 2008, η DARPA εισήγαγε το πρόγραμμα Ακεραιότητας και Αξιοπιστίας Ολοκληρωμένων Κυκλωμάτων (IRIS) για την ανάπτυξη τεχνικών για την ακεραιότητα και τη διασφάλιση αξιοπιστίας υλικού μέσω καταστροφικής και μη καταστροφικής ανάλυσης. Το 2012, μια έκθεση που δημοσιεύθηκε από τις ένοπλες δυνάμεις της Γερουσίας έδειξε ότι ένα σύνολο πλαστών συσκευών ανακαλύφθηκε σε διάφορους κλάδους της Πολεμικής Αεροπορίας των ΗΠΑ επιτείνοντας τη σοβαρότητα του προβλήματος.

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

ΣΥΜΠΕΡΑΣΜΑΤΑ

Η ασφάλεια υλικού υπολογιστών είναι ένας κρίσιμος τομέας στον ευρύτερο τομέα της κυβερνοασφάλειας, που περιλαμβάνει την προστασία στοιχείων υλικού, συστημάτων και δικτύων από φυσικές απειλές και απειλές στον κυβερνοχώρο. Όσον αφορά τη «φυσική» ασφάλεια, η ασφάλεια υλικού ουσιαστικά συνεπάγεται την προστασία των συστημάτων εσωτερικής εγκατάστασης από φυσική ή ανθρώπινη παραβίαση ή καταστροφή. Αυτό είναι ιδιαίτερα απαραίτητο καθώς οι επιθέσεις που στοχεύουν υπολογιστές καθώς και μη υπολογιστικές συνδεδεμένες συσκευές, όπως περιβάλλοντα μηχανής με μηχανή (M2M) ή internet of things (IoT) γίνονται πιο διαδεδομένες καθώς αυξάνεται η υιοθέτησή τους.

Η μελέτη της ασφάλειας υλικού, είναι σχετικά νέα, δεδομένου ότι μέχρι πρόσφατα το υλικό θεωρείται παραδοσιακά απρόσβλητο σε επιθέσεις και ως εκ τούτου χρησιμοποιείται χωρίς να λαμβάνονται τα αντίστοιχα μέτρα ασφάλειας. Η παγκοσμιοποίηση, ο κατακερματισμός της παραγωγής ακόμη και εξειδικευμένων υλικών ψηφιακών συστημάτων σε εταιρείες σε ολόκληρο τον κόσμο και οι τεχνολογικές εξελίξεις, έχουν αναγάγει το υλικό σε ευπαθή είδος, για επιθέσεις κυβερνοασφάλειας.

Η εξαιρετικά εξειδικευμένη μορφή σχεδίασης και παραγωγής ειδικά ολοκληρωμένων κυκλωμάτων που είναι γνωστά στο ευρύ κοινό σαν τσιπ και η τεράστια ζήτηση τους από κάθε βιομηχανία που παράγει ψηφιακά μηχανήματα και εξαρτήματα, έχει δημιουργήσει νέες προκλήσεις και δυσκολίες ελέγχου, ενώ η εκθετικά αυξημένη διασύνδεση των πάντων στο διαδίκτυο έχουν δημιουργήσει μια πρόσθετη κατάσταση ασφάλειας σε κάθε ψηφιακό σύστημα. Δισεκατομμύρια συσκευές στο διαδίκτυο των πραγμάτων που από τη φύση τους είναι μικρές και φθηνές, χωρίς τη δυνατότητα ουσιαστικής σημασίας, συνδέονται σε ένα εκτεταμένο δίκτυο και μπορεί να αποτελέσουν την κερκόπορτα σε ασφαλή συστήματα, δυσκολεύοντας ακόμη περισσότερο τον ολοκληρωμένο έλεγχο της ασφάλειας.

