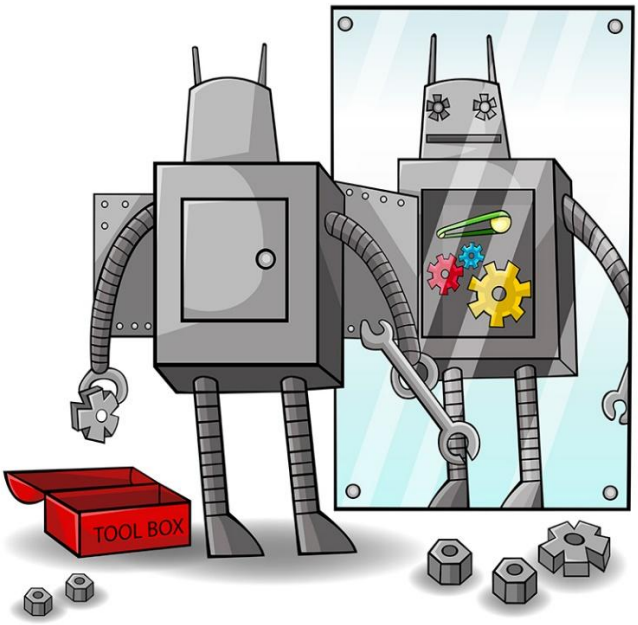
ΔΙΕΘΝΕΣ
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΤΗΣ ΕΛΛΑΔΟΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«ΜΟΝΤΕΛΑ ΑΥΤΟΪΑΣΗΣ ΚΑΙ ΑΠΟΚΑΤΑΣΤΑΣΗΣ IoT ΣΤΗΡΙΖΟΜΕΝΑ ΣΤΗ ΜΗΧΑΝΙΚΗ ΜΑΘΗΣΗ»



Του φοιτητή
Εμμανουηλίδη Παναγιώτη
Αρ. Μητρώου: 03/2022

Επιβλέπων
Ηλιούδης Χρήστος
Καθηγητής

Ημερομηνία 12/09/2025

Τίτλος Δ.Ε. Μοντέλα αυτοΐασης και αποκατάστασης IoT στηριζόμενα στη μηχανική μάθηση
Κωδικός Δ.Ε. **23247**
Ονοματεπώνυμο φοιτητή: Εμμανουηλίδης Παναγιώτης
Ονοματεπώνυμο εισηγητή: Ηλιούδης Χρήστος
Ημερομηνία ανάληψης Δ.Ε. : 10-10-2023
Ημερομηνία περάτωσης Δ.Ε. 12-09-2025

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

Η έγκριση της διπλωματικής εργασίας από το Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του Διεθνούς Πανεπιστημίου της Ελλάδος, δεν υποδηλώνει απαραιτήτως και αποδοχή των απόψεων του συγγραφέα, εκ μέρους του Τμήματος.

Η διπλωματική εργασία αυτή αφιερώνεται στη μνήμη του πατέρα μου Ανέστη, που υπήρξε πάντα στήριγμα σε κάθε μου βήμα και με το παράδειγμά του μου έδειξε τη σημασία της δύναμης, της αγάπης και της προσφοράς.

Στη γυναίκα μου Αθηνά, που με στήριξε με αγάπη και υπομονή, και στις κόρες μας Σοφία και Ειρήνη που με το χαμόγελό τους έδωσαν αξία σε κάθε θυσία…

Στη μητέρα μου Σοφία, το θείο Νίκο και τους άλλους συγγενείς που με τους κόπους τους τόσα χρόνια μου έδωσαν τα μεγαλύτερα εφόδια ζωής.

Τέλος, στον εξαίρετο συνάδελφο Πασπάτη Ιωάννη που τόσα χρόνια αποτέλεσε ένα πρότυπο, ένα φωτεινό φάρο γνώσης και μεθοδικότητας.

Πρόλογος

Η παρούσα διπλωματική εργασία αποτελούσε για μένα μία περίπτωση έρευνας τόσο πάνω στα καθημερινά όσο και στα επιστημονικά μου ενδιαφέροντά. Η έρευνα πραγματεύεται ένα ζήτημα που βρίσκεται στο επίκεντρο της σύγχρονης τεχνολογικής πραγματικότητας: την ασφάλεια και τη διαλειτουργικότητα του Διαδικτύου των Πραγμάτων (Internet of Things – IoT). Η αλματώδης ανάπτυξη των «έξυπνων» συσκευών και η ολοένα αυξανόμενη διείσδυση τους στην καθημερινή ζωή, στη βιομηχανία, στην υγεία και στις έξυπνες πόλεις, αναδεικνύει την ανάγκη ύπαρξης αξιόπιστων προτύπων και πρωτοκόλλων που να εξασφαλίζουν την ασφαλή και αποδοτική τους λειτουργία. Το IoT αποτελεί μία από τις πιο δυναμικά αναπτυσσόμενες τεχνολογικές τάσεις, η οποία όμως συνοδεύεται από προκλήσεις σε επίπεδο ασφάλειας δεδομένων, προστασίας ιδιωτικότητας και ενεργειακής αποδοτικότητας. Στόχος της είναι η διερεύνηση των διεθνών οργανισμών που συμβάλλουν στη θέσπιση προτύπων, καθώς και η αναλυτική παρουσίαση των επικοινωνιακών και κρυπτογραφικών πρωτοκόλλων που αποτελούν τον θεμέλιο λίθο για ένα αξιόπιστο οικοσύστημα IoT.

Η ανάλυση ξεκινά με τη θεωρητική θεμελίωση της αναγκαιότητας προτύπων, συνεχίζοντας με την παρουσίαση των διεθνών οργανισμών και φτάνοντας στην ανάλυση των πρωτοκόλλων επικοινωνίας και ασφάλειας, μελετώνται παραδείγματα εφαρμογών σε πραγματικά περιβάλλοντα. Τέλος, η εργασία καταλήγει σε συμπεράσματα και προτάσεις για το μέλλον της ασφάλειας στο IoT. Έτσι, με την εργασία αυτή ο αναγνώστης μπορεί να κατανοήσει ένα ιδιαίτερα κρίσιμο και πολυδιάστατο πεδίο, το οποίο αποτελεί το επίκεντρο της σύγχρονης πραγματικότητας.

Περίληψη

Η ραγδαία ανάπτυξη του IoT έχει οδηγήσει στη δημιουργία ενός τεράστιου οικοσυστήματος συσκευών, εφαρμογών και υπηρεσιών που αλληλεπιδρούν σε πραγματικό χρόνο, δημιουργώντας νέες δυνατότητες αλλά και προκλήσεις σε επίπεδο διαλειτουργικότητας, αξιοπιστίας και ασφάλειας. Η εργασία αυτή εξετάζει διεξοδικά τα πρότυπα και τα πρωτόκολλα που έχουν αναπτυχθεί για να εξασφαλίσουν την ομαλή λειτουργία των IoT συστημάτων, με ιδιαίτερη έμφαση τόσο στη διαχείριση της επικοινωνίας όσο και στη θωράκιση της ασφάλειας.

Αρχικά, αναλύεται η αναγκαιότητα ύπαρξης διεθνών προτύπων και οργανισμών (ISO, NIST, ETSI, IETF, OASIS, ENISA), που θέτουν τις βάσεις για αξιόπιστη και εναρμονισμένη ανάπτυξη λύσεων IoT σε παγκόσμια κλίμακα. Ιδιαίτερη αναφορά γίνεται στο OpenC^2, ένα πρωτόκολλο που επιδιώκει την τυποποίηση της αυτοματοποιημένης απόκρισης σε περιστατικά ασφαλείας. Στη συνέχεια, παρουσιάζονται και αναλύονται τα κυριότερα επικοινωνιακά πρωτόκολλα για IoT: MQTT, CoAP, AMQP, XMPP και DDS. Η μελέτη τους εστιάζει τόσο στην τεχνική αρχιτεκτονική όσο και στις λειτουργικές ιδιαιτερότητες τους, συμπεριλαμβάνοντας παραδείγματα εφαρμογών σε διαφορετικά σενάρια (π.χ. έξυπνα σπίτια, βιομηχανικό IoT, συστήματα υγείας).

Παράλληλα, εξετάζονται τα πρωτόκολλα ασφάλειας και κρυπτογράφησης που υποστηρίζουν την εμπιστευτικότητα, την ακεραιότητα και την αυθεντικοποίηση στις IoT επικοινωνίες, όπως το TLS/DTLS, η ελαφριά κρυπτογράφηση (lightweight cryptography), το OSCORE και οι τεχνικές End-to-End Encryption και Identity Management.

Τέλος, η εργασία καταλήγει στο συμπέρασμα ότι η τυποποίηση και η σωστή επιλογή πρωτοκόλλων αποτελούν κρίσιμους παράγοντες για την ευρεία υιοθέτηση του IoT και τη μετάβαση σε ένα ασφαλές και διαλειτουργικό τεχνολογικό περιβάλλον. Η συνεχής εξέλιξη και η συνεργασία διεθνών οργανισμών, βιομηχανίας και ερευνητικών φορέων είναι απαραίτητη, ώστε να αντιμετωπιστούν οι νέες προκλήσεις που αναδύονται σε θέματα ασφάλειας, προστασίας δεδομένων και διαχείρισης πόρων.

«IoT Self-Healing and Recovery Models Based on Machine Learning»

«Panagiotis Emmanouilidis»

Abstract

The rapid growth of the Internet of Things (IoT) has led to the emergence of a vast ecosystem of devices, applications, and services that interact in real time, creating new opportunities but also challenges in terms of interoperability, reliability, and security. This thesis provides an in-depth examination of the standards and protocols developed to ensure the smooth operation of IoT systems, with particular emphasis on both communication management and security mechanisms.

Initially, the necessity of international standards and organizations (ISO, NIST, ETSI, IETF, OASIS, ENISA) is analyzed, as they lay the foundations for reliable and harmonized IoT solutions at a global scale. Special attention is given to OpenC2, a protocol aiming to standardize automated incident response in cybersecurity. Subsequently, the study explores the major IoT communication protocols: MQTT, CoAP, AMQP, XMPP, and DDS. Their analysis focuses on both their technical architecture and functional characteristics, including practical examples of applications in different scenarios such as smart homes, industrial IoT (IIoT), and healthcare systems.

In parallel, the research investigates the security and cryptographic protocols that support confidentiality, integrity, and authentication in IoT communications, such as TLS/DTLS, lightweight cryptography, OSCORE, and End-to-End Encryption combined with Identity Management techniques.

Overall, the thesis concludes that standardization and the proper selection of protocols are key factors for the widespread adoption of IoT and the transition towards a secure and interoperable technological ecosystem. Continuous evolution and collaboration among international organizations, industry, and research institutions are essential in addressing the emerging challenges related to security, data protection, and resource management

Ευχαριστίες

Θερμές και ειλικρινείς ευχαριστίες εκφράζω από καρδιάς προς τον επιβλέποντα καθηγητή κ. Ηλιούδη Χρήστο, ο οποίος παρά τις δυσκολίες που αντιμετώπισα στην πορεία της έρευνας, στάθηκε δίπλα μου με καθοδήγηση, ενθάρρυνση και πολύτιμες συμβουλές, συμβάλλοντας καθοριστικά ώστε να μην εγκαταλείψω τον στόχο μου.

Ευχαριστώ επίσης τους προϊσταμένους μου, κ. Παπαπροδρόμου Γεώργιο και κ. Σερκετζή Νικόλαο, οι οποίοι με τις συστατικές τους επιστολές, αλλά και με το προσωπικό τους παράδειγμά της διά βίου μάθησης και αφοσίωσης στη γνώση, άνοιξαν τον δρόμο να εισέλθω στον κόσμο της επιστημονικής κοινότητας.

Περιεχόμενα

Συντομογραφίες

Δ.Ε.	Διπλωματική Εργασία
ΔΙΠΑΕ	Διεθνές Πανεπιστήμιο Ελλάδος
ΤΠΕ	Τεχνολογίες Πληροφορικής και Επικοινωνιών
IoT	Internet of Things (Διαδίκτυο των Πραγμάτων)
ISO	International Organization for Standardization (Διεθνής Οργανισμός Τυποποίησης)
NIST	National Institute of Standards and Technology (Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας)
ETSI	European Telecommunications Standards Institute (Ευρωπαϊκό Ινστιτούτο Προτύπων Τηλεπικοινωνιών)
IETF	Internet Engineering Task Force (Ομάδα Εργασίας Μηχανικών Διαδικτύου)
OASIS	Organization for the Advancement of Structured Information Standards (Οργανισμός για την Προώθηση Προτύπων Δομημένης Πληροφορίας)
ENISA	European Union Agency for Cybersecurity (Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια)
OpenC²	Open Command and Control (Ανοικτό Πλαίσιο Εντολών και Ελέγχου)
MQTT	Message Queuing Telemetry Transport (Μεταφορά Τηλεμετρικών Μηνυμάτων με Ουρές)
CoAP	Constrained Application Protocol (Πρωτόκολλο Περιορισμένων Εφαρμογών)
REST APIs	Representational State Transfer Application Programming Interfaces (Διεπαφές Προγραμματισμού Εφαρμογών REST)
AMQP	Advanced Message Queuing Protocol (Προηγμένο Πρωτόκολλο Ουράς Μηνυμάτων)
XMPP	Extensible Messaging and Presence Protocol (Επεκτάσιμο Πρωτόκολλο Μηνυμάτων και Παρουσίας)
DDS	Data Distribution Service (Υπηρεσία Διανομής Δεδομένων)
TLS	Transport Layer Security (Ασφάλεια Επίπεδου Μεταφοράς)
DTLS	Datagram Transport Layer Security (Ασφάλεια Επίπεδου Μεταφοράς Δεδομένο γραμμάτων)
OSCORE	Object Security for Constrained RESTful Environments (Ασφάλεια Αντικειμένων για Περιορισμένα RESTful Περιβάλλοντα)
E2EE	End-to-End Encryption (Κρυπτογράφηση από Άκρο σε Άκρο)
ECC	Elliptic Curve Cryptography (Κρυπτογράφηση Ελλειπτικών Καμπυλών)
RSA	Rivest–Shamir–Adleman (Αλγόριθμος κρυπτογράφησης)
AES-CCM	Advanced Encryption Standard – Counter with CBC-MAC (Πρότυπο Προηγμένης Κρυπτογράφησης με Μετρητή και CBC-MAC)
LWC	Lightweight Cryptography (Ελαφριά Κρυπτογράφηση)
AUTOSAR	Automotive Open System Architecture (Ανοικτή Αρχιτεκτονική Συστημάτων Αυτοκινήτου)
ISO 26262	Functional Safety for Road Vehicles (Λειτουργική Ασφάλεια για Οχήματα Δρόμου)

DO-178C	Software Considerations in Airborne Systems and Equipment Certification (Ζητήματα Λογισμικού για Πιστοποίηση Αεροπορικών Συστημάτων και Εξοπλισμού)
DO-254	Design Assurance Guidance for Airborne Electronic Hardware (Κατευθυντήριες Οδηγίες Σχεδίασης για Αεροπορικό Ηλεκτρονικό Υλικό)
AI	Artificial Intelligence (Τεχνητή Νοημοσύνη)
ML	Machine Learning (Μηχανική Μάθηση)
FLISR	Fault Location, Isolation, and System Restoration (Εντοπισμός Βλάβης, Απομόνωση και Αποκατάσταση Συστήματος)
ADA	Advanced Distribution Automation (Προηγμένος Αυτοματισμός Διανομής)
MAS	Multi-Agent Systems (Πολυπρακτορικά Συστήματα)
ODiS	Organic Distribution System (Οργανικό Σύστημα Διανομής)
DMS	Distribution Management System (Σύστημα Διαχείρισης Διανομής)
HEMS	Home Energy Management System (Σύστημα Διαχείρισης Ενέργειας Κατοικίας)
SHM	Structural Health Monitoring (Παρακολούθηση Δομικής Υγείας)
IoMT	Internet of Medical Things (Διαδίκτυο Ιατρικών Συσκευών)
V2X	Vehicle-to-Everything (Επικοινωνία Οχήματος με Οτιδήποτε)
HTTP	HyperText Transfer Protocol (Πρωτόκολλο Μεταφοράς Υπερκειμένου)
HTTPS	HTTP over TLS (Ασφαλές HTTP - HTTP πάνω από TLS)
TCP	Transmission Control Protocol (Πρωτόκολλο Ελέγχου Μεταδόσεων)
UDP	User Datagram Protocol (Πρωτόκολλο Δεδογραμμάτων Χρήστη)
WebSocket	(Πρωτόκολλο αμφίδρομης επικοινωνίας σε πραγματικό χρόνο)
M2M	Machine-to-Machine (Επικοινωνία Μηχάνημα-με-Μηχάνημα)
BLE	Bluetooth Low Energy (Bluetooth Χαμηλής Ενέργειας)
Wi-Fi	Wireless Fidelity (Ασύρματη Συνδεσιμότητα)
JSON	JavaScript Object Notation (Σημειογραφία Αντικειμένων JavaScript)
JWT	JSON Web Token (Διακριτικό Ιστού JSON -για έλεγχο ταυτότητας)
OAuth2	OAuth 2.0 (Πρωτόκολλο Ανοικτής Εξουσιοδότησης 2.0
RTPS	Real-Time Publish-Subscribe Protocol (Πρωτόκολλο Δημοσίευσης-Εγγραφής σε Πραγματικό Χρόνο)
QoS	Quality of Service (Ποιότητα Υπηρεσίας)
SSL	Secure Sockets Layer (Στρώμα Ασφαλών Συνδέσεων)
SASL	Simple Authentication and Security Layer (Απλό Στρώμα Αυθεντικοποίησης και Ασφάλειας)

AEAD	Authenticated Encryption with Associated Data (Αυθεντικοποιημένη Κρυπτογράφηση με Σχετιζόμενα Δεδομένα)
ChaCha20-Poly1305	Αλγόριθμος Αυθεντικοποιημένης Κρυπτογράφησης (AEAD)
ACK	Acknowledgement (Επιβεβαίωση)
CON	Confirmable (Επιβεβαιώσιμο μήνυμα CoAP)
NON	Non-Confirmable (Μη επιβεβαιώσιμο μήνυμα CoAP)
RST	Reset (Επαναφορά μηνύματος CoAP)
URI	Uniform Resource Identifier (Ομοιόμορφος Εντοπιστής Πόρου)
RFC	Request for Comments (Έγγραφο RFC)
OMG	Object Management Group (Ομάδα Διαχείρισης Αντικειμένων)
VoIP	Voice over IP (Φωνή μέσω IP)
CIA	Confidentiality, Integrity, Availability (εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα)
ISMS	Information Security Management System (Σύστημα διαχείρισης της ασφάλειας των πληροφοριών)
ML	Machine Learning (Μηχανική Μάθηση)
RL	Reinforcement Learning (Ενισχυτική Μάθηση)
IoMT	Internet of Medical Things (Διαδίκτυο Ιατρικών Συσκευών)
IIoT	Industrial Internet of Things (Βιομηχανικό IoT)
MAS	Multi-Agent Systems (Πολυπρακτορικά Συστήματα)
XAI	Explainable Artificial Intelligence (Επεξηγήσιμη Τεχνητή Νοημοσύνη)
FLISR	Fault Location, Isolation, and System Restoration (Εντοπισμός, Απομόνωση και Αποκατάσταση Βλαβών)
FL	Federated Learning (Ομοσπονδιακή Μάθηση)

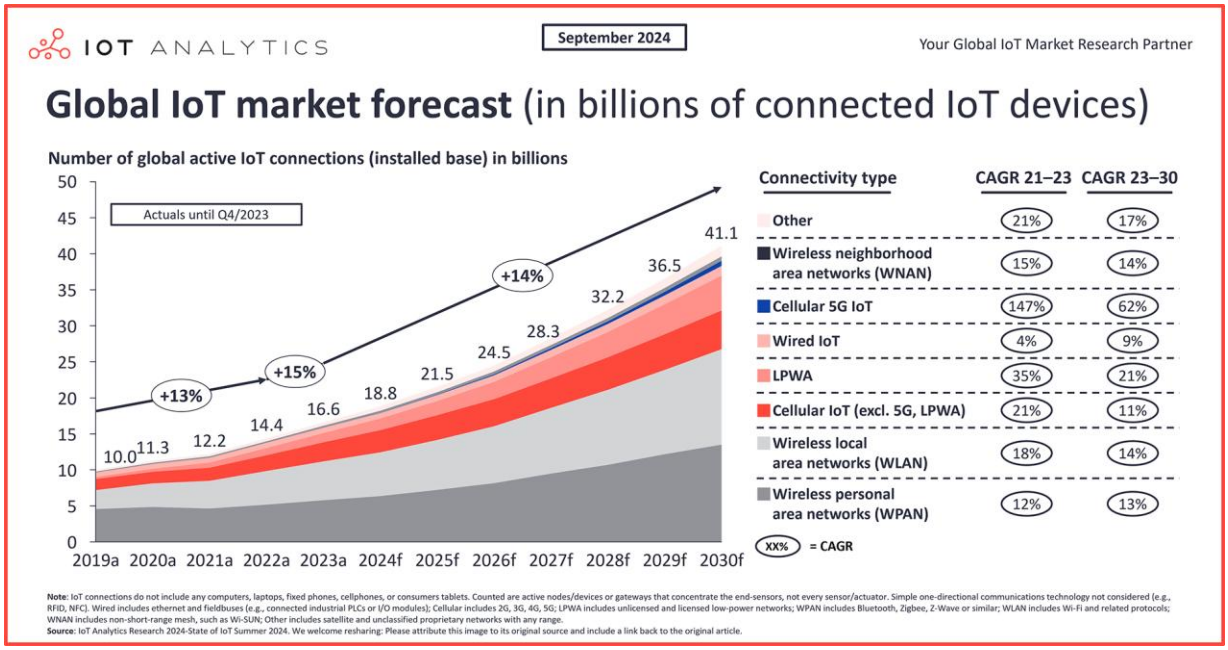
Κεφάλαιο 1ο: Εισαγωγή

Η έκρηξη του Διαδικτύου των Πραγμάτων (IoT) έχει σημάνει την έναρξη μιας πολύ γρήγορης αύξησης του αριθμού των συσκευών που είναι συνδεδεμένες στο δίκτυο και του όγκου των δεδομένων που ανταλλάσσονται σε πραγματικό χρόνο. Η πολυπλοκότητα αυτών των συστημάτων, μαζί με τις αυξημένες απαιτήσεις για αξιοπιστία, διαθεσιμότητα και ασφάλεια, έχει ως αποτέλεσμα να γίνεται απαραίτητη η ανάπτυξη μηχανισμών αυτόματης λειτουργίας και αποκατάστασης. Η χρήση τεχνικών μηχανικής μάθησης παρέχει νέες δυνατότητες για την ανίχνευση και την αυτόματη αντιμετώπιση βλαβών, με αποτέλεσμα να βελτιώνεται η αξιοπιστία και η αποτελεσματικότητα των συστημάτων IoT. Στην παρούσα εργασία γίνεται μια ανάλυση των πιο σύγχρονων προτάσεων που συνδυάζουν την αυτοματοποίηση με προηγμένους αλγορίθμους μηχανικής μάθησης, με στόχο να δημιουργηθεί ένα έξυπνο και αυτόνομο σύστημα λειτουργίας.

1.1 Αντικείμενο της διπλωματικής εργασίας

Η παρούσα Διπλωματική Εργασία (Δ.Ε.) επικεντρώνεται στη μελέτη των μοντέλων αυτοΐασης και αποκατάστασης βλαβών στις συσκευές που λειτουργούν μέσα σε ένα περιβάλλον του IoT και πως με τη χρήση της μηχανικής μάθησης μπορεί να επιτευχθεί ένα βέλτιστο αποτέλεσμα.

Το IoT έχει εδραιωθεί ως ένα αναπόσπαστο στοιχείο της καθημερινότητας στη σύγχρονη ζωή, επηρεάζοντας και συμβάλλοντας σε τεράστιο βαθμό πληθώρα τομέων και δημιουργώντας νέες δυνατότητες εφαρμογών. Η συνεχής ανάπτυξη των εφαρμογών αυτών αντικατοπτρίζεται και σε πραγματικούς αριθμούς όπου σύμφωνα με ειδικούς αναλυτές του IoT για το 2024 διαπιστώθηκε μια αύξηση κατά 13% και οι συνδεδεμένες συσκευές IoT να ξεπερνούν τα 18,8 δισεκατομμύρια. Εκτιμάται πως μέχρι το 2030 ο αριθμός αυτός θα φτάσει τις 40 δισεκατομμύρια συσκευές. [1]

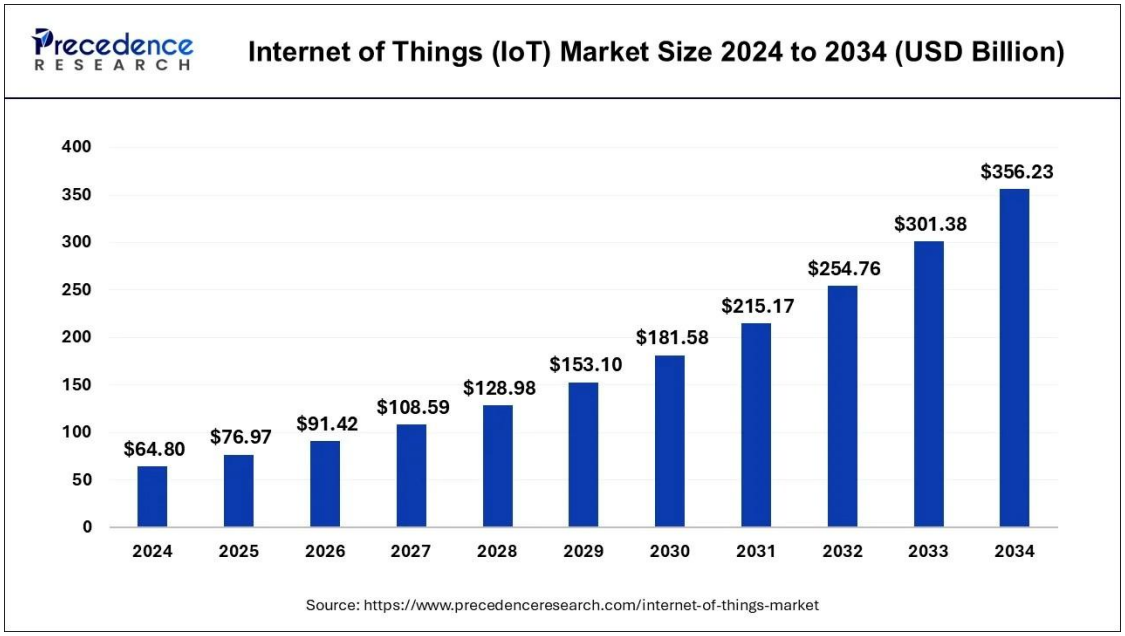


Εικόνα 1: Παγκόσμια διασύνδεση IoT συσκευών.

Πηγή: https://iotbusinessnews.com/state-of-iot-2024-number-of-connected-iot-devices-growing

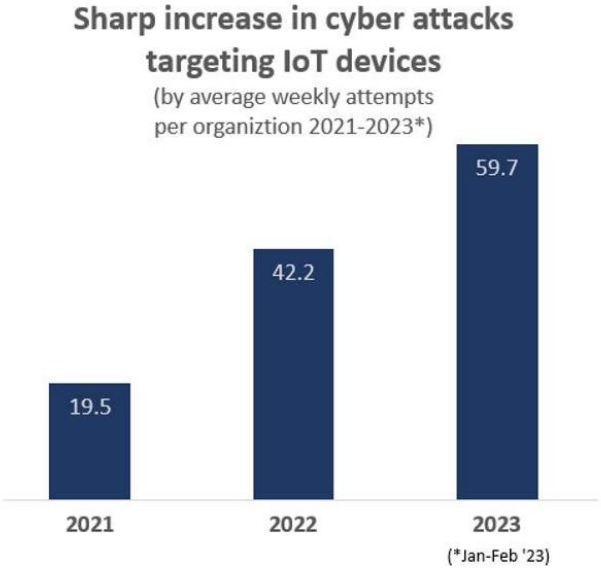
Οι οικονομικές επενδύσεις στον κλάδο του IoT εμφανίζουν αυξητική τάση. Οι δαπάνες για το 2024 άγγιξαν τα 65 δις δολάρια παγκοσμίως ενώ με την ολοένα αυξανόμενη πορεία εκτιμάται πως το 2030 θα ανέλθουν στα 181 δις δολάρια. Παρατηρούμε δηλαδή έναν τριπλασιασμό των επενδύσεων,

ενώ μέχρι το 2034 εκτιμάται πως οι επενδύσεις θα εξαπλασιαστούν αγγίζοντας τα 360 δις δολάρια, όπως φαίνεται και στον ακόλουθο πίνακα.



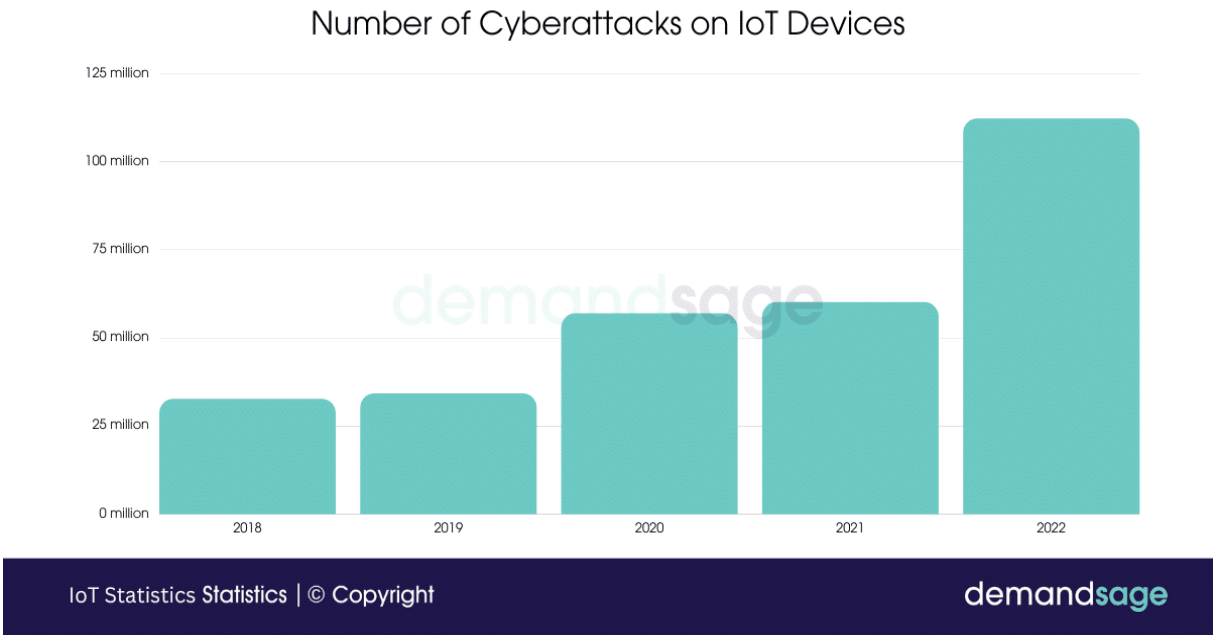
Πηγή: https://www.precedenceresearch.com/internet-of-things-market

Ωστόσο, ένα σημαντικό στοιχείο που δεν πρέπει να παραλειφθεί είναι η ασφάλεια αυτών των συσκευών. Η συνεχής αύξηση των διασυνδεδεμένων IoT συσκευών προσφέρει στους κακόβουλους χρήστες μεγαλύτερο πεδίο δράσης για την εξαπάτηση των χρηστών ή των οικοσυστημάτων για τους σκοπούς που χρησιμοποιούνται. Σύμφωνα με τα στοιχεία μίας έρευνας, οι κυβερνοεπιθέσεις από το 2021 μέχρι το 2023 τριπλασιάστηκαν, ενώ επίσης η ίδια έρευνα έδειξε πως εβδομαδιαίως το 54% των οργανισμών υπάρχουν κυβερνοεπιθέσεις κατά των IoT συσκευών [2], [3].



Πηγή: www.itsecuritypro.gr/apotomi-ayxisi-ton-kyvernoepitheseon-se-iot-syskeyes

Άλλη έρευνα έδειξε ότι από το 2018 που υπήρχαν 32.7 εκατομμύρια κυβερνοεπιθέσεις στις συσκευές IoT, μέσα σε τέσσερα χρόνια το 2022 ο αριθμός αυτός ανήλθε σε 112 εκατομμύρια κυβερνοεπιθέσεις, μια αύξηση της τάξης 400%. [4]



Πηγή: www.demandsage.com/internet-of-things-statistics/

Όπως γνωρίζουμε οι εφαρμογές του IoT εκτείνονται από το άμεσο οικιακό περιβάλλον με τα «έξυπνα σπίτια», ενώ ακόμα έχουν δημιουργηθεί μέχρι και «έξυπνα αυτόνομα χωριά», έως τον επαγγελματικό κλάδο που αξιοποιούνται σωρηδόν ώστε να συμβάλλουν στη βελτίωση της λειτουργικότητας των χρηστών είτε άμεσα στην παραγωγική διαδικασία των προϊόντων. Ακόμα, μπορούν να εντοπιστούν σε δημόσιες υποδομές και υπηρεσίες. Ζωτικής σημασίας αποτελεί η χρήση τους σε εφαρμογές της υγείας συμβάλλοντας στη βελτίωση της υγείας του ανθρώπου, ενώ ακόμα η χρήση τους σε εφαρμογές της γεωργίας προσφέρουν καλύτερη διαχείριση από τους γεωργούς με αποτέλεσμα την καλύτερη αποδοτικότητα καθώς και μεγαλύτερη παραγωγικότητα.

Όλες οι προαναφερθείσες κατηγορίες παρατηρούμε να χρησιμοποιούν τις συσκευές αυτές προκειμένου να αποκομίσουν οφέλη τόσο εξοικονόμησης πόρων και βελτίωσης της ζωής των πολιτών όσο και προς τους ίδιους τους διαχειριστές τους για την αποδοτικότερη λειτουργία του κλάδου τους. Θα μελετηθούν οι συσκευές που λειτουργούν σε αυτά τα περιβάλλοντα IoT και το πως επικοινωνούν μεταξύ τους ή με άλλες συσκευές, τι πρωτόκολλά επικοινωνίας χρησιμοποιούν, ώστε να αντιληφθούμε το πως αυτές οι συσκευές προβαίνουν στη συλλογή, τη μετάδοση και την ανταλλαγή των δεδομένων τους, προσφέροντας έτσι νέες δυνατότητες για την παρακολούθηση, τον έλεγχο και την αυτοματοποίηση σε ποικίλες εφαρμογές.

Είναι εμφανές ότι με δεδομένη την αυξητική τάση για νέες συσκευές, ολοένα αυξάνεται η πολυπλοκότητα των συστημάτων αυτών για την ορθή διαχείριση και επίβλεψη τους. Έτσι, θα δημιουργείται ένα ευρύτερο πεδίο προς εκμετάλλευση από επιτήδειους, με κακόβουλους σκοπούς, προκαλώντας ένα κλίμα ανασφάλειας, ενώ παράλληλα γίνεται επιτακτική η ανάγκη για την προστασία τους και την αποκατάσταση όσων εξ αυτών δεχθούν επίθεση ή υπέστησαν κάποια βλάβη. Ως εκ τούτου αποτελεί μείζονας σημασίας η μελέτη των μοντέλων αυτοΐασης, ακόμα και ο εντοπισμός νέων μοντέλων, που θα συμβάλει με αυτό τον τρόπο στην ασφάλεια, την ανθεκτικότητα, και την αξιοπιστία του περιβάλλοντος.

Οι απειλές που έχουν να αντιμετωπίσουν οι συσκευές ποικίλουν και έχουν να κάνουν ανάλογα με το βαθμό επικινδυνότητας, ή ακόμα και με το μέγεθος της τεχνικής βλάβης που μπορεί να υποστούν.

Σε αυτές τις περιπτώσεις μπορεί η αποκατάστασή τους να απαιτεί τη χρήση προηγμένων τεχνολογικών λύσεων και εφαρμογών που πολλές φορές θα είναι χρονοβόρες και κοστοβόρες.

Στο σημείο αυτό εισέρχεται και ο ρόλος της μηχανικής μάθησης όπου με τη χρήση μεθόδων και μοντέλων θα είναι σε θέση να συμβάλλει στην καλύτερη, αποτελεσματικότερή και ευφυέστερη επίλυση του προβλήματος είτε ασφαλείας είτε τεχνικού. Με τη μηχανική μάθηση κάνοντας χρήση ευέλικτων μοντέλων μπορεί να προβλεφθεί πιθανή ανωμαλία του συστήματος ή κάποια επίθεση, ενώ παράλληλα να είναι σε θέση με τις κατάλληλες παραμετροποιήσεις να εκτελεί ενέργειες προς αποτροπή της επίθεσης ή προς άμεση αποκατάσταση της βλάβης εφόσον υπάρξει.

1.2 Σκοπός – στόχος της διπλωματικής εργασίας

Ο κύριος σκοπός της παρούσας Διπλωματικής Εργασίας είναι η μελέτη των οικοσυστημάτων IoT και η διερεύνηση τρόπων υλοποίησης μηχανισμών αυτοΐασης των συσκευών που τα απαρτίζουν, σε συνδυασμό με τεχνικές μηχανικής μάθησης, με στόχο τη βελτιστοποίηση διορθωτικών και προληπτικών ενεργειών.

Πιο συγκεκριμένα, η εργασία στοχεύει στα εξής:

1. Μελέτη του θεωρητικού υποβάθρου της αυτοΐασης, με ανάλυση του τρόπου λειτουργίας της και της συνεισφοράς της σε διαφορετικά είδη συστημάτων.
2. Καταγραφή και ανάλυση προτύπων και πρωτοκόλλων επικοινωνίας που χρησιμοποιούνται σε περιβάλλοντα IoT, με ιδιαίτερη έμφαση στο πρότυπο OpenC^2.
3. Έλεγχο της εφαρμοσιμότητας των πρωτοκόλλων σε πραγματικές IoT συσκευές και αξιολόγηση της απόδοσής τους.
4. Ανάλυση μοντέλων Μηχανικής μάθησης (ML) που χρησιμοποιούνται σε εφαρμογές IoT.
5. Μελέτη περίπτωσης (case study) για την εξέταση της αρχιτεκτονικής του IoT, των μοντέλων επικοινωνίας που χρησιμοποιούνται, καθώς και την καταγραφή υπαρχουσών ευπαθειών και κινδύνων.
6. Διατύπωση προτάσεων βελτίωσης και ενσωμάτωσης μοντέλων αυτοΐασης, με στόχο την αύξηση της ασφάλειας, της ανθεκτικότητας και της αξιοπιστίας των IoT οικοσυστημάτων.

1.3 Επιτεύγματα της διπλωματικής εργασίας

Κατά την εκπόνηση της παρούσας Διπλωματικής Εργασίας επιτεύχθηκαν τα ακόλουθα:

1. Αναπτύχθηκε πλήρης βιβλιογραφική βάση για τα μοντέλα αυτοΐασης σε περιβάλλοντα IoT, καταγράφοντας τις επικρατούσες τεχνικές και τις ερευνητικές τάσεις
2. Καταγράφηκαν και αναλύθηκαν τα βασικά πρότυπα και πρωτόκολλα επικοινωνίας, με ιδιαίτερη έμφαση στο OpenC^2 και την εφαρμογή του σε IoT συσκευές
3. Πραγματοποιήθηκε αξιολόγηση της αποτελεσματικότητας των υφιστάμενων λύσεων, εντοπίζοντας σημεία βελτίωσης και πιθανές αδυναμίες
4. Υλοποιήθηκε μελέτη περίπτωσης, η οποία ανέδειξε συγκεκριμένες ευπάθειες και κινδύνους σε ένα αντιπροσωπευτικό IoT οικοσύστημα
5. Προτάθηκε βελτιωμένο μοντέλο αυτοΐασης, το οποίο αξιοποιεί τεχνικές μηχανικής μάθησης για την έγκαιρη ανίχνευση, διάγνωση και αποκατάσταση βλαβών

6. Διατυπώθηκαν πρακτικές κατευθύνσεις για την ενίσχυση της ασφάλειας, της ανθεκτικότητας και της αξιοπιστίας των IoT συστημάτων

1.4 Διάρθρωση της διπλωματικής εργασίας

Η Διπλωματική Εργασία αποτελείται από έξι κεφάλαια, τα οποία αναπτύσσονται ως εξής:

- Το Κεφάλαιο 1 – Εισαγωγή, περιλαμβάνει το υπόβαθρο και το αντικείμενο της εργασίας, ο σκοπός και οι στόχοι της, τα βασικά επιτεύγματα, καθώς και η συνολική δομή της μελέτης.
- Στο Κεφάλαιο 2 – Αυτοΐαση – Self Healing γίνεται η περιγραφή των τομέων και κλάδων στους οποίους εφαρμόζονται τεχνικές αυτοΐασης, με ανάλυση του θετικού αντίκτυπου που έχουν στις λειτουργίες τους.
- Στο Κεφάλαιο 3 – Πρότυπα και πρωτόκολλα για συστήματα αυτοΐασης αναλύονται τα πρότυπα και τα πρωτόκολλα επικοινωνίας που υποστηρίζουν τα μοντέλα αυτοΐασης, εξετάζοντας τα πλεονεκτήματα και τους περιορισμούς τους, καθώς και τα σημεία που μπορούν να αποτελέσουν στόχο κυβερνοεπιθέσεων ή να οδηγήσουν σε δυσλειτουργίες.
- Στο Κεφάλαιο 4 – Εφαρμογές IoT με ενσωματωμένα μοντέλα αυτοΐασης γίνεται παρουσίαση με παραδείγματα εφαρμογών IoT που ενσωματώνουν μηχανισμούς αυτοΐασης, οι τύποι επιθέσεων και βλαβών που αντιμετωπίζουν, οι υφιστάμενες διαδικασίες αποκατάστασης, καθώς και οι δυνατότητες βελτίωσής τους μέσω μηχανικής μάθησης.
- Στο Κεφάλαιο 5 - Μοντέλα Αυτοΐασης στηριζόμενα στη Μηχανική Μάθηση, όπου παρουσιάζονται τα υφιστάμενα μοντέλα αυτοΐασης που χρησιμοποιούν μοντέλα Μηχανικής Μάθησης για τη βελτιστοποίηση των εφαρμογών IoT.
- Στο Κεφάλαιο 6 – Μελέτη περίπτωσης έγινε μια ανάπτυξη ενός συγκεκριμένου IoT οικοσυστήματος που υπέστη παραβίαση και εντοπίζονται οι ευπάθειες, αξιολογείται η αποτελεσματικότητα και αναλύονται οι λύσεις που εφαρμόστηκαν, και τέλος γίνεται μια πρόταση προτεινόμενων μοντέλων αυτοΐασης.
- Τέλος, στο Κεφάλαιο 7 – Συμπεράσματα και μελλοντικές επεκτάσεις: Συνοψίζονται τα ευρήματα της εργασίας και προτείνονται κατευθύνσεις για μελλοντική έρευνα και εφαρμογή της μηχανικής μάθησης σε μοντέλα αυτοΐασης IoT.

1.5 Επίλογος

Στο πρώτο κεφάλαιο περιγράφεται η γενική αναφορά της Διπλωματικής Εργασίας, δίνεται έμφαση στον σκοπό, τους στόχους, τα επιτεύγματα και τη δομή της. Αναδεικνύεται η έκρηξη του Διαδικτύου των Πραγμάτων, η συνεχώς αυξανόμενη πολυπλοκότητα των συστημάτων του και οι προκλήσεις που προκύπτουν σε θέματα ασφάλειας, ανθεκτικότητας και αξιοπιστίας. Τονίζεται ιδιαίτερα η ανάγκη να δημιουργηθούν και να εφαρμοστούν μηχανισμοί αυτό-προστασίας, που θα βασίζονται σε τεχνικές μηχανικής μάθησης και θα είναι σε θέση να αντιμετωπίζουν με επιτυχία βλάβες και επιθέσεις, εξασφαλίζοντας τη συνεχή λειτουργία των οικοσυστημάτων IoT.