Στον τομέα της ασφάλειας υλικού υπολογιστών, οι Προγραμματιζόμενες Συστοιχίες Πυλών Πεδίου (FPGA) αντιπροσωπεύουν μια κρίσιμη επιλογή λόγω της ευελιξίας και

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

της ευρείας ανάπτυξής τους σε διάφορες ευαίσθητες και υψηλού κινδύνου εφαρμογές, που κυμαίνονται από τηλεπικοινωνιακά συστήματα και συστήματα αυτοκινήτου έως άμυνα και αεροδιαστημική.

Τα FPGA παρουσιάζουν ένα περίπλοκο αντικείμενο όσον αφορά την ασφάλεια υλικού. Παρόλο που προσφέρουν σημαντικά πλεονεκτήματα λόγω του επαναπρογραμματισμού και της ευελιξίας τους, εισάγουν επίσης συγκεκριμένα τρωτά σημεία που απαιτούν στοχευμένα μέτρα ασφαλείας. Καθώς τα FPGA γίνονται όλο και πιο σημαντικά στα κρίσιμα υπολογιστικά συστήματα, η εστίαση στην ασφάλειά τους πρέπει να ενταθεί μέσω ολοκληρωμένων στρατηγικών που περιλαμβάνουν κρυπτογράφηση, φυσική ασφάλεια και συνεχή επαγρύπνηση. Η εξισορρόπηση αυτών των παραγόντων είναι απαραίτητη για την αξιοποίηση του πλήρους δυναμικού των FPGA, προστατεύοντας παράλληλα τα συστήματα που ενισχύουν έναντι των εξελισσόμενων απειλών.

Σε σύγκριση με τα ASIC (Ειδικά Ολοκληρωμένα Κυκλώματα Εφαρμογής) και τις CPU, τα FPGA γενικά παρουσιάζουν πολλά πλεονεκτήματα. Τα ASIC, όντας ειδικά κατασκευασμένα, είναι λιγότερο ευέλικτα, αλλά συνήθως πιο ασφαλή από τροποποιήσεις μετά την ανάπτυξη, καθιστώντας τα λιγότερο ευάλωτα σε ορισμένους τύπους επιθέσεων, όπως αυτές που στοχεύουν μηχανισμούς επαναδιαμόρφωσης. Οι CPU, ενώ είναι εξαιρετικά τυποποιημένες και επομένως επωφελούνται από εκτεταμένη έρευνα ασφάλειας και στρατηγικές μετριασμού, δεν προσφέρουν το ίδιο επίπεδο λειτουργικής προσαρμοστικότητας ή απομόνωσης που προσφέρουν οι FPGA.

Οι αναδυόμενες τάσεις στην παραγωγή ηλεκτρονικού υλικού, όπως ο σχεδιασμός του συστήματος σε τσιπ (SoC) που βασίζεται σε πνευματική ιδιοκτησία (βασισμένο σε IP) και μια μακρά και κατανεμημένη αλυσίδα εφοδιασμού για την κατασκευή και τη διανομή ηλεκτρονικών εξαρτημάτων, οδηγούν σε μειωμένο έλεγχο κατασκευαστής τσιπ σχετικά με τα βήματα σχεδιασμού και κατασκευής και έχουν προκαλέσει πολλές αυξανόμενες ανησυχίες για την ασφάλεια.

Τα τελευταία χρόνια η ανάπτυξη της τεχνητής νοημοσύνης και η μηχανική μάθηση απαιτούν όλο και πιο εξελιγμένα ολοκληρωμένα κυκλώματα και πολύ ισχυρούς

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

υπολογιστές προκειμένου να επεξεργαστούν τον τεράστιο όγκο δεδομένων. Η απαίτηση για αυτό το υλικό, αυξάνει τη ζήτηση αλλά και τους κινδύνους επιθέσεων από κακόβουλο λογισμικό επί τους υλικού που μπορεί να έχει τοποθετηθεί πάνω του χωρίς να γίνεται αντιληπτό. Η τεχνητή νοημοσύνη και άλλες καινοτόμες τεχνολογίες έρχονται να δώσουν λύσεις στην ασφάλεια, αλλά ταυτόχρονα μπορούν να χρησιμοποιηθούν και για επιθέσεις παρακάμπτοντας τα ισχυρά σημεία ελέγχου και άμυνας των συστημάτων.