Σκοπός του κειμένου αυτού είναι να αναπτύξει τη θεωρητική βάση και την πρακτική κατανόηση του πως λειτουργεί η αυτοΐαση, διερευνώντας τις υπάρχουσες λύσεις και προτείνοντας βελτιωμένα μοντέλα που να ανταποκρίνονται στις ανάγκες και τις προκλήσεις του IoT. Το επόμενο κεφάλαιο επικεντρώνεται στους κύριους τομείς εφαρμογής της αυτοματοποίησης, με σκοπό να δώσει μια βάση για τις αναλύσεις και τα πειράματα που θα παρουσιαστούν στα επόμενα κεφάλαια.

Κεφάλαιο 2ο: Αυτοΐαση – Self Healing

Η έννοια της αυτοΐασης ξεκίνησε από τον ιατρικό τομέα όμως σήμερα έχει εξελιχθεί εφαρμόζεται σε πολλούς επιστημονικούς και τεχνολογικούς τομείς. Από τη φυσική ικανότητα του οργανισμού να επουλώνει τραύματα, μέχρι την ικανότητα των τεχνικών συστημάτων να εντοπίζουν, διαγιγνώσκουν και διορθώνουν προβλήματα χωρίς την ανθρώπινη παρέμβαση, η αυτοΐαση παίζει σημαντικό ρόλο στη διατήρηση της ομαλής λειτουργίας και της ανθεκτικότητας του ανθρώπου και των συστημάτων. Σε αυτό το κεφάλαιο, θα εξετάσουμε τον ιατρικό ορισμό της αυτοΐασης για να αντιληφθούμε τη βάση της, καθώς και τα υφιστάμενα μοντέλα αυτοΐασης και τις εφαρμογές της σε άλλους τομείς όπως η πληροφορική, η ενέργεια, η βιομηχανία, η υγεία και οι έξυπνες πόλεις. Επιπλέον, θα αναλύσουμε τις προκλήσεις ασφαλείας που προκύπτουν με τη χρήση της και τις δυνατότητες που προσφέρει σε απαιτητικά περιβάλλοντα, όπως τα δίκτυα του IoT.

2.1 Ιατρικός ορισμός αυτοΐασης και οι περαιτέρω εφαρμογές της

Ουκ ολίγες φορές στον τομέα της πληροφορικής και εν γένει στον τεχνολογικό τομέα, εντοπίζουμε ορισμούς και γενικότερα τον τρόπο λειτουργίας να προέρχονται από την ανθρώπινη ύπαρξη και δη από την ιατρική επιστήμη. Έτσι και σε αυτή την περίπτωση παρατηρούμε ότι η γένεση του ορισμού της αυτοΐασης προέρχεται απ' τον κλάδο της ιατρικής, όπου σύμφωνα με αυτόν μελετάται με ποιον τρόπο ο άνθρωπος μπορεί να επανακάμψει - αυτοϊαθεί σε διάφορες μορφές ασθένειας ή επιπλοκές που μπορεί να προκύψουν από διάφορες καταστάσεις.

Η έννοια της αυτοΐασης αποτελεί έναν βασικό πυλώνα στον τομέα της υγείας, προερχόμενη από την ιατρική επιστήμη, που εξετάζει τον τρόπο με τον οποίο ο άνθρωπος μπορεί να αυτοθεραπευτεί από διάφορες ασθένειες και επιπλοκές ή άλλες μη συνήθεις καταστάσεις. Σύμφωνα με τον ιατρικό ορισμό, η αυτοΐαση αναφέρεται στη δυνατότητα του οργανισμού να επαναφέρει τον εαυτό του σε μια φυσιολογική κατάσταση. Κυρίαρχος παράγοντας σε αυτή τη διαδικασία είναι το ανοσοποιητικό σύστημα του ανθρώπινου οργανισμού, το οποίο ολοκληρώνεται από την ανοσία. Με την ενίσχυση του ανοσοποιητικού μας συστήματος ουσιαστικά θωρακίζουμε τον οργανισμό προκειμένου να μη βρεθεί σε μια ανεπιθύμητη κατάσταση που θα θεωρεί ότι ο οργανισμός νοσεί. Έτσι, αντιλαμβανόμαστε ότι ο οργανισμός, μέσω μιας καλής και ισορροπημένης διατροφής και αρκετών ακόμα παραγόντων, στήνει ορισμένους μηχανισμούς προληπτικής άμυνας ισχυροποιώντας την δυναμική του για την καταπολέμηση αυτής της κατάστασης.

Εικόνα 2.1: Human Self-Healing

Πηγή: https://www.iatropedia.gr/66535/

Όταν ένας οργανισμός νοσήσει ή προσβληθεί από κάποια ασθένεια μετά διατηρεί σαν ιστορικό αυτό που τον προσέβαλε και «εκπαιδεύεται», αναγνωρίζει από τι νόσησε, τι τον επηρέασε, αποκτώντας με αυτό τον τρόπο την επονομαζόμενη ανοσία, όπου μελλοντικά να μπορεί να το αντιμετωπίσει με μεγαλύτερη αποτελεσματικότητα και ταχύτητα, ενώ υπάρχουν ορισμένες περιπτώσεις που μπορεί να ιαθεί χωρίς καν να παρουσιάσει τα συμπτώματα της ασθένειας.

Είδαμε πολύ επιφανειακά ότι η αυτοΐαση αποτελεί έναν σημαντικό παράγοντα για την υγεία του ανθρώπου. Πέραν όμως της φυσικής αυτοΐασης μπορούμε να διακρίνουμε και την τεχνητή αυτοΐαση, όπου η ιατρική επιστήμη έρχεται με διαφόρων ειδών παρεμβάσεις να προσφέρει στον άνθρωπο τη δυνατότητα να επανέλθει στην πρότερη φυσιολογική του κατάσταση. Κάποιες περιπτώσεις εξ αυτών αποτελούν για παράδειγμα οι σωματικές παρεμβάσεις, με πιο συνήθη περίπτωση την προσθήκη κάποιου ανθρώπινου μέλους του σώματος, ενώ ακόμα μπορεί να υπάρξει παρέμβαση με την επαναφορά εσωτερικών οργάνων ή στοιχείων που είναι ζωτικής σημασίας όπως για παράδειγμα η βελτίωση λειτουργίας της καρδιάς ή άλλων αιματολογικών και λοιπών λειτουργιών.

Η χρήση σχεδίων διαχείρισης για υποβοήθηση με τεχνητό τρόπο της αυτοΐαση προσφέρουν πολλαπλά οφέλη τόσο για τους ασθενείς που ανακάμπτουν ταχύτερα, ενώ παράλληλα δεν επιβαρύνει το εθνικό σύστημα υγείας του κάθε κράτους εξοικονομώντας πόρους λόγω της ταχύτερης ίασης.

2.2 Μοντέλα Αυτοΐασης

Πριν εξετάσουμε τις επιμέρους εφαρμογές της αυτοΐασης σε διαφορετικούς κλάδους, είναι σημαντικό να παρουσιαστούν τα θεωρητικά μοντέλα που περιγράφουν τη λειτουργία της. Η έννοια της αυτοΐασης στις μη ανθρώπινες εφαρμογές βασίζεται σε μεθοδολογίες και αρχιτεκτονικές που καθορίζουν το πώς ένα σύστημα ανιχνεύει ανωμαλίες, αναλύει τα αίτια και επανέρχεται σε πλήρη λειτουργία, συχνά χωρίς την παρέμβαση ανθρώπινου χειριστή.

Τα κυριότερα μοντέλα που καταγράφονται στη βιβλιογραφία περιλαμβάνουν [5], [6], [7], [8]:

1. Μοντέλο Ανίχνευσης και Ανάκαμψης (Detection and Recovery Model):
   Στηρίζεται σε μηχανισμούς συνεχούς παρακολούθησης που εντοπίζουν σφάλματα και ενεργοποιούν διαδικασίες αποκατάστασης, όπως επανεκκίνηση συστημάτων ή επαναφορά ρυθμίσεων.

2. Μοντέλο Αυτοπροσαρμογής (Self - Adaptive Model):
   Επιτρέπει στο σύστημα να μεταβάλλει παραμέτρους λειτουργίας, ώστε να παρακάμπτει προβλήματα και να συνεχίζει τη λειτουργία του με μειωμένες επιπτώσεις μέχρι την πλήρη αποκατάσταση.

3. Μοντέλο Αναπαραγωγής ή Αυτοαντικατάστασης (Replication/Replacement Model):
   Βασίζεται στη δημιουργία εφεδρικών αντιγράφων ή στην αυτόματη αντικατάσταση ελαττωματικών στοιχείων, συχνά σε περιβάλλοντα cloud ή κατανεμημένα δίκτυα.

4. Μοντέλο Πρόβλεψης και Πρόληψης (Predictive and Preventive Model):
   Εφαρμόζει τεχνικές ανάλυσης δεδομένων και μηχανικής μάθησης για την πρόβλεψη πιθανών δυσλειτουργιών πριν αυτές εκδηλωθούν, ενεργοποιώντας προληπτικές ενέργειες.

5. Υβριδικό Μοντέλο (Hybrid Model):
   Συνδυάζει στοιχεία από διαφορετικά μοντέλα για να καλύψει περίπλοκα περιβάλλοντα όπου απαιτείται τόσο πρόβλεψη όσο και ταχεία αποκατάσταση.

Η κατανόηση των παραπάνω μοντέλων είναι καθοριστική για την ερμηνεία των εφαρμογών που θα παρουσιαστούν στις επόμενες ενότητες, καθώς κάθε βιομηχανικός κλάδος υιοθετεί ή προσαρμόζει αυτά τα μοντέλα ανάλογα με τις ανάγκες, τις τεχνικές δυνατότητες και τις απαιτήσεις αξιοπιστίας.

2.3 Η αυτοΐαση σε διάφορους τομείς

Αφού εξετάσαμε τον ορισμό και τις βασικές αρχές της αυτοΐασης μέσα από το πρίσμα της ιατρικής επιστήμης και του ανθρώπινου οργανισμού, καθώς και τα κυριότερα μοντέλα αυτοΐασης, θα μελετήσουμε πλέον τις εφαρμογές που αφορούν μη βιολογικές οντότητες. Σε αυτούς τους τομείς, ο όρος «αυτοΐαση» αναφέρεται στην ικανότητα συστημάτων, συσκευών ή υλικών να ανιχνεύουν δυσλειτουργίες και να επανέρχονται αυτόνομα στην αρχική ή σε μια βέλτιστη λειτουργική τους κατάσταση, σύμφωνα με προκαθορισμένες διαδικασίες ή αλγοριθμικές προσεγγίσεις.

Η τεχνολογία της αυτοΐασης σε μη ανθρώπινες εφαρμογές έχει προκύψει μέσα από τη διεπιστημονική συνεργασία επιστημόνων και μηχανικών, με στόχο τη βελτίωση της αξιοπιστίας, της ανθεκτικότητας και της διάρκειας ζωής των συστημάτων. Η ανάπτυξη τέτοιων τεχνολογιών δεν περιορίζεται σε έναν κλάδο, αλλά επεκτείνεται σε κρίσιμες βιομηχανίες και υποδομές, από την πληροφορική και την ενέργεια έως την αυτοκινητοβιομηχανία και την αεροναυπηγική, και όχι μόνο.

Στις επόμενες υποενότητες μελετήθηκαν και παρουσιάζονται κάποιοι από τους πιο σημαντικούς κλάδους όπου η αυτοΐαση έχει βρει πρακτικές εφαρμογές, καθώς επίσης οι τεχνικές και οι προσεγγίσεις που υιοθετούνται, ώστε να επιτυγχάνεται η αυτόνομη αποκατάσταση λειτουργιών και η πρόληψη μελλοντικών αστοχιών.

2.3.1 Αυτοΐαση στον κλάδο της ΤΠΕ

Ο κλάδος των Τεχνολογιών Πληροφορικής και Επικοινωνιών (ΤΠΕ) περιλαμβάνει το σύνολο των τεχνολογιών υλικού υπολογιστών, του διαδικτύου, της τηλεφωνίας και του λογισμικού που υποστηρίζει εφαρμογές και υπηρεσίες. Στη σύγχρονη εποχή, η πληροφορική και οι τηλεπικοινωνίες αποτελούν πλέον έναν ενιαίο και άρρηκτα συνδεδεμένο επιστημονικό χώρο, ο οποίος έχει κατακλύσει την καθημερινότητα, επηρεάζοντας από απλές προσωπικές δραστηριότητες έως κρίσιμες επιχειρησιακές λειτουργίες.

Η συμβολή των ΤΠΕ στην οικονομία, στην παραγωγικότητα και στην ποιότητα ζωής είναι καθοριστική, καθώς επιτρέπουν την αυτοματοποίηση διαδικασιών, την ταχύτερη επικοινωνία και την αποτελεσματική διαχείριση δεδομένων. Ωστόσο, η ευρεία τους διάδοση δημιουργεί και προκλήσεις, όπως η αυξημένη εξάρτηση από την αδιάλειπτη λειτουργία των συστημάτων και η ανάγκη άμεσης αποκατάστασης τυχόν δυσλειτουργιών.

Στο πλαίσιο αυτό, η αυτοΐαση στις ΤΠΕ αποκτά ιδιαίτερη σημασία, καθώς αφορά την ικανότητα συστημάτων, είτε στο επίπεδο του υλικού είτε στο επίπεδο του λογισμικού, να ανιχνεύουν βλάβες και να επαναφέρουν τη λειτουργικότητά τους χωρίς εξωτερική παρέμβαση. Στην παρούσα μελέτη, ο κλάδος των ΤΠΕ εξετάζεται μέσα από δύο βασικούς άξονες:

1. Αυτοΐαση στο υλικό και τα δίκτυα πληροφορικής, που περιλαμβάνει την υποδομή των συσκευών και των επικοινωνιακών δικτύων.
2. Αυτοΐαση στο λογισμικό πληροφορικής, που επικεντρώνεται σε μηχανισμούς λογισμικού για την αυτόνομη αποκατάσταση λειτουργιών.

2.3.1.1 Αυτοΐαση στο υλικό και τα δίκτυα πληροφορικής

Ο κλάδος της πληροφορικής βασίζεται θεμελιωδώς στο υλικό (hardware) και στα δίκτυα επικοινωνίας, τα οποία αποτελούν τη ραχοκοκαλιά κάθε συστήματος επεξεργασίας και διακίνησης δεδομένων. Το υλικό περιλαμβάνει όλα τα φυσικά εξαρτήματα ενός υπολογιστικού συστήματος, όπως η μητρική πλακέτα, ο κεντρικός επεξεργαστής (CPU), οι μνήμες RAM, οι μονάδες αποθήκευσης (HDD, SSD), οι κάρτες γραφικών και οι ελεγκτές εισόδου-εξόδου, καθώς και οι απαραίτητες διασυνδέσεις και κυκλώματα τροφοδοσίας. Η αξιοπιστία αυτών των εξαρτημάτων είναι κρίσιμη, καθώς οποιαδήποτε βλάβη μπορεί να επηρεάσει τη συνολική λειτουργικότητα του συστήματος.

Η έννοια της αυτοΐασης στο υλικό αναφέρεται στην ενσωμάτωση μηχανισμών ανίχνευσης, διάγνωσης και αυτόνομης αποκατάστασης δυσλειτουργιών. Παραδείγματα τέτοιων μηχανισμών περιλαμβάνουν:

- Διπλή ή τριπλή εφεδρικότητα (redundancy) σε κρίσιμα εξαρτήματα, ώστε να αναλαμβάνει αυτόματα εφεδρική μονάδα σε περίπτωση βλάβης.
- Διορθωτικός κώδικας σφαλμάτων (ECC) σε μνήμες RAM, που ανιχνεύει και διορθώνει σφάλματα δεδομένων χωρίς να απαιτείται επανεκκίνηση του συστήματος.
- Αυτόματη ανακατεύθυνση (bad sector remapping) στους σκληρούς δίσκους και SSD, που απομονώνει κατεστραμμένους τομείς και μεταφέρει τα δεδομένα σε εφεδρικές περιοχές.

Στον τομέα των δικτύων πληροφορικής, η αυτοΐαση αποκτά ακόμα μεγαλύτερη σημασία λόγω του τεράστιου όγκου δεδομένων που διακινείται παγκοσμίως — εκτιμάται ότι η παγκόσμια διακίνηση θα ξεπεράσει τα 147 zettabytes ετησίως, με μέσο ετήσιο ρυθμό αύξησης περίπου 19,2%. Τα σύγχρονα δίκτυα, είτε ενσύρματα είτε ασύρματα, πρέπει να εξασφαλίζουν όχι μόνο την ορθή δρομολόγηση των πακέτων αλλά και τη συνεχή διαθεσιμότητα υπηρεσιών, ακόμη και σε περίπτωση βλαβών.

Η αυτοΐαση στα δίκτυα περιλαμβάνει τεχνικές όπως:

- Αυτόματη επαναδρομολόγηση (self-rerouting) σε περίπτωση αποτυχίας ενός κόμβου ή διασύνδεσης.
- Δυναμική ανακατανομή πόρων ώστε να αποφευχθεί συμφόρηση και να διασφαλιστεί η ομαλή ροή δεδομένων.
- Συστήματα αυτοπαρακολούθησης (self-monitoring) που εντοπίζουν ανωμαλίες και προσαρμόζουν τις παραμέτρους λειτουργίας σε πραγματικό χρόνο.

Η ύπαρξη τέτοιων μηχανισμών μειώνει την ανάγκη για άμεση ανθρώπινη παρέμβαση, ελαχιστοποιεί τον χρόνο αδράνειας και αυξάνει την ανθεκτικότητα των υποδομών πληροφορικής, κάτι που είναι απαραίτητο σε κρίσιμες εφαρμογές, όπως η υγεία, η άμυνα, η ενέργεια και οι χρηματοοικονομικές συναλλαγές.

2.3.1.2 Αυτοΐαση στο λογισμικό πληροφορικής

Η αυτοΐαση στο πλαίσιο του λογισμικού (self-healing software) εξετάζει τη δυνατότητα συστημάτων να ανιχνεύουν, να διαγιγνώσκουν και να αποκαθιστούν αυτόνομα τις βλάβες σε πραγματικό χρόνο, χωρίς ανθρώπινη παρέμβαση. Τέτοια συστήματα ενσωματώνουν μηχανισμούς συνεχούς παρακολούθησης, διάγνωσης και αυτόματων διορθωτικών ενεργειών (π.χ. επανεκκίνηση υπηρεσιών, rollback, rerouting), με στόχο αυξημένη αξιοπιστία, διαθεσιμότητα και μείωση του χρόνου διακοπής (downtime) [9].

Ένα σημαντικό πλαίσιο για την υλοποίηση της αυτοΐασης στο λογισμικό είναι το Autonomic Computing, όπως εδραιώθηκε από την IBM. Το μοντέλο αυτό περιλαμβάνει κλειστούς βρόγχους ελέγχου (control loops) με αισθητήρες, εκτελεστές ενεργειών, γνώση (knowledge) και προγραμματιστικές πολιτικές (policies) για αυτό-διαχείριση, αυτοσυγκρότηση, αυτοβελτιστοποίηση και αυτοπροστασία.

Παραδείγματα τεχνικών αυτοΐασης στο λογισμικό:

- Τεχνικές αντοχής σφαλμάτων (fault tolerance): χρήση σχεδιαστικών προτύπων όπως *retry, fallback, circuit-breaker* και *timeout* για διαχείριση σφαλμάτων και αποφυγή καταρρεύσεων.
- Αρχιτεκτονικές που βασίζονται σε μίμηση βιολογικών δομών: η προσέγγιση με βάση το «τεχνητό ανοσοποιητικό σύστημα» (artificial immune systems) προτείνει προγνωστικά σχήματα ανίχνευσης ανωμαλιών και αυτόνομης αντιμετώπισης τους.
- Μοντελο-οδηγούμενες τεχνικές (model-driven): πλαίσια (frameworks) που ενσωματώνουν προδιαγραφές λειτουργικότητας και αυτοΐασης σε συγκεκριμένα μοντέλα, τα οποία στη συνέχεια μετασχηματίζονται σε λειτουργικές λύσεις που ανιχνεύουν και διορθώνουν δυσλειτουργίες.
- Τεχνολογίες τεχνητής νοημοσύνης και μηχανικής μάθησης: όπου εργαλεία ανάλυσης καταγραφής (log analysis), στατικός έλεγχος κώδικα και μοντέλα AI λειτουργούν σαν αισθητήρες και ανάλυση για την αυτόνομη παραγωγή διορθώσεων — μιμούμενα τη βιολογική αυτοΐαση
- Πρακτικές υλοποιήσεις σε σύγχρονες πλατφόρμες: επιχειρήσεις όπως η Netflix, η Amazon Web Services (AWS) και η Google αξιοποιούν Kubernetes, Istio και Chaos Engineering για την έγκαιρη ανίχνευση προβλημάτων, την αυτόματη αποκατάσταση και την αδιάλειπτη διαχείριση της εφαρμογής χωρίς ανθρώπινη παρέμβαση.

Η αξία της αυτοΐασης στο λογισμικό δεν περιορίζεται στην τεχνική βελτιστοποίηση, αλλά επεκτείνεται στην οικονομική αποδοτικότητα και τη βελτίωση της εμπειρίας χρήστη. Η αυτοΐαση μειώνει το κόστος λειτουργίας, επιτυγχάνει υψηλότερη διαθεσιμότητα συστημάτων και αυξάνει την ασφάλεια και ευρωστία των εφαρμογών.

2.3.2 Τομέας ενέργειας

Η εξέλιξη των συστημάτων ηλεκτρικής ενέργειας προς τα «έξυπνα δίκτυα» (smart grids) ενσωματώνει μηχανισμούς αυτοΐασης, ώστε τα ενεργειακά συστήματα να γίνονται περισσότερο αξιόπιστα, ανθεκτικά και ικανά να επανακάμπτουν μετά από σφάλματα χωρίς ανθρώπινη παρέμβαση. Ο όρος *self-healing*, στον τομέα των δικτύων διανομής, περιγράφει διαδικασίες εντοπισμού βλαβών, απομόνωσης και αποκατάστασης – γνωστές ως Fault Location, Isolation, and System Restoration (FLISR) [10], [11]. Τα smart grids αναμένεται να μειώσουν τον χρόνο διακοπής ρεύματος έως και κατά 50%, βελτιώνοντας σημαντικά την αξιοπιστία και ποιότητα της παρεχόμενης ενέργειας (U.S. Department of Energy, 2020). Σύμφωνα με την International Energy Agency, η παγκόσμια διείσδυση των smart grids αναμένεται να φτάσει το 40% μέχρι το 2030, με σημαντική επίδραση στην ενεργειακή αποδοτικότητα και στην ενσωμάτωση ανανεώσιμων πηγών.

Οι μηχανισμοί αυτοΐασης υλοποιούνται μέσω προηγμένων συστημάτων όπως το Advanced Distribution Automation (ADA), το οποίο εφαρμόζει αλγορίθμους βελτιστοποίησης και κλειστούς βρόχους ελέγχου για την άμεση προσαρμογή στα μεταβαλλόμενα φορτία και τη δομή του δικτύου,

συχνά χωρίς ανάγκη τεχνικής παρέμβασης. Η ικανότητα αυτή αποκτά ολοένα και μεγαλύτερη σημασία λόγω της αυξανόμενης διείσδυσης κατανεμημένων πηγών ενέργειας, όπως οι φωτοβολταϊκοί σταθμοί και οι ανεμογεννήτριες, που το 2023 κάλυψαν το 28% της παγκόσμιας ηλεκτροπαραγωγής. Σε επίπεδο μικροδικτύων (microgrids), η χρήση multi-agent systems (MAS) για τη διαχείριση ενέργειας προσφέρει ευελιξία και αυτονομία στη διανομή και αποκατάσταση λειτουργιών. Σύμφωνα με τους Zhang και Li (2020), τα συστήματα αυτά μπορούν να επιτύχουν μείωση του χρόνου αποκατάστασης βλαβών έως και 40%, αυξάνοντας την ενεργειακή διαθεσιμότητα και μειώνοντας τα κόστη λειτουργίας. Φιλοσοφικές προσεγγίσεις όπως το Organic Distribution System (ODiS) προτείνουν την ενσωμάτωση μοντέλων «self-configuring, self-organising, self-healing και self-optimising» σε διαχειριστικά συστήματα διανομής (Distribution Management System - DMS), προάγοντας τη συνεργασία τοπικά διαχειριζόμενων ενεργειακών μονάδων (Home Energy Management System - HEMS) και την αυτονομία σε δίκτυα διανομής.

Τέλος, η ανάπτυξη πειραματικών – πιλοτικών υποδομών επιβεβαιώνει τη δυνατότητα λειτουργίας microgrids σε αυτόνομη λειτουργία (islanding) και την επανεκκίνηση του δικτύου (black start), ενισχύοντας περαιτέρω την πρακτική εφαρμογή της αυτοΐασης σε κρίσιμες καταστάσεις διακοπής παροχής.

2.3.3 Τομέας Αυτοκινητοβιομηχανίας

Ο τομέας της αυτοκινητοβιομηχανίας αποτελεί έναν από τους πιο δυναμικούς κλάδους, όπου η τεχνολογία της αυτοΐασης διαδραματίζει καθοριστικό ρόλο, καθώς η ασφάλεια, η αξιοπιστία και η αποδοτικότητα των οχημάτων αποτελούν κρίσιμοι παράμετροι. Η ενσωμάτωση συστημάτων αυτοΐασης αφορά τόσο τα μηχανικά όσο και τα ηλεκτρονικά μέρη, με στόχο τη μείωση των βλαβών, την ελαχιστοποίηση των διακοπών λειτουργίας και τη βελτίωση της συνολικής εμπειρίας του χρήστη.

Στα σύγχρονα οχήματα, η αυτοΐαση υλοποιείται κυρίως μέσω εξελιγμένων συστημάτων παρακολούθησης και διάγνωσης, που βασίζονται σε αισθητήρες, αλγορίθμους μηχανικής μάθησης και τεχνητής νοημοσύνης. Αυτά τα συστήματα ανιχνεύουν άμεσα βλάβες ή φθορές σε κρίσιμα εξαρτήματα όπως ο κινητήρας, το σύστημα πέδησης, τη μετάδοση και τα ηλεκτρικά κυκλώματα, και στη συνέχεια ενεργοποιούν διαδικασίες αυτόματης επισκευής ή προγραμματίζουν προληπτική συντήρηση. Επιπλέον, η χρήση αυτοθεραπευόμενων υλικών, όπως πολυμερή με ικανότητα αυτόματης επανασύνδεσης ρωγμών, αυξάνει σημαντικά την αντοχή και τη διάρκεια ζωής των εξαρτημάτων. Μια ιδιαίτερα σημαντική εξέλιξη αφορά την εφαρμογή των τεχνολογιών αυτοΐασης στα αυτόνομα και συνδεδεμένα οχήματα, όπου η διαχείριση σφαλμάτων δεν επηρεάζει μόνο τη λειτουργία, αλλά άμεσα την ασφάλεια των επιβατών και των πεζών. Οι τεχνικές αυτοΐασης σε αυτά περιλαμβάνουν την ανίχνευση και διόρθωση σφαλμάτων λογισμικού, τη ρύθμιση των αισθητήρων και την προσαρμογή των αλγορίθμων ελέγχου σε πραγματικό χρόνο.

Η χρήση αναλυτικών εργαλείων μεγάλης κλίμακας (big data analytics) και τεχνητής νοημοσύνης επιτρέπει την πρόβλεψη βλαβών πριν αυτές εμφανιστούν, με αποτέλεσμα τη μείωση του κόστους συντήρησης και την αύξηση της αξιοπιστίας των οχημάτων. Σύμφωνα με μελέτες, η πρόβλεψη βλαβών μέσω Artificial Intelligence (AI) μπορεί να μειώσει τα λειτουργικά κόστη έως και 20% και να αυξήσει το χρόνο λειτουργίας χωρίς βλάβη έως και 30%. Επιπλέον, η παγκόσμια αγορά συστημάτων αυτοΐασης στην αυτοκινητοβιομηχανία εκτιμάται ότι θα φτάσει σε αξία τα 12 δισεκατομμύρια δολάρια έως το 2027, με μέσο ετήσιο ρυθμό ανάπτυξης άνω του 15%. Η συνεχής πρόοδος στην αυτοΐαση θεωρείται κρίσιμη για τη μετάβαση σε πιο βιώσιμες, ασφαλείς και αποδοτικές μεταφορές, ανταποκρινόμενη στις σύγχρονες ανάγκες της αγοράς και της κοινωνίας.

2.3.4 Τομέας αεροναυπηγίας

Ο τομέας της αεροναυπηγίας είναι από τους πιο απαιτητικούς όσον αφορά την αξιοπιστία, την ασφάλεια και τη διαθεσιμότητα των συστημάτων. Η χρήση τεχνολογιών αυτοΐασης στα αεροναυπηγικά συστήματα έχει σαν κύριο στόχο την πρόληψη και την αυτόματη επισκευή βλαβών, μειώνοντας έτσι τις πιθανότητες ξαφνικών αστοχιών που μπορούν να θέσουν σε κίνδυνο ανθρώπινες ζωές και να προκαλέσουν σημαντικές οικονομικές ζημιές.

Σύμφωνα με δεδομένα του Παγκόσμιου Οργανισμού Πολιτικής Αεροπορίας (International Civil Aviation Organization - ICAO), τα ατυχήματα αεροσκαφών παγκοσμίως παρουσιάζουν μείωση περίπου 20% την τελευταία δεκαετία, ωστόσο τα τεχνικά σφάλματα συνεχίζουν να αποτελούν σημαντικό ποσοστό (περίπου 15-20%) των αιτιών (ICAO, 2023). Η υιοθέτηση συστημάτων αυτοΐασης αναμένεται να μειώσει περαιτέρω αυτό το ποσοστό, με μελέτες να εκτιμούν ότι η έγκαιρη ανίχνευση και αυτόματη επισκευή βλαβών μπορεί να μειώσει τα ατυχήματα που οφείλονται σε τεχνικές αστοχίες έως και 30%.

Η αυτοΐαση στην αεροναυπηγία αφορά τόσο τα υλικά και τις κατασκευές των αεροσκαφών όσο και τα ηλεκτρονικά και μηχανολογικά υποσυστήματα. Στα υλικά, η χρήση αυτοθεραπευόμενων σύνθετων υλικών επιτρέπει την αυτόματη επισκευή μικρορωγμών και άλλων φθορών χωρίς ανθρώπινη παρέμβαση, αυξάνοντας την ανθεκτικότητα και τη διάρκεια ζωής των αεροπορικών δομών. Παράλληλα, τα εξελιγμένα συστήματα παρακολούθησης της κατάστασης (Structural Health Monitoring - SHM) αξιοποιούν δίκτυα αισθητήρων και τεχνικές επεξεργασίας σημάτων για συνεχή ανίχνευση βλαβών σε κρίσιμα υποσυστήματα, όπως κινητήρες, πτερύγια και συστήματα προσγείωσης, επιτρέποντας την πρόληψη σοβαρών δυσλειτουργιών. Επιπλέον, στα συστήματα ελέγχου πτήσης, η αυτοΐαση επιτυγχάνεται μέσω ανθεκτικών αλγορίθμων ελέγχου (fault-tolerant control systems) που διασφαλίζουν τη σταθερότητα και την ασφάλεια της πτήσης ακόμη και σε περιπτώσεις βλαβών αισθητήρων ή ενεργοποιητών. Με την ενσωμάτωση προγνωστικής διάγνωσης και προσαρμοστικών μηχανισμών, τα συστήματα αυτά προσαρμόζουν αυτόματα τη λειτουργία τους, εξασφαλίζοντας συνεχή και ασφαλή πτήση.

Η ενσωμάτωση των τεχνολογιών αυτοΐασης στην αεροναυπηγία συνεισφέρει όχι μόνο στην αύξηση της ασφάλειας και αξιοπιστίας, αλλά και στη σημαντική μείωση του κόστους συντήρησης και του χρόνου ακινητοποίησης των αεροσκαφών, ενισχύοντας τη βιωσιμότητα και την ανταγωνιστικότητα των αεροπορικών εταιρειών.

2.3.5 Τομέας Υγείας και Βιοϊατρικής Τεχνολογίας

Ο τομέας της Υγείας και Βιοϊατρικής Τεχνολογίας αποτελεί έναν από τους πλέον δυναμικά αναπτυσσόμενους τομείς που αξιοποιούν τεχνολογίες αυτοΐασης, με στόχο τη βελτίωση της αξιοπιστίας, της ασφάλειας και της αποτελεσματικότητας των ιατρικών συσκευών και των βιοϊατρικών συστημάτων. Η αυτοΐαση στον τομέα αυτό αναφέρεται στην ικανότητα των συσκευών και των συστημάτων να ανιχνεύουν αυτόματα βλάβες ή δυσλειτουργίες και να αποκαθιστούν τη λειτουργικότητά τους, χωρίς άμεση ανθρώπινη παρέμβαση, εξασφαλίζοντας τη συνεχή και ασφαλή λειτουργία τους σε κρίσιμες συνθήκες[12].

Στις ιατρικές συσκευές, όπως οι εμφυτεύσιμοι βηματοδότες, τα συστήματα παροχής φαρμάκων (drug delivery systems) και οι φορητοί βιοαισθητήρες, η αυτοΐαση συμβάλλει στην αύξηση της διάρκειας ζωής και στην ελαχιστοποίηση των κινδύνων από ανεπιθύμητες διακοπές λειτουργίας. Για παράδειγμα, οι βιοαισθητήρες με δυνατότητες αυτοΐασης μπορούν να αναγνωρίζουν σημάδια φθοράς ή

παρεμβολών στα σήματα και να προσαρμόζουν τους αλγορίθμους επεξεργασίας τους ώστε να διατηρούν την ακρίβεια και αξιοπιστία των μετρήσεων. Επιπρόσθετα, η χρήση βιοσυμβατών αυτοθεραπευόμενων υλικών σε εμφυτεύματα και προσθετικά μέρη έχει επιτρέψει τη βελτίωση της βιοσυμβατότητας και την αυτόματη επιδιόρθωση μικροβλαβών, περιορίζοντας τον κίνδυνο απορρίψεων και φλεγμονών. Ταυτόχρονα, συστήματα τηλεϊατρικής (telemedicine) ενσωματώνουν αυτοΐαση στο λογισμικό τους για να διαχειρίζονται διακοπές σύνδεσης ή δυσλειτουργίες, εξασφαλίζοντας τη σταθερότητα της παροχής υπηρεσιών υγείας εξ αποστάσεως.

Οι αλγόριθμοι μηχανικής μάθησης και τεχνητής νοημοσύνης που εφαρμόζονται σε ιατρικά συστήματα ενισχύουν τις δυνατότητες αυτοΐασης, παρέχοντας προβλεπτική συντήρηση και προσαρμοστική διαχείριση λειτουργιών με βάση δεδομένα σε πραγματικό χρόνο, προλαμβάνοντας πιθανές αστοχίες. Η ενσωμάτωση των τεχνολογιών αυτών προωθεί μια νέα εποχή στην υγειονομική περίθαλψη, όπου τα ιατρικά συστήματα γίνονται πιο αξιόπιστα, ανθεκτικά και ικανά να υποστηρίξουν με μεγαλύτερη ασφάλεια και ακρίβεια τη φροντίδα των ασθενών.

2.3.6 Τομέας Περιβάλλοντος και Έξυπνων Πόλεων (Smart Cities)

Ο τομέας του Περιβάλλοντος και των Έξυπνων Πόλεων αποτελεί κρίσιμο πεδίο εφαρμογής των τεχνολογιών αυτοΐασης, καθώς η ολοένα αυξανόμενη ανάγκη για βιώσιμη και αποδοτική διαχείριση των αστικών υποδομών απαιτεί συστήματα με δυνατότητες αυτοδιόρθωσης και αυτορύθμισης. Η αυτοΐαση στις έξυπνες πόλεις αφορά κυρίως την ανάπτυξη «έξυπνων» δικτύων διαχείρισης πόρων, όπως είναι τα δίκτυα ηλεκτροδότησης (smart grids), τα συστήματα διαχείρισης ύδρευσης, οι αυτοματοποιημένοι φωτισμοί, καθώς και τα δίκτυα αισθητήρων που παρακολουθούν την ποιότητα του αέρα και τις περιβαλλοντικές συνθήκες.[13], [14],

Τα αυτοϊατά συστήματα σε αυτό το πλαίσιο διαθέτουν μηχανισμούς ανίχνευσης και αποκατάστασης βλαβών ή ανωμαλιών, επιτρέποντας τη συνεχή λειτουργία και τη μείωση του κόστους συντήρησης. Για παράδειγμα, τα έξυπνα δίκτυα ηλεκτρικής ενέργειας εφαρμόζουν αλγορίθμους πρόβλεψης και αυτοδιορθωτικών δράσεων που επιτρέπουν την αυτόματη αντιμετώπιση διακοπών ρεύματος ή την επαναδρομολόγηση ενέργειας, χωρίς να απαιτείται ανθρώπινη παρέμβαση. Παράλληλα, στα συστήματα διαχείρισης ύδατος, η αυτοΐαση συμβάλλει στην ανίχνευση διαρροών και στην αυτόματη προσαρμογή της παροχής, εξοικονομώντας πολύτιμους φυσικούς πόρους. Η χρήση τεχνολογιών τεχνητής νοημοσύνης και μηχανικής μάθησης ενισχύει τις δυνατότητες αυτοΐασης, καθώς τα συστήματα μαθαίνουν από τα δεδομένα σε πραγματικό χρόνο και βελτιώνουν τις διαδικασίες πρόβλεψης και αποκατάστασης. Επίσης, η διασύνδεση αισθητήρων και συσκευών στο πλαίσιο του IoT επιτρέπει τη συλλογή και ανάλυση μεγάλου όγκου δεδομένων, ενισχύοντας τις αποφάσεις αυτοΐασης και αυτορύθμισης των υποδομών των έξυπνων πόλεων.

Τέλος, η ενσωμάτωση αυτοϊαζόμενων συστημάτων σε έξυπνες πόλεις συμβάλλει σημαντικά στην αειφορία και στην αναβάθμιση της ποιότητας ζωής των κατοίκων, εξασφαλίζοντας ασφαλείς, αποδοτικές και ανθεκτικές αστικές υποδομές που προσαρμόζονται δυναμικά στις μεταβαλλόμενες ανάγκες και περιβαλλοντικές συνθήκες.

2.4 Η ασφάλεια στον κλάδο της Αυτοΐασης – Self healing

Η ασφάλεια αποτελεί πρωταρχικό παράγοντα στον σχεδιασμό και την υλοποίηση συστημάτων αυτοΐασης σε ποικίλους τομείς, όπως η πληροφορική, τα δίκτυα, η ενέργεια, η αυτοκινητοβιομηχανία και η αεροναυπηγική. Η έννοια της αυτοΐασης, πέρα από την ικανότητα του συστήματος να ανιχνεύει και να διορθώνει βλάβες αυτόματα, εμπλέκει και την διασφάλιση της ακεραιότητας, της αξιοπιστίας

και της ανθεκτικότητας έναντι επιθέσεων ή απρόβλεπτων σφαλμάτων, που θα μπορούσαν να θέσουν σε κίνδυνο τη λειτουργία ή την ασφάλεια των χρηστών. [15], [16]

Σύμφωνα με το κλασικό μοντέλο της ασφάλειας πληροφοριακών συστημάτων (Confidentiality – Integrity – Availability - CIA), η προστασία των δεδομένων και των υποδομών πρέπει να διασφαλίζει:

- Εμπιστευτικότητα (Confidentiality): ώστε μη εξουσιοδοτημένοι χρήστες να μην αποκτούν πρόσβαση σε ευαίσθητες πληροφορίες. Στα συστήματα αυτοΐασης, αυτό σημαίνει ότι οι μηχανισμοί διάγνωσης και αποκατάστασης πρέπει να λειτουργούν χωρίς να διαρρέουν κρίσιμα δεδομένα προς τρίτους ή προς κακόβουλους φορείς.
- Ακεραιότητα (Integrity): ώστε οι μηχανισμοί αυτοΐασης να βασίζονται σε αξιόπιστα και μη παραποιημένα δεδομένα. Εάν οι πληροφορίες σχετικά με τη βλάβη ή την κατάσταση του συστήματος αλλοιωθούν, το self-healing μπορεί να οδηγήσει σε λανθασμένες ή επικίνδυνες ενέργειες.
- Διαθεσιμότητα (Availability): ώστε οι κρίσιμες υπηρεσίες να παραμένουν προσβάσιμες και λειτουργικές ακόμη και κατά τη διάρκεια της διαδικασίας αυτοΐασης. Η υψηλή διαθεσιμότητα είναι κρίσιμη, ιδίως σε τομείς όπως τα έξυπνα δίκτυα ενέργειας και η αεροναυπηγική, όπου η διακοπή λειτουργίας μπορεί να έχει σοβαρές επιπτώσεις.
- Βιωσιμότητα (Sustainability): η πιο πρόσφατη διάσταση, που αφορά την ικανότητα του συστήματος να διατηρεί τη λειτουργικότητά του σε βάθος χρόνου με τρόπο αποδοτικό και ανθεκτικό. Στα συστήματα αυτοΐασης, η βιωσιμότητα σημαίνει ότι οι διαδικασίες επιδιόρθωσης δεν πρέπει να εξαντλούν δυσανάλογα πόρους (υπολογιστικούς, ενεργειακούς ή υλικούς), ούτε να δημιουργούν περιβαλλοντικό ή οικονομικό κόστος. Αντίθετα, ο στόχος είναι να επιτυγχάνεται μια ισορροπία μεταξύ άμεσης αποκατάστασης και μακροπρόθεσμης ανθεκτικότητας.

Η βιωσιμότητα, επομένως, δεν αποτελεί μόνο έναν νέο τεχνικό δείκτη, αλλά μια ολιστική διάσταση της ασφάλειας, που ενσωματώνει τόσο την ενεργειακή και περιβαλλοντική αποδοτικότητα όσο και τη μακροπρόθεσμη ανθεκτικότητα των συστημάτων. Στο πλαίσιο των συστημάτων αυτοΐασης, η βιωσιμότητα αφορά την ικανότητα ενός συστήματος να ανακάμπτει όχι μόνο βραχυπρόθεσμα από βλάβες ή επιθέσεις, αλλά και να παραμένει λειτουργικό και ενεργειακά αποδοτικό σε βάθος χρόνου, χωρίς να εξαντλεί πόρους ή να δημιουργεί υπερβολικό κόστος. Ένα βιώσιμο self-healing σύστημα δεν περιορίζεται στη διόρθωση στιγμιαίων αστοχιών, αλλά ενσωματώνει στρατηγικές μακροπρόθεσμης ανθεκτικότητας, μειώνοντας την ανάγκη για συχνές εξωτερικές παρεμβάσεις και προάγοντας τη σταθερότητα των υποδομών.

Πηγή: https://logstail.com/

Ενδεικτικά παραδείγματα:

- Στα έξυπνα δίκτυα ενέργειας (smart grids), η βιωσιμότητα εξασφαλίζει ότι οι μηχανισμοί αυτοΐασης δεν οδηγούν σε σπατάλη ενέργειας ή σε μη βέλτιστη κατανομή φορτίων, αλλά αντίθετα συνεισφέρουν στη βέλτιστη και αποδοτική χρήση των Ανανεώσιμων Πηγών Ενέργειας (ΑΠΕ).
- Στην αεροναυπηγική και την αυτοκινητοβιομηχανία, η βιωσιμότητα συνδέεται με την ανθεκτικότητα των υλικών και των τεχνολογιών, με σκοπό την ελαχιστοποίηση της ανάγκης για συντήρηση, μειώνοντας το κόστος συντήρησης και περιβαλλοντικές επιβαρύνσεις, δηλαδή το περιβαλλοντικό αποτύπωμα.
- Στα πληροφοριακά συστήματα, η έννοια sustainability μεταφράζεται στη δυνατότητα αυτόματης ανάκαμψης χωρίς υπερκατανάλωση υπολογιστικών πόρων ή υπερφόρτωση δικτύων, κάτι που είναι κρίσιμο σε περιβάλλοντα cloud και edge computing.

Η πρόκληση στη διασφάλιση της ασφάλειας στα συστήματα αυτοΐασης έγκειται επομένως στην ανάγκη για ισορροπία μεταξύ της αυτονομίας στην επιδιόρθωση και της δυνατότητας ανθρώπινης παρέμβασης και ελέγχου, ώστε να διασφαλίζεται η διαφάνεια και η λογοδοσία. Η ενσωμάτωση του παράγοντα βιωσιμότητας (sustainability) επεκτείνει αυτήν την πρόκληση, καθώς απαιτείται τα συστήματα όχι μόνο να «θεραπεύονται» αλλά να το κάνουν με τρόπο αποδοτικό, ανθεκτικό και περιβαλλοντικά υπεύθυνο.

Κεφάλαιο 3ο: Πρότυπα και πρωτόκολλα επικοινωνίας για συστήματα αυτοΐασης

Η αποτελεσματική λειτουργία και διαχείριση συστημάτων αυτοΐασης προϋποθέτει την τήρηση σαφών προτύπων και τη χρήση αξιόπιστων πρωτοκόλλων επικοινωνίας και ελέγχου. Τα πρότυπα εξασφαλίζουν τη διαλειτουργικότητα μεταξύ διαφορετικών υποσυστημάτων, την ασφάλεια της πληροφορίας, τη διασφάλιση της ακεραιότητας των διαδικασιών και την υψηλή διαθεσιμότητα των κρίσιμων λειτουργιών. Παράλληλα, τα πρωτόκολλα καθορίζουν τους κανόνες ανταλλαγής εντολών και δεδομένων, επιτρέποντας έτσι την έγκαιρη ανίχνευση και αποκατάσταση σφαλμάτων, την παρακολούθηση της κατάστασης των συστημάτων και τη διαχείριση κινδύνων.

Στο πλαίσιο της σύγχρονης βιβλιογραφίας γίνεται ιδιαίτερη αναφορά στα διεθνή πρότυπα, όπως αυτά που τεκμηριώνονται από οργανισμούς όπως το OpenC², το ISO, το NIST και άλλους, που αποτελούν βασικά στοιχεία για την ανάπτυξη συστημάτων τα οποία όχι μόνο είναι αυτοΐατα αλλά ασφαλή, αξιόπιστα και βιώσιμα. Στο κεφάλαιο αυτό αναλύονται τα κυριότερα πρότυπα και πρωτόκολλα που χρησιμοποιούνται σε ποικίλους τομείς εφαρμογής, όπως η πληροφορική, τα δίκτυα, η αυτοκινητοβιομηχανία, η αεροναυπηγική και τα έξυπνα δίκτυα ενέργειας, προσφέροντας ένα στέρεο θεωρητικό υπόβαθρο για την κατανόηση και αξιολόγηση των μηχανισμών αυτοΐασης.

3.1 Εισαγωγή

Η ανάπτυξη συστημάτων αυτοΐασης απαιτεί όχι μόνο προηγμένες τεχνολογικές υποδομές, αλλά και ένα συνεκτικό πλαίσιο προτύπων και πρωτοκόλλων που καθορίζουν τον τρόπο λειτουργίας, επικοινωνίας και διαχείρισης των υποσυστημάτων. Τα πρότυπα αυτά εξασφαλίζουν τη διαλειτουργικότητα μεταξύ διαφορετικών τεχνολογικών λύσεων, τη συνεπή εφαρμογή μηχανισμών ασφαλείας και την αξιοπιστία των διαδικασιών αποκατάστασης βλαβών, ενώ τα πρωτόκολλα επικοινωνίας καθορίζουν τη ροή πληροφοριών και εντολών με τρόπο που διασφαλίζεται η σωστή και έγκαιρη ανταπόκριση σε σφάλματα ή απρόβλεπτες καταστάσεις.

Στο πλαίσιο των σύγχρονων εφαρμογών η τήρηση διεθνών προτύπων και η υιοθέτηση δοκιμασμένων πρωτοκόλλων αποτελεί κρίσιμη προϋπόθεση για την ασφάλεια, την αξιοπιστία και τη βιωσιμότητα των συστημάτων αυτοΐασης. Τα πρότυπα αυτά περιλαμβάνουν κατευθύνσεις για την ασφάλεια πληροφοριακών συστημάτων (Confidentiality, Integrity, Availability – CIA), καθώς και σύγχρονες προσεγγίσεις που ενσωματώνουν την έννοια της βιωσιμότητας (Sustainability), διασφαλίζοντας ότι οι αυτοΐατες διαδικασίες δεν περιορίζονται μόνο στην τεχνική λειτουργία αλλά συνεισφέρουν και στην αποτελεσματική διαχείριση πόρων και την περιβαλλοντική υπευθυνότητα.

Το κεφάλαιο αυτό εστιάζει στη συστηματική παρουσίαση των κυριότερων προτύπων και πρωτοκόλλων που χρησιμοποιούνται για την υποστήριξη συστημάτων αυτοΐασης σε διάφορους τομείς, όπως η πληροφορική, τα δίκτυα, η ενέργεια, η αυτοκινητοβιομηχανία και η αεροναυπηγική. Η ανάλυση περιλαμβάνει τόσο τις βασικές αρχές λειτουργίας όσο και τις πρακτικές εφαρμογές, προσφέροντας ένα ολοκληρωμένο θεωρητικό υπόβαθρο που καθιστά δυνατή την αξιολόγηση και τη σύγκριση των διαθέσιμων λύσεων σε επίπεδο ασφάλειας, αποτελεσματικότητας και βιωσιμότητας.

3.1.1 Αναγκαιότητα προτύπων και πρωτοκόλλων

Η συνεχώς αυξανόμενη πολυπλοκότητα των σύγχρονων συστημάτων υπολογιστών και δικτύων καθιστά επιτακτική την ανάγκη για την ανάπτυξη και εφαρμογή καθορισμένων προτύπων και

πρωτοκόλλων. Αυτά τα πρότυπα διασφαλίζουν τη διαλειτουργικότητα, την ασφάλεια, την αξιοπιστία και την αποδοτικότητα των συστημάτων, επιτρέποντας την αποτελεσματική ανίχνευση, διάγνωση και αποκατάσταση βλαβών χωρίς ανθρώπινη παρέμβαση.

Στον τομέα των δικτύων, η εφαρμογή έξυπνων πρωτοκόλλων επιτρέπει την αυτόματη ανίχνευση και αποκατάσταση βλαβών, ενισχύοντας την ανθεκτικότητα και τη συνέχεια των υπηρεσιών. Αυτά τα πρωτόκολλα λειτουργούν ως "νευρικές οδοί" των δικτύων αυτοΐασης, επιτρέποντας την αναγνώριση ανωμαλιών και την αυτόματη ανάκαμψη από διακοπές, μειώνοντας έτσι τον χρόνο διακοπής και τα κόστη που σχετίζονται με την αποκατάσταση. Η ανάγκη για πρότυπα και πρωτόκολλα είναι επίσης επιτακτική στον τομέα της κυβερνοασφάλειας. Η εφαρμογή αυτοΐασης επιτρέπει την αυτόματη ανίχνευση και αποκατάσταση από κυβερνοεπιθέσεις, μειώνοντας τον χρόνο αντίδρασης και τα κόστη που σχετίζονται με την αποκατάσταση. Η χρήση τεχνητής νοημοσύνης και μηχανικής μάθησης σε συνδυασμό με αυτά τα πρότυπα ενισχύει την ικανότητα των συστημάτων να προβλέπουν και να αποτρέπουν επιθέσεις πριν αυτές προκαλέσουν ζημιά. Επιπλέον, η εφαρμογή προτύπων και πρωτοκόλλων συμβάλλει στην ενίσχυση της διαφάνειας και της υπευθυνότητας. Μέσω της τυποποίησης των διαδικασιών και της καταγραφής των ενεργειών, επιτυγχάνεται η καλύτερη παρακολούθηση και αξιολόγηση των επιδόσεων των συστημάτων, διευκολύνοντας την ανίχνευση προβλημάτων και την εφαρμογή διορθωτικών μέτρων.

Συνολικά, η εφαρμογή καθορισμένων προτύπων και πρωτοκόλλων είναι κρίσιμη για την ανάπτυξη και λειτουργία αποτελεσματικών και ασφαλών συστημάτων αυτοΐασης. Αυτά τα πρότυπα διασφαλίζουν την ομαλή λειτουργία των συστημάτων, την προστασία από απειλές και την αποδοτική διαχείριση των πόρων, συμβάλλοντας στην επίτευξη των στόχων της αυτοΐασης.

3.1.2 Διεθνείς οργανισμοί και ο ρόλος του OpenC²

Η ανάπτυξη και υιοθέτηση προτύπων και πρωτοκόλλων αποτελεί θεμελιώδη προϋπόθεση για τη διασφάλιση της συμβατότητας, της αξιοπιστίας και της ασφάλειας στα συστήματα αυτοΐασης. Σε διεθνές επίπεδο, πολυάριθμοι οργανισμοί και θεσμικά όργανα, όπως ο ISO, ο NIST, ο ETSI, ο IETF, ο OASIS και ο ENISA, έχουν καθορίσει πλαίσια, οδηγίες και τεχνικές προδιαγραφές που καθοδηγούν την ανάπτυξη συστημάτων που ενσωματώνουν μηχανισμούς ανθεκτικότητας, αυτόματης αποκατάστασης και ασφάλειας. Τα πρότυπα αυτά δεν αφορούν μόνο τη λειτουργική συμβατότητα των συστημάτων, αλλά και την προστασία των κρίσιμων υποδομών και των δεδομένων έναντι απρόβλεπτων βλαβών ή κακόβουλων επιθέσεων. Η πλήρης κατανόηση των οργανισμών αυτών και των σχετικών προτύπων παρέχει το θεωρητικό υπόβαθρο για την ενοποίηση των αρχών αυτοΐασης με τις διεθνείς βέλτιστες πρακτικές, ενώ ανοίγει το δρόμο για την εφαρμογή προηγμένων πρωτοκόλλων, όπως το OpenC², που υποστηρίζουν ασφαλείς και διαλειτουργικές διαδικασίες εντολών και ελέγχου.[21]

3.1.2.1 Διεθνής Οργανισμός Τυποποίησης - International Organization for Standardization (ISO)

Το πρότυπο ISO/IEC 27001 αποτελεί το διεθνώς αποδεκτό πλαίσιο για τη συστηματική διαχείριση της ασφάλειας πληροφοριών, γνωστό ως Information Security Management System (ISMS). Παρέχει έναν οργανωμένο μηχανισμό για την προστασία των δεδομένων ενός οργανισμού μέσω πολιτικών, διαδικασιών, τεχνικών και οργανωτικών ελέγχων. Η δομή του καλύπτει έντεκα βασικούς τομείς ασφάλειας, όπως η διαχείριση περιουσιακών στοιχείων, οι έλεγχοι πρόσβασης, η φυσική ασφάλεια και η επιχειρησιακή συνέχεια, ενώ η αρχιτεκτονική του στηρίζεται στον κύκλο Plan-Do-Check-Act (PDCA), που εξασφαλίζει τη διαρκή βελτίωση του συστήματος ασφάλειας.[17].

Ο κύκλος PDCA ξεκινά με τον σχεδιασμό πολιτικών και διαδικασιών ασφάλειας (Plan), συνεχίζει με την εφαρμογή τους στην πράξη (Do), ακολουθεί η συνεχής παρακολούθηση και αξιολόγηση της αποτελεσματικότητας των μέτρων (Check), και ολοκληρώνεται με την αναθεώρηση και βελτίωση των διαδικασιών (Act) βάσει των αποτελεσμάτων και των αναφορών κινδύνου. Στο επίκεντρο του ISO/IEC 27001 βρίσκονται οι αρχές εμπιστευτικότητας (Confidentiality), ακεραιότητας (Integrity) και διαθεσιμότητας (Availability), γνωστές ως CIA triad, οι οποίες διασφαλίζουν ότι τα δεδομένα παραμένουν προσβάσιμα μόνο από εξουσιοδοτημένα άτομα, προστατευμένα από μη εξουσιοδοτημένες αλλαγές και διαθέσιμα όταν απαιτούνται, συμβάλλοντας παράλληλα στη βιωσιμότητα των επιχειρησιακών διαδικασιών.

Η εφαρμογή του προτύπου περιλαμβάνει σημαντικές απαιτήσεις, όπως η δημιουργία συγκεκριμένων πολιτικών ασφάλειας, ο καθορισμός ρόλων και ευθυνών, η εκπαίδευση του προσωπικού, η συνεχής παρακολούθηση και αξιολόγηση καθώς και η τεκμηρίωση όλων των δραστηριοτήτων για σκοπούς συμμόρφωσης και ελέγχου. Η διαδικασία πιστοποίησης ακολουθεί συγκεκριμένα βήματα: Gap Analysis, Εφαρμογή ISMS, Εσωτερικός Έλεγχος, Εξωτερικός Έλεγχος και στο τέλος την Πιστοποίηση, με διάρκεια ισχύος τρία έτη και τακτικούς ελέγχους παρακολούθησης.

Η πιστοποίηση παρέχει πολλαπλά οφέλη, όπως η ενίσχυση της αξιοπιστίας και εμπιστοσύνης των πελατών και συνεργατών, η μείωση του κινδύνου παραβίασης δεδομένων, η συμμόρφωση με νομοθετικά και κανονιστικά πλαίσια (π.χ. GDPR) και η ενδυνάμωση της οργανωτικής κουλτούρας ασφάλειας. Στα σύγχρονα περιβάλλοντα τεχνολογίας, όπως τα συστήματα IoT και οι εφαρμογές μηχανικής μάθησης, η εφαρμογή του ISO/IEC 27001 καθίσταται κρίσιμη, αφού η διαχείριση μεγάλου όγκου δεδομένων σε πραγματικό χρόνο απαιτεί την προστασία τους από μη εξουσιοδοτημένη πρόσβαση ή αλλοίωση. Παρακάτω βλέπουμε τα οφέλη ταξινομημένα στον ακόλουθο πίνακα:

Πλεονεκτήματα Πιστοποίησης ISO/IEC 27001	Περιγραφή
Αξιοπιστία και εμπιστοσύνη	Οι πελάτες και οι συνεργάτες εμπιστεύονται τον οργανισμό για την ασφάλεια των δεδομένων τους.
Μείωση κινδύνου παραβίασης δεδομένων	Τα συστήματα προστασίας και οι διαδικασίες μειώνουν την πιθανότητα επιθέσεων ή διαρροών.
Συμμόρφωση με νομοθετικά πλαίσια	Διευκολύνεται η συμμόρφωση με νόμους όπως το GDPR, HIPAA και άλλες ρυθμιστικές απαιτήσεις.
Ενίσχυση οργανωτικής κουλτούρας ασφαλείας	Προάγεται η ευαισθητοποίηση και η εκπαίδευση προσωπικού σε θέματα ασφάλειας πληροφοριών.
Συνεχής βελτίωση	Η χρήση του κύκλου PDCA (Plan-Do-Check-Act) οδηγεί σε διαρκή αξιολόγηση και βελτίωση του ISMS.
Ανταγωνιστικό πλεονέκτημα	Η πιστοποίηση μπορεί να διαφοροποιεί τον οργανισμό στην αγορά και να προσελκύει πελάτες.

Σε πρακτικό επίπεδο, η εφαρμογή του προτύπου ISMS επιτρέπει την συνεχή αξιολόγηση κινδύνων, τη διαχείριση πρόσβασης και κρυπτογράφησης, την παρακολούθηση συμβάντων και τη λήψη διορθωτικών μέτρων, διασφαλίζοντας την αξιοπιστία, την ακεραιότητα και τη διαθεσιμότητα των δεδομένων. Επιπλέον, σε περιβάλλοντα μηχανικής μάθησης, η εφαρμογή του προτύπου προστατεύει τα δεδομένα εκπαίδευσης, περιορίζει την πιθανότητα διαρροής ή κακόβουλης τροποποίησης και ενισχύει την αξιοπιστία των μοντέλων. Συνολικά, το ISO/IEC 27001 παρέχει ένα ολοκληρωμένο, οργανωμένο και αποδοτικό πλαίσιο για τη διαχείριση ασφάλειας πληροφοριών, συνδυάζοντας αρχές συνεχιζόμενης βελτίωσης, διαχείρισης κινδύνων και συμμόρφωσης με διεθνή πρότυπα, καθιστώντας το απαραίτητο εργαλείο για οργανισμούς σε περιβάλλοντα υψηλής τεχνολογίας και IoT.

3.1.2.2 Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας - National Institute of Standards and Technology (NIST)

Το NIST αποτελεί έναν από τους πιο αναγνωρισμένους οργανισμούς παγκοσμίως, που αναπτύσσουν πρότυπα για την ασφάλεια πληροφοριών και την κυβερνοασφάλεια, με εφαρμογές τόσο σε δημόσιους όσο και σε ιδιωτικούς οργανισμούς. Το πιο γνωστό πρότυπο του NIST είναι το NIST Cybersecurity Framework (CSF), το οποίο παρέχει ένα δομημένο και ευέλικτο πλαίσιο για τη διαχείριση κινδύνων στον κυβερνοχώρο. Το NIST CSF οργανώνεται γύρω από πέντε βασικές λειτουργίες: Identify (Ταυτοποίηση), Protect (Προστασία), Detect (Ανίχνευση), Respond (Αντιμετώπιση), Recover (Αποκατάσταση), οι οποίες καλύπτουν ολόκληρο τον κύκλο διαχείρισης ασφάλειας πληροφοριών. Κάθε λειτουργία περιλαμβάνει κατηγορίες και υποκατηγορίες μέτρων που προσαρμόζονται στις ανάγκες κάθε οργανισμού, παρέχοντας ευελιξία και δυνατότητα κλιμάκωσης ανάλογα με το μέγεθος και τη φύση των δεδομένων.[18]

Λειτουργία NIST CSF	Περιγραφή
Identify (Ταυτοποίηση)	Αναγνώριση περιουσιακών στοιχείων, δεδομένων και συστημάτων, αξιολόγηση κινδύνων και ευπαθειών.
Protect (Προστασία)	Μέτρα πρόληψης όπως έλεγχος πρόσβασης, εκπαίδευση προσωπικού και διαχείριση ταυτότητας.
Detect (Ανίχνευση)	Έγκαιρη αναγνώριση περιστατικών μέσω συνεχούς παρακολούθησης και συστημάτων ανίχνευσης.
Respond (Αντιμετώπιση)	Διαδικασίες για αντιμετώπιση περιστατικών, περιορισμό επιπτώσεων και λήψη διορθωτικών μέτρων.
Recover (Αποκατάσταση)	Ταχεία αποκατάσταση συστημάτων και επιχειρησιακής λειτουργικότητας, ενίσχυση διαθεσιμότητας.

Η εφαρμογή του προτύπου NIST CSF παρέχει πολλαπλά οφέλη όπως: ενισχύει την ανθεκτικότητα των συστημάτων, μειώνει τον κινδύνου παραβίασης δεδομένων, ενισχύει την εμπιστοσύνη των πελατών και συνεργατών, και υποστηρίζει τη συμμόρφωση με νομοθετικά και κανονιστικά πλαίσια, όπως το GDPR ή το HIPAA. Επιπλέον, σε σύγχρονα περιβάλλοντα όπως IoT και εφαρμογές μηχανικής μάθησης, η χρήση του NIST CSF είναι κρίσιμη, αφού παρέχει δομημένα εργαλεία για τη διαχείριση μεγάλου όγκου δεδομένων σε πραγματικό χρόνο, προστατεύοντας τα μοντέλα και τα δεδομένα εκπαίδευσης από κακόβουλες τροποποιήσεις ή διαρροές.

Η εφαρμογή του πλαισίου ξεκινά με την αξιολόγηση της τρέχουσας κατάστασης (Current Profile), συνεχίζει με τον καθορισμό του στοχευόμενου επιπέδου ασφάλειας (Target Profile) και ακολουθεί η κατάρτιση σχεδίου δράσης για την κάλυψη των κενών (Action Plan). Με αυτόν τον τρόπο, οι οργανισμοί μπορούν να παρακολουθούν την πρόοδο τους, να αξιολογούν την αποτελεσματικότητα των μέτρων και να αναθεωρούν συνεχώς τις διαδικασίες, διασφαλίζοντας τόσο την ασφάλεια όσο και τη βιωσιμότητα των πληροφοριακών τους συστημάτων. Συνολικά, το NIST παρέχει ένα ολοκληρωμένο, ευέλικτο και δυναμικό πλαίσιο διαχείρισης κυβερνοασφάλειας, το οποίο προσαρμόζεται στις ανάγκες οργανισμών σε περιβάλλοντα υψηλής τεχνολογίας, IoT και μηχανικής μάθησης, συνδυάζοντας πρόληψη, ανίχνευση, αντιμετώπιση και αποκατάσταση κινδύνων

3.1.2.3 Ευρωπαϊκό Ινστιτούτο Προτύπων Τηλεπικοινωνιών - European Telecommunications Standards Institute (ETSI)

Το ETSI αποτελεί έναν από τους κύριους οργανισμούς τυποποίησης στην Ευρώπη, που εστιάζει στην ανάπτυξη προτύπων για τηλεπικοινωνίες, ηλεκτρονικές επικοινωνίες και τεχνολογίες

πληροφορικής, συμπεριλαμβανομένων και των δικτύων IoT και της ασφάλειας πληροφοριών. Το ETSI παρέχει ένα ολοκληρωμένο πλαίσιο προτύπων που διασφαλίζει συμβατότητα, ασφάλεια και διαλειτουργικότητα μεταξύ συσκευών, δικτύων και υπηρεσιών, κάτι που είναι ιδιαίτερα κρίσιμο σε περιβάλλοντα IoT και συστημάτων μεγάλης κλίμακας. Η δράση του επικεντρώνεται τόσο σε τεχνικές προδιαγραφές όσο και σε κατευθυντήριες οδηγίες, οι οποίες υποστηρίζουν τους οργανισμούς στην ανάπτυξη ασφαλών και αξιόπιστων υποδομών. [19]

Ένα από τα βασικά πλεονεκτήματα της χρήσης των προτύπων του ETSI είναι η διαλειτουργικότητα: οι συσκευές και οι εφαρμογές που συμμορφώνονται με τα πρότυπα ETSI μπορούν να συνεργάζονται απρόσκοπτα, μειώνοντας τις τεχνικές δυσκολίες και αυξάνοντας την αποδοτικότητα των συστημάτων. Επιπλέον, τα πρότυπα αυτά ενισχύουν την ασφάλεια πληροφοριών και τη διαχείριση κινδύνων, παρέχοντας κατευθυντήριες γραμμές για την προστασία δεδομένων, τον έλεγχο πρόσβασης και την ανθεκτικότητα των δικτύων σε επιθέσεις. Η συμμόρφωση με τα πρότυπα ETSI προσφέρει επίσης νομοθετικό πλεονέκτημα, διευκολύνοντας τη συμμόρφωση με κανονιστικά πλαίσια της Ευρωπαϊκής Ένωσης, όπως το GDPR, και ενισχύει την εμπιστοσύνη πελατών και συνεργατών.

Η εφαρμογή των προτύπων του ETSI ακολουθεί συνήθως μια διαδικασία αξιολόγησης και πιστοποίησης, που περιλαμβάνει την αναγνώριση των τεχνικών απαιτήσεων, την ανάπτυξη κατάλληλων πολιτικών και διαδικασιών, την εκπαίδευση προσωπικού και τη συνεχή παρακολούθηση των συστημάτων. Σε συνδυασμό με σύγχρονες τεχνολογίες όπως το IoT και η μηχανική μάθηση, τα πρότυπα ETSI παρέχουν ένα ευέλικτο και προσαρμόσιμο πλαίσιο που υποστηρίζει την αυτοΐαση και αποκατάσταση συστημάτων, ενώ διασφαλίζει την ασφάλεια, αξιοπιστία και βιωσιμότητα των δεδομένων.

3.1.2.4 Ομάδα Εργασίας Μηχανικών Διαδικτύου - Internet Engineering Task Force (IETF)

Ο IETF αποτελεί έναν διεθνή οργανισμό που επικεντρώνεται στην ανάπτυξη και προώθηση προτύπων και πρωτοκόλλων για το διαδίκτυο, διασφαλίζοντας τη λειτουργικότητα, διαλειτουργικότητα και ασφάλεια των δικτύων. Το IETF δεν είναι επίσημος φορέας πιστοποίησης, αλλά οι οδηγίες και τα πρότυπα που δημοσιεύει (RFC – Requests for Comments) γίνονται ευρέως αποδεκτά ως βέλτιστες πρακτικές για την κατασκευή και συντήρηση των διαδικτυακών υποδομών. Τα πρότυπα αυτά καλύπτουν κρίσιμους τομείς όπως IP πρωτόκολλα, ασφάλεια δικτύων, επικοινωνίες IoT, μεταφορά δεδομένων και εφαρμογές διαδικτύου. Η δράση του IETF είναι ιδιαίτερα σημαντική σε περιβάλλοντα υψηλής τεχνολογίας και IoT, όπου η συμβατότητα μεταξύ διαφορετικών συσκευών και δικτύων αποτελεί προαπαιτούμενο για την αποτελεσματική λειτουργία των συστημάτων.

Τα πρότυπα του IETF υποστηρίζουν την ασφάλεια, αξιοπιστία και ανθεκτικότητα των δικτύων, με έμφαση σε ζητήματα όπως η κρυπτογράφηση, η αυθεντικοποίηση, η ανίχνευση και αποτροπή επιθέσεων, καθώς και η διαχείριση της κυκλοφορίας και της συμφόρησης των δεδομένων. Η εφαρμογή των προτύπων αυτών συμβάλλει στη βελτίωση της διαλειτουργικότητας μεταξύ διαφορετικών συστημάτων, μειώνοντας τεχνικά προβλήματα και ενισχύοντας την αποδοτικότητα και τη βιωσιμότητα των υποδομών. Παράλληλα, η χρήση των προτύπων IETF διευκολύνει τη συμμόρφωση με διεθνή και εθνικά κανονιστικά πλαίσια και ενισχύει την εμπιστοσύνη των χρηστών και των συνεργατών. Η διαδικασία ενσωμάτωσης των προτύπων του IETF περιλαμβάνει την αξιολόγηση των αναγκών του οργανισμού, την υιοθέτηση κατάλληλων τεχνολογικών λύσεων και πρωτοκόλλων, την εκπαίδευση προσωπικού και την συνεχή παρακολούθηση της αποτελεσματικότητας των μέτρων. Σε συνδυασμό με σύγχρονες τεχνολογίες όπως το IoT και η μηχανική μάθηση, η εφαρμογή των προτύπων IETF παρέχει

ένα ευέλικτο πλαίσιο που ενισχύει την αυτοΐαση και αποκατάσταση συστημάτων, διασφαλίζοντας την ασφάλεια, αξιοπιστία και διαθεσιμότητα των δεδομένων και υπηρεσιών.

3.1.2.5 Οργανισμός για την Προώθηση Προτύπων Δομημένης Πληροφορίας - Organization for the Advancement of Structured Information Standards (OASIS)

Ο OASIS αποτελεί έναν διεθνή μη κερδοσκοπικό οργανισμό που εστιάζει στην ανάπτυξη ανοιχτών προτύπων για τη διαχείριση και ανταλλαγή δομημένων πληροφοριών. Ο οργανισμός αυτός έχει καθοριστική σημασία σε τομείς όπως ασφάλεια πληροφοριών, υπηρεσίες διαδικτύου (Web Services), XML, IoT και blockchain, παρέχοντας τα κατάλληλα πλαίσια για την διαλειτουργικότητα και την ασφάλεια των πληροφοριακών συστημάτων. Ο OASIS δημιουργεί πρότυπα που επιτρέπουν στους οργανισμούς να ανταλλάσσουν δεδομένα με συνέπεια, ασφάλεια και αξιοπιστία, διασφαλίζοντας ότι οι διαφορετικές τεχνολογικές υποδομές μπορούν να συνεργάζονται χωρίς προβλήματα.

Η εφαρμογή των προτύπων του OASIS προσφέρει σημαντικά πλεονεκτήματα. Καταρχάς, ενισχύει την ασφάλεια πληροφοριών, με πρότυπα όπως το SAML (Security Assertion Markup Language) για έλεγχο ταυτότητας και εξουσιοδότησης. Επιπλέον, προάγει τη διαλειτουργικότητα και την αποδοτικότητα των συστημάτων, καθώς οι οργανισμοί που υιοθετούν τα πρότυπα OASIS μπορούν να ανταλλάσσουν δεδομένα και να συνεργάζονται απρόσκοπτα. Η χρήση αυτών των προτύπων διευκολύνει επίσης τη συμμόρφωση με διεθνείς κανονισμούς και πρότυπα, ενισχύοντας την εμπιστοσύνη των πελατών και των συνεργατών. Τέλος, η εφαρμογή των προτύπων OASIS υποστηρίζει τη βιωσιμότητα και ανθεκτικότητα των πληροφοριακών συστημάτων, ιδιαίτερα όταν συνδυάζεται με τεχνολογίες IoT και μηχανικής μάθησης για αυτοΐαση και αποκατάσταση συστημάτων. Η ενσωμάτωση των προτύπων OASIS σε έναν οργανισμό περιλαμβάνει αξιολόγηση των αναγκών και απαιτήσεων, ανάπτυξη κατάλληλων διαδικασιών και πολιτικών, εκπαίδευση προσωπικού και συνεχή παρακολούθηση της αποτελεσματικότητας των μέτρων. Με αυτόν τον τρόπο, οι οργανισμοί μπορούν να επιτύχουν ένα ασφαλές, αξιόπιστο και διαλειτουργικό περιβάλλον, ενώ ταυτόχρονα ενισχύουν τη συμμόρφωση με διεθνή πρότυπα και την εμπιστοσύνη των χρηστών και συνεργατών.

3.1.2.6 Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια - European Union Agency for Cybersecurity (ENISA)

Ο ENISA αποτελεί τον κύριο φορέα της Ευρωπαϊκής Ένωσης για την ασφάλεια στον κυβερνοχώρο, παρέχοντας κατευθυντήριες οδηγίες, πολιτικές και υποστήριξη σε κράτη μέλη, οργανισμούς και επιχειρήσεις σχετικά με την κυβερνοασφάλεια και την προστασία δεδομένων. Ο ρόλος του ENISA είναι κρίσιμος σε περιβάλλοντα υψηλής τεχνολογίας και IoT, όπου η ασφάλεια πληροφοριών και η διαχείριση κινδύνων αποτελούν προτεραιότητα. Η υπηρεσία συνεργάζεται με δημόσιους και ιδιωτικούς φορείς για την ανίχνευση, πρόληψη και αντιμετώπιση κυβερνοαπειλών, ενώ προωθεί την ανάπτυξη βέλτιστων πρακτικών και προτύπων ασφάλειας που είναι σύμφωνες με τους κανονισμούς της ΕΕ, όπως ο GDPR. [20].

Η δράση του ENISA επικεντρώνεται σε διάφορους τομείς: ανθεκτικότητα δικτύων και πληροφοριακών συστημάτων, διαχείριση κρίσεων ασφάλειας, υποστήριξη πολιτικών κυβερνοασφάλειας και ανάπτυξη εργαλείων εκπαίδευσης και ευαισθητοποίησης. Η συμμόρφωση με τις κατευθυντήριες οδηγίες της ενισχύει την ασφάλεια και αξιοπιστία των συστημάτων, μειώνει τον κίνδυνο επιθέσεων και διευκολύνει την ενίσχυση της εμπιστοσύνης των χρηστών και συνεργατών. Επιπλέον, ο ENISA προωθεί τη διαλειτουργικότητα και την συνεργασία μεταξύ ευρωπαϊκών και διεθνών οργανισμών, διασφαλίζοντας ότι οι οργανισμοί μπορούν να ανταλλάσσουν πληροφορίες και

να αντιμετωπίζουν αποτελεσματικά τις απειλές στον κυβερνοχώρο. Η εφαρμογή των συστάσεων και οδηγιών του ENISA περιλαμβάνει αξιολόγηση κινδύνων, ανάπτυξη πολιτικών ασφάλειας, εκπαίδευση προσωπικού, παρακολούθηση και βελτίωση των διαδικασιών. Με αυτόν τον τρόπο, οι οργανισμοί μπορούν να δημιουργήσουν ένα ασφαλές, ανθεκτικό και βιώσιμο περιβάλλον, ενώ ενισχύεται η ικανότητά τους για αυτοΐαση και αποκατάσταση συστημάτων, ιδιαίτερα όταν συνδυάζονται με τεχνολογίες IoT και μηχανικής μάθησης.

3.1.2.7 Ανοικτό Πλαίσιο Εντολών και Ελέγχου - Open Command and Control (OpenC²)

Μετά την παρουσίαση των κύριων οργανισμών και προτύπων στον χώρο της ασφάλειας πληροφοριών, όπως το ISO/IEC 27001, NIST, ETSI, IETF, OASIS και ENISA, καθίσταται εμφανής η ανάγκη για ένα ενιαίο και πρακτικό πλαίσιο αυτοΐασης και διαχείρισης ασφάλειας. Σε αυτό το πλαίσιο, το OpenC² αναδεικνύεται ως μια συγκεκριμένη γλώσσα εντολών και πρωτόκολλο που υιοθετεί και ενσωματώνει τις αρχές και τις βέλτιστες πρακτικές που προωθούν οι παραπάνω οργανισμοί. Το OpenC² σχεδιάστηκε για να επιτρέπει την αυτόματη και απομακρυσμένη διαχείριση συστημάτων κυβερνοασφάλειας, υποστηρίζοντας την ανίχνευση, αντιμετώπιση και αποκατάσταση απειλών με ταχύτητα και συνέπεια.

Η χρήση του OpenC² προσφέρει τη δυνατότητα για συνεχή αυτοΐαση συστημάτων, καθώς οι εντολές που διαβιβάζονται μπορούν να εκτελούνται άμεσα από διαφορετικές συσκευές και πλατφόρμες, εξασφαλίζοντας διαλειτουργικότητα και συμμόρφωση με πρότυπα όπως αυτά του IETF, OASIS και ETSI. Παράλληλα, το OpenC² ενισχύει τη βιωσιμότητα και ανθεκτικότητα των πληροφοριακών υποδομών, μειώνοντας τον ανθρώπινο παράγοντα και τον χρόνο αντίδρασης σε επιθέσεις, ενώ υποστηρίζει και την ενσωμάτωση μηχανικής μάθησης για πιο έξυπνη και προγνωστική διαχείριση απειλών. Στην πράξη, η ενσωμάτωση του OpenC² σε οργανισμούς περιλαμβάνει την αξιολόγηση των υπαρχόντων συστημάτων ασφάλειας, την ανάπτυξη πολιτικών αυτοματοποιημένης αντίδρασης, τη διασύνδεση με υπάρχοντα πρότυπα και εργαλεία, καθώς και την συνεχή παρακολούθηση και βελτίωση της αποτελεσματικότητας των εντολών. Με αυτόν τον τρόπο, το OpenC² παρέχει ένα συνολικό πλαίσιο αυτοΐασης και αποκατάστασης, το οποίο είναι σύμφωνο με τα διεθνή πρότυπα και τις κατευθυντήριες γραμμές των κύριων οργανισμών στον χώρο της κυβερνοασφάλειας.

3.2 Πρότυπα Ασφάλειας και Διαχείρισης Κινδύνων

Στην ενότητα αυτή παρουσιάζονται τα κύρια διεθνή και ευρωπαϊκά πρότυπα ασφάλειας, οι οργανισμοί που τα υποστηρίζουν και η σχέση τους με τη διαχείριση κινδύνων και την αυτοΐαση συστημάτων. Η κατανόηση αυτών των προτύπων είναι απαραίτητη για την εφαρμογή ενός ολοκληρωμένου πλαισίου ασφάλειας σε οργανισμούς και IoT συστήματα.

3.2.1 ISO/IEC 27000 Series και NIST Cybersecurity Framework

Η ασφάλεια των πληροφοριών αποτελεί θεμέλιο για κάθε οργανισμό που επιδιώκει τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων του. Σε αυτό το πλαίσιο, τα πρότυπα ISO/IEC 27000 Series και το NIST Cybersecurity Framework (CSF) αποτελούν δύο από τα πιο καθιερωμένα εργαλεία για τη διαχείριση της κυβερνοασφάλειας και των κινδύνων.[18]

Το ISO/IEC 27000 Series, και ειδικότερα το ISO/IEC 27001, προσφέρει ένα ολοκληρωμένο πλαίσιο Information Security Management System (ISMS), το οποίο καθορίζει πολιτικές, διαδικασίες και ελέγχους για τη συστηματική προστασία των πληροφοριών. Η φιλοσοφία του βασίζεται στην αρχή

Plan-Do-Check-Act (PDCA), η οποία προωθεί τη συνεχή βελτίωση του συστήματος ασφάλειας. Μέσα από το ISMS, οι οργανισμοί μπορούν να εντοπίζουν κινδύνους, να εφαρμόζουν μέτρα προστασίας και να αξιολογούν την αποτελεσματικότητά τους σε τακτά χρονικά διαστήματα. Παράλληλα, η τήρηση των βασικών αρχών του CIA triad (Confidentiality, Integrity, Availability) εξασφαλίζει ότι οι πληροφορίες παραμένουν προστατευμένες, ακριβείς και διαθέσιμες όταν χρειάζονται. Η πιστοποίηση κατά ISO/IEC 27001 προσφέρει πρόσθετα οφέλη, όπως ενίσχυση της αξιοπιστίας προς πελάτες και συνεργάτες, συμμόρφωση με κανονιστικά πλαίσια (π.χ. GDPR) και βελτίωση της οργανωτικής κουλτούρας ασφάλειας.

Από την άλλη, το NIST Cybersecurity Framework παρέχει ένα λειτουργικό και πρακτικό πλαίσιο για τη διαχείριση των κινδύνων ασφάλειας, επικεντρωμένο στις πέντε βασικές λειτουργίες: Identify, Protect, Detect, Respond, Recover. Το πλαίσιο αυτό δίνει έμφαση στην αναγνώριση και αξιολόγηση των απειλών, στην υλοποίηση προστατευτικών μέτρων, στην ανίχνευση παραβιάσεων, στην ανταπόκριση σε περιστατικά και στην αποκατάσταση των λειτουργιών. Η προσεκτική εφαρμογή του NIST CSF επιτρέπει στους οργανισμούς να διαχειρίζονται αποτελεσματικά τους κινδύνους, ενώ ταυτόχρονα διατηρούν τη δυνατότητα συνεχούς προσαρμογής στις μεταβαλλόμενες απειλές.

Παρακάτω παρουσιάζεται ένας συγκριτικός πίνακας που αποτυπώνει τα βασικά χαρακτηριστικά των δύο προτύπων και τις διαφορές τους:

Χαρακτηριστικό	ISO/IEC 27001	NIST CSF
Σκοπός	Ολοκληρωμένο ISMS για διαχείριση ασφάλειας πληροφοριών	Cybersecurity risk management framework για λειτουργική προστασία και αντίδραση
Βασικές αρχές	PDCA, CIA triad	Identify, Protect, Detect, Respond, Recover
Εστίαση	Πολιτικές, διαδικασίες, πιστοποίηση οργανισμού	Λειτουργικές κατηγορίες, πρακτικές εφαρμογής σε καθημερινή λειτουργία
Οφέλη	Εμπιστοσύνη, συμμόρφωση με κανονιστικά πλαίσια, μείωση κινδύνων	Βελτίωση ασφάλειας, διαχείριση κινδύνων, ταχύτερη ανταπόκριση σε περιστατικά

Η επιλογή και η εφαρμογή του κατάλληλου προτύπου εξαρτάται από το μέγεθος, τον κλάδο και τις ανάγκες του οργανισμού. Σε γενικές γραμμές, το ISO/IEC 27001 παρέχει ένα συστηματικό και πιστοποιήσιμο πλαίσιο, ενώ το NIST CSF δίνει πρακτικές κατευθύνσεις για καθημερινή διαχείριση και αντιμετώπιση απειλών. Η συνδυαστική χρήση τους μπορεί να προσφέρει ολοκληρωμένη προσέγγιση διαχείρισης κινδύνων, εξασφαλίζοντας τόσο τη στρατηγική συμμόρφωση όσο και την επιχειρησιακή ανθεκτικότητα.

Ένας μεσαίου μεγέθους οργανισμός πληροφορικής αποφασίζει να ενισχύσει την ασφάλεια των πληροφοριών του. Αρχικά, ξεκινά με την ISO/IEC 27001 πιστοποίηση, δημιουργώντας ένα ISMS που καθορίζει πολιτικές για τον έλεγχο πρόσβασης, την κρυπτογράφηση δεδομένων και τη διαχείριση συμβάντων ασφαλείας. Μέσω της διαδικασίας PDCA, ο οργανισμός πραγματοποιεί τακτικούς ελέγχους και αναθεωρήσεις για συνεχή βελτίωση της ασφάλειας.

Παράλληλα, για την καθημερινή διαχείριση απειλών και περιστατικών, εφαρμόζεται το NIST Cybersecurity Framework. Ο οργανισμός χρησιμοποιεί τις πέντε λειτουργίες του CSF:

- Identify: χαρτογραφεί όλα τα πληροφοριακά του περιουσιακά στοιχεία και τις ευπάθειες τους.
- Protect: εφαρμόζει μέτρα όπως firewalls, κωδικούς πρόσβασης και πολιτικές εκπαίδευσης προσωπικού.

- Detect: εγκαθιστά συστήματα ανίχνευσης παραβιάσεων (IDS/IPS) για γρήγορη εντοπισμό απειλών.
- Respond: δημιουργεί σχέδια αντιμετώπισης περιστατικών και ομάδες άμεσης αντίδρασης.
- Recover: σχεδιάζει διαδικασίες επαναφοράς δεδομένων και επιχειρησιακής συνέχειας σε περίπτωση παραβίασης.

Με αυτό τον τρόπο, ο οργανισμός επωφελείται ταυτόχρονα από τη στρατηγική συμμόρφωση και πιστοποίηση (ISO/IEC 27001) και από την πρακτική διαχείριση κινδύνων και περιστατικών (NIST CSF), δημιουργώντας ένα πλήρες και λειτουργικό πλαίσιο ασφάλειας.

3.2.2 ETSI, ENISA και βιομηχανικά πρότυπα (COBIT, ITIL)

Στον σύγχρονο ψηφιακό κόσμο, η διαχείριση της ασφάλειας πληροφοριών και των επιχειρησιακών διαδικασιών απαιτεί όχι μόνο διεθνή πρότυπα όπως το ISO/IEC 27001 ή το NIST CSF, αλλά και τη στήριξη από εξειδικευμένους οργανισμούς και βιομηχανικά πρότυπα που παρέχουν καθοδήγηση και βέλτιστες πρακτικές σε τομείς όπως οι τηλεπικοινωνίες, η κυβερνοασφάλεια και η διαχείριση IT.

Ο ETSI είναι ένας οργανισμός που εκδίδει πρότυπα για τις τηλεπικοινωνίες, τα δίκτυα και τις ψηφιακές τεχνολογίες στην Ευρώπη. Τα πρότυπα ETSI καλύπτουν θέματα όπως η ασφάλεια των επικοινωνιών, η διαλειτουργικότητα των συστημάτων και οι διαδικασίες διαχείρισης κινδύνων στον τομέα των τηλεπικοινωνιών. Η εφαρμογή των προτύπων αυτών επιτρέπει στους οργανισμούς να εξασφαλίζουν ότι τα δίκτυά τους είναι ασφαλή, αξιόπιστα και συμμορφώνονται με τις ευρωπαϊκές απαιτήσεις, ενώ παράλληλα ενισχύουν την καινοτομία μέσω κοινών τεχνικών προδιαγραφών.

Ο ENISA αποτελεί τον κύριο φορέα υποστήριξης και προώθησης της κυβερνοασφάλειας στην Ευρωπαϊκή Ένωση. Ο ENISA εκδίδει κατευθυντήριες οδηγίες, μελέτες και εργαλεία για τη διαχείριση κινδύνων, την ανίχνευση απειλών και την ετοιμότητα απέναντι σε περιστατικά κυβερνοασφάλειας. Επιπλέον, ο ENISA συνεργάζεται με κυβερνήσεις και βιομηχανικούς φορείς για την ανάπτυξη κοινών στρατηγικών ασφάλειας, την εκπαίδευση προσωπικού και την υποστήριξη συμμόρφωσης με ευρωπαϊκές οδηγίες, όπως η NIS Directive.

Παράλληλα, τα βιομηχανικά πρότυπα COBIT και ITIL παρέχουν εργαλεία και πλαίσια για την οργάνωση και διαχείριση των IT διαδικασιών με στόχο τη μεγιστοποίηση της αξίας των τεχνολογιών και τη μείωση κινδύνων. Το COBIT (Control Objectives for Information and Related Technologies) επικεντρώνεται στη διακυβέρνηση και τη διαχείριση IT, παρέχοντας έναν σαφή οδηγό για την παρακολούθηση, την αξιολόγηση και τη βελτίωση των διαδικασιών IT. Αντίστοιχα, το ITIL (Information Technology Infrastructure Library) προσφέρει βέλτιστες πρακτικές για την υποστήριξη υπηρεσιών IT, καλύπτοντας θέματα όπως incident management, problem management και service lifecycle management. Η εφαρμογή αυτών των πλαισίων βοηθά τους οργανισμούς να βελτιστοποιούν τις υπηρεσίες τους, να μειώνουν τα σφάλματα και να αυξάνουν την επιχειρησιακή συνέχεια.