Οι εξελίξεις είναι συνεχείς στο τομέα του υλικού, όπως και οι προσπάθειες άμυνας και ασφάλειας σε παγκόσμιο επίπεδο.

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

ΒΙΒΛΙΟΓΡΑΦΙΑ

- Adee, S. (2008). *The Hunt for the Kill Switch.* IEEE Spectrum 2008.
- Brown, S., & Rose, J. (2012). *Architecture of FPGAs and CPLDs: A Tutorial.* IEEE Design & Test of Computers.
- Dalton, G. (2024). *Artificial Intelligence. Background, Risks and Policies.* USA: Nova Science Publishers, Inc.
- DeNardis, L. (2020). *The Internet in Everything. Freedom and Security in a World with No off Switch.* USA: Yale University Press.
- Farooq, U., & Mehrez, H. (2015). *Interconnect-centric Design for Advanced SOC and NOC.* Switzerland: Springer.
- Guha, K, Saha, S., Chakrabarti, A. (2021). *Self-Aware Security for Real Time Task Schedules in Reconfigurable Hardware Platforms.* Switzerland: Springer.
- Kaspar, M., Tuan La, N., Grunchevski, K., Pham, K., & Dirk, K. (2020). Invited Tutorial: FPGA Hardware Security for Datacenters and Beyond. *In 2020 ACM/SIGDA International Symposium on Field-Programmable Gate Arrays (FPGA'20), February 23–25, 2020, Seaside, CA, USA. ACM, New York, NY, USA, 10 pages.*
- Kim, D. & Solomon, M. (2018). *Fundamentals of information systems security.* USA: Jones & Bartlett Lear.
- Koylu, T. C., Reinbrecht, C., Gebregiorgis, A. B., Hamdioui, S., & Taouil, M. (2023). A Survey on Machine Learning in Hardware Security. *ACM Journal on Emerging Technologies in Computing Systems, 19(2), Article 18.*
- Maglaras, L., & Kantzavelou, I. (2021). *Cybersecurity Issues in Emerging Technologies.* USA: CRC Press.
- Marinescu, D. (2022). *Cloud Computing. Theory and Practice.* USA: Elsevier Inc.
- Martin, K. (2018). *Digital Integrated Circuit Design from VLSI Architectures to CMOS Fabrication.* U.K.: Cambridge University Press.

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

- Mavromoustakis, C., Mastorakis, G., & Dobre, C. (2017). *Advances in Mobile Cloud Computing and Big Data in the 5G Era.* Springer. Switzerland.
- Qadir, F., Ahmad, P., Wani, S., & Peer, M. (2013). Quantum-Dot Cellular Automata: Theory and Application. *2013 International Conference on Machine Intelligence and Research Advancement, Katra, India, 2013, pp. 540-544*
- Qureshi, K, & Newe, T. (2024). *Artificial Intelligence of Things (AIoT) New Standards, Technologies and Communication Systems.* USA: CRC Press.
- Rangarajan, N., Patnaik, S., Knechtel, J., Rakheja, S., & Sinanoglu, O. (2021). *The Next Era in Hardware Security: A Perspective on Emerging Technologies for Secure Electronics.* Springer.
- Ross, A. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems.* USA: Wiley Publishing.
- Ryan, J., (2010). *A History of the Internet and the Digital Future*. London: Reaktion Books
- Smith, S. (2020). *Blockchain, Artificial Intelligence and Financial Services. Implications and Applications for Finance and Accounting Professionals.* Switzerland: Springer.
- Tadashi Miyazaki, T., Oda, N., Goto, Y., & Hayashi, T. (2009). Qualification of FPGA-Based Safety-Related PRM System. Japan: Toshiba Corporation.
- Tang, X., Giacomin, E., Chauviere, B., Alacchi, A., & Gaillardon, P. (2020). OpenFPGA: An Opensource Framework for Agile Prototyping Customizable FPGAs. *IEEE Micro. PP. 1-1. 10.1109/MM.2020.2995854.*
- Tang, X., Kim, G., Gaillardon, E., & De Micheli, G. (2016). A study on the programming structures for RRAM-based FPGA architectures. *IEEE transactions on circuits and systems I: regular papers, VOL. 63, NO. 4, APRIL 2016.*
- Tehranipoor, M., & Bhunia, S. (2019). *Hardware Security. A Hands-on Learning Approach.* USA: Morgan Kaufmann (2019).
- Tu, K., Tang, X., Yu, C., Josipović, L., & Chu, Z. (2024). *FPGA EDA. Design Principles and Implementation.* Singapore: Springer.