Η συνδυαστική χρήση των ETSI, ENISA και των βιομηχανικών προτύπων παρέχει στους οργανισμούς ένα ολιστικό πλαίσιο ασφάλειας και διαχείρισης IT. Ενώ τα πρότυπα των ETSI και ENISA επικεντρώνονται περισσότερο στις εξειδικευμένες απαιτήσεις ασφάλειας και συμμόρφωσης στον ευρωπαϊκό χώρο, τα COBIT και ITIL προσφέρουν λειτουργική και διαχειριστική καθοδήγηση για τον οργανισμό. Η παράλληλη χρήση τους διασφαλίζει ότι οι τεχνολογικές υποδομές και οι διαδικασίες IT είναι αξιόπιστες, ασφαλείς και πλήρως εναρμονισμένες με τις βέλτιστες πρακτικές.

Για μεγαλύτερη σαφήνεια, ο παρακάτω πίνακας παρουσιάζει τις βασικές ιδιότητες και τομείς εστίασης κάθε προτύπου/οργανισμού:

Οργανισμός / Πρότυπο	Τομέας Εστίασης	Κύριος Σκοπός
ETSI	Τηλεπικοινωνίες, δίκτυα	Διαλειτουργικότητα, ασφάλεια δικτύων
ENISA	Κυβερνοασφάλεια	Κατευθυντήριες οδηγίες, διαχείριση κινδύνων
COBIT	Διακυβέρνηση IT	Διαχείριση και έλεγχος IT διαδικασιών
ITIL	Διαχείριση υπηρεσιών IT	Βέλτιστες πρακτικές IT service management

Η κατανόηση και εφαρμογή αυτών των προτύπων προσφέρει στους οργανισμούς ένα ολοκληρωμένο πλαίσιο για τη διαχείριση ασφάλειας, κινδύνων και IT υπηρεσιών, δημιουργώντας μια σταθερή βάση για την ενσωμάτωση προηγμένων συστημάτων αυτοΐασης και αποκατάστασης, όπως αυτά που υποστηρίζονται από τεχνολογίες IoT και μηχανική μάθηση.

3.3 Πρωτόκολλα Εντολών και Ελέγχου

Η ανάπτυξη προηγμένων συστημάτων αυτοΐασης και αποκατάστασης στον χώρο του IoT και της κυβερνοασφάλειας απαιτεί όχι μόνο την εφαρμογή προτύπων και πλαισίων διαχείρισης κινδύνων, αλλά και τη χρήση πρωτοκόλλων εντολών και ελέγχου (Command and Control Protocols). Τα πρωτόκολλα αυτά καθορίζουν τον τρόπο επικοινωνίας μεταξύ των συστημάτων, επιτρέπουν την εκτέλεση εντολών, τη συλλογή δεδομένων και την αντίδραση σε περιστατικά σε πραγματικό χρόνο. Σε επίπεδο λειτουργικότητας, τα πρωτόκολλα εντολών και ελέγχου προσφέρουν συγκεντρωμένη διαχείριση των συσκευών και των υποδομών, εξασφαλίζοντας ότι οι ενέργειες αποκατάστασης και αυτοΐασης εκτελούνται με συνέπεια, ασφάλεια και διαφάνεια. Αυτό είναι ιδιαίτερα σημαντικό σε περιβάλλοντα IoT, όπου οι συσκευές είναι κατανεμημένες και συχνά λειτουργούν σε συνθήκες περιορισμένων πόρων ή υψηλής ευαισθησίας.[24]

Ένα από τα πλέον σημαντικά παραδείγματα τέτοιου πρωτοκόλλου είναι το OpenC² (Open Command and Control), που αποτελεί διεθνές πρότυπο για την απομακρυσμένη διαχείριση ασφάλειας. Το OpenC² παρέχει μια ανοικτή γλώσσα εντολών που μπορεί να ενσωματωθεί με διάφορα συστήματα και πρότυπα, όπως τα ISO/IEC 27001, NIST CSF και τα βιομηχανικά πρότυπα ITIL και COBIT, προσφέροντας ένα κοινό πλαίσιο για την ανίχνευση απειλών, την αντίδραση σε περιστατικά και την αυτοΐαση. Η ευελιξία του OpenC² επιτρέπει στους οργανισμούς να καθορίζουν πολιτικές ασφαλείας και να εκτελούν αυτοματοποιημένες ενέργειες χωρίς να απαιτείται ανθρώπινη παρέμβαση σε κάθε βήμα. [25], [26], [27].

Τα πρωτόκολλα εντολών και ελέγχου μπορούν να χωριστούν σε τρεις βασικές κατηγορίες:

1. Στατικά πρωτόκολλα: Καθορίζουν προκαθορισμένες εντολές που εκτελούνται με συγκεκριμένη σειρά. Είναι κατάλληλα για περιβάλλοντα με σταθερές διαδικασίες, αλλά εμφανίζουν περιορισμένη ευελιξία.
2. Δυναμικά πρωτόκολλα: Επιτρέπουν την προσαρμογή των εντολών σε πραγματικό χρόνο, ανάλογα με τις συνθήκες ή τα περιστατικά που ανιχνεύονται. Η αυτοΐαση συχνά βασίζεται σε τέτοια πρωτόκολλα.
3. Πρωτόκολλα με ανατροφοδότηση (feedback-driven): Συνδυάζουν την εκτέλεση εντολών με συνεχή παρακολούθηση της κατάστασης του συστήματος, επιτρέποντας συνεχή βελτιστοποίηση των ενεργειών και της απόδοσης.

Η χρήση αυτών των πρωτοκόλλων προσφέρει σημαντικά οφέλη: βελτιωμένη ασφάλεια, ταχύτητα αντίδρασης, μείωση ανθρώπινου λάθους και αυξημένη αξιοπιστία των συστημάτων. Επιπλέον, όταν συνδυάζονται με συστήματα μηχανικής μάθησης, μπορούν να επιτυγχάνουν προβλεπτική αντίδραση, αναγνωρίζοντας πρότυπα απειλών και αυτοματοποιώντας την αποκατάσταση πριν προκληθεί ζημία.

Για μεγαλύτερη σαφήνεια, ο παρακάτω πίνακας συνοψίζει τις βασικές κατηγορίες πρωτοκόλλων εντολών και ελέγχου και τα χαρακτηριστικά τους:

Κατηγορία Πρωτοκόλλου	Περιγραφή	Χαρακτηριστικά	Πλεονεκτήματα
Στατικά (Static)	Προκαθορισμένες εντολές	Απλά, προβλέψιμα	Αξιοπιστία, εύκολη υλοποίηση
Δυναμικά (Dynamic)	Εντολές προσαρμοζόμενες σε πραγματικό χρόνο	Ευέλικτα, αυτοματοποιημένα	Αυξημένη προσαρμοστικότητα και αυτοΐαση
Με ανατροφοδότηση (Feedback-driven)	Συνδυάζουν εκτέλεση εντολών με συνεχή παρακολούθηση	Προβλεπτικά, βελτιστοποιημένα	Μείωση κινδύνου, πρόβλεψη και αποκατάσταση σφαλμάτων

Η υιοθέτηση τέτοιων πρωτοκόλλων είναι κρίσιμη για την ενοποίηση ασφάλειας, διαχείρισης κινδύνων και λειτουργικής αυτοΐασης, ειδικά σε περιβάλλοντα που στηρίζονται σε IoT και τεχνολογίες μηχανικής μάθησης. Με τον σωστό σχεδιασμό, τα πρωτόκολλα αυτά διασφαλίζουν ότι οι οργανισμοί μπορούν να αντιμετωπίζουν απειλές σε πραγματικό χρόνο, ενώ παράλληλα συμμορφώνονται με διεθνή πρότυπα και καλές πρακτικές.

3.3.1 OpenC² και εφαρμογές του

Το OpenC² αποτελεί ένα διεθνές πρότυπο που αναπτύχθηκε με σκοπό να παρέχει μια κοινή γλώσσα εντολών για την αυτοματοποιημένη διαχείριση της ασφάλειας σε συστήματα πληροφορικής και IoT. Το πρότυπο επιτρέπει την εκτέλεση εντολών σε κατανεμημένα συστήματα, τη συλλογή πληροφοριών ασφαλείας και την άμεση αντίδραση σε περιστατικά, συνδυάζοντας λειτουργίες εντολών και ελέγχου με τις αρχές αυτοΐασης και αυτοματοποίησης. Η κύρια φιλοσοφία του OpenC² βασίζεται στην ενσωμάτωση καλών πρακτικών από διεθνή πρότυπα όπως τα ISO/IEC 27001, NIST CSF και τα βιομηχανικά πλαίσια ITIL και COBIT. Μέσω της γλώσσας OpenC², οι οργανισμοί μπορούν να ορίζουν πολιτικές ασφαλείας, να συντονίζουν την αντίδραση σε περιστατικά και να αυτοματοποιούν διαδικασίες αποκατάστασης, διασφαλίζοντας ότι οι ενέργειες συμμορφώνονται με τα πρότυπα ασφάλειας και διαχείρισης κινδύνου. Η γλώσσα OpenC² είναι προσαρμόσιμη και επεκτάσιμη, επιτρέποντας την επικοινωνία μεταξύ διαφορετικών τύπων συσκευών και συστημάτων, ανεξάρτητα από τον κατασκευαστή ή την τεχνολογική πλατφόρμα. Η σύνταξη των εντολών ακολουθεί απλή και κατανοητή δομή, η οποία μπορεί να μεταφραστεί σε εκτελέσιμες ενέργειες από τα διαχειριζόμενα συστήματα. Αυτό είναι κρίσιμο σε περιβάλλοντα IoT, όπου οι συσκευές είναι συχνά περιορισμένες σε υπολογιστική ισχύ και μνήμη, αλλά απαιτούν άμεση και ασφαλή αντίδραση σε απειλές ή ανωμαλίες.

Οι εφαρμογές του OpenC² είναι οι ακόλουθες:

1. Αυτοματοποιημένη Αντίδραση σε Κυβερνοεπιθέσεις (Automated Threat Response)

   Το OpenC² επιτρέπει την άμεση εκτέλεση εντολών για την αντιμετώπιση επιθέσεων, όπως η απομόνωση μιας μολυσμένης συσκευής ή η απενεργοποίηση συγκεκριμένων θυρών επικοινωνίας, χωρίς την ανάγκη ανθρώπινης παρέμβασης. Αυτό μειώνει το χρόνο αντίδρασης και περιορίζει την εξάπλωση απειλών σε όλο το δίκτυο.

2. Συντονισμός Διαχείρισης Πολιτικών Ασφαλείας (Policy Enforcement)

   Μέσω του OpenC² οι οργανισμοί μπορούν να εφαρμόζουν και να τροποποιούν πολιτικές ασφαλείας σε πραγματικό χρόνο. Για παράδειγμα, η αλλαγή κανόνων firewall ή η εφαρμογή νέων κανόνων πρόσβασης γίνεται με εντολές OpenC², εξασφαλίζοντας ομοιομορφία και συμμόρφωση με διεθνή πρότυπα.

3. Υποστήριξη Αυτοΐασης (Self-Healing)

   Συνδυάζοντας OpenC² με συστήματα μηχανικής μάθησης, είναι δυνατή η προβλεπτική ανίχνευση και αυτοματοποιημένη αποκατάσταση προβλημάτων. Οι συσκευές IoT μπορούν να προσαρμόζουν τη λειτουργία τους σε πραγματικό χρόνο, αποτρέποντας καταστάσεις που θα οδηγούσαν σε σφάλματα ή διακοπές υπηρεσιών.

4. Συνεργασία μεταξύ Πολλαπλών Πλατφορμών (Cross-Platform Interoperability)

   Το OpenC² προσφέρει ένα κοινό πρότυπο εντολών, επιτρέποντας την επικοινωνία και τον συντονισμό μεταξύ διαφορετικών συστημάτων, όπως δίκτυα IoT, κέντρα δεδομένων και cloud υποδομές. Αυτό εξασφαλίζει ότι η ασφάλεια και η διαχείριση συμβαδίζουν σε όλο το περιβάλλον της επιχείρησης.

Η ευελιξία και η επεκτασιμότητα του OpenC² το καθιστούν κρίσιμο εργαλείο για οργανισμούς που επιδιώκουν ασφαλή και αυτοματοποιημένη διαχείριση IoT συστημάτων, ενοποιώντας τις διαδικασίες παρακολούθησης, ανίχνευσης και απόκρισης. Με τη σωστή ενσωμάτωση, τα συστήματα μπορούν να λειτουργούν προληπτικά, μειώνοντας σημαντικά τους κινδύνους και ενισχύοντας την ανθεκτικότητα των υποδομών.

3.3.2 Ανταλλαγή πληροφοριών ασφαλείας - STIX, TAXII, SCAP

Η ανταλλαγή πληροφοριών ασφαλείας αποτελεί κρίσιμο στοιχείο στη διαχείριση απειλών σε περιβάλλοντα IoT και κυβερνοασφάλειας γενικότερα. Προκειμένου να επιτευχθεί συνεργασία μεταξύ οργανισμών, συστημάτων και υπηρεσιών, έχουν αναπτυχθεί διεθνή πρότυπα που καθορίζουν μορφή, πρωτόκολλα και διαδικασίες για τη μεταφορά πληροφοριών ασφάλειας. Τα πιο σημαντικά από αυτά είναι το STIX (Structured Threat Information eXpression - Έκφραση πληροφοριών δομημένης απειλής), TAXII (Trusted Automated eXchange of Indicator Information - Αξιόπιστη αυτοματοποιημένη ανταλλαγή δεικτών πληροφοριών) και SCAP (Security Content Automation Protocol - Πρωτόκολλο Αυτοματοποίησης Περιεχομένου Ασφαλείας).

Το STIX είναι ένα μορφότυπο για την αναπαράσταση πληροφοριών απειλών με δομημένο και τυποποιημένο τρόπο. Η κύρια λειτουργία του είναι η περιγραφή των δεικτών απειλών (Indicators of Compromise), των τεχνικών επίθεσης, των παραμέτρων ευπάθειας και των σχέσεων μεταξύ αυτών. Μέσω του STIX, οι οργανισμοί μπορούν να καταγράψουν και να κοινοποιήσουν πληροφορίες σχετικά με επιθέσεις, malware ή κακόβουλες δραστηριότητες με ακριβή και κατανοητό τρόπο, εξασφαλίζοντας διαλειτουργικότητα μεταξύ διαφορετικών συστημάτων και εργαλείων ανάλυσης.

Το TAXII αποτελεί το πρωτόκολλο επικοινωνίας και μεταφοράς των δεδομένων STIX. Ενώ το STIX καθορίζει το περιεχόμενο των πληροφοριών, το TAXII προσδιορίζει πώς οι πληροφορίες ανταλλάσσονται μεταξύ οργανισμών ή συστημάτων. Υποστηρίζει διάφορους τύπους υπηρεσιών, όπως συλλογή (collection), συνδρομή (subscription) και αποστολή (push/pull), και διασφαλίζει ότι τα δεδομένα φτάνουν με ασφαλή και συγχρονισμένο τρόπο στον προορισμό τους. Η χρήση TAXII επιτρέπει σε οργανισμούς και κοινότητες ασφάλειας να ανταποκρίνονται γρήγορα σε απειλές, δημιουργώντας ένα οικοσύστημα συνεργασίας και έγκαιρης προειδοποίησης.

Το SCAP είναι ένα πρότυπο αυτοματοποίησης αξιολόγησης και συμμόρφωσης ασφάλειας. Στόχος του είναι να παρέχει ένα σύνολο εργαλείων και δεδομένων για αυτόματη αξιολόγηση συστημάτων, εφαρμογή πολιτικών ασφαλείας και διαχείριση ευπαθειών. Το SCAP περιλαμβάνει συνιστώσες όπως το CVE (Common Vulnerabilities and Exposures), το CPE (Common Platform Enumeration) και το CCE (Common Configuration Enumeration), επιτρέποντας την ομοιογενή αναγνώριση και αντιμετώπιση ευπαθειών σε μεγάλα δίκτυα και περιβάλλοντα IoT.

Συνδυαστικά, τα STIX, TAXII και SCAP επιτρέπουν τη συλλογή, την τυποποίηση και την ανταλλαγή πληροφοριών ασφαλείας, προσφέροντας τα εξής πλεονεκτήματα:

1. Έγκαιρη αντίδραση σε απειλές: Μέσω άμεσης κοινοποίησης δεικτών απειλών, οι οργανισμοί μπορούν να προλαμβάνουν επιθέσεις και να περιορίζουν τον αντίκτυπο.
2. Αυτοματοποίηση διαδικασιών: Η τυποποίηση δεδομένων και η χρήση αυτοματοποιημένων εργαλείων μειώνει την ανάγκη για χειροκίνητες ενέργειες.
3. Διαλειτουργικότητα συστημάτων: Τα πρότυπα επιτρέπουν συνεργασία μεταξύ διαφορετικών λογισμικών και οργανισμών, ενισχύοντας την συνολική ασφάλεια.
4. Συμμόρφωση και αξιοπιστία: Η χρήση τυποποιημένων διαδικασιών διευκολύνει την πιστοποίηση και την τήρηση κανονιστικών απαιτήσεων.

Ο παρακάτω πίνακας συνοψίζει τα βασικά χαρακτηριστικά των τριών προτύπων:

Πρότυπο	Λειτουργία	Κύρια Χρήση	Οφέλη
STIX	Μορφοποίηση δεδομένων απειλών	Αναπαράσταση δεικτών, τεχνικών και παραμέτρων	Διαλειτουργικότητα, σαφήνεια πληροφοριών
TAXII	Πρωτόκολλο μεταφοράς	Ασφαλής ανταλλαγή STIX δεδομένων	Έγκαιρη κοινοποίηση, συνεργασία
SCAP	Αυτοματοποίηση συμμόρφωσης	Αξιολόγηση συστημάτων, διαχείριση ευπαθειών	Αυτοματοποίηση, τυποποίηση, αξιοπιστία

Η ενσωμάτωση αυτών των προτύπων σε συστήματα αυτοΐασης και αυτοματοποιημένης απόκρισης σε IoT περιβάλλοντα είναι κρίσιμη για την πρόληψη, ανίχνευση και αποκατάσταση απειλών σε πραγματικό χρόνο. Η χρήση τους ενισχύει την συνολική ανθεκτικότητα των υποδομών και διευκολύνει την υιοθέτηση πρακτικών ασφαλούς και αυτοματοποιημένης διαχείρισης πληροφοριών.

3.3.3 Επικοινωνία σε δίκτυα και IoT (MQTT, CoAP, REST APIs)

Η επικοινωνία μεταξύ συσκευών σε δίκτυα IoT αποτελεί θεμελιώδη παράμετρο για την αποτελεσματική λειτουργία και ασφάλεια των συστημάτων. Τα πρωτόκολλα επικοινωνίας που χρησιμοποιούνται στα περιβάλλοντα IoT πρέπει να είναι ελαφριά, αποδοτικά και ασφαλή, δεδομένων των περιορισμένων πόρων των συσκευών, όπως μνήμη, επεξεργαστική ισχύς και ενέργεια. Τα πιο διαδεδομένα πρότυπα για την επικοινωνία σε IoT περιβάλλοντα είναι τα MQTT (Message Queuing Telemetry Transport - Μεταφορά Τηλεμετρίας Ουράς Μηνυμάτων), CoAP (Constrained Application Protocol - Πρωτόκολλο Περιορισμένων Εφαρμογών) και RESTful APIs (REpresentational State Transfer Application Programming Interfaces - Διεπαφές Προγραμματισμού Εφαρμογών με Μεταφορά Αναπαραστάσεων Κατάστασης)

3.3.3.1 Message Queuing Telemetry Transport – MQTT

Το MQTT αποτελεί ένα από τα πιο δημοφιλή πρωτόκολλα επικοινωνίας για συστήματα IoT, κυρίως λόγω της απλότητας, ευελιξίας και χαμηλής κατανάλωσης πόρων. Σχεδιάστηκε αρχικά από την IBM τη δεκαετία του 1990 για εφαρμογές τηλεμετρίας, όπου η μετάδοση δεδομένων έπρεπε να γίνεται σε δίκτυα με περιορισμένο εύρος ζώνης και υψηλή πιθανότητα απώλειας πακέτων. Το MQTT βασίζεται σε ένα αρχιτεκτονικό μοντέλο publish/subscribe, που διαφοροποιείται σημαντικά από τα παραδοσιακά πρωτόκολλα τύπου client-server. [25]

Η αρχιτεκτονική του είναι της μορφής publish/subscribe, οι συσκευές IoT δεν επικοινωνούν απευθείας μεταξύ τους. Αντίθετα, υπάρχει ένας κεντρικός broker, ο οποίος λειτουργεί ως ενδιάμεσος διαχειριστής των μηνυμάτων. Οι συσκευές χωρίζονται σε δύο βασικούς ρόλους:

1. Publisher (εκδότης): Η συσκευή που παράγει δεδομένα ή γεγονότα, π.χ., ένας αισθητήρας θερμοκρασίας που στέλνει μετρήσεις.
2. Subscriber (συνδρομητής): Η συσκευή ή εφαρμογή που ενδιαφέρεται να λάβει τα δεδομένα αυτά, π.χ., ένα σύστημα παρακολούθησης ή ένα dashboard.

Όταν ο publisher αποστέλλει ένα μήνυμα σε ένα συγκεκριμένο topic (θέμα), ο broker αναλαμβάνει να το προωθήσει σε όλους τους subscribers που έχουν εγγραφεί σε αυτό το topic. Αυτή η αρχιτεκτονική παρέχει ασύγχρονη επικοινωνία, μειώνει την εξάρτηση των συσκευών μεταξύ τους και επιτρέπει την εύκολη κλιμάκωση του συστήματος.

Τα πλεονεκτήματα του MQTT είναι τα ακόλουθα:

- Χαμηλή κατανάλωση ενέργειας: Η επικοινωνία είναι ελαφριά, ιδανική για συσκευές με περιορισμένη μπαταρία.
- Αξιοπιστία: Το πρωτόκολλο υποστηρίζει τρία επίπεδα ποιότητας υπηρεσίας (QoS):
  - QoS 0: Το μήνυμα παραδίδεται μία φορά χωρίς επιβεβαίωση.
  - QoS 1: Το μήνυμα παραδίδεται τουλάχιστον μία φορά, με επιβεβαίωση από τον subscriber.
  - QoS 2: Το μήνυμα παραδίδεται ακριβώς μία φορά, εξασφαλίζοντας πλήρη αξιοπιστία.
- Αντοχή σε ασταθή δίκτυα: Το MQTT μπορεί να επανασυνδεθεί αυτόματα σε περίπτωση αποσύνδεσης, εξασφαλίζοντας τη συνέχεια της επικοινωνίας.
- Επεκτασιμότητα: Η χρήση broker επιτρέπει την εύκολη διαχείριση μεγάλου αριθμού συσκευών χωρίς αλλαγές στην υποδομή.

Οι εφαρμογές του MQTT συναντώνται σε διάφορους τομείς:

- Έξυπνα σπίτια (Smart Homes): Αισθητήρες φωτός, θερμοκρασίας και καπνού επικοινωνούν με κεντρικές εφαρμογές, επιτρέποντας αυτοματοποίηση και ειδοποιήσεις.
- Βιομηχανικό IoT (IIoT): Παρακολούθηση μηχανημάτων σε πραγματικό χρόνο, πρόβλεψη βλαβών και απομακρυσμένη συντήρηση.
- Συστήματα τηλεμετρίας: Μεταφορά δεδομένων από αισθητήρες περιβαλλοντικών παραμέτρων σε κεντρικά συστήματα παρακολούθησης.

Η ακολουθία της τυπικής ροής του μηνύματος είναι:

1. Ο publisher παράγει ένα μήνυμα και το αποστέλλει στο broker με το καθορισμένο topic.

2. Ο broker λαμβάνει το μήνυμα και το καταχωρεί στα subscribers που ενδιαφέρονται για αυτό το topic.
3. Οι subscribers λαμβάνουν τα δεδομένα, τα επεξεργάζονται ή τα εμφανίζουν σε εφαρμογές ή dashboards.

Η χρήση του MQTT επιτρέπει την αποτελεσματική και αξιόπιστη διαχείριση μεγάλου όγκου δεδομένων σε πραγματικό χρόνο, διασφαλίζοντας την ομαλή λειτουργία πολύπλοκων συστημάτων IoT, χωρίς να απαιτείται υψηλό εύρος ζώνης ή ισχυρός υπολογιστικός εξοπλισμός.

3.3.3.2 Constrained Application Protocol – CoAP

Το CoAP είναι ένα ελαφρύ πρωτόκολλο εφαρμογής σχεδιασμένο ειδικά για συσκευές με περιορισμένους πόρους, όπως αισθητήρες, actuators και μικροελεγκτές στο περιβάλλον του IoT. Ο κύριος στόχος του CoAP είναι η αποτελεσματική επικοινωνία σε δίκτυα με περιορισμένο εύρος ζώνης και περιορισμένους υπολογιστικούς πόρους, διατηρώντας παράλληλα την αξιοπιστία και την ευελιξία που προσφέρουν τα πρωτόκολλα υψηλότερου επιπέδου, όπως το HTTP.

Τα βασικά χαρακτηριστικά του είναι:

1. Βασισμένο στην αρχιτεκτονική REST:
   Το CoAP ακολουθεί την αρχιτεκτονική REST (Representational State Transfer), που σημαίνει ότι οι πόροι (resources) αναπαρίστανται με URI (Uniform Resource Identifier) και οι ενέργειες εκτελούνται μέσω τυπικών μεθόδων όπως GET, POST, PUT, DELETE. Αυτό επιτρέπει την εύκολη ενσωμάτωση με υπάρχουσες web υπηρεσίες και cloud πλατφόρμες.
2. Χρήση UDP αντί για TCP:
   Σε αντίθεση με το HTTP που βασίζεται στο TCP, το CoAP χρησιμοποιεί το UDP (User Datagram Protocol). Η χρήση του UDP μειώνει σημαντικά το overhead, καθιστώντας το πρωτόκολλο πιο ελαφρύ και γρήγορο για τη μεταφορά μικρών πακέτων δεδομένων. Αν και το UDP από μόνο του δεν προσφέρει αξιόπιστη παράδοση, το CoAP ενσωματώνει μηχανισμούς επιβεβαίωσης (confirmable messages) για κρίσιμες πληροφορίες και μη επιβεβαίωσης (non-confirmable messages) για λιγότερο κρίσιμα δεδομένα.
3. Αξιοπιστία και ελαχιστοποίηση κατανάλωσης ενέργειας:
   Το CoAP επιτρέπει την επιβεβαίωση παραλαβής μηνυμάτων όταν απαιτείται, ενώ παράλληλα μειώνει την κατανάλωση ενέργειας και την κυκλοφορία στο δίκτυο, καθιστώντας το ιδανικό για συσκευές που λειτουργούν με μπαταρία ή δίκτυα μεγάλης κλίμακας με περιορισμένους πόρους.
4. Υποστήριξη multicast:
   Το CoAP μπορεί να στέλνει μηνύματα σε πολλές συσκευές ταυτόχρονα μέσω multicast, γεγονός που είναι ιδιαίτερα χρήσιμο για εφαρμογές όπως ομαδικός έλεγχος αισθητήρων ή μαζική ενημέρωση συσκευών.
5. Ασφάλεια:
   Το CoAP ενσωματώνει ασφάλεια μέσω του DTLS (Datagram Transport Layer Security), παρέχοντας κρυπτογράφηση και αυθεντικοποίηση σε ένα ελαφρύ και αποδοτικό πρωτόκολλο κατάλληλο για IoT συσκευές.

Η αρχιτεκτονική του είναι της μορφής κλασικής ροής επικοινωνίας CoAP:

1. Ο client στέλνει ένα αίτημα (request) σε έναν server για έναν συγκεκριμένο πόρο (π.χ., θερμοκρασία ενός αισθητήρα).

2. Ο server απαντά με ένα μήνυμα απόκρισης (response), είτε επιβεβαιωμένο είτε μη επιβεβαιωμένο ανάλογα με τη σημασία του δεδομένου.
3. Αν απαιτείται, οι συσκευές μπορούν να εγγραφούν σε ένα resource μέσω μηχανισμού observe, ώστε να λαμβάνουν ενημερώσεις αυτόματα όταν αλλάζει η τιμή του πόρου.

Αυτή η αρχιτεκτονική επιτρέπει την ασύγχρονη και αποδοτική επικοινωνία μεταξύ συσκευών και υπηρεσιών, μειώνοντας την καθυστέρηση και αυξάνοντας την αξιοπιστία σε περιβάλλοντα με περιορισμένους πόρους.

Οι εφαρμογές CoAP συναντώνται σε διάφορους τομείς του IoT:

- Έξυπνα σπίτια: Έλεγχος φωτισμού, θερμοκρασίας, αισθητήρων καπνού και άλλων συσκευών.
- Βιομηχανικό IoT: Παρακολούθηση μηχανημάτων, συλλογή δεδομένων αισθητήρων σε πραγματικό χρόνο.
- Δίκτυα αισθητήρων περιβάλλοντος: Μέτρηση θερμοκρασίας, υγρασίας, ποιότητας αέρα και άλλων παραμέτρων.
- Συνδυασμός με cloud υπηρεσίες: Δυνατότητα άμεσης ενσωμάτωσης με REST APIs, διευκολύνοντας την αποθήκευση και ανάλυση δεδομένων στο cloud.

Χαρακτηριστικά	Περιγραφή
Ελαφρύ και γρήγορο	Χρήση UDP και ελαχιστοποίηση overhead
Ενσωμάτωση με REST	Άμεση επικοινωνία με web υπηρεσίες και cloud
Αξιοπιστία	Confirmable/Non-confirmable μηνύματα
Εξοικονόμηση ενέργειας	Ιδανικό για συσκευές που κινούνται με μπαταρίες
Υποστήριξη multicast	Μαζική επικοινωνία με πολλές συσκευές ταυτόχρονα
Ασφάλεια	Υποστήριξη DTLS για κρυπτογράφηση και αυθεντικοποίηση

3.3.3.3 Representational State Transfer – REST APIs

Τα RESTful APIs αποτελούν ένα αρχιτεκτονικό πρότυπο επικοινωνίας για web υπηρεσίες, το οποίο βασίζεται σε πρωτόκολλα όπως το HTTP/HTTPS [26]. Η κύρια φιλοσοφία των REST APIs είναι η αλληλεπίδραση με πόρους (resources), οι οποίοι αναπαρίστανται με μοναδικά URI (Uniform Resource Identifier). Κάθε πόρος μπορεί να ανακτηθεί, τροποποιηθεί, δημιουργηθεί ή διαγραφεί μέσω τυποποιημένων HTTP μεθόδων:

- GET: Ανάκτηση δεδομένων από έναν πόρο.
- POST: Δημιουργία νέου πόρου ή αποστολή δεδομένων σε έναν server.
- PUT: Ενημέρωση ή αντικατάσταση ενός υπάρχοντος πόρου.
- DELETE: Διαγραφή ενός πόρου.

Η χρήση των REST APIs σε περιβάλλοντα IoT, αποτελούν την κύρια γέφυρα επικοινωνίας μεταξύ συσκευών, κεντρικών συστημάτων και υπηρεσιών cloud. Η απλότητά τους και η ευκολία ενσωμάτωσης επιτρέπουν στις IoT συσκευές να στέλνουν δεδομένα αισθητήρων, να λαμβάνουν εντολές ή να ενημερώνουν την κατάστασή τους με αξιόπιστο και ευέλικτο τρόπο.

Μερικά βασικά χαρακτηριστικά που καθιστούν τα REST APIs κατάλληλα για IoT περιβάλλοντα είναι:

1. Αρχιτεκτονική χωρίς κατάσταση (stateless):
   Κάθε αίτημα περιέχει όλες τις απαραίτητες πληροφορίες για την εκτέλεσή του. Αυτό μειώνει την πολυπλοκότητα στη διαχείριση συνεδριών και επιτρέπει στις συσκευές να επικοινωνούν ακόμα και σε δίκτυα με περιορισμένους πόρους.

2. Ευέλικτη μορφή δεδομένων:
   Τα REST APIs υποστηρίζουν διαφορετικά formats όπως JSON, XML ή plain text, με το JSON να είναι η πιο δημοφιλής επιλογή σε IoT, λόγω μικρού μεγέθους και απλότητας στην επεξεργασία.

3. Εύκολη ενσωμάτωση με cloud υπηρεσίες και dashboards:
   Οι πληροφορίες που συλλέγονται από τις IoT συσκευές μπορούν να αποθηκεύονται σε cloud πλατφόρμες, να επεξεργάζονται σε πραγματικό χρόνο και να παρουσιάζονται σε dashboards για παρακολούθηση ή ανάλυση.

4. Ασφάλεια:
   Τα REST APIs μπορούν να συνδυαστούν με HTTPS και πρότυπα authentication όπως OAuth2, API keys ή JWT (JSON Web Tokens), εξασφαλίζοντας την εμπιστευτικότητα και την αυθεντικοποίηση των δεδομένων.

Η αρχιτεκτονική του είναι της βασικής ροής λειτουργίας ενός REST API σε IoT περιβάλλον:

1. Η IoT συσκευή ή ο client στέλνει ένα HTTP request σε έναν server ή cloud endpoint για έναν συγκεκριμένο πόρο, π.χ., την τρέχουσα θερμοκρασία ενός αισθητήρα.

2. Ο server επεξεργάζεται το αίτημα και επιστρέφει ένα HTTP response με τα απαιτούμενα δεδομένα ή επιβεβαίωση της ενέργειας (π.χ., επιτυχής ενημέρωση).

3. Οι συσκευές μπορούν να επαναλαμβάνουν ή να αυτοματοποιούν αιτήματα, ενσωματώνοντας τις λειτουργίες τους σε μεγαλύτερα συστήματα ή εφαρμογές.

Χαρακτηριστικά	Περιγραφή
Ελαφρύ και γρήγορο	Εύκολη υλοποίηση και κατανόηση
Απλότητα	Λειτουργεί με οποιοδήποτε client/server που υποστηρίζει HTTP
Ανεξαρτησία πλατφόρμας	Εύκολη προσθήκη νέων πόρων και λειτουργιών
Επεκτασιμότητα	Συνδέει IoT συσκευές με cloud υπηρεσίες, dashboards και αναλυτικά εργαλεία
Διαλειτουργικότητα	Υποστήριξη HTTPS, OAuth2, JWT και άλλων μηχανισμών authentication
Ασφάλεια	Υποστήριξη JSON, XML, plain text
Ευέλικτη μορφή δεδομένων	Εύκολη υλοποίηση και κατανόηση

Εντοπίζεται στις εξής περιπτώσεις:

- Έξυπνα σπίτια: Διαχείριση φωτισμού, θερμοκρασίας, αισθητήρων κίνησης και συναγερμών.

- Βιομηχανικό IoT: Παρακολούθηση παραγωγικών γραμμών, συλλογή δεδομένων αισθητήρων και έλεγχος μηχανών.
- Υπηρεσίες cloud και dashboards: Αποστολή δεδομένων σε analytics platforms για real-time επεξεργασία.

3.4 Βιομηχανικά και Τομεακά Πρότυπα

Στον σύγχρονο τεχνολογικό κόσμο, η ανάπτυξη συστημάτων υψηλής αξιοπιστίας και ασφάλειας απαιτεί τη συμμόρφωση με βιομηχανικά και τομεακά πρότυπα. Τα πρότυπα αυτά καθορίζουν οδηγίες, διαδικασίες και απαιτήσεις για τον σχεδιασμό, την ανάπτυξη, τη λειτουργία και τη συντήρηση συστημάτων σε κρίσιμους τομείς όπως η αυτοκινητοβιομηχανία, η αεροναυπηγική, η υγεία, οι έξυπνες πόλεις και τα δίκτυα ενέργειας.

Η εφαρμογή τους προσφέρει πολλαπλά πλεονεκτήματα:

1. Ασφάλεια και αξιοπιστία: Τα πρότυπα εξασφαλίζουν ότι τα συστήματα λειτουργούν με ασφάλεια και μειώνουν τον κίνδυνο αποτυχίας, ιδιαίτερα σε κρίσιμες εφαρμογές.
2. Συμμόρφωση και νομοθετικό πλαίσιο: Σε πολλούς τομείς, η συμμόρφωση με διεθνή πρότυπα είναι νομική απαίτηση ή προϋπόθεση για πιστοποίηση.
3. Διαλειτουργικότητα: Οι καθιερωμένες προδιαγραφές επιτρέπουν σε συστήματα και συσκευές διαφορετικών κατασκευαστών να συνεργάζονται ομαλά.
4. Βελτιστοποίηση διαδικασιών ανάπτυξης: Η τήρηση προτύπων προσφέρει σαφείς κατευθύνσεις στον κύκλο ζωής ανάπτυξης, μειώνοντας την πιθανότητα σφαλμάτων και αυξάνοντας την αποτελεσματικότητα των ομάδων ανάπτυξης.

Τα πρότυπα αυτά είναι συχνά τομεακά εξειδικευμένα, δηλαδή επικεντρώνονται στις ανάγκες και τις προκλήσεις συγκεκριμένων βιομηχανιών, όπως:

- Αυτοκινητοβιομηχανία: Προτυποποίηση ηλεκτρονικών συστημάτων οχημάτων και διαδικασιών ασφάλειας οδήγησης (π.χ., AUTOSAR, ISO 26262).
- Αεροναυπηγική: Σχεδιασμός και πιστοποίηση λογισμικού και hardware αεροσκαφών και αεροδιαστημικών συστημάτων (π.χ., DO-178C, DO-254).
- Υγεία, Έξυπνες Πόλεις και Δίκτυα Ενέργειας: Διαχείριση κρίσιμων δεδομένων και υποδομών, εξασφάλιση ασφάλειας και αξιοπιστίας σε περιβάλλοντα με μεγάλο αριθμό συνδεδεμένων συσκευών και αισθητήρων.

Η υιοθέτηση αυτών των προτύπων είναι κρίσιμη όχι μόνο για τη συμμόρφωση με κανονιστικά πλαίσια, αλλά και για τη βελτίωση της ποιότητας, της ασφάλειας και της εμπιστοσύνης στα προϊόντα και τις υπηρεσίες που προσφέρονται από κάθε βιομηχανικό κλάδο. Επιπλέον, η πιστοποίηση κατά αυτά τα πρότυπα αποτελεί σημαντικό ανταγωνιστικό πλεονέκτημα, καθώς αποδεικνύει τη δέσμευση μιας εταιρείας σε υψηλά πρότυπα ποιότητας και ασφάλειας.

Στη συνέχεια, η ανάλυση θα επικεντρωθεί στα τομεακά πρότυπα της αυτοκινητοβιομηχανίας, τα οποία αποτελούν χαρακτηριστικό παράδειγμα εφαρμογής βιομηχανικών προτύπων σε σύνθετα και κρίσιμα συστήματα.

3.4.1 Αυτοκινητοβιομηχανία (AUTOSAR, ISO 26262)

Η αυτοκινητοβιομηχανία αποτελεί έναν από τους πιο απαιτητικούς τεχνολογικούς τομείς όσον αφορά την ασφάλεια, την αξιοπιστία και τη συμμόρφωση με διεθνή πρότυπα. Τα σύγχρονα οχήματα δεν είναι απλώς μηχανικά μέσα μεταφοράς, αλλά σύνθετα συστήματα ηλεκτρονικών και λογισμικού, όπου εκατοντάδες υποσυστήματα επικοινωνούν μεταξύ τους μέσω ενσωματωμένων δικτύων και πρωτοκόλλων. Σε αυτό το πλαίσιο, τα πρότυπα όπως το AUTOSAR και το ISO 26262 καθίστανται απαραίτητα για τη διασφάλιση της ασφάλειας και της λειτουργικότητας των οχημάτων.[28]

3.4.1.1 Automotive Open System Architecture (AUTOSAR)

Το AUTOSAR (Automotive Open System Architecture - Ανοικτή Αρχιτεκτονική Συστημάτων Αυτοκινήτου) αποτελεί μια διεθνή πρωτοβουλία και πρότυπο, το οποίο σχεδιάστηκε για να αντιμετωπίσει τις ολοένα αυξανόμενες απαιτήσεις σε λογισμικό και ηλεκτρονικά συστήματα στα σύγχρονα οχήματα. Η φιλοσοφία του βασίζεται στη δημιουργία μιας κοινής αρχιτεκτονικής λογισμικού, η οποία επιτρέπει την αποσύνδεση των εφαρμογών λογισμικού από το υλικό (hardware), προάγοντας τη διαλειτουργικότητα, την επαναχρησιμοποίηση κώδικα και την τυποποίηση σε ολόκληρο τον κλάδο της αυτοκινητοβιομηχανίας. Η σημασία του AUTOSAR προκύπτει από το γεγονός ότι τα σύγχρονα αυτοκίνητα ενσωματώνουν δεκάδες έως εκατοντάδες ECUs (Electronic Control Units – Ηλεκτρονικές Μονάδες Ελέγχου), τα οποία ελέγχουν κρίσιμες λειτουργίες όπως συστήματα πέδησης, κινητήρα, αερόσακους, καθώς και μη-κρίσιμα συστήματα όπως το infotainment. Χωρίς ένα κοινό πρότυπο, η ανάπτυξη και συντήρηση του λογισμικού γίνεται εξαιρετικά πολύπλοκη, με αυξημένο κόστος και κίνδυνο λαθών.

Τα βασικά χαρακτηριστικά του AUTOSAR είναι τα ακόλουθα:

1. Layered Architecture (Επίπεδη Αρχιτεκτονική):

   Το AUTOSAR οργανώνει το λογισμικό σε διαφορετικά επίπεδα:

   - Application Layer: Περιέχει τις εφαρμογές του οχήματος (π.χ. σύστημα ABS, cruise control).
   - Runtime Environment (RTE): Δρα ως “middleware” που επιτρέπει την επικοινωνία των εφαρμογών με τις βασικές υπηρεσίες, χωρίς οι εφαρμογές να εξαρτώνται από το υποκείμενο hardware.
   - Basic Software Layer: Περιλαμβάνει το λειτουργικό σύστημα (AUTOSAR OS), τους device drivers και το hardware abstraction layer, επιτρέποντας την εύκολη μεταφορά λογισμικού σε διαφορετικές πλατφόρμες.

   Με αυτό το μοντέλο ένας κατασκευαστής μπορεί να αναπτύξει μια εφαρμογή και να τη χρησιμοποιήσει σε διαφορετικά οχήματα, ανεξάρτητα από τον προμηθευτή του hardware.

2. Διαλειτουργικότητα (Interoperability):

   Το AUTOSAR έχει σχεδιαστεί ώστε να επιτρέπει την απρόσκοπτη συνεργασία πολλών προμηθευτών λογισμικού και hardware. Αυτό είναι ιδιαίτερα σημαντικό σε μια βιομηχανία όπου μεγάλοι κατασκευαστές (OEMs) συνεργάζονται με δεκάδες μικρότερους προμηθευτές για την ανάπτυξη εξειδικευμένων υποσυστημάτων.

3. Αναβάθμιση και Συντήρηση:

Η τυποποιημένη αρχιτεκτονική καθιστά δυνατή την εύκολη αναβάθμιση λογισμικού, χωρίς να απαιτείται επανασχεδιασμός ολόκληρου του συστήματος. Για παράδειγμα, μια νέα λειτουργία ADAS (Advanced Driver Assistance System) μπορεί να προστεθεί χωρίς να χρειαστεί να αλλάξει το σύστημα ελέγχου του κινητήρα. Αυτό μειώνει τον χρόνο ανάπτυξης, αλλά και το κόστος συντήρησης, ενώ αυξάνει τη διάρκεια ζωής των οχημάτων.

4. Ασφάλεια και Αξιοπιστία:

   Μέσω της σαφούς τυποποίησης και του διαχωρισμού των επιπέδων, το AUTOSAR συμβάλλει στη μείωση σφαλμάτων και στην ενίσχυση της λειτουργικής ασφάλειας (functional safety), κάτι που είναι κρίσιμο σε συστήματα που σχετίζονται με την ανθρώπινη ζωή (π.χ. πέδηση, αερόσακοι).

Η υιοθέτηση του AUTOSAR προσφέρει σημαντικά οφέλη και πλεονεκτήματα στην αυτοκινητοβιομηχανία, όπως:

- Μείωση κόστους ανάπτυξης μέσω επαναχρησιμοποίησης κώδικα.
- Ταχύτερη ανάπτυξη και λανσάρισμα νέων λειτουργιών στην αγορά.
- Ευκολία συνεργασίας μεταξύ διαφορετικών κατασκευαστών και προμηθευτών.
- Υψηλότερη ποιότητα και ασφάλεια λόγω τυποποίησης και modular σχεδιασμού.
- Υποστήριξη προηγμένων τεχνολογιών όπως αυτόνομη οδήγηση, IoT integration και V2X επικοινωνίες.

Ορισμένα παραδείγματα εφαρμογών AUTOSAR είναι τα ακόλουθα:

- Συστήματα Υποβοήθησης Οδήγησης (ADAS): Η modular αρχιτεκτονική επιτρέπει την ενσωμάτωση λογισμικού από διαφορετικούς προμηθευτές για λειτουργίες όπως adaptive cruise control, lane keeping assistance και αυτόματο φρενάρισμα.
- Infotainment: Συστήματα ψυχαγωγίας και πληροφόρησης μπορούν να συνδεθούν με mobile εφαρμογές και υπηρεσίες cloud, χωρίς αλλαγές στο υπόλοιπο ηλεκτρονικό σύστημα.
- Ηλεκτροκίνηση: Το AUTOSAR υποστηρίζει την ανάπτυξη λογισμικού για διαχείριση μπαταριών και συστήματα φόρτισης, επιτρέποντας καλύτερη ενσωμάτωση στις πλατφόρμες ηλεκτρικών οχημάτων.

3.4.1.2 Functional Safety for Road Vehicles - Λειτουργική Ασφάλεια για Οχήματα δρόμου (ISO 26262)

Το ISO 26262 είναι ένα διεθνές πρότυπο που καθορίζει απαιτήσεις και κατευθυντήριες γραμμές για τη διασφάλιση της λειτουργικής ασφάλειας (functional safety) στα ηλεκτρικά και ηλεκτρονικά συστήματα που χρησιμοποιούνται στα οχήματα. Πρόκειται για προσαρμογή του γενικότερου προτύπου IEC 61508 στον χώρο της αυτοκινητοβιομηχανίας, με στόχο την αντιμετώπιση των ιδιαίτερων προκλήσεων που προκύπτουν από την αυξημένη πολυπλοκότητα των οχημάτων και τη χρήση πολλαπλών ECUs (Electronic Control Units).

Η ανάγκη για το ISO 26262 προέκυψε από τη συνεχή αύξηση της εξάρτησης των οχημάτων από το λογισμικό και τα ηλεκτρονικά συστήματα, τα οποία αναλαμβάνουν κρίσιμες λειτουργίες, όπως τα συστήματα πέδησης, διεύθυνσης, κινητήρα, αλλά και τις νέες τεχνολογίες

αυτόνομης οδήγησης. Σε αυτά τα συστήματα, ακόμη και μία μικρή δυσλειτουργία μπορεί να οδηγήσει σε σοβαρά ατυχήματα, γι' αυτό και είναι απαραίτητο να υπάρχει ένα σαφές πλαίσιο που να διασφαλίζει την ανάπτυξή τους με βάση αρχές ασφάλειας.

Οι βασικές αρχές του ISO 26262 είναι οι εξής:

1. Διαχείριση Κινδύνων (Risk Assessment):
   Στον πυρήνα του προτύπου βρίσκεται η αξιολόγηση των κινδύνων που μπορεί να προκύψουν από πιθανές αποτυχίες συστημάτων. Η διαδικασία περιλαμβάνει την ανάλυση κινδύνων και επικινδυνότητας (hazard analysis and risk assessment), ώστε να εντοπίζονται οι πιθανές αιτίες ατυχημάτων και να αξιολογείται η σοβαρότητά τους.
2. ASIL Classification (Automotive Safety Integrity Level):
   Οι κίνδυνοι κατηγοριοποιούνται μέσω της μεθοδολογίας ASIL, σε επίπεδα από A έως D, όπου:
   - ASIL A αντιπροσωπεύει τον χαμηλότερο κίνδυνο.
   - ASIL D αντιπροσωπεύει τον υψηλότερο κίνδυνο και απαιτεί τις πιο αυστηρές διαδικασίες διασφάλισης.

   Η κατάταξη αυτή βασίζεται σε τρία κριτήρια:
   - Severity (Σοβαρότητα): Πόσο σοβαρές μπορεί να είναι οι συνέπειες ενός ατυχήματος.
   - Exposure (Έκθεση): Πόσο συχνά μπορεί να συμβεί η επικίνδυνη κατάσταση.
   - Controllability (Ελεγχόμενη κατάσταση): Κατά πόσο ο οδηγός μπορεί να αποφύγει το ατύχημα.
3. Functional Safety Management:
   Το ISO 26262 δεν αφορά μόνο τον τεχνικό σχεδιασμό, αλλά και την οργάνωση της διαδικασίας ανάπτυξης. Απαιτεί από τις εταιρείες να ακολουθούν συστηματικές πρακτικές σχεδιασμού, δοκιμών, επαλήθευσης και επικύρωσης, ώστε να διασφαλίζεται ότι κάθε βήμα του κύκλου ζωής του συστήματος λαμβάνει υπόψη την ασφάλεια. Αυτό περιλαμβάνει τα εξής:
   - Ορισμό υπευθύνων για την ασφάλεια.
   - Διαχείριση τεκμηρίωσης και ιχνηλασιμότητας.
   - Επαναλαμβανόμενες αξιολογήσεις (safety assessments).
4. Ολικός Κύκλος Ζωής (Lifecycle Approach):
   Το πρότυπο καλύπτει ολόκληρο τον κύκλο ζωής των ηλεκτρονικών συστημάτων οχημάτων:
   - Σχεδιασμό
   - Ανάπτυξη (software & hardware)
   - Δοκιμές και επαλήθευση
   - Ενσωμάτωση στο όχημα
   - Λειτουργία και συντήρηση
   - Απόσυρση συστημάτων

Με αυτόν τον τρόπο, το ISO 26262 εξασφαλίζει ότι η ασφάλεια δεν αποτελεί μεμονωμένο στάδιο, αλλά μια συνεχής διαδικασία που συνοδεύει το σύστημα σε όλη τη διάρκεια ζωής του.

Η εφαρμογή του ISO 26262 προσφέρει πολλαπλά οφέλη για την αυτοκινητοβιομηχανία:

- Μείωση ατυχημάτων: Ελαχιστοποιεί την πιθανότητα καταστροφικών αποτυχιών σε κρίσιμα συστήματα.
- Αύξηση εμπιστοσύνης: Παρέχει στους κατασκευαστές και στους πελάτες την πεποίθηση ότι τα οχήματα πληρούν αυστηρά πρότυπα ασφάλειας.
- Νομική συμμόρφωση: Αποτελεί προϋπόθεση σε πολλές αγορές και δικαιοδοσίες για την πιστοποίηση νέων οχημάτων.
- Διευκόλυνση καινοτομίας: Επιτρέπει την ασφαλή εισαγωγή νέων τεχνολογιών, όπως αυτόνομη οδήγηση και συστήματα υποστήριξης οδηγού (ADAS).

Και ορισμένα παραδείγματα εφαρμογής είναι:

- Συστήματα πέδησης (Brake-by-wire): Αξιολόγηση του κινδύνου απώλειας πέδησης και εφαρμογή μηχανισμών εφεδρείας.
- Ημιαυτόνομα και αυτόνομα συστήματα οδήγησης: Χρήση της μεθοδολογίας ASIL για τον καθορισμό του επιπέδου ασφαλείας που απαιτείται σε αλγόριθμους ανίχνευσης εμποδίων και λήψης αποφάσεων.
- Ηλεκτρικά οχήματα: Διαχείριση συστημάτων υψηλής τάσης ώστε να αποτρέπονται βραχυκυκλώματα ή επικίνδυνες καταστάσεις κατά τη φόρτιση.

3.4.2 Αεροναυπηγική (DO-178C, DO-254)

Ο τομέας της αεροναυπηγικής χαρακτηρίζεται από ιδιαίτερα αυστηρές απαιτήσεις σε θέματα ασφάλειας, αξιοπιστίας και πιστοποίησης, καθώς οποιαδήποτε αποτυχία σε συστήματα πτήσης μπορεί να έχει καταστροφικές συνέπειες. Η αυξανόμενη χρήση ψηφιακών συστημάτων ελέγχου πτήσης, ηλεκτρονικών υπολογιστών αεροσκαφών (avionics) και ενσωματωμένων λογισμικών καθιστά απαραίτητη την υιοθέτηση εξειδικευμένων προτύπων που να διασφαλίζουν την ορθή ανάπτυξη, επαλήθευση και λειτουργία τους.

Σε αυτό το πλαίσιο, δύο από τα πλέον καθιερωμένα πρότυπα είναι το DO-178C και το DO-254:

- Το DO-178C αποτελεί το βασικό πρότυπο για την ανάπτυξη και πιστοποίηση λογισμικού αεροναυπηγικών συστημάτων, καθορίζοντας τις διαδικασίες και τις μεθοδολογίες που πρέπει να ακολουθούνται καθ’ όλη τη διάρκεια ζωής ενός λογισμικού.
- Το DO-254, από την άλλη, αφορά τον τομέα του υλικού (hardware) και χρησιμοποιείται για την ανάπτυξη και πιστοποίηση ηλεκτρονικών εξαρτημάτων και συστημάτων που ενσωματώνονται σε αεροσκάφη.

Και τα δύο πρότυπα έχουν υιοθετηθεί από διεθνείς ρυθμιστικούς οργανισμούς, όπως η FAA (Federal Aviation Administration - Ομοσπονδιακή Υπηρεσία Αεροπορίας των ΗΠΑ) και η EASA (European Union Aviation Safety Agency - Οργανισμός Ασφαλείας Αεροπορίας της Ευρωπαϊκής Ένωσης) και αποτελούν θεμέλιο για την πιστοποίηση νέων τεχνολογιών στην αεροναυπηγική.

Η σημασία τους είναι κρίσιμη, καθώς η εφαρμογή τους όχι μόνο συμβάλλει στην πρόληψη ατυχημάτων, αλλά και ενισχύει την εμπιστοσύνη των αεροπορικών εταιρειών, των κατασκευαστών και των επιβατών στη λειτουργία των αεροσκαφών. Παράλληλα, αποτελούν τη βάση πάνω στην οποία αναπτύσσονται νέες τεχνολογίες, όπως τα ημιαυτόνομα και αυτόνομα αεροπορικά συστήματα, καθώς

και τα UAVs (Unmanned Aerial Vehicles). Παρακάτω θα εξεταστούν αναλυτικά τα πρότυπα DO-178C και DO-254, οι βασικές τους αρχές, τα επίπεδα πιστοποίησης, καθώς και οι πρακτικές εφαρμογές τους στον τομέα της αεροναυπηγικής.

3.4.2.1 Software Considerations in Airborne Systems and Equipment Certification - Ζητήματα Λογισμικού για Πιστοποίηση Αεροπορικών Συστημάτων και Εξοπλισμού (DO-178C)

Το πρότυπο DO-178C, που εκδόθηκε από τη RTCA (Radio Technical Commission for Aeronautics) το 2011, αποτελεί το καθιερωμένο πλαίσιο αναφοράς για την ανάπτυξη και πιστοποίηση λογισμικού σε συστήματα αεροναυπηγικής. Η σημασία του είναι καθοριστική, καθώς το λογισμικό βρίσκεται πλέον στον πυρήνα της λειτουργίας των αεροσκαφών, ελέγχοντας κρίσιμα συστήματα όπως ο αυτόματος πιλότος, οι μηχανισμοί πλοήγησης, οι αισθητήρες και τα συστήματα επικοινωνίας (Knight, 2012).

Ο κύριος στόχος του DO-178C είναι να διασφαλίσει ότι το λογισμικό αεροπορικών συστημάτων αναπτύσσεται και λειτουργεί με τέτοιο τρόπο ώστε να πληροί τις απαιτήσεις λειτουργικής ασφάλειας (functional safety). Αυτό επιτυγχάνεται μέσω ενός αυστηρά καθορισμένου κύκλου ζωής ανάπτυξης, που περιλαμβάνει:

- Καθορισμό απαιτήσεων: Οι απαιτήσεις λογισμικού πρέπει να είναι ακριβείς, κατανοητές, ιχνηλάσιμες και χωρίς αμφισημίες.
- Σχεδιασμό και υλοποίηση: Το λογισμικό σχεδιάζεται με βάση ιεραρχική δομή και σαφή διαχωρισμό λειτουργιών, ώστε να μειώνεται η πολυπλοκότητα.
- Επαλήθευση και επικύρωση (Verification & Validation): Κάθε στάδιο ανάπτυξης συνοδεύεται από διαδικασίες ελέγχου και δοκιμών, ώστε να διασφαλίζεται ότι το τελικό προϊόν ανταποκρίνεται πλήρως στις προδιαγραφές.
- Διαχείριση διαμόρφωσης (Configuration Management): Εξασφαλίζεται η αυστηρή ιχνηλασιμότητα και ο έλεγχος εκδόσεων λογισμικού, ώστε να αποφεύγονται σφάλματα κατά την εξέλιξη του έργου.
- Ανεξαρτησία ελέγχων (Independence of Verification): Οι δοκιμές και οι έλεγχοι πρέπει να πραγματοποιούνται από ανεξάρτητες ομάδες, ώστε να αποφεύγονται συγκρούσεις συμφερόντων και να ενισχύεται η αντικειμενικότητα.

Το DO-178C κατηγοριοποιεί το λογισμικό σε πέντε επίπεδα κρισιμότητας (DAL A – E), ανάλογα με τον αντίκτυπο που μπορεί να έχει μια πιθανή αποτυχία στη λειτουργία του αεροσκάφους:

- Level A: Αποτυχία που μπορεί να οδηγήσει σε καταστροφή αεροσκάφους και απώλεια ανθρώπινων ζωών.
- Level B: Αποτυχία που μπορεί να προκαλέσει σοβαρό τραυματισμό ή μείζον κίνδυνο για τους επιβάτες.
- Level C: Αποτυχία που μπορεί να προκαλέσει σημαντική αύξηση του φόρτου εργασίας του πληρώματος ή να επηρεάσει την ασφάλεια πτήσης.
- Level D: Αποτυχία που έχει περιορισμένο αντίκτυπο στη λειτουργία του αεροσκάφους.
- Level E: Αποτυχία που δεν επηρεάζει την ασφάλεια πτήσης.

Αντίστοιχα, όσο υψηλότερο είναι το επίπεδο DAL, τόσο αυστηρότερες είναι οι απαιτήσεις σε τεκμηρίωση, δοκιμές και ανεξάρτητη αξιολόγηση (RTCA, 2011).

Το DO-178C έχει υιοθετηθεί από διεθνείς ρυθμιστικές αρχές όπως η FAA στις Ηνωμένες Πολιτείες και η EASA στην Ευρώπη, αποτελώντας υποχρεωτικό σημείο αναφοράς για την πιστοποίηση αεροπορικού λογισμικού. Η συμμόρφωση με το πρότυπο αποτελεί προϋπόθεση για την έγκριση και την εμπορική εκμετάλλευση ενός νέου αεροσκάφους ή συστήματος (FAA, 2014). Ένα χαρακτηριστικό παράδειγμα εφαρμογής του DO-178C είναι η ανάπτυξη του λογισμικού για τα Fly-by-Wire συστήματα, τα οποία αντικαθιστούν τις παραδοσιακές μηχανικές συνδέσεις με ηλεκτρονικά σήματα. Σε τέτοια συστήματα, μια αποτυχία λογισμικού θα μπορούσε να έχει καταστροφικές συνέπειες (επίπεδο DAL A). Για τον λόγο αυτό, εφαρμόζονται εκτενείς δοκιμές προσομοίωσης, επαναλαμβανόμενοι έλεγχοι σε συνθήκες πτήσης και αυστηρή τεκμηρίωση, ώστε να διασφαλιστεί ότι το σύστημα πληροί τα πρότυπα ασφαλείας (Leanna, 2015).

Το DO-178C δεν αποτελεί απλώς μια τεχνική κατευθυντήρια οδηγία αλλά έναν θεσμικό πυλώνα της αεροναυπηγικής βιομηχανίας, καθώς προσφέρει το απαραίτητο πλαίσιο για την ανάπτυξη λογισμικού υψηλής ασφάλειας και αξιοπιστίας. Η εφαρμογή του ενισχύει τη διαλειτουργικότητα μεταξύ προμηθευτών, μειώνει τον κίνδυνο ανθρώπινων λαθών και συμβάλλει στη διατήρηση των υψηλότερων επιπέδων ασφάλειας που απαιτούνται σε ένα τόσο ευαίσθητο περιβάλλον όπως η αεροπλοΐα.

3.4.2.2 Design Assurance Guidance for Airborne Electronic Hardware - Κατευθυντήριες Οδηγίες Σχεδίασης για Αεροπορικό Ηλεκτρονικό Υλικό (DO-254)

Το DO-254, που εκδόθηκε από τη RTCA το 2000, αποτελεί το θεμελιώδες πρότυπο για την ανάπτυξη και την πιστοποίηση ηλεκτρονικού υλικού (hardware) σε αεροπορικά συστήματα. Εάν το DO-178C ρυθμίζει τη διαδικασία για το λογισμικό, το DO-254 καλύπτει αντίστοιχα το hardware, δηλαδή εξαρτήματα όπως μικροεπεξεργαστές, ASICs (Application-Specific Integrated Circuits), FPGAs (Field Programmable Gate Arrays), καθώς και σύνθετες ηλεκτρονικές πλακέτες (Printed Circuit Boards – PCBs). Η ανάγκη για το DO-254 προέκυψε από τη ραγδαία αύξηση της πολυπλοκότητας των ηλεκτρονικών συστημάτων στα αεροσκάφη. Τα σύγχρονα αεροπλάνα δεν βασίζονται πλέον αποκλειστικά σε μηχανικά ή απλά ηλεκτρικά συστήματα· αντιθέτως, περιλαμβάνουν ολοένα και περισσότερα ψηφιακά κυκλώματα υψηλής πολυπλοκότητας, τα οποία είναι κρίσιμα για την ασφάλεια πτήσης. Έτσι, η τυποποίηση της ανάπτυξης και του ελέγχου αυτών των συστημάτων έγινε αναπόφευκτη (RTCA, 2000).

Το DO-254 καθορίζει ένα πλήρες πλαίσιο ανάπτυξης και διαχείρισης, με στόχο τη λειτουργική ασφάλεια και την αξιοπιστία του hardware. Οι κύριες αρχές του περιλαμβάνουν:

1. Καθορισμός απαιτήσεων (Requirements Capture):
   Όλες οι λειτουργικές και μη λειτουργικές απαιτήσεις του hardware πρέπει να τεκμηριώνονται με σαφήνεια, ώστε να εξασφαλίζεται ιχνηλασιμότητα σε όλη τη διάρκεια του κύκλου ζωής.
2. Σχεδίαση και υλοποίηση (Design & Implementation):
   Το υλικό σχεδιάζεται βάσει ιεραρχικής μεθοδολογίας, από την αρχιτεκτονική περιγραφή έως την φυσική σχεδίαση. Σε αυτή τη φάση περιλαμβάνονται λεπτομέρειες για κυκλώματα, ολοκληρωμένα συστήματα και σχέδια πλακετών.
3. Επαλήθευση (Verification):
   Το DO-254 δίνει ιδιαίτερη έμφαση στην επαλήθευση, η οποία πρέπει να καλύπτει λειτουργικό

έλεγχο, προσομοιώσεις, δοκιμές υλικού και ανασκόπηση σχεδίασης. Ο στόχος είναι να διασφαλιστεί ότι το hardware πληροί πλήρως τις απαιτήσεις που έχουν τεθεί.

4. Διαχείριση διαμόρφωσης (Configuration Management):
   Κάθε αλλαγή στο hardware πρέπει να καταγράφεται και να τεκμηριώνεται με απόλυτη ακρίβεια, ώστε να αποφεύγονται σφάλματα κατά τις επαναλήψεις ανάπτυξης.
5. Διαχείριση ποιότητας και ασφάλειας (Process Assurance):
   Ειδικές διαδικασίες παρακολούθησης διασφαλίζουν ότι όλα τα βήματα ανάπτυξης εκτελούνται σύμφωνα με το πρότυπο και ότι τηρούνται οι υψηλές απαιτήσεις ασφάλειας.

Όπως και το DO-178C, το DO-254 εισάγει κατηγορίες επιπέδων κρισιμότητας (DAL A – E) για το hardware, ανάλογα με τις συνέπειες μιας πιθανής αποτυχίας:

- DAL A: Αποτυχία που μπορεί να οδηγήσει σε καταστροφικό ατύχημα.
- DAL B: Αποτυχία που μπορεί να προκαλέσει σοβαρό τραυματισμό ή σημαντικό κίνδυνο.
- DAL C: Αποτυχία που μπορεί να επιφέρει αυξημένο φόρτο στο πλήρωμα ή λειτουργικούς περιορισμούς.
- DAL D: Αποτυχία με περιορισμένο αντίκτυπο.
- DAL E: Αποτυχία που δεν επηρεάζει την ασφάλεια πτήσης.

  Όσο υψηλότερο είναι το επίπεδο DAL, τόσο πιο αυστηρές είναι οι απαιτήσεις επαλήθευσης και τεκμηρίωσης (EASA, 2015).

Τα δύο πρότυπα συχνά εφαρμόζονται παράλληλα, καθώς πολλά αεροναυπηγικά συστήματα συνδυάζουν λογισμικό και hardware. Για παράδειγμα, ένας μικροελεγκτής (hardware) που τρέχει έναν αλγόριθμο ελέγχου πτήσης (software) πρέπει να πιστοποιηθεί με βάση και τα δύο πρότυπα. Ο συνδυασμός DO-178C και DO-254 εξασφαλίζει ότι τόσο το λογισμικό όσο και το υλικό πληρούν τις ίδιες αυστηρές απαιτήσεις ασφάλειας. Ένα χαρακτηριστικό παράδειγμα εφαρμογής του DO-254 είναι η ανάπτυξη συστημάτων ελέγχου κινητήρων (Engine Control Units – ECUs). Σε τέτοια συστήματα, ακόμη και ένα μικρό σφάλμα στο hardware (π.χ. ένας εσφαλμένος χρονισμός σε FPGA) θα μπορούσε να προκαλέσει δυσλειτουργία στον κινητήρα, με σοβαρές συνέπειες για την πτήση. Για αυτό, τα συστήματα αυτά σχεδιάζονται, δοκιμάζονται και τεκμηριώνονται με βάση τις διαδικασίες του DO-254 (Moir & Seabridge, 2012).

Το DO-254 αποτελεί θεμέλιο λίθο για την πιστοποίηση ηλεκτρονικού υλικού σε συστήματα αεροναυπηγικής. Με την αυξανόμενη εξάρτηση των αεροσκαφών από ψηφιακά και προγραμματιζόμενα κυκλώματα, το πρότυπο αυτό διασφαλίζει ότι τα κρίσιμα ηλεκτρονικά εξαρτήματα αναπτύσσονται με τον ίδιο βαθμό αυστηρότητας και αξιοπιστίας όπως και το λογισμικό. Η παράλληλη εφαρμογή του με το DO-178C δημιουργεί ένα ολιστικό πλαίσιο ασφάλειας, καλύπτοντας όλες τις πτυχές ανάπτυξης, από τον κώδικα μέχρι το φυσικό κύκλωμα.

3.4.3 Υγεία, Έξυπνες Πόλεις και Δίκτυα Ενέργειας

Η εξέλιξη του IoT έχει δημιουργήσει σημαντικές προοπτικές σε τομείς που σχετίζονται άμεσα με την καθημερινότητα του ανθρώπου και τη λειτουργία της κοινωνίας. Μεταξύ αυτών ξεχωρίζουν οι τομείς της Υγείας (e-Health, m-Health, IoMT), οι Έξυπνες Πόλεις (Smart Cities) και τα Έξυπνα Δίκτυα Ενέργειας (Smart Grids). Και στις τρεις περιπτώσεις, η χρήση προτύπων και βέλτιστων πρακτικών είναι

κρίσιμη, ώστε να διασφαλιστούν η ασφάλεια, η αξιοπιστία, η διαλειτουργικότητα και η προστασία των δεδομένων.[10], [11].

Στον τομέα της υγείας, το IoT μετουσιώνεται σε Internet of Medical Things (IoMT), όπου ιατρικές συσκευές, αισθητήρες, φορετά συστήματα (wearables) και εφαρμογές συνδέονται σε δίκτυα με στόχο την παρακολούθηση και τη βελτίωση της υγείας των ασθενών. Παραδείγματα αποτελούν οι συσκευές παρακολούθησης καρδιακού ρυθμού, τα έξυπνα εμφυτεύματα και οι τηλεϊατρικές πλατφόρμες.

Η χρήση τέτοιων τεχνολογιών ενισχύει την ποιότητα περίθαλψης, μειώνει τα κόστη και επιτρέπει την έγκαιρη διάγνωση μέσω ανάλυσης δεδομένων σε πραγματικό χρόνο. Ωστόσο, εγείρονται σοβαρά ζητήματα ασφάλειας και προστασίας προσωπικών δεδομένων. Για τον λόγο αυτό, έχουν υιοθετηθεί πρότυπα όπως:

- HL7 (Health Level Seven): πρότυπο για τη διαλειτουργικότητα ιατρικών δεδομένων.
- ISO/IEEE 11073: για επικοινωνία φορητών και ιατρικών συσκευών.
- GDPR (General Data Protection Regulation): στην Ευρωπαϊκή Ένωση, που διασφαλίζει την ιδιωτικότητα των προσωπικών δεδομένων υγείας.

Οι Έξυπνες Πόλεις αποτελούν μια από τις πιο χαρακτηριστικές εφαρμογές του IoT, όπου συστήματα διαχείρισης ενέργειας, μεταφορών, υδάτων, απορριμμάτων και ασφάλειας συνδέονται σε ένα ενιαίο οικοσύστημα. Η υιοθέτηση προτύπων και τεχνολογικών πλαισίων είναι απαραίτητη για τη διαλειτουργικότητα μεταξύ διαφορετικών συστημάτων και προμηθευτών.

Ορισμένα σημαντικά πρότυπα και πρωτοβουλίες περιλαμβάνουν:

- ISO 37120 (Indicators for Smart Cities): καθορίζει δείκτες για τη μέτρηση της απόδοσης μιας πόλης.
- ETSI CIM (Context Information Management): πλαίσιο για την ανταλλαγή δεδομένων σε smart city εφαρμογές.
- FIWARE: ανοικτή πλατφόρμα για ανάπτυξη εφαρμογών έξυπνων πόλεων.

Παραδείγματα εφαρμογής περιλαμβάνουν: έξυπνη διαχείριση κυκλοφορίας με χρήση αισθητήρων και big data, έξυπνος φωτισμός που προσαρμόζεται σε πραγματικό χρόνο, καθώς και συστήματα έξυπνης διαχείρισης απορριμμάτων που μειώνουν κόστη και περιβαλλοντικό αποτύπωμα.

Τα Έξυπνα Δίκτυα Ενέργειας (Smart Grids) συνδυάζουν τεχνολογίες IoT, συστήματα επικοινωνίας και αυτοματισμούς για τη βελτιστοποίηση της παραγωγής, διανομής και κατανάλωσης ηλεκτρικής ενέργειας. Σε αντίθεση με τα παραδοσιακά δίκτυα, τα Smart Grids επιτρέπουν διπλή κατεύθυνση ροής πληροφορίας και ενέργειας, βελτιώνοντας την αποδοτικότητα, μειώνοντας τις απώλειες και υποστηρίζοντας τις ανανεώσιμες πηγές ενέργειας.

Στα Smart Grids εφαρμόζονται διεθνή πρότυπα, όπως:

- IEC 61850: για επικοινωνία σε υποσταθμούς ηλεκτρικής ενέργειας.
- IEEE 2030: για διαλειτουργικότητα συστημάτων ενέργειας με IoT και ICT.
- NIST Framework: για ασφάλεια και προστασία κρίσιμων υποδομών.

Ένα παράδειγμα εφαρμογής αποτελεί η χρήση έξυπνων μετρητών (smart meters), οι οποίοι επιτρέπουν την ακριβή μέτρηση και διαχείριση κατανάλωσης σε πραγματικό χρόνο, δίνοντας τη δυνατότητα σε καταναλωτές και παρόχους να βελτιώσουν την αποδοτικότητα και να μειώσουν κόστη.

Οι τομείς της Υγείας, των Έξυπνων Πόλεων και των Δικτύων Ενέργειας αντιπροσωπεύουν βασικούς άξονες εφαρμογής του IoT με άμεσο κοινωνικό αντίκτυπο. Η υιοθέτηση και εφαρμογή βιομηχανικών και τομεακών προτύπων διασφαλίζει όχι μόνο την τεχνική αρτιότητα και διαλειτουργικότητα των συστημάτων, αλλά και την προστασία των πολιτών και των υποδομών. Καθώς οι τεχνολογίες εξελίσσονται, οι τομείς αυτοί θα συνεχίσουν να αποτελούν πυρήνες καινοτομίας με άμεση σχέση με την ποιότητα ζωής, την ασφάλεια και τη βιωσιμότητα.

3.5 Μελλοντικές Κατευθύνσεις

Η ταχεία εξέλιξη των δικτύων επικοινωνίας, των προτύπων διαλειτουργικότητας και των τεχνολογιών IoT δημιουργεί νέες προοπτικές, αλλά και προκλήσεις, για το μέλλον. Η ενσωμάτωση όλο και πιο σύνθετων συστημάτων, η διαχείριση μεγάλου όγκου δεδομένων και οι αυξανόμενες απαιτήσεις για ασφάλεια, αποδοτικότητα και βιωσιμότητα καθιστούν αναγκαία την υιοθέτηση καινοτόμων προσεγγίσεων.

Δύο από τις σημαντικότερες κατευθύνσεις που αναδεικνύονται είναι:

- Η αξιοποίηση της Τεχνητής Νοημοσύνης (AI) και της Μηχανικής Μάθησης (ML) για την ανάπτυξη αυτοΐατων συστημάτων (self-healing systems) και την ενίσχυση της διαλειτουργικότητας, και
- Η ενοποίηση προτύπων σε συνδυασμό με την ανάγκη για βιώσιμη ανάπτυξη (sustainability), ώστε να διασφαλιστεί η αποδοτική και υπεύθυνη χρήση πόρων.

Η συζήτηση γύρω από τις μελλοντικές κατευθύνσεις δεν περιορίζεται μόνο στις τεχνικές βελτιώσεις, αλλά αφορά και ζητήματα κανονιστικού πλαισίου, ηθικής χρήσης των δεδομένων και κοινωνικού αντίκτυπου. Καθώς οι τεχνολογίες αυτές εισχωρούν σε κρίσιμους τομείς, όπως η υγεία, οι μεταφορές και η ενέργεια, είναι απαραίτητο να εξεταστεί πώς θα διαμορφωθεί ένα οικοσύστημα καινοτομίας που να συνδυάζει ασφάλεια, αξιοπιστία και βιωσιμότητα.

3.5.1 AI/ML για αυτοΐαση και διαλειτουργικότητα

Η αξιοποίηση της Τεχνητής Νοημοσύνης (Artificial Intelligence – AI) και της Μηχανικής Μάθησης (Machine Learning – ML) στον τομέα της κυβερνοασφάλειας και της διαχείρισης συστημάτων δικτύων αποτελεί μία από τις πλέον υποσχόμενες κατευθύνσεις για το μέλλον. Η συνεχώς αυξανόμενη πολυπλοκότητα των δικτυακών υποδομών και η ανάγκη για αυτοματοποιημένη ανίχνευση, διάγνωση και αποκατάσταση σφαλμάτων καθιστούν τα εργαλεία αυτά θεμελιώδη για την ανάπτυξη αυτοΐατων συστημάτων (self-healing systems).

Η έννοια της αυτοΐασης βασίζεται στην ικανότητα ενός συστήματος να εντοπίζει αυτόματα δυσλειτουργίες ή επιθέσεις, να εκτιμά το επίπεδο κινδύνου και να αναλαμβάνει διορθωτικές ενέργειες χωρίς την ανάγκη άμεσης ανθρώπινης παρέμβασης. Τα μοντέλα ML μπορούν να αξιοποιούν ιστορικά δεδομένα, μοτίβα κανονικής λειτουργίας και συμπεριφορές ανωμαλιών, ώστε να εντοπίζουν αποκλίσεις σε πραγματικό χρόνο. Για παράδειγμα, η χρήση τεχνικών anomaly detection με βάση αλγορίθμους clustering ή deep learning επιτρέπει την ανίχνευση ασυνήθιστης δραστηριότητας δικτύου που ενδέχεται να υποδηλώνει κυβερνοεπίθεση. Παράλληλα, τα συστήματα AI/ML συμβάλλουν στη διαλειτουργικότητα μεταξύ ετερογενών προτύπων και πρωτοκόλλων. Στον χώρο του IoT, όπου

συνυπάρχουν ποικίλες πλατφόρμες και διαφορετικές γλώσσες επικοινωνίας (π.χ. MQTT, CoAP, REST APIs), τα μοντέλα μάθησης μπορούν να λειτουργούν ως «γέφυρες», επιτρέποντας την αυτόματη αντιστοίχιση και προσαρμογή δεδομένων. Η εφαρμογή τεχνικών semantic interoperability και ontology-based learning καθιστά εφικτή την ενιαία διαχείριση πληροφορίας, ακόμη και όταν αυτή προέρχεται από συσκευές διαφορετικών κατασκευαστών.

Η συμβολή της AI/ML δεν περιορίζεται μόνο στην ανίχνευση και απόκριση, αλλά επεκτείνεται και στην πρόβλεψη (predictive maintenance). Μέσω της ανάλυσης δεδομένων αισθητήρων, μπορούν να προβλεφθούν πιθανές αστοχίες υλικού ή λογισμικού και να ληφθούν προληπτικά μέτρα, μειώνοντας σημαντικά το downtime και το κόστος υποστήριξης. Στον τομέα της ασφάλειας, οι αλγόριθμοι reinforcement learning δίνουν τη δυνατότητα στα συστήματα να «μαθαίνουν» βέλτιστες στρατηγικές αντίδρασης σε επιθέσεις, βελτιώνοντας την αποτελεσματικότητα άμυνας σε δυναμικά και αβέβαια περιβάλλοντα. Ωστόσο, η εφαρμογή της AI/ML σε κρίσιμα περιβάλλοντα δεν είναι χωρίς προκλήσεις. Ζητήματα όπως η ερμηνευσιμότητα των μοντέλων (explainability), η αξιοπιστία σε πραγματικό χρόνο και οι κίνδυνοι από επιθέσεις adversarial ML αποτελούν σημαντικούς παράγοντες που πρέπει να αντιμετωπιστούν. Επιπλέον, η ενοποίηση με υφιστάμενα πρότυπα, όπως το ISO/IEC 27001 και το NIST Cybersecurity Framework, παραμένει κρίσιμη, ώστε να διασφαλιστεί η συμμόρφωση με διεθνείς κανόνες και βέλτιστες πρακτικές.

Συνοψίζοντας, η χρήση της AI/ML για αυτοΐαση και διαλειτουργικότητα αποτελεί μια κατεύθυνση που μπορεί να μετασχηματίσει ριζικά τον τρόπο με τον οποίο σχεδιάζονται και λειτουργούν τα σύγχρονα συστήματα. Η προοπτική δημιουργίας συστημάτων που μαθαίνουν, προσαρμόζονται και αυτοδιορθώνονται ανοίγει τον δρόμο για ένα νέο μοντέλο ανθεκτικής και ευφυούς κυβερνοασφάλειας, εναρμονισμένο με τις απαιτήσεις της τέταρτης βιομηχανικής επανάστασης.

Παραδείγματα Εφαρμογής AI/ML για Αυτοΐαση και Διαλειτουργικότητα

1. Έξυπνα Δίκτυα Ενέργειας (Smart Grids):
   Σε ένα έξυπνο δίκτυο ηλεκτρικής ενέργειας, η συνεχής παρακολούθηση των αισθητήρων μπορεί να επιτρέψει την πρόβλεψη βλαβών σε μετασχηματιστές. Ένα μοντέλο ML, εκπαιδευμένο με ιστορικά δεδομένα θερμοκρασίας, φορτίου και κατανάλωσης, μπορεί να εντοπίζει μοτίβα που προηγούνται μίας βλάβης. Όταν ανιχνευτεί πιθανή δυσλειτουργία, το σύστημα ενεργοποιεί προληπτική ανακατεύθυνση φορτίου σε άλλες γραμμές, μειώνοντας τον κίνδυνο διακοπής ρεύματος.

2. Διαλειτουργικότητα σε Έξυπνες Πόλεις:
   Σε μια «έξυπνη πόλη», διαφορετικοί προμηθευτές μπορεί να χρησιμοποιούν διαφορετικά πρωτόκολλα (π.χ. ένας αισθητήρας στάθμευσης να επικοινωνεί με CoAP και ένας με MQTT). Ένα AI middleware μπορεί να μάθει να αναγνωρίζει τα σχήματα δεδομένων (data schemas) και να τα ενοποιεί αυτόματα. Έτσι, οι εφαρμογές της πόλης (π.χ. ένα ενιαίο dashboard για στάθμευση, κυκλοφορία και φωτισμό) μπορούν να διαχειρίζονται όλα τα δεδομένα σε κοινή γλώσσα χωρίς να χρειάζεται χειροκίνητη προσαρμογή.

3. Αυτοΐαση σε Βιομηχανικά IoT Συστήματα (IIoT):
   Σε ένα εργοστάσιο, τα μηχανήματα είναι συνδεδεμένα μέσω IoT. Εάν παρουσιαστεί ασυνήθιστη δόνηση σε μια μηχανή, ένα ML μοντέλο anomaly detection μπορεί να το εντοπίσει σε πραγματικό χρόνο. Το σύστημα, χωρίς ανθρώπινη παρέμβαση, μειώνει προσωρινά την ταχύτητα λειτουργίας της μηχανής, ειδοποιεί το κέντρο ελέγχου και προγραμματίζει αυτόματα συντήρηση. Με αυτόν τον τρόπο αποφεύγεται μια πιθανή καταστροφική βλάβη.

4. Κυβερνοασφάλεια Δικτύων:
   Ένα AI σύστημα που χρησιμοποιεί deep reinforcement learning μπορεί να μαθαίνει από προηγούμενες επιθέσεις (π.χ. DDoS, phishing) και να αναπτύσσει στρατηγικές άμυνας. Σε περίπτωση που εντοπιστεί ύποπτη δραστηριότητα, το δίκτυο μπορεί να αναδρομολογεί αυτόματα την κίνηση ή να απομονώνει τις ύποπτες συσκευές, διατηρώντας παράλληλα την κανονική λειτουργία για τους υπόλοιπους χρήστες.

Παρακάτω αναφέρονται ορισμένα παραδείγματα εφαρμογών με στατιστικά στοιχεία για να γίνει αντιληπτή καλύτερα, με μετρήσιμα δεδομένα, η συμβολή του AI /ML στο IoTQ

1. Έξυπνες Πόλεις (Smart Cities)

- Το 2023, το 80% των έξυπνων πόλεων χρησιμοποίησαν λύσεις AI-driven IoT, και προβλέπεται ότι το ποσοστό αυτό θα αυξηθεί στο 83% μέσα σε τρία χρόνια.
- Η χρήση του AI σε IoT για έξυπνο φωτισμό μείωσε την κατανάλωση ενέργειας κατά 30% το 2023.
- Επιπλέον, η χρήση AI σε συστήματα διαχείρισης απορριμμάτων μείωσε το κόστος λειτουργίας κατά 18%.

Για παράδειγμα, ένα σύστημα φωτισμού δρόμων με αισθητήρες IoT και AI ρυθμίζει αυτόματα το φωτισμό ανάλογα με την κίνηση και συνθήκες. Όταν μειωθεί η κυκλοφορία, μειώνεται και η ένταση, εξοικονομώντας ενέργεια. Αυτό δείχνει την αυτοΐαση σε δράση.

2. Υγεία (IoMT)

- Μέχρι το 2023, το 65% των υγειονομικών υποδομών χρησιμοποιούσαν IoT συσκευές με AI υποστήριξη και πέτυχαν μείωση στις νοσηλείες κατά 20%.
- Επηρεάστηκε επίσης θετικά η ακρίβεια διάγνωσης, η οποία βελτιώθηκε κατά 25% με τη βοήθεια AI-powered IoT ιατρικών συσκευών.

Για παράδειγμα, μια φορητή συσκευή συνεχούς παρακολούθησης καρδιακής λειτουργίας στέλνει δεδομένα σε cloud όπου ML μοντέλο ανιχνεύει ανώμαλους καρδιακούς ρυθμούς. Το σύστημα ειδοποιεί αυτόματα ιατρικό προσωπικό πριν προκύψει σοβαρό συμβάν – μια μορφή αυτοΐασης.

3. Δίκτυα Ενέργειας (Smart Grids)

- Το 2025, η χρήση AI για προληπτική συντήρηση σε ενεργειακά δίκτυα έχει ήδη μειώσει τις διακοπές ρεύματος σημαντικά, καθώς utilities όπως Duke Energy αναπτύσσουν ML μοντέλα για ανίχνευση προβλημάτων σε μετασχηματιστές.
- Η ενσωμάτωση AI επιτρέπει στην ενεργειακή υποδομή να προσαρμόζεται σε πραγματικό χρόνο, διατηρώντας σταθερότητα μέσα στην κρίση της αυξημένης ζήτησης.

Για παράδειγμα, ένα σύστημα AI με αισθητήρες παρακολουθεί τους μετασχηματιστές ενός δικτύου. Αν οι μετρήσεις δείξουν υπερθερμία ή τάση βλάβης, ενεργοποιείται αυτόματα εφεδρικός μετασχηματιστής και ειδοποιείται το τεχνικό προσωπικό για επιθεώρηση — προληπτική αποκατάσταση σε πραγματικό χρόνο.

3.5.2 Ενοποίηση προτύπων και sustainability

Η ενοποίηση προτύπων αποτελεί βασικό πυλώνα για την επίτευξη βιώσιμης ανάπτυξης, καθώς διαμορφώνει ένα κοινό πλαίσιο αναφοράς που επιτρέπει στις επιχειρήσεις, στους οργανισμούς και στα

κράτη να ευθυγραμμίζουν τις πρακτικές τους με τους Στόχους Βιώσιμης Ανάπτυξης (SDGs) των Ηνωμένων Εθνών, προωθώντας τη διαφάνεια, τη διαλειτουργικότητα και την υπευθυνότητα (ISO, 2020). Διεθνή πρότυπα όπως το ISO 14001 για τα συστήματα περιβαλλοντικής διαχείρισης και το ISO 26000 για την κοινωνική ευθύνη αποτελούν θεμέλια εργαλεία που διευκολύνουν την ενσωμάτωση περιβαλλοντικών και κοινωνικών παραμέτρων στις στρατηγικές των οργανισμών, ενώ το ISO 50001 για τη διαχείριση ενέργειας έχει αποδείξει ότι μειώνει σημαντικά την κατανάλωση ενέργειας και τις εκπομπές CO_2.

Ενδεικτικά, η Delta Electronics στην Κίνα, μέσω της υιοθέτησης του ISO 50001, μείωσε την κατανάλωση ενέργειας κατά 10,51 εκατομμύρια kWh, αποφεύγοντας περισσότερους από 10.000 τόνους εκπομπών CO_2 και εξοικονομώντας περίπου 8 εκατομμύρια Γιουάν (Wikipedia, 2024). Η ενοποίηση προτύπων αποκτά ιδιαίτερη σημασία και στις εφοδιαστικές αλυσίδες, όπου πρότυπα όπως το ISO 20400 για την αειφόρο προμήθεια καθιστούν δυνατή την επιλογή προμηθευτών βάσει κριτηρίων βιωσιμότητας, μειώνοντας αρνητικές κοινωνικές και περιβαλλοντικές επιπτώσεις. Ωστόσο, η εφαρμογή τυποποιημένων πλαισίων δεν στερείται προκλήσεων, καθώς το κόστος υλοποίησης, η ανάγκη εκπαίδευσης και η προσαρμογή των επιχειρησιακών μοντέλων μπορούν να αποτελέσουν εμπόδια, ιδιαίτερα για μικρομεσαίες επιχειρήσεις.