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

- Vacca, J. (2017). *Cloud computing security. Foundations and challenges.* USA: CRC Press.
- Wanderley, E, et al, (2011). Security FPGA Analysis. From Secured to Secure *Reconfigurable Systems, 7-46.*
- Xu, X., & Zhang, J. (2020). Rethinking FPGA Security in the New Era of Artificial Intelligence. *Conference: In the 21st International Symposium on Quality Electronic Design (ISQED) At: Santa Clara, California, USA.*
- Zhang, J., & Qu, G. (2019). Recent Attacks and Defenses on FPGA-based Systems. *ACM Transactions on Reconfigurable Technology and Systems. 12. 1-25. 10.1145/3340557.*
- Γκορίλας, Δ. (2022). Τεχνητή νοημοσύνη και οι εφαρμογές της στην ιατρική. ΑΘΗΝΑ. ΙΔΙΩΤΙΚΗ
- Δρόσος, Δ. (2015). *Εισαγωγή στην Επιστήμη των Υπολογιστών & Επικοινωνιών.* Αθήνα: Σύνδεσμος Ελληνικών ακαδημαϊκών βιβλιοθηκών.

ΔΙΑΔΙΚΤΥΟ

- https://www.candtsolution.com/news_events-detail/what-is-asic-application-specific-integrated-circuits/ what is ASIC? Application Specific Integrated Circuits. (Ανάκτηση 10.6.2024)
- https://anysilicon.com/fpga-vs-asic-choose/ FPGA vs ASIC, What to Choose? (Ανάκτηση 10.6.2024)
- Τα Tensor Processing Units (TPU) είναι τα προσαρμοσμένα ανεπτυγμένα ολοκληρωμένα κυκλώματα (ASIC) της Google για συγκεκριμένες εφαρμογές που χρησιμοποιούνται για την επιτάχυνση του φόρτου εργασίας μηχανικής εκμάθησης. Το Cloud TPU είναι μια υπηρεσία ιστού που καθιστά διαθέσιμες τις TPU ως κλιμακωτούς υπολογιστικούς πόρους στο Google Cloud. (Ανάκτηση 12.6.2024 από https://cloud.google.com/tpu/docs/intro-to-tpu).
- Ένα σύστημα σε ένα τσιπ είναι ένα ολοκληρωμένο κύκλωμα που συμπιέζει όλα τα απαιτούμενα εξαρτήματα ενός συστήματος σε ένα κομμάτι πυριτίου . Εξαλείφοντας την ανάγκη για ξεχωριστά και μεγάλα εξαρτήματα συστήματος, τα SoCs βοηθούν στην απλούστευση του σχεδιασμού της πλακέτας κυκλώματος, με αποτέλεσμα βελτιωμένη ισχύ και ταχύτητα χωρίς συμβιβασμούς στη λειτουργικότητα του συστήματος. (Ανάκτηση 12.6.2024 από https://www.ansys.com/blog/what-is-system-on-a-chip)

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250

- https://fpgainsights.com/fpga/fpga-security-challenges-and-best-practices/ FPGAs security: challenges and best practices. (Ανάκτηση 22.6.2024)

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 04:59:53 EEST - 216.73.216.250