Παρ’ όλα αυτά, η συνεχής εξέλιξη των διεθνών προτύπων, σε συνδυασμό με την υποστήριξη κυβερνήσεων και διεθνών οργανισμών, ενισχύει τη διείσδυσή τους και δημιουργεί ένα ισχυρό θεμέλιο για βιώσιμη ανάπτυξη σε παγκόσμιο επίπεδο. Συνεπώς, η ενοποίηση προτύπων δεν περιορίζεται στη συμμόρφωση, αλλά συνιστά στρατηγικό μοχλό καινοτομίας, ανταγωνιστικότητας και μετάβασης σε ένα πιο βιώσιμο και ανθεκτικό μέλλον.

Κεφάλαιο 4ο: Πρότυπα και Πρωτόκολλα Ασφάλειας στις IoT Συσκευές

Η ταχεία εξάπλωση του IoT έχει οδηγήσει σε μια νέα εποχή ψηφιακής διασύνδεσης, όπου δισεκατομμύρια συσκευές ανταλλάσσουν δεδομένα και αλληλεπιδρούν μεταξύ τους σε πραγματικό χρόνο. Από τα έξυπνα σπίτια και τις φορητές συσκευές υγείας, μέχρι τα βιομηχανικά δίκτυα αισθητήρων και τις έξυπνες πόλεις, το IoT μετασχηματίζει την καθημερινότητα και τις επιχειρησιακές διαδικασίες, προσφέροντας αυξημένη αποδοτικότητα, αυτοματοποίηση και εξατομικευμένες υπηρεσίες. Ωστόσο, η συνεχώς αυξανόμενη διασύνδεση συνοδεύεται και από σημαντικές προκλήσεις στον τομέα της ασφάλειας και της προστασίας των δεδομένων. Η ποικιλομορφία των IoT συσκευών, που χαρακτηρίζονται από περιορισμένους υπολογιστικούς πόρους, χαμηλή κατανάλωση ενέργειας και διαφορετικά περιβάλλοντα χρήσης, καθιστά αναγκαία την ανάπτυξη εξειδικευμένων πρωτοκόλλων επικοινωνίας και μηχανισμών ασφάλειας. Τα κλασικά πρότυπα του Διαδικτύου δεν επαρκούν, καθώς δεν είναι σχεδιασμένα για περιβάλλοντα περιορισμένων πόρων, όπου η ελαφρότητα, η αξιοπιστία και η ενεργειακή αποδοτικότητα αποτελούν κρίσιμους παράγοντες.

Στο παρόν κεφάλαιο αναλύονται συστηματικά τα βασικά επικοινωνιακά πρωτόκολλα που χρησιμοποιούνται στο IoT, όπως τα MQTT, CoAP, AMQP, XMPP και DDS, τα οποία επιτρέπουν την αποδοτική και ασφαλή ανταλλαγή δεδομένων σε διαφορετικά σενάρια χρήσης. Παράλληλα, παρουσιάζονται οι κύριοι μηχανισμοί ασφάλειας και κρυπτογράφησης που εφαρμόζονται στο IoT, με έμφαση σε τεχνολογίες όπως το TLS/DTLS, η ελαφριά κρυπτογραφία και τα πρωτόκολλα end-to-end προστασίας. Τέλος, για την καλύτερη κατανόηση της πρακτικής αξίας των παραπάνω τεχνολογιών, παρουσιάζονται μελέτες περίπτωσης από διαφορετικούς τομείς εφαρμογής, όπως τα έξυπνα σπίτια, η βιομηχανία, η υγεία και οι έξυπνες πόλεις. Μέσα από τις εφαρμογές αυτές αναδεικνύονται τόσο τα οφέλη όσο και οι προκλήσεις που συνοδεύουν την ενσωμάτωση προτύπων και πρωτοκόλλων ασφάλειας στις IoT συσκευές. Η μελέτη των παραπάνω αποτελεί κρίσιμο βήμα για την κατανόηση του τρόπου με τον οποίο η τυποποίηση και η ασφάλεια μπορούν να ενισχύσουν τη βιωσιμότητα, την εμπιστοσύνη και την ανθεκτικότητα των IoT οικοσυστημάτων.

4.1 Επικοινωνιακά Πρωτόκολλα για IoT

Η επιτυχία και η ευρεία υιοθέτηση του IoT στηρίζεται σε μεγάλο βαθμό στην αποτελεσματικότητα των επικοινωνιακών πρωτοκόλλων που χρησιμοποιούνται για τη διασύνδεση και την αλληλεπίδραση των συσκευών. Σε αντίθεση με τα παραδοσιακά δίκτυα υπολογιστών, τα IoT συστήματα χαρακτηρίζονται από ετερογένεια, περιορισμένους πόρους (υπολογιστική ισχύ, μνήμη, ενέργεια) και διαφορετικές απαιτήσεις ως προς την καθυστέρηση (latency), την αξιοπιστία και την κλιμάκωση. Για τον λόγο αυτό έχουν αναπτυχθεί εξειδικευμένα πρωτόκολλα, σχεδιασμένα ώστε να εξασφαλίζουν αποδοτική επικοινωνία ακόμα και σε περιβάλλοντα με περιορισμούς.

Τα πρωτόκολλα επικοινωνίας στο IoT χωρίζονται σε διάφορες κατηγορίες, με βάση τον προσανατολισμό τους σε ελαφριά ανταλλαγή μηνυμάτων (π.χ. MQTT, CoAP), σε πιο σύνθετους μηχανισμούς διαχείρισης ουρών και δεδομένων (π.χ. AMQP) ή σε αρχιτεκτονικές peer-to-peer επικοινωνίας και πραγματικού χρόνου (π.χ. XMPP, DDS). Η επιλογή του κατάλληλου πρωτοκόλλου εξαρτάται από το εκάστοτε σενάριο χρήσης: για παράδειγμα, οι εφαρμογές έξυπνων σπιτιών απαιτούν ελαφριά και χαμηλής κατανάλωσης επικοινωνία, ενώ τα βιομηχανικά περιβάλλοντα προϋποθέτουν υψηλή αξιοπιστία και δυνατότητες real-time ανταλλαγής δεδομένων.

Η ενότητα αυτή παρουσιάζει αναλυτικά τα κυριότερα επικοινωνιακά πρωτόκολλα που έχουν επικρατήσει στο IoT, συγκρίνοντας τα χαρακτηριστικά, τις δυνατότητες και τις αδυναμίες τους. Μέσα από τη μελέτη τους, αναδεικνύεται η σημασία της σωστής επιλογής πρωτοκόλλου για την εξασφάλιση τόσο της τεχνικής απόδοσης όσο και της ασφάλειας ενός IoT συστήματος.

4.1.1 Message Queuing Telemetry Transport - Μεταφορά Τηλεμετρικών Μηνυμάτων με Ουρές (MQTT)

Το MQTT αποτελεί το προκαθορισμένο πρωτόκολλο επικοινωνίας για IoT συσκευές, ειδικά σχεδιασμένο για περιβάλλοντα με περιορισμένους πόρους [25]. Όπως ορίζεται στα επίσημα έγγραφα:

«Το MQTT είναι ένα ελαφρού βάρους, ανοιχτό, απλό πρωτόκολλο publish / subscribe, σχεδιασμένο για εύκολη υλοποίηση... ιδανικό για M2M και IoT περιβάλλοντα όπου είναι κρίσιμο να υπάρχει μικρό αποτύπωμα κώδικα και περιορισμένο εύρος ζώνης.»

Η αρχιτεκτονική του MQTT στηρίζεται στο μοντέλο publish/subscribe, το οποίο διαφέρει από το κλασικό client-server μοντέλο (π.χ. HTTP). Αντί οι πελάτες να συνδέονται απευθείας μεταξύ τους, επικοινωνούν μέσω ενός ενδιάμεσου κόμβου, του Broker, ο οποίος είναι υπεύθυνος για τη δρομολόγηση και τη διανομή των μηνυμάτων.

Τα βασικά χαρακτηριστικά που απαρτίζουν το MQTT είναι:

Clients (Publishers & Subscribers):

- Οι Publishers δημιουργούν και αποστέλλουν μηνύματα σε συγκεκριμένα topics.
- Οι Subscribers εκδηλώνουν ενδιαφέρον (subscription) για συγκεκριμένα topics και λαμβάνουν τα μηνύματα που δημοσιεύονται σε αυτά.
- Ένας client μπορεί ταυτόχρονα να είναι publisher και subscriber.

Broker:

- Είναι το “κέντρο” του συστήματος, υπεύθυνο για τη λήψη, αποθήκευση και προώθηση των μηνυμάτων.
- Διαχειρίζεται τη σύνδεση των clients, τις συνδρομές τους και τις παραδόσεις μηνυμάτων.
- Υποστηρίζει μηχανισμούς ασφάλειας (π.χ. TLS), authentication και authorization.
- Μπορεί να λειτουργεί σε cluster, αυξάνοντας την αντοχή σε αποτυχίες και την απόδοση.

Topics:

- Τα topics είναι ιεραρχικές συμβολοσειρές που κατηγοριοποιούν τα μηνύματα. Παράδειγμα:

  «home/livingroom/temperature

  factory/machine1/status»
- Οι subscribers εγγράφονται σε συγκεκριμένα topics ή χρησιμοποιούν wildcards για ευρύτερη κάλυψη (π.χ. home/+/temperature).

Ο τρόπος επικοινωνίας στο MQTT πραγματοποιείται σε τρία στάδια:

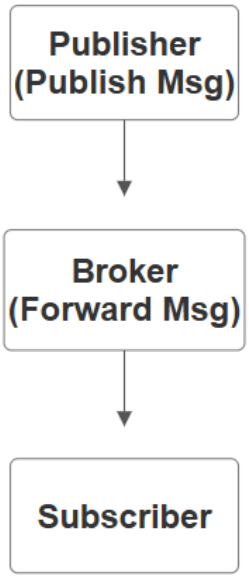
1. Connect:
   Ο client συνδέεται στον broker (συχνά με authentication – username, password, ή TLS certificates).

2. Publish / Subscribe:
    - Ο publisher στέλνει ένα μήνυμα σε ένα συγκεκριμένο topic.
    - Ο broker καταγράφει το μήνυμα και το προωθεί σε όλους τους subscribers που έχουν δηλώσει ενδιαφέρον για το συγκεκριμένο topic.
3. Disconnect:
   Ο client αποσυνδέεται. Αν έχει ενεργοποιήσει persistent session, ο broker θυμάται τις συνδρομές του για μελλοντική χρήση.

Με σκοπό την κάλυψη όλων των διαφορετικών απαιτήσεων αξιοπιστίας, το MQTT υποστηρίζει τρία επίπεδα QoS (Quality of Service):

Επίπεδο QoS	Περιγραφή	Χρήση
QoS 0	Το μήνυμα παραδίδεται το πολύ μία φορά (fire-and-forget). Δεν υπάρχει επιβεβαίωση	Ιδανικό για δεδομένα που ανανεώνονται συχνά (π.χ. αισθητήρας θερμοκρασίας)
QoS 1	Το μήνυμα παραδίδεται τουλάχιστον μία φορά, με επιβεβαίωση. Μπορεί να δημιουργήσει διπλότυπα	Χρήσιμο σε βιομηχανικές εφαρμογές
QoS 2	Το μήνυμα παραδίδεται ακριβώς μία φορά, μέσω τετραπλής χειραψίας (handshake).	Κατάλληλο για κρίσιμα δεδομένα (π.χ. φαρμακευτικές δοσολογίες)

Παρακάτω βλέπουμε ένα απλουστευμένο διάγραμμα ροής:



Με αυτόν τον μηχανισμό, οι publishers δεν χρειάζεται να γνωρίζουν ποιοι subscribers θα λάβουν τα δεδομένα, ούτε αντίστροφα· το μόνο που χρειάζονται είναι ο broker και τα topics. Αυτό επιτρέπει ευελιξία, επεκτασιμότητα και χαμηλή πολυπλοκότητα στο δίκτυο IoT.

Τα κύρια χαρακτηριστικά του και τα πλεονεκτήματα είναι:

- Ελαφρύ και αποδοτικό: Ελάχιστη χρήση bandwidth και μικρή κατανάλωση επεξεργαστικών πόρων, καθιστώντας το ιδανικό για IoT.

- QoS επίπεδα: Τρία επίπεδα αξιοπιστίας μεταφοράς:
    - *QoS 0:* "fire-and-forget"
    - *QoS 1:* τουλάχιστον μία παράδοση
    - *QoS 2:* ακριβώς μία παράδοση.
- Stateful sessions & Last Will: Τα sessions παραμένουν ενεργά, και σε περίπτωση απώλειας σύνδεσης, μπορεί να σταλεί μήνυμα “Last Will” ως ενημέρωση της αποσύνδεσης.
- Binary μορφή μηνυμάτων: Μικρότερο μέγεθος και ταχύτερη μεταφορά σε σχέση με text-based πρωτόκολλα.
- Αποδοτική κλιμάκωση: Χρησιμοποιείται σε εκατομμύρια συσκευές ταυτόχρονα, με δυνατότητα clustering brokers.
- Σύμφωνα με έρευνα του HiveMQ (2022), το 48–50 % των εταιρειών θεωρούν το MQTT στρατηγικό για την ενσωμάτωση τους στο IIoT, ενώ 55 % το χρησιμοποιούν ως σημαντικό εργαλείο δεδομένων—πριν ακόμα το HTTP (51 %).
- Αναμένεται αύξηση της χρήσης κατά 29 % τα επόμενα δύο χρόνια.

Τομέας	Εφαρμογή
Έξυπνα σπίτια	Έλεγχος θερμοστάτη ή φωτιστικών από smartphone μέσω MQTT broker (π.χ., Node-RED + ESP32).
Βιομηχανία (IIoT)	Monitoring αισθητήρων γραμμής παραγωγής με QoS 1 για αξιόπιστη παράδοση.
Αυτοματοποίηση	Ροή δεδομένων μεταξύ PLC και SCADA μέσω broker με προαιρετικό clustering.

4.1.2 Constrained Application Protocol - Πρωτόκολλο Περιορισμένων Εφαρμογών (CoAP)

Το CoAP είναι ένα ελαφρύ πρωτόκολλο επικοινωνίας που σχεδιάστηκε από την IETF (Internet Engineering Task Force) με στόχο να καλύψει τις ανάγκες συσκευών με περιορισμένους πόρους σε περιβάλλοντα IoT (Internet of Things). Χρησιμοποιεί το UDP αντί του TCP, επιτρέποντας γρήγορη, ενεργειακά αποδοτική και απλή επικοινωνία, ιδανική για συσκευές όπως αισθητήρες, ενεργοποιητές (actuators), και μικροελεγκτές. Η αρχιτεκτονική του CoAP βασίζεται σε ένα απλοποιημένο μοντέλο client-server, το οποίο έχει σχεδιαστεί ειδικά για συσκευές και δίκτυα με περιορισμένους πόρους (constrained environments). Παρόλο που ακολουθεί τη λογική του HTTP (RESTful αρχιτεκτονική), διαφοροποιείται σε αρκετά σημεία ώστε να καλύπτει τις ανάγκες του IoT.

- Clients:
  Οι CoAP clients είναι οι συσκευές που ξεκινούν την επικοινωνία στέλνοντας αιτήματα (requests). Συνήθως πρόκειται για αισθητήρες ή φορητές IoT συσκευές, που ζητούν δεδομένα ή στέλνουν εντολές.
  Παράδειγμα: Ένας αισθητήρας θερμοκρασίας που ζητά από έναν server να του επιστρέψει την τρέχουσα θερμοκρασία (CoAP GET).
- Servers:
  Οι CoAP servers είναι συσκευές ή εφαρμογές που φιλοξενούν πόρους (resources) και απαντούν στα αιτήματα των clients. Ένας πόρος μπορεί να είναι μια παράμετρος (π.χ. θερμοκρασία,

φωτεινότητα) ή μια υπηρεσία (π.χ. ενεργοποίηση συναγερμού). *Παράδειγμα:* Ένας smart home controller που δέχεται εντολή (CoAP PUT) για να ενεργοποιήσει ένα κλιματιστικό.

Η αλληλεπίδραση είναι request/response, όμως λόγω της χρήσης του UDP και του απλούστερου message format, η επικοινωνία είναι ελαφρύτερη και ταχύτερη από το HTTP.

Η δομή μνημάτων στο CoAP είναι πολύ πιο απλή και ελαφριά από τα HTTP. Περιλαμβάνουν:

- Fixed Header (4 bytes): Περιέχει τον τύπο του μηνύματος, κωδικό αιτήματος/απάντησης, μήκος κ.ά.
- Token: Ένα αναγνωριστικό που αντιστοιχίζει τα requests με τα responses.
- Options: Παρέχουν επιπλέον πληροφορίες (π.χ. τύπος περιεχομένου).
- Payload: Το πραγματικό περιεχόμενο του μηνύματος (π.χ. δεδομένα αισθητήρα).

Το CoAP ορίζει τέσσερις βασικούς τύπους μηνυμάτων για να εξισορροπήσει την αξιοπιστία και την αποδοτικότητα:

1. Confirmable (CON):
    - Χρησιμοποιούνται όταν απαιτείται αξιόπιστη παράδοση.
    - Ο server απαντά με Acknowledgement (ACK). Αν δεν ληφθεί ACK, το μήνυμα αναμεταδίδεται.
    - *Παράδειγμα:* Εντολή ενεργοποίησης συναγερμού.
2. Non-Confirmable (NON):
    - Δεν απαιτούν επιβεβαίωση.
    - Κατάλληλα για μηνύματα όπου η απώλεια δεν είναι κρίσιμη.
    - *Παράδειγμα:* Ενημέρωση θερμοκρασίας κάθε 10 δευτερόλεπτα.
3. Acknowledgement (ACK):
    - Χρησιμοποιείται για να επιβεβαιώσει την παραλαβή ενός CON μηνύματος.
4. Reset (RST):
    - Αποστέλλεται όταν το μήνυμα ληφθεί αλλά δεν μπορεί να επεξεργαστεί (π.χ. λάθος μορφή).

Ένα από τα σημαντικά πλεονεκτήματα του CoAP είναι η δυνατότητα multicast επικοινωνίας. Αυτό σημαίνει ότι ένας client μπορεί να στείλει ένα request σε πολλούς servers ταυτόχρονα, εξοικονομώντας χρόνο και πόρους.

- *Παράδειγμα:* Ένας αισθητήρας φωτός στέλνει εντολή για άναμμα όλων των λαμπτήρων σε μια περιοχή smart city με ένα multicast CoAP request.

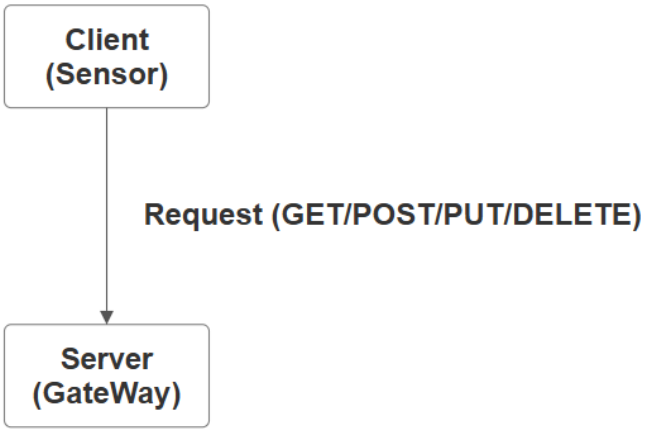
Η ασφάλεια στο CoAP υλοποιείται μέσω του DTLS (Datagram Transport Layer Security), το οποίο προσφέρει:

- Κρυπτογράφηση των δεδομένων.
- Πιστοποίηση (authentication) για έλεγχο ταυτότητας συσκευών.

- Ακεραιότητα (integrity) των μηνυμάτων.

Αυτό καθιστά το CoAP ασφαλές ακόμα και σε δίκτυα χαμηλής ισχύος, χωρίς σημαντική επιβάρυνση.

Παρακάτω βλέπουμε το Διάγραμμα Αρχιτεκτονικής CoAP:



- Ο Client (αισθητήρας/actuator) στέλνει CoAP αιτήματα.
- Ο Server (IoT gateway, cloud node) απαντά ανάλογα.
- Η επικοινωνία μπορεί να είναι μονοκατευθυντική (NON) ή αξιόπιστη με επιβεβαίωση (CON/ACK).

Τα κύρια χαρακτηριστικά το CoAP είναι:

Ελαφρύ και αποδοτικό:

- Σχεδιάστηκε για συσκευές με περιορισμένη υπολογιστική ισχύ, μνήμη και ενεργειακούς πόρους.
- Το μέγεθος των μηνυμάτων είναι μικρό, ώστε να περιορίζεται η κατανάλωση εύρους ζώνης.

Βασισμένο στο REST μοντέλο:

- Το CoAP μιμείται το μοντέλο του HTTP (με GET, POST, PUT, DELETE), ώστε να είναι συμβατό με τον Παγκόσμιο Ιστό.
- Η διαφορά είναι ότι το CoAP είναι πολύ πιο ελαφρύ και αποδοτικό.

Επικοινωνία μέσω UDP:

- Χρησιμοποιεί το User Datagram Protocol (UDP) για να μειώσει το overhead.
- Υποστηρίζει αξιόπιστη μετάδοση μέσω confirmable (CON) και non-confirmable (NON) μηνυμάτων.

Υποστήριξη Multicast:

- Σε αντίθεση με το HTTP, το CoAP υποστηρίζει multicast επικοινωνία, κάτι που το καθιστά ιδανικό για σενάρια όπου πολλές συσκευές πρέπει να ενημερώνονται ταυτόχρονα (π.χ. ενεργοποίηση φωτισμού σε smart city).

Ασφάλεια:

- Εφαρμόζεται μέσω DTLS (Datagram Transport Layer Security).

- Υποστηρίζει κρυπτογράφηση, πιστοποίηση και ακεραιότητα δεδομένων.

Συγκριτικός Πίνακας CoAP – HTTP – MQTT

Πρωτόκολλο	**Τύπος Μοντέλου**	**Μεταφορά**	**Καταλληλότητα**
HTTP	Request/Response	TCP	Βαρύ, όχι κατάλληλο για IoT
MQTT	Publish/Subscribe	TCP	Ιδανικό για πολλά nodes & messaging
CoAP	Request/Response (RESTful)	UDP	Ελαφρύ, για constrained συσκευές

4.1.3 Advanced Message Queuing Protocol - Προηγμένο Πρωτόκολλο Μηνυμάτων Ουράς (AMQP)

Το AMQP είναι ένα ανοικτό, wire-level πρωτόκολλο middleware, σχεδιασμένο για αξιόπιστη, ασφαλή και διαλειτουργική ανταλλαγή μηνυμάτων. Αν και πρωτοεμφανίστηκε στον χρηματοπιστωτικό τομέα (όπως τη J.P. Morgan), έχει γίνει διεθνές πρότυπο μέσω του OASIS και του ISO/IEC 19494:2014

Το AMQP βασίζεται σε μια πιο γενικευμένη αρχιτεκτονική messaging—εκτενέστερη και πιο πολύπλοκη από αυτή άλλων ελαφρών πρωτοκόλλων όπως το MQTT:

- Exchanges: δέχονται μηνύματα από τους παραγωγούς (producers) και τα δρομολογούν σε queues σύμφωνα με κανόνες (bindings). Υπάρχουν τέσσερις τύποι:
    - Direct: στοχευμένη δρομολόγηση, ένα-προς-ένα.
    - Fanout: αποστολή σε όλες τις συνδεδεμένες ουρές.
    - Topic: δρομολόγηση βάσει μοτίβων (π.χ. sensor.*.temp).
    - Headers: δρομολόγηση βάσει τιμών στο header.
- Queues: αποθηκεύουν μηνύματα μέχρι να τα καταναλώσει κάποιος consumer. Υποστηρίζουν durability και dead-lettering.
- Bindings: κανόνες που συνδέουν exchanges με queues, κατευθύνοντας τα μηνύματα.
- Channels: ελαφρές, εικονικές συνδέσεις εντός ενός TCP socket—επιτρέπουν πολυκαναλική επικοινωνία χωρίς να αυξηθεί ο φόρτος του πρωτοκόλλου.
- Sessions & Framing: Το AMQP 1.0 χρησιμοποιεί frames για έλεγχο συνδέσεων, ροής και παράδοσης, με δυνατότητα ακρίβειας παράδοσης: «at-most-once», «at-least-once», «exactly-once».

Το παραπάνω αυξημένο επίπεδο ελέγχου το καθιστά κατάλληλο για σύνθετα, επιχειρησιακά και IoT περιβάλλοντα μεγάλης κλίμακας.

Παρακάτω περιγράφονται τα πλεονεκτήματα και οι προκλήσεις που αντιμετωπίζουν τα AMQPQ:

Τα πλεονεκτήματα είναι:

- *Αξιοπιστία*: εγγυημένη παράδοση μηνυμάτων με επιβεβαίωση από τον consumer.
- *Ασφάλεια*: υποστηρίζονται SSL/TLS και SASL authentication.
- *Διαλειτουργικότητα*: wire-level standard επιτρέπει επικοινωνία μεταξύ διαφορετικών υλοποιήσεων.
- *Ευελιξία*: υποστηρίζεται publish/subscribe, point-to-point και άλλες τοπολογίες.

Και οι προκλήσεις:

- Πολυπλοκότητα: δυσκολότερος σχεδιασμός και υλοποίηση σε σχέση με MQTT ή CoAP.
- Υψηλότερη κατανάλωση πόρων και εύρους ζώνης.
- Περιορισμένη υποστήριξη για resource discovery ή constrained περιβάλλοντα.

Εφαρμογές και παράδειγμα

Τομέας	Χρήση
Enterprise IoT	Σύνδεση edge devices με cloud ή enterprise backends (π.χ. Azure IoT).
Industry & Smart Cities	Διαχείριση δεδομένων αισθητήρων και εντολών με αξιόπιστη παράδοση.
FedComm (Federated Learning)	Σε πειράματα, πρωτόκολλα όπως AMQP μείωσαν τον χρόνο επικοινωνίας κατά 2.5× συγκριτικά με TCP, χωρίς χάσιμο ακρίβειας.

4.1.4 XMPP & DDS (Data Distribution Service)

Η ενότητα αυτή εξετάζει δύο εδραιωμένες αλλά ουσιωδώς διαφορετικές προσεγγίσεις ανταλλαγής μηνυμάτων για IoT: το XMPP (Extensible Messaging and Presence Protocol - Επεκτάσιμο Πρωτόκολλο Μηνυμάτων και Παρουσίας), ένα επεκτάσιμο πρωτόκολλο με ρίζες στην ανταλλαγή μηνυμάτων και μοντέλο publish/subscribe μέσω επεκτάσεων· και το DDS (Data Distribution Service - Υπηρεσία Διανομής Δεδομένων), ένα πρότυπο με έμφαση σε real-time, data-centric επικοινωνία, με πλούσιες πολιτικές ποιότητας υπηρεσίας (QoS) για συστήματα αποστολής κρίσιμων αποστολών (mission-/safety-critical). [23]

Το XMPP ορίζεται από τα RFC 6120/6121 (core, IM/presence) και αξιοποιεί XML streams πάνω από TCP/TLS για την ανταλλαγή δομημένων μηνυμάτων σχεδόν σε πραγματικό χρόνο. Η επέκταση XEP-0060 εισάγει το Publish-Subscribe (PubSub) ως γενικό μηχανισμό διανομής γεγονότων (events) προς πολλούς συνδρομητές, κάτι που αποτελεί τη βάση για σενάρια IoT.

Η αρχιτεκτονική του XMPP για περιβάλλοντα IoT στηρίζεται στο παραδοσιακό μοντέλο client–server, το οποίο προσφέρει ευελιξία, δυνατότητα κλιμάκωσης και ισχυρή διαχείριση ασφάλειας.

1. Clients: Οι XMPP clients στις εφαρμογές IoT είναι συνήθως συσκευές-αισθητήρες, πύλες (gateways) ή ενεργοποιητές (actuators), οι οποίοι εκκινούν συνδέσεις προς έναν XMPP server. Η επικοινωνία πραγματοποιείται μέσω ασφαλούς καναλιού TLS, όπως ορίζεται στο RFC 7590, εξασφαλίζοντας εμπιστευτικότητα και ακεραιότητα.

2. Server/Broker (Domain): Ο XMPP server λειτουργεί ως κεντρικό σημείο διαχείρισης (domain broker) που διασφαλίζει την αυθεντικοποίηση των clients, την εφαρμογή πολιτικών ελέγχου πρόσβασης και την προώθηση μηνυμάτων προς τους κατάλληλους προορισμούς. Μέσω του μηχανισμού SASL (Simple Authentication and Security Layer), κάθε client πιστοποιείται και λαμβάνει συγκεκριμένα δικαιώματα πρόσβασης.

3. PubSub Nodes: Η ανταλλαγή δεδομένων οργανώνεται σε θεματικούς κόμβους (nodes) με βάση το πρότυπο XEP-0060 (Publish-Subscribe). Οι clients που λειτουργούν ως publishers στέλνουν δεδομένα σε συγκεκριμένα nodes, ενώ οι subscribers ενημερώνονται σε πραγματικό χρόνο για τις αλλαγές. Ο server ελέγχει ποιοι clients έχουν άδεια πρόσβασης (ανά node) και σε ποια λειτουργία (publish, subscribe, both).

Η XMPP Standards Foundation (XSF) έχει αναπτύξει εξειδικευμένα πρότυπα επεκτάσεων (XEPs) με στόχο την υποστήριξη εφαρμογών στο πεδίο του Διαδικτύου των Πραγμάτων (IoT), τα οποία καλύπτουν τόσο τη συλλογή δεδομένων όσο και τον έλεγχο συσκευών. Το πρότυπο XEP-0323 (Sensor Data) καθορίζει τον τρόπο με τον οποίο μοντελοποιούνται και μεταφέρονται τα δεδομένα αισθητήρων, παρέχοντας σχήματα για παραμέτρους όπως η συχνότητα μέτρησης και ο τύπος δεδομένων, ενώ περιλαμβάνει και μηχανισμούς για περιοδική συλλογή μέσω “scans”. Συμπληρωματικά, το XEP-0325 (Control of Actuators) επικεντρώνεται στη διαχείριση ενεργοποιητών, δηλαδή συσκευών που εκτελούν εντολές, όπως η ενεργοποίηση φωτισμού ή η ρύθμιση θερμοστάτη, ορίζοντας μεθόδους αποστολής εντολών, επιβεβαίωσης εκτέλεσης, ανατροφοδότησης κατάστασης και διαχείρισης σφαλμάτων. Το XEP-0324 (Provisioning) παρέχει δυνατότητες παραμετροποίησης και ελέγχου δικαιωμάτων, επιτρέποντας τον καθορισμό ποιοι clients έχουν πρόσβαση σε συγκεκριμένους αισθητήρες ή ενεργοποιητές. Τέλος, το XEP-0326 (Concentrators) εισάγει την έννοια του συγκεντρωτή, ενός ενδιάμεσου client που λειτουργεί ως αντιπρόσωπος για πολλαπλούς αισθητήρες ή ενεργοποιητές, μειώνοντας τον αριθμό των απαιτούμενων συνδέσεων προς τον XMPP server και καθιστώντας εφικτή τη διαχείριση εγκαταστάσεων μεγάλης κλίμακας με μεγαλύτερη αποδοτικότητα.

Ένα χαρακτηριστικό παράδειγμα εφαρμογής των παραπάνω προτύπων εντοπίζεται σε ένα έξυπνο κτίριο (smart building). Σε αυτό το πλαίσιο, ένας αισθητήρας θερμοκρασίας (*sensor.office7.temp*) δημοσιεύει περιοδικά δεδομένα στο node *building/office7/temp* μέσω του προτύπου XEP-0323, επιτρέποντας την αξιόπιστη συλλογή μετρήσεων. Ο θερμοστάτης (*actuator.office7.hvac*) παρακολουθεί τον ίδιο node και, με τη χρήση του XEP-0325, δέχεται εντολές από το σύστημα διαχείρισης κτιρίου (BMS) για την προσαρμογή της θερμοκρασίας στον συγκεκριμένο χώρο. Η πρόσβαση σε αυτόν τον actuator ελέγχεται από το XEP-0324, το οποίο διασφαλίζει ότι μόνο εξουσιοδοτημένοι clients μπορούν να στέλνουν εντολές, ενισχύοντας την ασφάλεια και τον έλεγχο του συστήματος. Επιπλέον, σε περιπτώσεις όπου υπάρχουν εκατοντάδες αισθητήρες σε έναν όροφο, ένας concentrator (XEP-0326) μπορεί να συγκεντρώνει τα δεδομένα και να τα προωθεί στον XMPP server, μειώνοντας την πολυπλοκότητα των συνδέσεων και βελτιστοποιώντας τη συνολική απόδοση του δικτύου.

Η ασφάλεια στο XMPP αποτελεί έναν από τους βασικούς πυλώνες που επιτρέπουν τη χρήση του σε κρίσιμα περιβάλλοντα IoT, όπου η προστασία δεδομένων και η αξιόπιστη διακυβέρνηση συσκευών είναι καθοριστικής σημασίας. Η μετάδοση των δεδομένων πραγματοποιείται μέσω Transport Layer Security (TLS), σύμφωνα με τις προδιαγραφές του RFC 7590, εξασφαλίζοντας εμπιστευτικότητα και ακεραιότητα σε όλα τα κανάλια επικοινωνίας. Η αυθεντικοποίηση των συσκευών και των χρηστών γίνεται μέσω του μηχανισμού SASL (Simple Authentication and Security Layer), ο οποίος υποστηρίζει πολλαπλά σχήματα ελέγχου ταυτότητας (π.χ. username/password, token-based, certificate-based), προσφέροντας ευελιξία ανάλογα με τις απαιτήσεις της εφαρμογής. Πέρα από την προστασία της ίδιας της σύνδεσης, ιδιαίτερη έμφαση δίνεται στη διακυβέρνηση της πρόσβασης στα δεδομένα και στις υπηρεσίες που προσφέρονται μέσω του μοντέλου Publish-Subscribe (XEP-0060). Οι πολιτικές ελέγχου πρόσβασης επιτρέπουν την αυστηρή ρύθμιση δικαιωμάτων σε επίπεδο node, ορίζοντας ποιοι clients έχουν τη δυνατότητα να δημοσιεύουν ή/και να εγγράφονται σε συγκεκριμένα ροή δεδομένων. Με αυτόν τον τρόπο αποφεύγεται η ανεξέλεγκτη πρόσβαση σε κρίσιμες ροές, όπως δεδομένα αισθητήρων ή εντολές προς ενεργοποιητές. Το γεγονός ότι το XMPP βασίζεται σε XML προσφέρει ένα επεκτάσιμο και ευέλικτο μοντέλο, στο οποίο μπορούν να οριστούν granular πολιτικές ασφαλείας ανά συσκευή, υπηρεσία ή ροή πληροφορίας. Για παράδειγμα, σε ένα σενάριο έξυπνου σπιτιού, μπορεί να καθοριστεί ότι ένας συγκεκριμένος αισθητήρας θερμοκρασίας θα είναι ορατός μόνο από τον τοπικό ελεγκτή, ενώ

οι εντολές προς τον θερμοστάτη θα γίνονται αποκλειστικά από εξουσιοδοτημένες συσκευές με έλεγχο μέσω XEP-0324.

Συνολικά, το XMPP συνδυάζει την ασφάλεια επιπέδου μεταφοράς (TLS) με μηχανισμούς αυθεντικοποίησης (SASL) και πολιτικές διακυβέρνησης σε επίπεδο εφαρμογής (Access Control Policies στα PubSub nodes), παρέχοντας ένα πολυεπίπεδο πλαίσιο προστασίας που το καθιστά ιδιαίτερα ελκυστικό για χρήση σε IoT περιβάλλοντα όπου η αξιοπιστία και η ασφάλεια είναι αδιαπραγμάτευτες.

Το XMPP για IoT παρουσιάζει μια σειρά από πλεονεκτήματα αλλά και ορισμένους περιορισμούς. Από τη μία πλευρά, διαθέτει ένα ώριμο οικοσύστημα με μακροχρόνια χρήση στον χώρο των υπηρεσιών ανταλλαγής μηνυμάτων, το οποίο υποστηρίζει federation και παρέχει ευκολία διασύνδεσης με ήδη υπάρχουσες πλατφόρμες messaging. Παράλληλα, η δυνατότητα επέκτασης του πρωτοκόλλου μέσω των εξειδικευμένων XMPP Extension Protocols (XEPs) το καθιστά ιδιαίτερα ευέλικτο ως προς τη μοντελοποίηση δεδομένων και εντολών, κάτι που το κάνει κατάλληλο για πολύπλοκα περιβάλλοντα IoT. Ωστόσο, η χρήση XML για τη δομή των μηνυμάτων συνεπάγεται μεγαλύτερο βάρος επικεφαλίδων, γεγονός που το καθιστά λιγότερο «ελαφρύ» σε σχέση με πρωτόκολλα όπως το CoAP ή το MQTT, ιδιαίτερα σε κόμβους με αυστηρά περιορισμένους πόρους. Επιπλέον, σε αντίθεση με το DDS, η χρονική προβλεψιμότητα δεν αποτελεί τον πρωταρχικό του στόχο, με αποτέλεσμα να μην ενδείκνυται για εφαρμογές όπου η αυστηρή τήρηση χρονικών περιορισμών είναι κρίσιμη.

Το DDS έχει αναπτυχθεί και τυποποιηθεί από τον Object Management Group (OMG), αποτελεί ένα από τα πλέον διαδεδομένα πρότυπα για επικοινωνία σε συστήματα IoT και Cyber-Physical Systems (CPS), με έμφαση σε εφαρμογές που απαιτούν χαμηλή καθυστέρηση, υψηλή αξιοπιστία και προβλεψιμότητα σε πραγματικό χρόνο. Η βασική αρχή του DDS είναι το Data-Centric Publish-Subscribe (DCPS) μοντέλο, στο οποίο η επικοινωνία δεν βασίζεται στην απευθείας ανταλλαγή μηνυμάτων μεταξύ εφαρμογών, αλλά στην έννοια των Topics. Συγκεκριμένα, οι DataWriters είναι υπεύθυνοι για τη δημοσίευση δεδομένων σε ένα συγκεκριμένο Topic, ενώ οι DataReaders εγγράφονται (subscribe) σε αυτό το Topic για να λαμβάνουν τα αντίστοιχα δεδομένα. Με αυτό τον τρόπο, επιτυγχάνεται αποσύζευξη (decoupling) μεταξύ παραγωγών και καταναλωτών πληροφορίας, τόσο σε επίπεδο χρόνου (οι δύο πλευρές δεν χρειάζεται να είναι ταυτόχρονα ενεργές) όσο και σε επίπεδο χώρου (δεν απαιτείται γνώση της τοπολογίας ή της ταυτότητας των κόμβων).

Ένα από τα βασικά πλεονεκτήματα του DDS είναι η δυνατότητα διαμόρφωσης επικοινωνίας μέσω πολιτικών Ποιότητας Υπηρεσίας (QoS policies). Οι πολιτικές αυτές καθορίζουν με ακρίβεια το πώς θα διακινηθούν τα δεδομένα και ποιο επίπεδο αξιοπιστίας, ανεκτής καθυστέρησης ή ανθεκτικότητας απαιτείται. Παραδείγματα τέτοιων πολιτικών είναι:

- Reliability (αξιοπιστία): καθορίζει αν τα δεδομένα πρέπει να φτάσουν με εγγυημένη παράδοση ή αν μπορεί να γίνει αποδοχή απωλειών για μεγαλύτερη ταχύτητα.
- Deadline: ορίζει χρονικά όρια εντός των οποίων ο DataReader αναμένει νέα δεδομένα, υποστηρίζοντας την έγκαιρη ενημέρωση σε κρίσιμες εφαρμογές.
- LatencyBudget: θέτει όρια για την αποδεκτή καθυστέρηση στην παράδοση δεδομένων.
- Durability: επιτρέπει τη διατήρηση δεδομένων ώστε νέοι DataReaders να μπορούν να λάβουν ιστορικά δεδομένα κατά την εγγραφή τους.

Για να εξασφαλιστεί διαλειτουργικότητα σε επίπεδο «wire», το DDS χρησιμοποιεί το πρωτόκολλο DDSI-RTPS (Real-Time Publish-Subscribe), το οποίο ορίζει πώς μεταφέρονται τα

μηνύματα στο δίκτυο και επιτρέπει την επικοινωνία μεταξύ διαφορετικών υλοποιήσεων DDS από διαφορετικούς κατασκευαστές. Αυτή η τυποποίηση έχει συμβάλει στη μεγάλη διάδοση του DDS σε τομείς όπως η αεροδιαστημική, η αυτοκινητοβιομηχανία, η ρομποτική, αλλά και σε εφαρμογές έξυπνων δικτύων ενέργειας (smart grids) και βιομηχανικού IoT, όπου η προβλεψιμότητα και η αξιοπιστία της επικοινωνίας αποτελούν κρίσιμες παραμέτρους (Pardo-Castellote, 2003· Wang et al., 2019).

Η αρχιτεκτονική του DDS αποτελείται από μια ιεραρχία οντοτήτων που διαμορφώνουν το πλαίσιο της επικοινωνίας. Στον ανώτερο βαθμό βρίσκεται ο DomainParticipant, που αντιπροσωπεύει έναν «κόμβο» ή μια εφαρμογή εντός ενός DDS domain· κάθε domain λειτουργεί ως ένας λογικός χώρος ανταλλαγής δεδομένων, απομονωμένος από άλλα domains. Ο κάθε DomainParticipant μπορεί να δημιουργήσει Publishers και Subscribers, οι οποίοι αποτελούν τα βασικά μέσα οργάνωσης της ροής πληροφορίας. Οι Publishers περιλαμβάνουν DataWriters, δηλαδή οντότητες που δημοσιεύουν δεδομένα σε συγκεκριμένα Topics, ενώ οι Subscribers περιλαμβάνουν DataReaders, που λαμβάνουν αυτά τα δεδομένα. Τα Topics αποτελούν τον λογικό δεσμό μεταξύ παραγωγών και καταναλωτών δεδομένων, καθορίζοντας τον τύπο και τη σημασιολογία της ανταλλασσόμενης πληροφορίας (OMG, 2015).

Η πραγματική ισχύς του DDS έγκειται στις πλούσιες πολιτικές ποιότητας υπηρεσίας (QoS), οι οποίες καθορίζουν με ακρίβεια το πώς μεταφέρονται, αποθηκεύονται και καταναλώνονται τα δεδομένα. Οι πολιτικές QoS λειτουργούν συμμετρικά μεταξύ DataWriters και DataReaders: για να δημιουργηθεί μια επικοινωνιακή σχέση, πρέπει να υπάρξει συμφωνία (matching) των παραμέτρων QoS και από τις δύο πλευρές. Εάν για παράδειγμα ένας DataWriter ορίζει αξιόπιστη παράδοση (reliable), αλλά ο αντίστοιχος DataReader έχει ρυθμιστεί μόνο για best-effort, τότε η επικοινωνία δεν θα είναι εφικτή έως ότου επιτευχθεί συμβατότητα. [28]

Μεταξύ των σημαντικότερων QoS policies ξεχωρίζουν:

- Reliability: Καθορίζει αν τα δεδομένα αποστέλλονται με best-effort (χωρίς εγγύηση παράδοσης, ελαχιστοποιώντας καθυστερήσεις και overhead) ή reliable (με μηχανισμούς επιβεβαίωσης και επαναμετάδοσης για εγγυημένη παράδοση).
- Durability: Ορίζει αν τα δεδομένα παραμένουν διαθέσιμα και μετά τη δημοσίευσή τους, ώστε νέοι DataReaders να μπορούν να τα λάβουν εκ των υστέρων (π.χ. transient ή persistent).
- Deadline: Επιτρέπει τον καθορισμό χρονικού διαστήματος εντός του οποίου πρέπει να παραχθούν δεδομένα· αν παραβιαστεί, ειδοποιείται το αντίστοιχο σύστημα.
- Latency Budget: Θέτει περιορισμό στον μέγιστο χρόνο που μπορεί να μεσολαβήσει μεταξύ παραγωγής και κατανάλωσης δεδομένων.
- Liveliness: Εξασφαλίζει ότι οι συμμετέχοντες (writers/readers) παραμένουν ενεργοί και «ζωντανοί»· αν μια οντότητα χαθεί, γίνεται άμεση ενημέρωση του συστήματος.
- Time-based Filter: Επιτρέπει στον DataReader να ζητήσει δεδομένα με συγκεκριμένο ρυθμό (π.χ. 1 update/sec), αποφεύγοντας υπερφόρτωση από συνεχείς ενημερώσεις.
- Ownership: Χρησιμοποιείται όταν πολλαπλοί DataWriters μπορούν να γράφουν στο ίδιο Topic· ορίζεται προτεραιότητα ώστε να υπάρχει ένας «κυρίαρχος» writer.

Αυτές οι πολιτικές παρέχουν ένα εξαιρετικά λεπτομερές και προσαρμοστικό πλαίσιο επικοινωνίας, ικανό να ικανοποιήσει διαφορετικές απαιτήσεις εφαρμογών: από real-time βιομηχανικά δίκτυα (όπου η χαμηλή καθυστέρηση και η αξιοπιστία είναι κρίσιμες), μέχρι συστήματα υγείας (όπου χρειάζεται αυστηρή διασφάλιση συνέπειας και διαθεσιμότητας).

Η δυνατότητα παραμετροποίησης QoS καθιστά το DDS ένα από τα πιο ισχυρά middleware πρότυπα για IoT και Cyber-Physical Systems (CPS), καθώς μπορεί να υποστηρίξει ταυτόχρονα διαφορετικά προφίλ επικοινωνίας στο ίδιο δίκτυο, προσαρμόζοντας τη συμπεριφορά του ανάλογα με τις ανάγκες κάθε εφαρμογής.

Η υιοθέτηση του DDS στη βιομηχανία έχει ενισχυθεί σημαντικά χάρη στην ύπαρξη πολλαπλών υλοποιήσεων, τόσο εμπορικών όσο και ανοικτού κώδικα, γεγονός που συμβάλλει στη διαλειτουργικότητα και στη διάδοση του προτύπου. Μεταξύ των πιο διαδεδομένων υλοποιήσεων περιλαμβάνονται το RTI Connext DDS, το οποίο θεωρείται από τα πλέον ώριμα και χρησιμοποιείται εκτενώς σε κρίσιμες εφαρμογές αεροδιαστημικής και άμυνας· το eProsima Fast DDS, που έχει ανοιχτό κώδικα και έχει γίνει ιδιαίτερα δημοφιλές λόγω της ευελιξίας και της ελαφριάς αρχιτεκτονικής του· το Eclipse Cyclone DDS, που αναπτύσσεται στο πλαίσιο του οργανισμού Eclipse Foundation με στόχο την ανοιχτή και διαλειτουργική ανάπτυξη· καθώς και το OpenDDS, μια σταθερή πλατφόρμα ανοικτού κώδικα που χρησιμοποιείται σε ακαδημαϊκό και βιομηχανικό επίπεδο. Η πληθώρα αυτών των υλοποιήσεων ενισχύει την εμπιστοσύνη στη βιωσιμότητα του προτύπου, καθώς εξασφαλίζει στους χρήστες εναλλακτικές επιλογές και αποτρέπει το φαινόμενο vendor lock-in.

Ένα ιδιαίτερα σημαντικό παράδειγμα εκτεταμένης υιοθέτησης αποτελεί το ROS 2 (Robot Operating System 2), το οποίο βασίζεται σε υλοποιήσεις DDS για τη διαχείριση της επικοινωνίας μεταξύ των επιμέρους ρομποτικών κόμβων. Στην πράξη, το ROS 2 επιτρέπει την ενσωμάτωση DDS ως middleware και υποστηρίζει «πλήρεις» ή «μερικές» υλοποιήσεις, ανάλογα με τις απαιτήσεις της εκάστοτε εφαρμογής (π.χ. real-time έλεγχος, διανομή δεδομένων αισθητήρων, συγχρονισμός κίνησης). Η επιλογή αυτή δεν είναι τυχαία, καθώς το DDS παρέχει εγγυήσεις αξιοπιστίας, χαμηλής καθυστέρησης και προβλεψιμότητας που είναι κρίσιμες για αυτόνομα οχήματα, ρομποτικά συστήματα, βιομηχανικό αυτοματισμό και γενικότερα εφαρμογές όπου η ανταλλαγή δεδομένων σε πραγματικό χρόνο είναι απαραίτητη. Το γεγονός ότι ολόκληρο το οικοσύστημα της σύγχρονης ρομποτικής έχει ευθυγραμμιστεί με το DDS αποτελεί ένδειξη της στρατηγικής σημασίας του προτύπου για το μέλλον του βιομηχανικού IoT και των κυβερνοφυσικών συστημάτων (cyber-physical systems).

Η ασφάλεια και η πιστοποίηση αποτελούν κρίσιμους παράγοντες για την ευρεία υιοθέτηση του DDS σε βιομηχανίες με υψηλές απαιτήσεις αξιοπιστίας, όπως η αυτοκινητοβιομηχανία, η αεροδιαστημική και η άμυνα. Οι προμηθευτές DDS έχουν ενσωματώσει επεκτάσεις ασφαλείας που συμμορφώνονται με το πρότυπο DDS Security (OMG Specification), το οποίο καλύπτει βασικές λειτουργίες όπως ταυτοποίηση (authentication), έλεγχος πρόσβασης (access control) και κρυπτογράφηση δεδομένων (encryption), διασφαλίζοντας ότι μόνο εξουσιοδοτημένοι κόμβοι μπορούν να συμμετέχουν στην ανταλλαγή πληροφοριών και ότι τα δεδομένα προστατεύονται έναντι υποκλοπών ή μη εξουσιοδοτημένων τροποποιήσεων. Επιπλέον, πολλά εργαλεία παρακολούθησης (monitoring) και auditing έχουν αναπτυχθεί για την ανίχνευση ανωμαλιών και την έγκαιρη αντίδραση σε επιθέσεις ή δυσλειτουργίες, στοιχείο που ενισχύει την αξιοπιστία σε περιβάλλοντα παραγωγής.

Στο πεδίο της πιστοποίησης, το DDS έχει ήδη χρησιμοποιηθεί σε εφαρμογές που απαιτούν συμμόρφωση με αυστηρά πρότυπα. Ενδεικτικά, στην αυτοκινητοβιομηχανία υπάρχουν τεκμηριωμένες διαδρομές ένταξης του DDS στο πλαίσιο του προτύπου ISO 26262, ακόμα και στο υψηλότερο επίπεδο ασφάλειας ASIL-D, κάτι που καταδεικνύει τη δυνατότητά του να υποστηρίζει συστήματα κρίσιμα για την ασφάλεια. Αντίστοιχα, στην αεροδιαστημική και στις αμυντικές εφαρμογές, το DDS χρησιμοποιείται σε έργα που υπόκεινται σε πιστοποίηση σύμφωνα με τα πρότυπα DO-178C και DO-254, τα οποία καθορίζουν τις απαιτήσεις για την ασφάλεια λογισμικού και υλικού σε αεροπορικά

συστήματα. Η συμμόρφωση με τέτοια πρότυπα δεν αποτελεί μόνο τεχνική πρόκληση αλλά και απόδειξη της ωριμότητας του DDS ως middleware για mission-critical εφαρμογές.

Το DDS προσφέρει σημαντικά πλεονεκτήματα σε εφαρμογές που απαιτούν προβλεψιμότητα χρόνου και έλεγχο καθυστερήσεων, καθώς οι πολιτικές QoS επιτρέπουν την ακριβή διαχείριση παραμέτρων όπως αξιοπιστία παράδοσης, χρονικά όρια (deadlines), προτεραιότητες μηνυμάτων και διάρκεια ζωής δεδομένων. Η επικοινωνία πραγματοποιείται με peer-to-peer μοντέλο μέσω του πρωτοκόλλου RTPS, χωρίς την ανάγκη ύπαρξης κεντρικού broker, γεγονός που μειώνει τα σημεία συμφόρησης και αυξάνει την ανθεκτικότητα του συστήματος. Παρά τα σημαντικά αυτά πλεονεκτήματα, η χρήση του DDS συνοδεύεται από ορισμένους περιορισμούς. Η ρύθμιση και παραμετροποίηση των πολιτικών QoS, καθώς και η διαχείριση της ανακάλυψης κόμβων (discovery tuning), προσθέτουν πολυπλοκότητα στη διαχείριση του συστήματος, απαιτώντας ειδικές γνώσεις και εμπειρία από τους μηχανικούς. Επιπλέον, οι απαιτήσεις πόρων του DDS είναι υψηλότερες σε σχέση με πολύ «ελαφρά» πρωτόκολλα όπως το raw CoAP ή MQTT, γεγονός που μπορεί να περιορίσει τη χρήση του σε συσκευές με περιορισμένη υπολογιστική ισχύ ή μνήμη. Συνεπώς, η επιλογή του DDS πρέπει να γίνεται με προσεκτική αξιολόγηση των απαιτήσεων της εφαρμογής και της διαθεσιμότητας πόρων, ώστε να επιτευχθεί η βέλτιστη ισορροπία μεταξύ αξιοπιστίας, χρονικής προβλεψιμότητας και αποτελεσματικότητας.

4.2 Πρωτόκολλα Ασφάλειας και Κρυπτογράφησης

Η ασφάλεια αποτελεί θεμελιώδη παράγοντα για τη λειτουργία και την αξιοπιστία των συστημάτων IoT, καθώς οι συσκευές και τα δίκτυα που τις συνδέουν συχνά βρίσκονται σε περιβάλλοντα με περιορισμένους πόρους και εκτεθειμένα σε ποικίλες απειλές. Η ανάγκη για ασφαλή επικοινωνία, ακεραιότητα δεδομένων και προστασία της ιδιωτικότητας καθιστά απαραίτητη την υιοθέτηση εξειδικευμένων πρωτοκόλλων κρυπτογράφησης και διαχείρισης ταυτότητας. Στο πλαίσιο αυτό, τα πρωτόκολλα TLS/DTLS εξασφαλίζουν προστασία σε επίπεδο μεταφοράς για TCP και UDP συνδέσεις αντίστοιχα, ενώ οι προσεγγίσεις Lightweight Cryptography, σύμφωνα με τις οδηγίες των NIST και ISO, προσφέρουν αποτελεσματική κρυπτογράφηση για συσκευές με περιορισμένη υπολογιστική ισχύ. Παράλληλα, το OSCORE επιτρέπει ασφαλή μεταφορά δεδομένων σε περιβάλλοντα RESTful με περιορισμένους πόρους, ενώ οι μηχανισμοί end-to-end encryption και identity management ενισχύουν την εμπιστευτικότητα, την αυθεντικοποίηση και την ακεραιότητα των δεδομένων σε ολόκληρο τον κύκλο ζωής των IoT συσκευών. Η ενότητα αυτή θα εξετάσει τόσο τις βασικές αρχές των παραπάνω πρωτοκόλλων όσο και τις εφαρμογές τους, παρέχοντας μια πλήρη εικόνα των σύγχρονων πρακτικών ασφάλειας σε IoT περιβάλλοντα.

4.2.1 Transport Layer Security / Datagram TLS (TLS/DTLS)

Το Transport Layer Security (Ασφάλεια Επίπεδου Μεταφοράς - TLS) και η παραλλαγή του για datagram περιβάλλοντα, το Datagram TLS (Ασφάλεια Επίπεδου Μεταφοράς Δενδρογραμμάτων - DTLS), αποτελούν τα πλέον διαδεδομένα πρωτόκολλα ασφάλειας για την προστασία της επικοινωνίας σε δίκτυα υπολογιστών και IoT συσκευών. Ο βασικός στόχος τους είναι η παροχή εμπιστευτικότητας, ακεραιότητας, αυθεντικοποίησης και, σε ορισμένα σενάρια, προστασίας από επαναχρησιμοποίηση πακέτων (replay protection).

Το TLS λειτουργεί στο Transport Layer (πάνω από TCP), ενώ το DTLS υλοποιείται πάνω από UDP, ώστε να υποστηρίζει εφαρμογές real-time και low-latency (π.χ. VoIP, CoAP, online gaming, IoT αισθητήρες).

Η λειτουργία του TLS/DTLS χωρίζεται σε τρία κύρια επίπεδα:

1. Handshake Protocol: υπεύθυνο για την αυθεντικοποίηση των μερών, την ανταλλαγή κλειδιών και τη διαπραγμάτευση κρυπτογραφικών αλγορίθμων.

   Χρησιμοποιεί μηχανισμούς ασύμμετρης κρυπτογράφησης (RSA, ECDSA, EdDSA) για την αυθεντικοποίηση και την ασφαλή ανταλλαγή μυστικών, ενώ υποστηρίζει Diffie–Hellman Ephemeral (DHE) και Elliptic Curve Diffie–Hellman Ephemeral (ECDHE) ώστε να εξασφαλίζεται Perfect Forward Secrecy (PFS), διασφαλίζοντας ότι ακόμη και αν παραβιαστεί ένα κλειδί στο μέλλον, οι παλαιότερες επικοινωνίες παραμένουν ασφαλείς. Η διαδικασία ολοκληρώνεται με την παραγωγή ενός Master Secret, από το οποίο παράγονται τα session keys μέσω key derivation functions (HKDF).

2. Record Protocol: χειρίζεται τη συσκευασία των δεδομένων.

   Το πρωτόκολλο διαχωρίζει τα δεδομένα σε records, τα οποία συμπιέζονται, υπογράφονται με MAC και στη συνέχεια κρυπτογραφούνται, ενώ υποστηρίζει σύγχρονους αλγόριθμους όπως AES-GCM και ChaCha20-Poly1305 (Authenticated Encryption with Associated Data – AEAD), οι οποίοι παρέχουν ταυτόχρονα εμπιστευτικότητα και ακεραιότητα.

3. Alert & Change Cipher Spec Protocols: μηχανισμοί για ειδοποιήσεις λαθών, αλλαγές στα κλειδιά ή ενημέρωση για τερματισμό της σύνδεσης.

Σε αντίθεση με το TLS που βασίζεται σε TCP, το DTLS πρέπει να αντιμετωπίσει προκλήσεις όπως απώλεια πακέτων, επαναταξινόμηση και διπλοπαραδόσεις. Για τον σκοπό αυτό, χρησιμοποιεί sequence numbers και explicit epochs για την προστασία από replay attacks, ενώ ενσωματώνει μηχανισμούς αναμετάδοσης (retransmissions) στο Handshake ώστε να διασφαλίζεται η αξιοπιστία. Επιπλέον, έχει σχεδιαστεί ώστε να είναι on-the-wire compatible με το TLS, διευκολύνοντας έτσι τη μεταφορά εφαρμογών που βασίζονται σε αυτό χωρίς σημαντικές τροποποιήσεις.

Οι πιο διαδεδομένες εκδόσεις σήμερα είναι το TLS 1.2, το TLS 1.3 και τα αντίστοιχα DTLS 1.2/1.3. Το TLS 1.3 (RFC 8446) εισάγει σημαντικές βελτιώσεις, όπως μειωμένο Handshake latency (1-RTT ή ακόμη και 0-RTT για επανασυνδέσεις), υποχρεωτική χρήση αλγορίθμων AEAD και αφαίρεση παλαιών, λιγότερο ασφαλών αλγορίθμων, όπως το RSA key exchange και τα CBC ciphers. Το DTLS 1.3 ενσωματώνει τα ίδια χαρακτηριστικά, προσαρμοσμένα όμως για το UDP και για constrained συσκευές, όπως τα IoT nodes.

Στον χώρο του IoT, το TLS/DTLS χρησιμοποιείται ευρέως για την ασφαλή μετάδοση δεδομένων πάνω από CoAP (DTLS + CoAP) ή MQTT (TLS + MQTT). Οι προκλήσεις που ανακύπτουν περιλαμβάνουν:

- Υψηλό overhead σε constrained συσκευές (λόγω handshake και μεγάλων headers).
- Κατανάλωση ενέργειας από τις επαναλαμβανόμενες κρυπτογραφικές πράξεις.
- Η ανάγκη για session resumption και pre-shared keys (PSK) σε resource-constrained nodes, ώστε να μειωθεί η υπολογιστική πολυπλοκότητα.

Ενδεικτικά, σε αισθητήρες χαμηλής ισχύος (Class 1 IoT devices με <100 KB RAM), η πλήρης υποστήριξη TLS 1.3 μπορεί να είναι απαιτητική· για τον λόγο αυτόν χρησιμοποιούνται lightweight TLS stacks όπως mbedTLS, wolfSSL, TinyDTLS, τα οποία παρέχουν βελτιστοποιημένες υλοποιήσεις.

4.2.2 Lightweight Cryptography (LWC - NIST, ISO) για IoT συσκευές

Η lightweight κρυπτογραφία (LWC) αναφέρεται σε κρυπτογραφικούς αλγορίθμους και πρωτόκολλα που έχουν σχεδιαστεί ώστε να παρέχουν ισχυρή ασφάλεια, αλλά με ελάχιστες απαιτήσεις σε υπολογιστική ισχύ, μνήμη και κατανάλωση ενέργειας. Αυτό είναι απαραίτητο για συσκευές IoT με περιορισμένους πόρους, όπως αισθητήρες χαμηλής κατανάλωσης, RFID tags και embedded controllers.

Οι αλγόριθμοι LWC έχουν σχεδιαστεί ειδικά για περιβάλλοντα με αυστηρούς περιορισμούς σε υπολογιστικούς πόρους και κατανάλωση ενέργειας. Οι συσκευές-στόχοι, όπως μικροελεγκτές 8-bit ή 16-bit, διαθέτουν ελάχιστη μνήμη RAM και Flash, συχνά μόλις λίγα kilobytes, καθώς και περιορισμένη επεξεργαστική ισχύ. Παράλληλα, πολλές από αυτές τις συσκευές λειτουργούν με μπαταρία ή μέσω energy harvesting, γεγονός που καθιστά κρίσιμη την ελαχιστοποίηση της κατανάλωσης ενέργειας. Ένας ακόμη βασικός παράγοντας είναι το μικρό latency, καθώς απαιτείται οι αλγόριθμοι να μπορούν να υποστηρίζουν real-time επικοινωνίες, κάτι που είναι ιδιαίτερα σημαντικό σε εφαρμογές όπως IoT, αισθητήρες και βιομηχανικά δίκτυα.

Για να ανταποκριθούν σε αυτές τις απαιτήσεις, οι LWC αλγόριθμοι υιοθετούν συγκεκριμένες σχεδιαστικές αρχές. Χρησιμοποιούν δομές όπως τα Substitution-Permutation Networks (SPN) και οι Feistel structures, προσαρμοσμένες με απλοποιημένους γύρους ώστε να μειώνεται η πολυπλοκότητα και το υπολογιστικό κόστος. Επιπλέον, βασίζονται σε μικρότερα μήκη κλειδιών και μπλοκ (π.χ. 64–128 bit block, 80–128 bit key), τα οποία θεωρούνται επαρκή για το επίπεδο ασφαλείας που απαιτούνται σε constrained περιβάλλοντα, μειώνοντας ταυτόχρονα τις ανάγκες σε μνήμη και ενέργεια. Τέλος, πολλοί αλγόριθμοι LWC ενσωματώνουν σε μία ενιαία διαδικασία την κρυπτογράφηση και την ακεραιότητα μέσω τεχνικών AEAD (Authenticated Encryption with Associated Data), εξασφαλίζοντας έτσι τόσο την εμπιστευτικότητα όσο και την προστασία από τροποποιήσεις, χωρίς την ανάγκη για πρόσθετους αλγόριθμους ή ξεχωριστά στάδια επεξεργασίας.

Το NIST Lightweight Cryptography Project ξεκίνησε το 2015 ως μία διεθνής πρωτοβουλία με στόχο τον καθορισμό και την τυποποίηση αλγορίθμων κρυπτογράφησης ειδικά σχεδιασμένων για συσκευές με περιορισμένους πόρους. Οι παραδοσιακοί αλγόριθμοι, όπως το AES ή το SHA-2, θεωρούνται ασφαλείς και αποδοτικοί σε ισχυρότερο υλικό, ωστόσο σε μικροελεγκτές με λίγα kilobytes μνήμης και χαμηλή υπολογιστική ισχύ δεν είναι πάντα πρακτικοί. Για αυτόν τον λόγο, το NIST προκήρυξε έναν διαγωνισμό, καλώντας την παγκόσμια ερευνητική κοινότητα να προτείνει λύσεις που να συνδυάζουν ασφάλεια με χαμηλή κατανάλωση πόρων. Μετά από μια εκτενή διαδικασία αξιολόγησης που διήρκησε οκτώ χρόνια και περιλάμβανε πολλαπλές φάσεις δοκιμών, κριτικές αναλύσεις και πρακτικές υλοποιήσεις, το 2023 το NIST ανακοίνωσε τον Ascon ως τον νικητή του διαγωνισμού. Ο Ascon επιλέχθηκε τόσο για την κατηγορία του Authenticated Encryption (AEAD), που παρέχει ταυτόχρονα εμπιστευτικότητα και ακεραιότητα στα δεδομένα, όσο και για την κατηγορία του Hashing, προσφέροντας ασφαλείς hash συναρτήσεις με χαμηλό υπολογιστικό κόστος. Η σχεδίαση του Ascon βασίζεται σε permutation-based sponge construction, με εσωτερική κατάσταση (state) 320-bit. Αυτή η αρχιτεκτονική επιτρέπει την επίτευξη υψηλής ασφάλειας με σχετικά απλή υλοποίηση, ενώ παράλληλα εξασφαλίζει αποδοτικότητα τόσο σε software (τρέχοντας σε μικρούς μικροελεγκτές με περιορισμένη μνήμη) όσο και σε hardware (ASIC/FPGA υλοποιήσεις με χαμηλή κατανάλωση και υψηλή απόδοση). Έτσι, ο Ascon είναι ιδιαίτερα κατάλληλος για εφαρμογές σε IoT συσκευές,

αισθητήρες και συστήματα πραγματικού χρόνου, όπου απαιτείται ταυτόχρονα ασφάλεια, αξιοπιστία και αποδοτική χρήση των περιορισμένων διαθέσιμων πόρων.

Η σειρά προτύπων ISO/IEC 29192 αποτελεί ένα από τα πρώτα διεθνή πρότυπα που ασχολήθηκαν αποκλειστικά με την lightweight κρυπτογραφία, καλύπτοντας τεχνικές κατάλληλες για συσκευές με περιορισμένους πόρους, όπως έξυπνες κάρτες, αισθητήρες και IoT nodes. Στόχος των προτύπων αυτών είναι να παρέχουν ισορροπία ανάμεσα στην ασφάλεια και την αποδοτικότητα, ώστε οι αλγόριθμοι να μπορούν να υλοποιηθούν τόσο σε περιορισμένο hardware όσο και σε low-power embedded συστήματα.

Στην κατηγορία των block ciphers, το πρότυπο περιλαμβάνει τους PRESENT και CLEFIA. Ο PRESENT είναι ένας block cipher με block μεγέθους 64-bit και κλειδί 80 ή 128-bit, σχεδιασμένος με αρχιτεκτονική SPN (Substitution-Permutation Network). Είναι ιδιαίτερα αποδοτικός σε υλοποιήσεις hardware, με εξαιρετικά μικρό αποτύπωμα της τάξης των ~2000 gates, γεγονός που τον καθιστά ιδανικό για RFID tags και συσκευές με ελάχιστους υπολογιστικούς πόρους. Από την άλλη πλευρά, ο CLEFIA, που προτάθηκε από τη Sony, είναι block cipher με block μεγέθους 128-bit. Παρουσιάζει υψηλή ασφάλεια και καλή απόδοση, ενώ χρησιμοποιείται σε πλήθος embedded συστημάτων, κυρίως σε εφαρμογές όπου απαιτείται ισχυρότερη προστασία δεδομένων.

Στην κατηγορία των stream ciphers, το πρότυπο περιλαμβάνει τους Trivium και Grain-128, δύο αλγόριθμους που έχουν σχεδιαστεί για αποδοτική λειτουργία σε περιορισμένο hardware, προσφέροντας ταχύτητα και χαμηλή κατανάλωση ενέργειας. Για την κατηγορία των hash functions, προτείνονται οι PHOTON και SPONGENT, οι οποίοι χρησιμοποιούν ελαφριές κατασκευές τύπου sponge και είναι σχεδιασμένοι ώστε να παρέχουν επαρκή ασφάλεια με χαμηλό κόστος σε μνήμη και λογική πύλη. Τέλος, στην κατηγορία των Message Authentication Codes (MACs), περιλαμβάνονται οι LightMAC και ALE, οι οποίοι προσφέρουν μηχανισμούς ακεραιότητας και αυθεντικοποίησης δεδομένων με ελάχιστες απαιτήσεις σε υπολογιστικούς πόρους. Έτσι, το ISO/IEC 29192 παρέχει μια ολοκληρωμένη σειρά από lightweight κρυπτογραφικούς αλγόριθμους, καλύπτοντας όλες τις βασικές ανάγκες: κρυπτογράφηση, hashing και αυθεντικοποίηση, πάντα με γνώμονα τη χρήση σε περιβάλλοντα όπου η μνήμη, η ισχύς και η υπολογιστική δυνατότητα είναι περιορισμένα.

Η παραδοσιακή δημόσια κρυπτογραφία, όπως το RSA, θεωρείται σε μεγάλο βαθμό ακατάλληλη για constrained συσκευές, καθώς απαιτεί μεγάλα μήκη κλειδιών και βαριές υπολογιστικές πράξεις, γεγονός που οδηγεί σε υψηλή κατανάλωση ενέργειας και σημαντικές απαιτήσεις μνήμης. Για αυτόν τον λόγο, στο πλαίσιο της lightweight cryptography (LWC), η ερευνητική κοινότητα και οι οργανισμοί τυποποίησης στράφηκαν σε πιο αποδοτικές τεχνικές δημόσιας κρυπτογραφίας. Η σημαντικότερη κατηγορία που χρησιμοποιείται σήμερα είναι η Elliptic Curve Cryptography (ECC), η οποία επιτυγχάνει το ίδιο επίπεδο ασφάλειας με πολύ μικρότερα κλειδιά. Για παράδειγμα, ένα κλειδί ECC 256-bit προσφέρει ασφάλεια αντίστοιχη με ένα RSA κλειδί 3072-bit, μειώνοντας δραματικά τόσο το μέγεθος των δεδομένων που πρέπει να αποθηκευτούν ή να μεταδοθούν όσο και το κόστος των πράξεων. Αυτό καθιστά την ECC ιδιαίτερα ελκυστική για εφαρμογές σε IoT, έξυπνες κάρτες και ασύρματα αισθητήρια δίκτυα.

Πάνω σε αυτή τη βάση έχουν αναπτυχθεί πιο σύγχρονοι αλγόριθμοι, όπως η EdDSA (Edwards-curve Digital Signature Algorithm), που προσφέρει γρήγορη και ασφαλή δημιουργία/επικύρωση ψηφιακών υπογραφών, και το ECDH (Elliptic Curve Diffie–Hellman), το οποίο χρησιμοποιείται για την ασφαλή ανταλλαγή κλειδιών. Τα πρότυπα Curve25519 και Ed25519 έχουν επικρατήσει σε πλήθος εφαρμογών, καθώς προσφέρουν υψηλή ασφάλεια, εξαιρετική ταχύτητα και μικρό overhead, ενώ ταυτόχρονα είναι ανθεκτικά σε διάφορες κατηγορίες επιθέσεων. Με αυτόν τον τρόπο, η Lightweight

Public-Key Cryptography καθιστά δυνατή την ασφαλή αυθεντικοποίηση και την ανταλλαγή κλειδιών ακόμη και σε συσκευές με ελάχιστους πόρους, διασφαλίζοντας ότι το οικοσύστημα του IoT και των embedded συστημάτων μπορεί να λειτουργεί με ασφάλεια χωρίς να θυσιάζει την αποδοτικότητα.

Η ανάγκη για ασφαλείς, αλλά ταυτόχρονα αποδοτικές υλοποιήσεις κρυπτογραφίας οδήγησε στην ανάπτυξη έτοιμων βιβλιοθηκών και εργαλείων που υποστηρίζουν lightweight cryptography σε περιβάλλοντα με περιορισμένους πόρους. Μία από τις πιο γνωστές είναι η TinyCrypt, η οποία σχεδιάστηκε ειδικά για συσκευές με περιορισμένη μνήμη και υπολογιστική ισχύ και ενσωματώνεται εύκολα στο ARM mbed OS. Η TinyCrypt παρέχει βασικούς αλγορίθμους κρυπτογράφησης, hashing και MAC, προσφέροντας αξιόπιστες και ελαφριές λύσεις για embedded εφαρμογές. Άλλη δημοφιλής βιβλιοθήκη είναι η wolfSSL, η οποία προσφέρει υποστήριξη για σύγχρονους lightweight αλγορίθμους όπως ο Ascon και ο ChaCha20-Poly1305. Η wolfSSL χρησιμοποιείται ευρέως σε εφαρμογές IoT και ενσωματωμένα συστήματα, καθώς παρέχει ταυτόχρονα ασφάλεια, χαμηλή κατανάλωση πόρων και ευκολία ενσωμάτωσης σε υπάρχουσες πλατφόρμες. Για πιο εξειδικευμένες ανάγκες Elliptic Curve Cryptography (ECC) σε constrained περιβάλλοντα, το Relic Toolkit προσφέρει ένα ευρύ φάσμα επιλογών, από βασικές πράξεις ECC μέχρι advanced protocols, βελτιστοποιημένα για μικροελεγκτές και άλλες συσκευές με περιορισμένους πόρους. Αυτό καθιστά δυνατή την ασφαλή αυθεντικοποίηση, την ανταλλαγή κλειδιών και την υπογραφή/επικύρωση δεδομένων σε περιβάλλοντα όπου οι παραδοσιακές βιβλιοθήκες θα ήταν υπερβολικά βαριές.

Παράλληλα, πολλές σύγχρονες πλατφόρμες μικροελεγκτών, όπως οι ARM Cortex-M, υποστηρίζουν hardware acceleration για συγκεκριμένους αλγορίθμους, όπως το AES, μειώνοντας σημαντικά το latency και την κατανάλωση ενέργειας. Αυτή η υποστήριξη επιτρέπει την εκτέλεση σύνθετων κρυπτογραφικών πράξεων σε πραγματικό χρόνο χωρίς να επιβαρύνει το κύριο λογισμικό της συσκευής. Συνολικά, οι παραπάνω βιβλιοθήκες και τεχνολογίες καθιστούν τη lightweight cryptography άμεσα εφαρμόσιμη σε πραγματικά συστήματα, επιτρέποντας σε IoT συσκευές, αισθητήρες και άλλες embedded εφαρμογές να λειτουργούν με ασφάλεια και αποδοτικότητα.

Η lightweight cryptography βρίσκει πρακτική εφαρμογή σε πληθώρα συσκευών και συστημάτων όπου η ασφάλεια πρέπει να συνδυάζεται με περιορισμένους πόρους. Στα RFID και NFC συστήματα, για παράδειγμα, χρησιμοποιούνται αλγόριθμοι όπως ο PRESENT και ο Grain για την κρυπτογράφηση και την ταυτοποίηση των χρηστών. Οι συγκεκριμένοι αλγόριθμοι είναι εξαιρετικά αποδοτικοί σε hardware, με μικρή κατανάλωση μνήμης και ενέργειας, επιτρέποντας την ταχεία και ασφαλή επικοινωνία σε συσκευές με ελάχιστους υπολογιστικούς πόρους, όπως κάρτες πρόσβασης και έξυπνες ταυτότητες.

Στον τομέα των smart meters, όπου απαιτείται η ασφαλής μετάδοση δεδομένων κατανάλωσης ενέργειας, χρησιμοποιείται συχνά ο αλγόριθμος Ascon AEAD. Η κρυπτογράφηση με AEAD διασφαλίζει ταυτόχρονα εμπιστευτικότητα και ακεραιότητα των μετρήσεων, ενώ η επικοινωνία υλοποιείται συνήθως πάνω από πρωτόκολλα DTLS over CoAP, που είναι κατάλληλα για constrained περιβάλλοντα IoT. Αυτό εξασφαλίζει ότι τα δεδομένα των χρηστών παραμένουν προστατευμένα από υποκλοπές ή τροποποιήσεις κατά τη μεταφορά τους προς τους παρόχους ενέργειας.

Στον ιατρικό τομέα, ειδικά σε Medical IoT Devices όπως εμφυτεύσιμους αισθητήρες ή φορητές συσκευές υγείας, η ασφάλεια είναι κρίσιμη λόγω της ευαίσθητης φύσης των δεδομένων. Εδώ χρησιμοποιείται η Elliptic Curve Cryptography (ECC), και συγκεκριμένα η Curve25519, για ασφαλή ανταλλαγή κλειδιών μεταξύ των συσκευών. Η χρήση ECC επιτρέπει μικρότερα κλειδιά και χαμηλότερη υπολογιστική επιβάρυνση σε σύγκριση με παραδοσιακά συστήματα RSA, διασφαλίζοντας παράλληλα

υψηλή ασφάλεια, ταχύτητα και αξιοπιστία στην επικοινωνία μεταξύ ιατρικών συσκευών και εφαρμογών παρακολούθησης υγείας.

4.2.3 Object Security for Constrained RESTful Environments - Ασφάλεια Αντικειμένων για Περιορισμένα RESTful Περιβάλλοντα (OSCORE)

Το OSCORE αποτελεί πρότυπο (RFC 8613) για την ασφάλεια εφαρμογών IoT που χρησιμοποιούν το CoAP, ένα RESTful πρωτόκολλο ειδικά σχεδιασμένο για συσκευές με περιορισμένους πόρους. Η βασική καινοτομία του OSCORE είναι ότι παρέχει end-to-end ασφάλεια σε επίπεδο εφαρμογής, ανεξάρτητα από το underlying transport protocol (UDP, DTLS, ή ακόμη και proxy relay), διασφαλίζοντας εμπιστευτικότητα, ακεραιότητα και προστασία κατά των replay attacks για κάθε CoAP message. [14]

Το OSCORE υιοθετεί μια διαφορετική προσέγγιση σε σχέση με το DTLS, παρέχοντας ασφάλεια όχι σε επίπεδο transport (point-to-point), αλλά directly πάνω στα μηνύματα CoAP. Αυτό σημαίνει ότι κάθε μήνυμα κρυπτογραφείται και υπογράφεται ανεξάρτητα, εξασφαλίζοντας ότι η ασφάλεια δεν περιορίζεται μόνο στη σύνδεση μεταξύ δύο κόμβων, αλλά επεκτείνεται σε όλη τη διαδρομή του μηνύματος. Έτσι, ακόμη και αν τα μηνύματα περάσουν μέσω intermediaries, όπως proxy nodes ή gateways, η εμπιστευτικότητα και η ακεραιότητά τους παραμένουν διασφαλισμένες, καθώς οι ενδιάμεσοι κόμβοι μπορούν να προωθούν τα μηνύματα χωρίς να έχουν πρόσβαση στο περιεχόμενο. Για την κρυπτογράφηση και την επικύρωση των μηνυμάτων, το OSCORE χρησιμοποιεί lightweight AEAD ciphers (Authenticated Encryption with Associated Data), όπως οι AES-CCM και ChaCha20-Poly1305. Αυτοί οι αλγόριθμοι επιτρέπουν την ταυτόχρονη διασφάλιση εμπιστευτικότητας και ακεραιότητας, ενώ παραμένουν αποδοτικοί ακόμη και σε περιορισμένους κόμβους, όπως αισθητήρες και μικροελεγκτές IoT. Το AEAD παρέχει την πρόσθετη δυνατότητα προστασίας των επικεφαλίδων των μηνυμάτων (associated data), εξασφαλίζοντας ότι κρίσιμα μεταδεδομένα δεν μπορούν να τροποποιηθούν χωρίς ανίχνευση. Η προσέγγιση του OSCORE, συνδυάζοντας end-to-end ασφάλεια με αποδοτικούς αλγορίθμους, το καθιστά ιδανικό για περιβάλλοντα IoT και constrained συσκευές, όπου η ασφάλεια πρέπει να παρέχεται χωρίς να επιβαρύνεται σημαντικά η υπολογιστική ισχύς ή η κατανάλωση ενέργειας. Αυτή η αρχιτεκτονική επιτρέπει τη δημιουργία ασφαλών, scalable και ελαφριών εφαρμογών στο Internet of Things, ενώ ταυτόχρονα υποστηρίζει ευέλικτες διαδρομές μηνυμάτων μέσω διαμεσολαβητών χωρίς συμβιβασμούς στην ασφάλεια.

Το OSCORE παρέχει ασφάλεια σε κάθε CoAP μήνυμα μέσω μιας σειράς τεχνικών βημάτων που εξασφαλίζουν εμπιστευτικότητα, ακεραιότητα και προστασία από replay attacks. Αρχικά, στο στάδιο του Key Derivation, από ένα κοινό master key που μοιράζονται ο client και ο server παράγονται context-specific keys για κάθε session ή ακόμη και για κάθε μήνυμα. Αυτή η διαδικασία εξασφαλίζει ότι κάθε μήνυμα χρησιμοποιεί μοναδικά κλειδιά, περιορίζοντας τον κίνδυνο εκμετάλλευσης ενός συμβιβασμένου κλειδιού σε μελλοντικά μηνύματα και ενισχύοντας την ασφάλεια end-to-end. Στη συνέχεια, πραγματοποιείται η Message Encryption. Το κύριο μέρος του CoAP μηνύματος, δηλαδή το payload, κρυπτογραφείται χρησιμοποιώντας AEAD αλγόριθμους όπως AES-CCM ή ChaCha20-Poly1305. Επιπλέον, ορισμένα header fields του CoAP, όπως το URI Path ή το Content-Format, ενσωματώνονται ως Associated Data στην AEAD λειτουργία. Αυτό διασφαλίζει ότι κρίσιμα μεταδεδομένα παραμένουν αμετάβλητα κατά τη μεταφορά, προσφέροντας ακεραιότητα πέρα από το ίδιο το payload.Για την Replay Protection, κάθε μήνυμα περιέχει sequence numbers, γνωστά και ως Partial IVs, τα οποία επιτρέπουν στον παραλήπτη να ανιχνεύει και να απορρίπτει επαναλαμβανόμενα ή καθυστερημένα πακέτα. Αυτό είναι κρίσιμο σε περιβάλλοντα IoT, όπου τα δίκτυα μπορεί να έχουν

καθυστερήσεις, απώλειες ή επανατάξεις πακέτων, εξασφαλίζοντας ότι δεν μπορεί να επαναχρησιμοποιηθεί ένα παλιό μήνυμα για κακόβουλους σκοπούς.

Τέλος, στο στάδιο της Serialization, το κρυπτογραφημένο payload αντικαθιστά το αρχικό CoAP payload, ενώ τα header fields που χρησιμοποιήθηκαν ως Associated Data μεταφέρονται μέσω ειδικών OSCORE options. Αυτό επιτρέπει στη συσκευή εφαρμογής να παραμείνει συμβατή με proxy nodes και gateways, καθώς τα μηνύματα μπορούν να προωθηθούν χωρίς αποκρυπτογράφηση, διατηρώντας παράλληλα πλήρως την ασφάλεια end-to-end. Αυτή η ολοκληρωμένη διαδικασία καθιστά το OSCORE μια αποδοτική και ασφαλή λύση για constrained περιβάλλοντα IoT, όπου η προστασία των δεδομένων πρέπει να συνδυάζεται με χαμηλή κατανάλωση πόρων και πλήρη λειτουργική συμβατότητα.

Στον τομέα του Smart Home IoT, το OSCORE χρησιμοποιείται για την ασφαλή επικοινωνία μεταξύ έξυπνων συσκευών και cloud εφαρμογών. Για παράδειγμα, ένας έξυπνος θερμοστάτης λαμβάνει κρυπτογραφημένα commands από την cloud εφαρμογή μέσω OSCORE. Ένας proxy gateway μπορεί να δρομολογεί αυτά τα μηνύματα, χωρίς να έχει πρόσβαση στο plaintext περιεχόμενο, διασφαλίζοντας έτσι την εμπιστευτικότητα και την ακεραιότητα των δεδομένων ακόμη και όταν τα μηνύματα περνούν από ενδιάμεσα δίκτυα. Αυτή η προσέγγιση επιτρέπει την υλοποίηση ασφαλών smart home συστημάτων χωρίς να απαιτείται κάθε συσκευή να συνδέεται άμεσα στην cloud υπηρεσία ή να διαχειρίζεται πλήρη DTLS sessions.

Στον τομέα του Smart Grid / Energy IoT, τα meter nodes στέλνουν τις μετρήσεις κατανάλωσης ενέργειας σε έναν κεντρικό data collector χρησιμοποιώντας OSCORE. Με αυτόν τον τρόπο, εξασφαλίζεται ότι κανένα ενδιάμεσο δίκτυο ή gateway δεν μπορεί να παραποιήσει ή να διαβάσει τα δεδομένα, διατηρώντας την ασφάλεια των κρίσιμων ενεργειακών πληροφοριών. Η χρήση OSCORE επιτρέπει την end-to-end προστασία των δεδομένων, ενώ η ελαφριά κρυπτογράφηση περιορίζει την επιβάρυνση σε συσκευές με περιορισμένους πόρους.

Στον Industrial IoT, όπου μεγάλος αριθμός αισθητήρων λειτουργεί σε παραγωγικές γραμμές, το OSCORE χρησιμοποιείται για end-to-end ασφάλεια των δεδομένων που αποστέλλονται από τους αισθητήρες στο κεντρικό σύστημα ελέγχου. Σε αντίθεση με πλήρη DTLS connections για κάθε συσκευή, που θα προκαλούσαν σημαντικό overhead σε υπολογιστική ισχύ και δίκτυο, η χρήση OSCORE επιτρέπει την προστασία των μηνυμάτων με χαμηλότερο κόστος, διατηρώντας ταυτόχρονα υψηλά επίπεδα ασφάλειας και αξιοπιστίας.

Με αυτόν τον τρόπο, το OSCORE αποδεικνύεται ιδιαίτερα αποδοτικό για εφαρμογές IoT, προσφέροντας ασφάλεια end-to-end, συμβατότητα με intermediaries και χαμηλή επιβάρυνση σε περιορισμένους κόμβους.

Το OSCORE προσφέρει πολλαπλά πλεονεκτήματα, καθιστώντας το ιδιαίτερα κατάλληλο για constrained nodes και δίκτυα IoT. Παρέχει end-to-end ασφάλεια, διασφαλίζοντας την εμπιστευτικότητα και την ακεραιότητα των μηνυμάτων ανεξάρτητα από ενδιάμεσους κόμβους ή proxy. Είναι πλήρως συμβατό με RESTful αρχιτεκτονικές και υποστηρίζει τη χρήση CoAP proxy relay, επιτρέποντας την ασφαλή δρομολόγηση μηνυμάτων χωρίς αποκρυπτογράφηση. Επιπλέον, το OSCORE έχει χαμηλό overhead τόσο σε επίπεδο bytes όσο και σε υπολογιστική ισχύ, καθιστώντας το ιδανικό για μικροελεγκτές με περιορισμένη μνήμη RAM ή Flash. Τέλος, παρέχει replay protection χωρίς να απαιτεί συνεδρίες ή stateful transport, χρησιμοποιώντας sequence numbers σε κάθε μήνυμα. Παρά τα πλεονεκτήματα αυτά, υπάρχουν και ορισμένοι περιορισμοί. Το OSCORE δεν προστατεύει τα transport layer metadata, όπως τα IP headers, γεγονός που σημαίνει ότι ενδιάμεσοι παρατηρητές μπορούν να δουν πληροφορίες όπως διευθύνσεις και αριθμούς θυρών. Επιπλέον, απαιτείται προ-κοινό κλειδί ή κάποιο

μηχανισμός διαχείρισης κλειδιών, όπως τα EDHOC ή το ACE framework, για την ασφαλή εγκαθίδρυση session keys. Τέλος, η διαχείριση των sequence numbers σε μεγάλα δίκτυα μπορεί να απαιτεί επιπλέον state management για κάθε κόμβο, αυξάνοντας την πολυπλοκότητα σε μεγάλα ή δυναμικά περιβάλλοντα IoT.

4.2.4 End-to-End Encryption & Identity Management σε IoT - Κρυπτογράφηση από Άκρο σε Άκρο & Διαχείριση Ταυτότητας στο IoT (E2EE)

Η E2EE αποτελεί κρίσιμο μηχανισμό ασφάλειας για συσκευές IoT, διασφαλίζοντας ότι τα δεδομένα παραμένουν κρυπτογραφημένα από την πηγή μέχρι τον τελικό αποδέκτη, ακόμη και όταν διακινούνται μέσω ενδιάμεσων nodes ή cloud πλατφόρμες. Η χρήση της E2EE σε IoT περιβάλλοντα απαιτεί στενή σύνδεση με Identity Management (IdM) συστήματα, ώστε να εξασφαλίζεται η αυθεντικοποίηση των συμμετεχόντων, η ανάθεση δικαιωμάτων και η διαχείριση κλειδιών. Στα IoT περιβάλλοντα, η E2EE βασίζεται συνήθως σε έναν συνδυασμό συμμετρικής και ασύμμετρης κρυπτογράφησης, ώστε να διασφαλίζεται η εμπιστευτικότητα και η ακεραιότητα των δεδομένων ακόμη και σε constrained συσκευές. Για το payload των μηνυμάτων, οι συσκευές χρησιμοποιούν συμμετρικούς αλγορίθμους όπως AES (128 ή 256-bit) ή ChaCha20, οι οποίοι είναι ταχύτατοι και αποδοτικοί σε μικροελεγκτές και άλλες συσκευές με περιορισμένους πόρους. Τα session keys για την κρυπτογράφηση του payload παράγονται μέσω πρωτοκόλλων key exchange, όπως το Elliptic Curve Diffie–Hellman (ECDH), επιτρέποντας την ασφαλή κοινή χρήση κλειδιών μεταξύ των συσκευών χωρίς να μεταφέρονται απευθείας στο δίκτυο. [15]

Η ασύμμετρη κρυπτογραφία χρησιμοποιείται για τη διαχείριση των κλειδιών και την αυθεντικοποίηση των συσκευών. Κάθε IoT device διαθέτει ένα public/private key pair, όπως Ed25519 ή P-256 ECC, όπου τα public keys καταχωρούνται σε ένα trusted registry ή PKI, ενώ οι private keys παραμένουν αποθηκευμένες τοπικά στη συσκευή, διασφαλίζοντας ότι μόνο η ίδια μπορεί να δημιουργήσει ψηφιακές υπογραφές ή να αποκρυπτογραφήσει μηνύματα. Για την ασφαλή παραγωγή των session keys χρησιμοποιούνται authenticated key exchange πρωτόκολλα, όπως το EDHOC (Ephemeral Diffie–Hellman Over COSE) ή οι μηχανισμοί key exchange του TLS 1.3. Αυτά τα πρωτόκολλα εξασφαλίζουν Perfect Forward Secrecy (PFS), δηλαδή ακόμη και αν ένα session key παραβιαστεί στο μέλλον, οι προηγούμενες επικοινωνίες παραμένουν προστατευμένες. Με αυτόν τον τρόπο, η E2EE σε IoT συνδυάζει υψηλή ασφάλεια με αποδοτικότητα, επιτρέποντας τη λειτουργία σε περιορισμένα και κατανεμημένα περιβάλλοντα.

Το Identity Management (IdM) σε IoT αποτελεί βασικό στοιχείο για την ασφάλεια των κατανεμημένων συσκευών και δικτύων. Κάθε κόμβος (device) αποκτά μια μοναδική ταυτότητα, η οποία συνήθως υλοποιείται μέσω credentials όπως X.509 certificates, raw public keys ή COSE keys. Αυτή η μοναδική ταυτότητα επιτρέπει τον έλεγχο και την παρακολούθηση των συσκευών στο δίκτυο, διασφαλίζοντας ότι μόνο αναγνωρισμένοι και εξουσιοδοτημένοι κόμβοι μπορούν να συμμετέχουν στην επικοινωνία.

Μέρος του IdM είναι και ο έλεγχος πρόσβασης (Access Control). Οι πολιτικές πρόσβασης καθορίζουν ποιοι clients ή servers έχουν δικαίωμα να διαβάζουν ή να γράφουν δεδομένα από κάθε συσκευή. Αυτό είναι κρίσιμο σε περιβάλλοντα IoT, όπου διαφορετικές συσκευές και εφαρμογές μπορεί να χρειάζονται διαφορετικά επίπεδα πρόσβασης σε δεδομένα, όπως σε smart home, smart grid ή industrial IoT συστήματα. Το IdM περιλαμβάνει επίσης το Key Lifecycle Management, που αφορά τη δημιουργία, ανανέωση και ανάκληση κλειδιών σε μεγάλης κλίμακας IoT δίκτυα. Η διαχείριση των κλειδιών είναι κρίσιμη για τη διατήρηση της ασφάλειας σε όλα τα στάδια ζωής των συσκευών, από την

αρχική εγκατάσταση μέχρι την απόσυρση ή αντικατάσταση μιας συσκευής. Στην πράξη, η εφαρμογή του IdM συνδυάζει διάφορες τεχνολογίες. Η Public Key Infrastructure (PKI), ή σε περιβάλλοντα με περιορισμένους πόρους μια lightweight PKI, παρέχει τις βάσεις για ασφαλή διανομή και επαλήθευση δημόσιων κλειδιών. Για την εξουσιοδότηση και τον έλεγχο πρόσβασης σε RESTful APIs, χρησιμοποιούνται πλαίσια όπως το OAuth 2.0 ή το ACE framework (Authentication and Authorization for Constrained Environments). Τέλος, για συσκευές που απαιτούν υψηλή ασφάλεια, η αποθήκευση κλειδιών υλοποιείται σε Hardware Security Modules (HSMs) ή Secure Elements, εξασφαλίζοντας ότι τα κλειδιά παραμένουν προστατευμένα ακόμη και αν η συσκευή παραβιαστεί. Με αυτόν τον τρόπο, το IdM σε IoT παρέχει μια ολοκληρωμένη υποδομή για την αυθεντικοποίηση, εξουσιοδότηση και ασφαλή διαχείριση κλειδιών, επιτρέποντας ασφαλή και αξιόπιστη λειτουργία των συσκευών σε μεγάλης κλίμακας κατανεμημένα δίκτυα.

Στον τομέα του Smart Home IoT, οι έξυπνοι αισθητήρες και οι συσκευές επικοινωνούν συνεχώς με τον cloud controller, αποστέλλοντας δεδομένα που κρυπτογραφούνται end-to-end. Η αυθεντικοποίηση των συσκευών γίνεται μέσω device certificates, διασφαλίζοντας ότι μόνο οι αναγνωρισμένοι κόμβοι μπορούν να συμμετάσχουν στην επικοινωνία. Το Building Management System (BMS) αποκρυπτογραφεί τα μηνύματα μόνο για τις εξουσιοδοτημένες συσκευές, προστατεύοντας τα προσωπικά και ευαίσθητα δεδομένα των χρηστών από μη εξουσιοδοτημένη πρόσβαση ή ενδιάμεσους κόμβους που δρομολογούν τα μηνύματα. Αυτή η προσέγγιση διασφαλίζει την εμπιστευτικότητα, την ακεραιότητα και την αυθεντικότητα των δεδομένων σε ένα περιβάλλον με πολλά κατανεμημένα και περιορισμένα σε πόρους nodes.

Στον IIoT, οι βιομηχανικοί αισθητήρες, τα robot arms και οι controllers επικοινωνούν μεταξύ τους μέσω E2EE για την ασφαλή ανταλλαγή commands και δεδομένων κατά τη λειτουργία της παραγωγικής γραμμής. Αυτό προστατεύει τα συστήματα από malicious insiders και επιθέσεις στο δίκτυο, διασφαλίζοντας ότι μόνο τα αξιόπιστα nodes μπορούν να εκτελέσουν κρίσιμες εντολές. Η εφαρμογή του Identity Management μέσω PKI εγγυάται ότι μόνο οι εγκεκριμένες συσκευές έχουν δικαίωμα συμμετοχής στην επικοινωνία, αποτρέποντας μη εξουσιοδοτημένη πρόσβαση και συμβάλλοντας στη συνολική ασφάλεια του βιομηχανικού περιβάλλοντος.

Στον τομέα του Healthcare IoT, τα wearable sensors και τα implantable devices συλλέγουν και μεταδίδουν βιοϊατρικά δεδομένα, όπως καρδιολογικές μετρήσεις ή επίπεδα γλυκόζης, σε ασφαλή ιατρικά συστήματα. Τα δεδομένα μεταφέρονται με end-to-end encryption, διασφαλίζοντας ότι μόνο οι εξουσιοδοτημένοι ιατροί ή εφαρμογές μπορούν να τα αποκρυπτογραφήσουν και να τα επεξεργαστούν. Η χρήση Identity Management εγγυάται ότι οι πληροφορίες παραμένουν προστατευμένες ακόμη και σε κατανεμημένα δίκτυα, εξασφαλίζοντας ότι οι ευαίσθητες ιατρικές πληροφορίες δεν θα παραβιαστούν ή υποκλαπούν από μη εξουσιοδοτημένα συστήματα ή χρήστες.

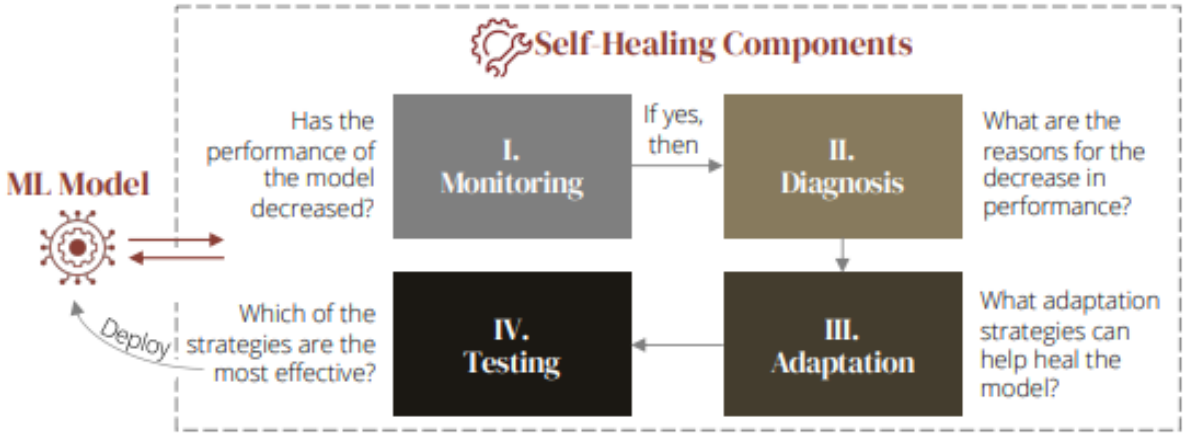
Με αυτόν τον τρόπο, η συνδυαστική χρήση E2EE και IdM σε IoT περιβάλλοντα επιτρέπει την ασφαλή λειτουργία συσκευών σε ποικίλα σενάρια – από έξυπνα σπίτια και βιομηχανικές εγκαταστάσεις μέχρι κρίσιμες εφαρμογές υγείας – παρέχοντας προστασία των δεδομένων, έλεγχο ταυτότητας και αυθεντικοποίηση των κόμβων.

Κεφάλαιο 5ο: Μοντέλα Αυτοΐασης στηριζόμενα στη Μηχανική Μάθηση

5.1 Εισαγωγή

Η έννοια του self-healing στα συστήματα πληροφορικής και ειδικότερα στο IoT αναφέρεται στην ικανότητα ενός συστήματος να ανιχνεύει δυσλειτουργίες, να τις διαγιγνώσκει και να τις επιδιορθώνει με ή χωρίς την ανθρώπινη παρέμβαση. Καθώς οι υποδομές των συστημάτων IoT αυξάνονται σε κλίμακα και πολυπλοκότητα, γίνεται επιτακτική η ανάγκη για τη χρήση έξυπνων μηχανισμών αυτοΐασης. Οι κλασικές προσεγγίσεις - τεχνικές, αν και σημαντικές, συχνά δεν επαρκούν σε περιβάλλοντα όπου οι βλάβες είναι απρόβλεπτες και ο όγκος δεδομένων είναι τεράστιος και διαδίδονται με τεράστια ταχύτητα [32].

Η Μηχανική Μάθηση (Machine Learning – ML) εισάγει μια νέα διάσταση στην αυτοΐαση, καθώς παρέχει στο σύστημα τη δυνατότητα της «εκμάθησης» από το παρελθόν, δηλαδή υπάρχει η δυνατότητα να μπορεί να αναγνωρίζει μοτίβα και εν συνεχεία να λαμβάνει αποφάσεις σε πραγματικό χρόνο. Εν αντιθέσει με τα στατικά μοντέλα, τα μοντέλα ML μπορούν να εξελίσσονται και να γίνονται πιο προσαρμοστικά, ανθεκτικά και ικανότερα στο να αντιμετωπίσουν ακόμα και άγνωστες μορφές δυσλειτουργιών. Η συμβολή αυτή έχει τεκμηριωθεί εκτενώς στη βιβλιογραφία, όπου αναλύονται προσεγγίσεις που κυμαίνονται από απλή ανίχνευση ανωμαλιών μέχρι προηγμένα πλαίσια ενισχυτικής μάθησης [33], [34].



Σχήμα 5.1: Κύρια συστατικά ενός Self-Healing ML συστήματος: Monitoring, Diagnosis, Adaptation, Testing (Rauba et al. 2024) [32].

5.2 Κατηγορίες Μοντέλων ML για Αυτοΐαση

Η εφαρμογή ML στην αυτοΐαση διακρίνεται σε διάφορες κατηγορίες, οι οποίες αντανακλούν διαφορετικά επίπεδα ευφυΐας και αυτονομίας. οι οποίες αντανακλούν διαφορετικά επίπεδα ευφυΐας και αυτονομίας. Οι κατηγορίες αυτές περιλαμβάνουν μοντέλα ανίχνευσης ανωμαλιών, προβλεπτικά μοντέλα, μοντέλα ενισχυτικής μάθησης και υβριδικά σχήματα τα οποία θα αναλύονται παρακάτω:

5.2.1 Μοντέλα Ανίχνευσης Ανωμαλιών

Η ανίχνευση ανωμαλιών (anomaly detection) είναι κρίσιμη, καθώς οι περισσότερες βλάβες εκδηλώνονται αρχικά μέσα από μικρές αποκλίσεις στη συμπεριφορά του συστήματος. Οπότε ο βασικός

στόχος αποτελεί την αρχική αναγνώριση τυχόν αποκλίσεων από την κανονική λειτουργία του συστήματος, αντιλαμβανόμενο πως υπάρχει κάποια ένδειξη βλάβης ή απειλής.

Μοντέλα όπως τα clustering (π.χ. K-means, DBSCAN), One-Class SVM και Isolation Forest χρησιμοποιούνται σε περιβάλλοντα όπου δεν υπάρχουν επαρκή δεδομένα με ετικέτες (label data). Παράλληλα, οι autoencoders και οι παραλλαγές τους αλγόριθμοι υποστήριξης διανυσμάτων (Variational Autoencoders) έχουν αποδειχθεί εξαιρετικά αποτελεσματικοί στην ανάλυση χρονοσειρών και τη διάγνωση αποκλίσεων. Για παράδειγμα, σε IoT δίκτυα αισθητήρων τέτοιες τεχνικές που παρακολουθούν περιβαλλοντικές συνθήκες, η ML μπορεί να εντοπίσει τους αισθητήρες που παρουσιάζουν αποκλίσεις από τα φυσιολογικά δεδομένα, υποδεικνύοντας βλάβη ή κακόβουλη αλλοίωση [32]. Τα μοντέλα αυτά μπορούν να λειτουργούν σε πραγματικό χρόνο και να παρέχουν alerts, τα οποία ενεργοποιούν μηχανισμούς αυτοΐασης. Επίσης, η χρήση ερμηνευτικών μεθόδων (π.χ. SHAP, LIME) επιτρέπει την καλύτερη κατανόηση των αιτίων της ανωμαλίας, αυξάνοντας την εμπιστοσύνη στα συστήματα.

Επιπλέον, τα μοντέλα χωρίς επίβλεψη (unsupervised models) προσφέρουν πλεονέκτημα σε περιβάλλοντα όπου δεν υπάρχουν επαρκή επισημασμένα δεδομένα για εκπαίδευση, δηλαδή η έλλειψη δεδομένων μπορούν να προσφέρουν σε ένα απλοποιημένο σύστημα που δε χρησιμοποιεί ML καλύτερα αποτελέσματα.

5.2.2 Μοντέλα Πρόβλεψης και Πρόληψης Βλαβών

Η πρόληψη είναι εξίσου σημαντική με τη θεραπεία. Μέσω προγνωστικών μοντέλων (predictive analytics), συστήματα ML αναλύουν ιστορικά δεδομένα και προβλέπουν επικείμενες βλάβες ώστε να προγραμματίσουν εγκαίρως ενέργειες συντήρησης. Αλγόριθμοι όπως Random Forests, Gradient Boosting και Recurrent Neural Networks (RNNs) χρησιμοποιούνται ευρέως σε εφαρμογές προληπτικής συντήρησης (predictive maintenance).

Σε βιομηχανικά IoT, τα μοντέλα προληπτικής συντήρησης (predictive maintenance) έχουν μειώσει το κόστος λειτουργίας και συντήρησης, ενώ ταυτόχρονα έχουν αυξήσει τον χρόνο ζωής του εξοπλισμού, καθώς επίσης και στα δίκτυα υγείας (MIoT) επιτρέπουν την έγκαιρη συντήρηση ιατρικών συσκευών [33]. Επίσης, σε cloud-native περιβάλλοντα τα μοντέλα πρόβλεψης εφαρμόζονται στην παρακολούθηση containers και microservices και με την συλλογή logs και metrics δίνεται η δυνατότητα στα ML μοντέλα να προβλέψουν μέσω του εντοπισμού προτύπων συμπεριφοράς πότε μια υπηρεσία θα οδηγηθεί δυσλειτουργία ή θα παρουσιάσει σφάλματα, και με τη χρήση προληπτικών μέτρων, όπως scaling ή επανεκκίνηση, να αποτραπεί η διακοπή των υπηρεσιών.

5.2.3 Ενισχυτική Μάθηση (Reinforcement Learning – RL)

Η RL αντιπροσωπεύει μια από τις πιο προηγμένες προσεγγίσεις. Αντί να βασίζεται σε προκαθορισμένα δεδομένα, επιτρέπει στο σύστημα να «δοκιμάζει» ενέργειες (π.χ. restart, rollback, scaling) και λαμβάνει ανταμοιβές ανάλογα με το αποτέλεσμα, εκπαιδεύοντας έτσι το σύστημα να μαθαίνει από τις συνέπειες. Σε αυτοΐατα συστήματα όταν η αβεβαιότητα είναι υψηλή, και η κλασική ανάλυση δεν επαρκεί, η RL μπορεί να χρησιμοποιηθεί για βέλτιστη κατανομή πόρων, δυναμική αναδιάρθρωση υπηρεσιών και αυτόματη αποκατάσταση από επιθέσεις. Για παράδειγμα, σε δίκτυα edge, ένας agent μπορεί να μάθει πότε είναι βέλτιστο να μεταφέρει φόρτο σε άλλο κόμβο για να αποφευχθεί υπερφόρτωση ή αστοχία. Παράλληλα, η RL μπορεί να χρησιμοποιηθεί σε multi-agent συστήματα, όπου πράκτορες συνεργάζονται για την αποκατάσταση σε κατανεμημένα περιβάλλοντα [32], [34]. Παράδειγμα αποτελεί η χρήση Q-learning σε edge nodes για επιλογή της βέλτιστης πολιτικής

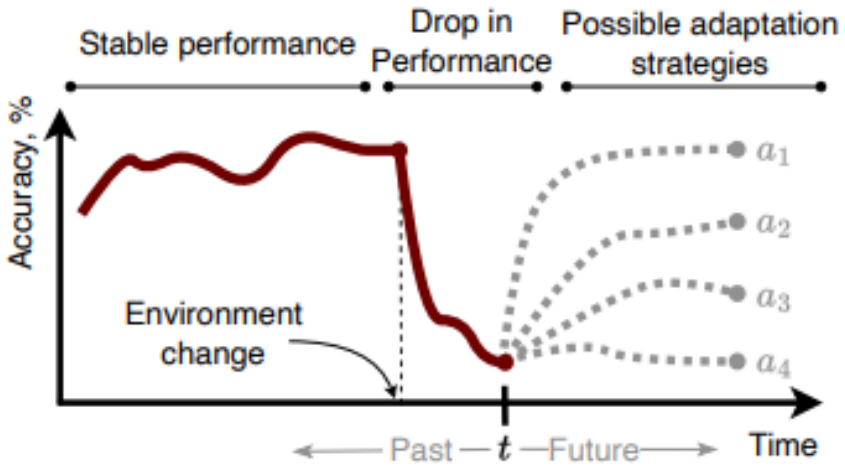
αποκατάστασης με βάση το ιστορικό απόδοσης και τα τρέχοντα metrics. Τέλος, η εφαρμογή RL απαιτεί προσοχή σε θέματα ασφάλειας και sample efficiency, καθώς η λανθασμένη εκπαίδευση μπορεί να οδηγήσει σε ανεπιθύμητες ενέργειες και σημαντικό ρόλο παίζουν οι τεχνικές ασφαλούς μάθησης (safe RL).

5.2.4 Υβριδικά Μοντέλα ML

Στην πράξη, συχνά απαιτείται συνδυασμός διαφορετικών μεθόδων αφού ένα μοντέλο μπορεί να μην καλύψει τις ανάγκες. Τα υβριδικά μοντέλα ενώνουν την ισχύ της ανίχνευσης ανωμαλιών, της πρόβλεψης και της RL (π.χ. anomaly detection + prediction + RL), ώστε να καλύψουν ένα πλήρες φάσμα σεναρίων. Παρόλο που η ανάπτυξή τους είναι πολύπλοκη, τα υβριδικά μοντέλα προσφέρουν ισχυρή ακρίβεια και ευελιξία. Ένα παράδειγμα είναι η χρήση deep learning σε συνδυασμό με multi-agent RL συστήματα για τη διαχείριση της αποκατάστασης [33]. Επίσης, η συνδυαστική χρήση federated learning με anomaly detection επιτρέπει σε διαφορετικούς κόμβους να συνεργάζονται χωρίς να ανταλλάσσουν τα ευαίσθητα δεδομένα τους, κάτι το οποίο αποτελεί ιδιαίτερα σημαντικό όταν πρόκειται για εφαρμογές υγείας και βιομηχανίας..

5.3 Αρχιτεκτονικές και Πλαίσια Εφαρμογής

Η απόδοση και η πραγματική χρησιμότητα των μοντέλων ML στην αυτοΐαση εξαρτάται σε μεγάλο βαθμό από την αρχιτεκτονική και το πλαίσιο μέσα στο οποίο αυτά ενσωματώνονται. Η αρχιτεκτονική καθορίζει τον τρόπο με τον οποίο συλλέγονται, επεξεργάζονται και αναλύονται τα δεδομένα, καθώς και τον τρόπο με τον οποίο ενεργοποιούνται οι μηχανισμοί αποκατάστασης. Διαφορετικές αρχιτεκτονικές καλύπτουν διαφορετικές ανάγκες σε όρους υπολογιστικής ισχύος, χρόνου απόκρισης και κλίμακας. Παρακάτω θα αναλυθούν οι αρχιτεκτονικές που έχουν εντοπιστεί:



Σχήμα 5.2: Παράδειγμα στρατηγικών προσαρμογής μετά από πτώση απόδοσης μοντέλου (Rauba et al. 2024) [1]

5.3.1 Cloud-native αυτοΐαση

Η προσέγγιση του cloud-native χαρακτηρίζεται από τη χρήση κεντρικών υποδομών (cloud servers, data centers) προκειμένου να γίνει εκπαίδευση και να χρησιμοποιούνται πολύπλοκα μοντέλα ML. Η άφθονη υπολογιστική ισχύς των data centers, η εύκολη πρόσβαση σε μεγάλα datasets και η δυνατότητα συνεχούς ενημέρωσης των μοντέλων επιτρέπει την αξιοποίηση πολύπλοκων deep learning

μοντέλων. Σε σύγχρονα (containerized) περιβάλλοντα, όπως το Kubernetes, μηχανισμοί ML ενσωματώνονται στα εργαλεία παρακολούθησης, ελέγχουν τις εγγραφές (logs) των pods και μέσω των προβλέψεων τους ενεργοποιούν μηχανισμούς αυτοΐασης, όπως αυτόματη επανεκκίνηση ή scaling. Ωστόσο, η εξάρτηση από το cloud μπορεί να οδηγήσει σε καθυστερήσεις (latency) καθώς και σε κόστος μεταφοράς των δεδομένων αυτών, όπου ορισμένες εφαρμογές, όπως πχ. την υγεία, τα αυτόνομα οχήματα ή την αεροναυπηγική στα συστήματα των αεροπλάνων, οι επιπλοκές αυτές δεν είναι ανεκτές και μπορούν να αποβούν μοιραίες. Ως εκ τούτου η αποκλειστική χρήση cloud native εφαρμογών δεν είναι εφαρμόσιμη παντού. [33].

5.3.2 Edge-based αυτοΐαση

Για εφαρμογές που απαιτούν απόκριση σε πραγματικό χρόνο, η αυτοΐαση μεταφέρεται στο άκρο του δικτύου. Η ML εφαρμόζεται τοπικά σε edge ή fog κόμβους, ώστε οι αποφάσεις να λαμβάνονται κοντά στις συσκευές, μειώνοντας κατ' αυτόν τον τρόπο την ανάγκη επικοινωνίας με το cloud και άρα τον χρόνο απόκρισης [34]. Έτσι, πχ. σε ένα δίκτυο αυτόνομων οχημάτων οι αποφάσεις αποκατάστασης λαμβάνονται τοπικά, μειώνοντας τον χρόνο αντίδρασης.

Παραδείγματος χάριν, σε ένα έξυπνο εργοστάσιο IIoT, οι edge κόμβοι μπορούν να εντοπίζουν σε κλάσματα δευτερολέπτου ανωμαλίες σε μηχανές και να ενεργοποιούν διορθωτικές ενέργειες κοντά στις μηχανές ώστε να μην προλάβουν να προκληθούν σοβαρές ζημιές.

Η αρχιτεκτονική edge βελτιώνει την αυτονομία σε περιβάλλοντα με περιορισμένη συνδεσιμότητα, όπως αγροτικές περιοχές ή αυτόνομα drones, όμως η περιορισμένη υπολογιστική ισχύς των edge συσκευών καθιστά απαραίτητη την ανάπτυξη ελαφρών και αποδοτικών μοντέλων ML.

5.3.3 Κατανεμημένα Multi-Agent Συστήματα (MAS)

Σε μεγάλης κλίμακας και ετερογενή περιβάλλοντα IoT, η χρήση κατανεμημένων multi-agent συστημάτων αποτελεί μια ιδιαίτερα αποτελεσματική αρχιτεκτονική. Σε αυτά τα συστήματα, πολλοί πράκτορες (agents), καθένας με περιορισμένες δυνατότητες ML, συνεργάζονται για την ανίχνευση και αποκατάσταση βλαβών. Η συνεργατική αυτή μάθηση καθιστά το σύστημα πιο ανθεκτικό σε κατανεμημένες επιθέσεις [32].

Παράλληλα, η προσέγγιση αυτή είναι ανθεκτική σε επιθέσεις και βλάβες, καθώς η αποτυχία ενός πράκτορα δεν οδηγεί σε συνολική κατάρρευση. Έτσι, η χρήση MAS συστημάτων επιτρέπει στους πράκτορες την αυτόνομη λήψη αποφάσεων με βάση τοπικές συνθήκες και την ανταλλαγή εμπειρίας που μοιράζονται με τους υπόλοιπους πράκτορες επιτρέποντας με αυτό τον τρόπο πιο γρήγορη προσαρμογή σε νέες καταστάσεις. Επίσης, τα MAS είναι κλιμακώσιμα, αφού μπορούν να ενσωματώνουν νέους πράκτορες χωρίς σημαντικές αλλαγές στην αρχιτεκτονική. [32].

5.3.4 Autonomic Computing με ML (Αυτόνομη Υπολογιστική με ML)

Η κλασική δομή MAPE-K (Monitor, Analyze, Plan, Execute – Knowledge - Παρακολούθηση, Ανάλυση, Σχεδιασμός, Εκτέλεση – Γνώση) αποτελεί τη βάση για πολλά αυτοΐατα συστήματα. Ωστόσο η ενσωμάτωση με ML σε αυτό το πλαίσιο μπορεί να προσδώσει μια νέα διάσταση, καθώς οι φάσεις της ανάλυσης και του σχεδιασμού να βελτιώνονται συνεχώς, γίνονται «εξυπνότερες» και πιο αποδοτικές [33]. Στο στάδιο της Παρακολούθησης τα δεδομένα συλλέγονται από αισθητήρες και αρχεία. Στη φάση της Ανάλυσης χρησιμοποιούνται τεχνικές anomaly detection για την ανίχνευση προβλημάτων. Στο Σχεδιασμό εφαρμόζεται ενισχυτική μάθηση ώστε το σύστημα να επιλέγει την πιο κατάλληλη πολιτική αποκατάστασης. Ενώ τέλος, στην Εκτέλεση εκτελούνται οι ενέργειες αποκατάστασης, και εν συνεχεία στη Γνώση ενημερώνεται η βάση με τα αποτελέσματα ώστε να ανανεωθεί ο κύκλος της μάθησης [33].

5.4 Εφαρμογές σε IoT

Η ενσωμάτωση μοντέλων ML σε μηχανισμούς αυτοΐασης του IoT έχει οδηγήσει σε πρακτικές εφαρμογές σε κρίσιμους τομείς. Τα μοντέλα αυτά επιτρέπουν την έγκαιρη διάγνωση, την πρόβλεψη και την αυτόνομη αποκατάσταση δυσλειτουργιών, ενισχύοντας την ανθεκτικότητα των συστημάτων. Καθίσταται αντιληπτό ότι η χρήση ML όχι μόνο αυτοματοποιεί την αποκατάσταση, αλλά ενισχύει και την ανθεκτικότητα του συστήματος, μειώνοντας τον ανθρώπινο παράγοντα. Ορισμένα παραδείγματα θα αναλυθούν παρακάτω:

5.4.1 Έξυπνα Δίκτυα Ενέργειας (Smart Grids)

Στα Smart Grids, μοντέλα ανίχνευσης ανωμαλιών με ML χρησιμοποιούνται για να προβλέψουν σφάλματα σε υποσταθμούς ή γραμμές μεταφοράς. Τεχνικές ενισχυτικής μάθησης (RL) συμβάλλουν στην αυτόματη αναδρομολόγηση ισχύος και στη βελτιστοποίηση του φορτίου, μειώνοντας τον χρόνο αποκατάστασης μετά από βλάβη (FLISR). Η χρήση ML αυξάνει τη δυνατότητα πρόβλεψης blackouts την αυτόματη απομόνωση προβληματικών περιοχών και την ταχεία αποκατάσταση μειώνοντας έτσι σημαντικά τον χρόνο απόκρισης – αποκατάστασης της βλάβης. Επιπλέον, η χρήση anomaly detection για την αναγνώριση μη φυσιολογικής κατανάλωσης επιτρέπει τον έγκαιρο εντοπισμό πιθανών επιθέσεων. Μελέτες έδειξαν ότι ο χρόνος αποκατάστασης μπορεί να μειωθεί έως και 40% [34].

5.4.2 Υγεία και IoMT

Στον τομέα της υγείας οι συνδεδεμένες συσκευές απαιτούν υψηλή αξιοπιστία. Τα μοντέλα ML επιτρέπουν την αυτοΐαση συστημάτων που συλλέγουν δεδομένα από αισθητήρες (wearables, εμφυτεύσιμες συσκευές). Με την ανίχνευση ανωμαλιών στα βιοσήματα (π.χ. καρδιακός ρυθμός, επίπεδα γλυκόζης, αντλίες ινσουλίνης ή καρδιογράφου), τα συστήματα μπορούν να ενεργοποιήσουν αυτόματες διορθωτικές ενέργειες ή ειδοποιήσεις, βελτιώνοντας την ασφάλεια των ασθενών. Το Federated Learning υποστηρίζει την εκπαίδευση μοντέλων χωρίς μεταφορά ευαίσθητων δεδομένων, διατηρώντας την ιδιωτικότητα των ασθενών [33]. Συστήματα anomaly detection έχουν εφαρμοστεί σε IoMT για την αποτροπή ψευδών μετρήσεων, που θα μπορούσαν να οδηγήσουν σε λάθος ιατρικές αποφάσεις.

5.4.3 Βιομηχανικό IoT (IIoT)

Στα βιομηχανικά περιβάλλοντα, η ML ενσωματώνεται σε πλατφόρμες predictive maintenance. Τα συστήματα αυτοΐασης προβλέπουν βλάβες σε μηχανήματα, ρυθμίζουν αυτόματα παραμέτρους και εκτελούν προληπτικές ενέργειες. Η προληπτική συντήρηση με ML μειώνει το κόστος και αυξάνει τη διαθεσιμότητα. Σύμφωνα με πρόσφατα στοιχεία, η εφαρμογή ML στην προληπτική συντήρηση έχει οδηγήσει σε μείωση του κόστους έως 20% και αύξηση της διαθεσιμότητας κατά 30% [32]. Για παράδειγμα, η ανάλυση δονήσεων ή θερμοκρασίας με deep learning μοντέλα μπορεί να οδηγήσει σε άμεση απόσυρση ενός εξαρτήματος πριν προκληθεί σοβαρή αστοχία Επιπλέον, η χρήση federated learning επιτρέπει τη συνεργασία μεταξύ διαφορετικών εργοστασίων χωρίς ανταλλαγή ευαίσθητων δεδομένων.

5.4.4 Edge/Fog Υποδομές

Η αυτοΐαση μέσω ML αποκτά ιδιαίτερη σημασία σε Edge/Fog υποδομές, όπου οι πόροι είναι περιορισμένοι και οι απαιτήσεις σε χρόνο απόκρισης είναι υψηλές. Η τοπική επεξεργασία μέσω ML επιτρέπει την άμεση ανίχνευση και αποκατάσταση, προσφέροντας ανθεκτικότητα σε συνθήκες

χαμηλής συνδεσιμότητας [34]. Lightweight μοντέλα ML ανιχνεύουν τοπικές ανωμαλίες και ενεργοποιούν μηχανισμούς ανάκαμψης χωρίς να απαιτείται cloud επεξεργασία. Έτσι μειώνεται η καθυστέρηση (latency) και αυξάνεται η αυτονομία, ιδιαίτερα σε εφαρμογές όπως τα connected vehicles ή τα smart factories Σενάρια όπως αυτόνομα drones ή συστήματα έξυπνων πόλεων επωφελούνται ιδιαίτερα από την αρχιτεκτονική αυτή.

5.5 Προκλήσεις και Περιορισμοί

Η εφαρμογή μοντέλων αυτοΐασης που βασίζονται στη ML στο IoT είναι πολλά υποσχόμενη, ωστόσο συνοδεύεται από σημαντικούς περιορισμούς και ανοιχτά ερευνητικά ζητήματα. Οι προκλήσεις αυτές δεν πρέπει να γίνουν αντιληπτές ως αδυναμίες, αλλά ως οδηγοί για μελλοντική πρόοδο, καθώς η υπέρβασή τους θα καθορίσει τον βαθμό υιοθέτησης των self-healing IoT συστημάτων στην πράξη.

5.5.1 Επεξηγησιμότητα (Explainability)

Πολλά ML μοντέλα, ιδίως τα deep learning, λειτουργούν ως «μαύρα κουτιά». Η έλλειψη διαφάνειας δυσχεραίνει την κατανόηση και την εμπιστοσύνη στις αποφάσεις [32]. Οι μηχανικοί και οι διαχειριστές IoT συστημάτων χρειάζονται σαφείς εξηγήσεις για τις αποφάσεις ενός αλγορίθμου, ώστε να μπορούν να τις εμπιστευθούν, ειδικά όταν πρόκειται για αποφάσεις που σχετίζονται με την ασφάλεια ή την αδιάλειπτη παροχή υπηρεσιών. Η ανάπτυξη τεχνικών Explainable AI (XAI) αποτελεί επιτακτική ανάγκη, καθώς συνδυάζει τη δύναμη των αλγορίθμων με την απαραίτητη διαφάνεια [33].

5.5.2 Κατανάλωση Πόρων

Οι IoT συσκευές χαρακτηρίζονται από περιορισμένη υπολογιστική ισχύ, μνήμη και ενέργεια. Η εκπαίδευση και εκτέλεση σύνθετων ML μοντέλων μπορεί να είναι δυσανάλογα βαριά για τέτοια περιβάλλοντα, καθώς οι ανάγκες των σύνθετων ML απαιτούν υψηλή υπολογιστική ισχύ και ενέργεια. Παράδειγμα αποτελούν τα δίκτυα αισθητήρων σε Smart Cities, όπου η συνεχής λειτουργία αλγορίθμων ανίχνευσης ανωμαλιών θα εξαντλούσε τη διάρκεια ζωής των μπαταριών. Για τον λόγο αυτό προτείνονται lightweight ML μοντέλα, συμπιεσμένα δίκτυα (model compression) και συνεργατικές αρχιτεκτονικές cloud-edge, όπου το υπολογιστικό φορτίο κατανέμεται ανάλογα με τις δυνατότητες κάθε κόμβου και να υπάρχει μια καλύτερή αξιοποίηση του hardware acceleration. [34].

5.5.3 Ασφάλεια ML

Παρότι τα μοντέλα ML χρησιμοποιούνται για την ενίσχυση της ασφάλειας, παραμένουν τα ίδια ευάλωτα σε επιθέσεις. Οι λεγόμενες adversarial attacks μπορούν να μεταβάλουν ελάχιστα τα δεδομένα εισόδου ώστε να οδηγήσουν τον αλγόριθμο σε λάθος πρόβλεψη, με καταστροφικά αποτελέσματα [32], [34]. Στον χώρο του IoMT, μια τέτοια παραπλανητική είσοδος θα μπορούσε να οδηγήσει σε λάθος διάγνωση ή σε απενεργοποίηση κρίσιμης λειτουργίας. Η ενσωμάτωση μηχανισμών ανθεκτικότητας (robust ML) και η συνδυαστική χρήση με blockchain είναι ερευνητικές κατευθύνσεις και συνεχούς εκπαίδευσης θεωρείται απαραίτητη για την ασφαλή λειτουργία των αυτοΐατων IoT συστημάτων [5].

5.5.4 Διαλειτουργικότητα

Το IoT χαρακτηρίζεται από μεγάλη ετερογένεια συσκευών, πρωτοκόλλων και πλατφορμών. Η ενσωμάτωση ML μοντέλων σε τόσο διαφορετικά περιβάλλοντα (π.χ. OpenC2, NIST, ETSI) καθίσταται δύσκολη, καθώς κάθε πλατφόρμα μπορεί να έχει διαφορετικούς περιορισμούς ή APIs. Η έλλειψη τυποποίησης καθυστερεί την ευρεία υιοθέτηση self-healing μηχανισμών [33]. Οι διεθνείς οργανισμοί

(ISO, NIST, ETSI) έχουν ήδη θέσει σε προτεραιότητα την ανάπτυξη προτύπων που θα διευκολύνουν τη διαλειτουργικότητα, γεγονός που θα ενισχύσει την πρακτική εφαρμογή των ML μοντέλων σε ποικίλα IoT οικοσυστήματα [8].

5.5.5 Ιδιωτικότητα

Η εκπαίδευση ML μοντέλων βασίζεται σε μεγάλο όγκο δεδομένων, τα οποία συχνά περιλαμβάνουν ευαίσθητες πληροφορίες. Σε εφαρμογές υγείας IoMT η συλλογή δεδομένων υγείας εγείρει σοβαρά ζητήματα προστασίας προσωπικών δεδομένων, ενώ το ίδιο ισχύει και στον τομέα της βιομηχανίας. Η ανάπτυξη privacy-preserving τεχνικών, όπως Federated Learning (κατανεμημένη εκπαίδευση χωρίς μεταφορά δεδομένων) και η ομοιόμορφή κρυπτογράφηση (homomorphic encryption), είναι κρίσιμες για την αποδοχή των συστημάτων αυτών και προτείνονται για να διασφαλίσουν την ιδιωτικότητα, ωστόσο η πρακτική τους εφαρμογή είναι ακόμα σε πρώιμο στάδιο λόγω υψηλού υπολογιστικού κόστους [34].. Συνολικά, οι προκλήσεις δείχνουν ότι η επιτυχία της ML στην αυτοΐαση δεν είναι απλώς τεχνικό ζήτημα, αλλά απαιτεί συνδυασμένη προσέγγιση που λαμβάνει υπόψη ασφάλεια, επεξηγησιμότητα, κανονιστικά πλαίσια και κοινωνική αποδοχή.

Συνοψίζοντας, το κεφάλαιο αυτό ανέδειξε τη σημασία της μηχανικής μάθησης ως καταλύτη για την ανάπτυξη μοντέλων αυτοΐασης στο IoT. Αναλύθηκαν οι κατηγορίες μοντέλων, τα πλαίσια υλοποίησης, οι εφαρμογές τους σε κρίσιμους τομείς, αλλά και οι προκλήσεις που συνοδεύουν την πρακτική τους αξιοποίηση. Η κατανόηση αυτών των στοιχείων αποτελεί θεμέλιο για την περαιτέρω εμβάθυνση που ακολουθεί στο επόμενο κεφάλαιο, όπου μέσω μιας μελέτης περίπτωσης θα παρουσιαστεί πώς τα θεωρητικά μοντέλα μεταφράζονται σε πραγματικές εφαρμογές, επιβεβαιώνοντας τη δυναμική και τα όρια της αυτοΐασης στο IoT

Κεφάλαιο 6ο: Μελέτη Περίπτωσης

Σε αυτό το κεφάλαιο παρουσιάζεται μια αναλυτική μελέτη περίπτωσης πραγματικού IoT συστήματος, με στόχο να αποτυπωθούν οι τεχνικές προκλήσεις, οι ευπάθειες και οι επιπτώσεις ασφαλείας που σχετίζονται με την αυτοΐαση και τη λειτουργία έξυπνων συσκευών. Η μελέτη επικεντρώνεται στη λεπτομερή ανάλυση της αρχιτεκτονικής υλικού και λογισμικού, των επικοινωνιακών πρωτοκόλλων, των διαδικασιών authentication και των μηχανισμών κρυπτογράφησης, παρέχοντας παράλληλα παραδείγματα exploits και πρακτικές αντιμετώπισης. Μέσα από την παρουσίαση αυτή, αναδεικνύονται τα μαθήματα που μπορούν να εξαχθούν για τη βελτίωση της ασφάλειας και της αξιοπιστίας των IoT συστημάτων, συνδέοντας την θεωρητική γνώση με πρακτικά σενάρια και βέλτιστες πρακτικές.

6.1 Εισαγωγή στη μελέτη περίπτωσης – επιλογή & σημασία

Η παρούσα μελέτη περίπτωσης που θα αναλυθεί εξετάζει περιστατικά παραβίασης της ιδιωτικότητας μέσω οικιακών ρομποτικών συσκευών με ενσωματωμένη κάμερα και μικρόφωνο, συγκεκριμένα τα μοντέλα Ecovacs Deebot (όπως X-σειρά) και το ρομπότ-υπηρεσίας temi. Κατά τα έτη 2024–2025. Ερευνητές και μέσα ενημέρωσης κατέγραψαν σοκαριστικά περιστατικά όπου οι συσκευές αυτές έπεσαν θύματα κακόβουλων ενεργειών, με αποτέλεσμα τη στέρηση ιδιωτικότητας και την ανησυχητική αίσθηση εισβολής. Σε αρκετές περιπτώσεις, όπως αυτή του δικηγόρου από τη Μινεσότα, η οικιακή ρομποτική σκούπα “Deebot X2” άρχισε ξαφνικά να κινείται και να εκπέμπει φωνητικά μηνύματα με ρατσιστικές βρισιές μέσω των ενσωματωμένων ηχείων, ενώ παράλληλα ο hacker είχε πρόσβαση σε live feed της κάμερας και του μικροφώνου [29],[30]. Παρόμοια περιστατικά καταγράφηκαν σε άλλες περιοχές των ΗΠΑ, όπως στο Τέξας και το Λος Άντζελες, όπου τα ρομπότ είτε επιτέθηκαν σε κατοικίδια είτε παρενόχλησαν τους ιδιοκτήτες τους.

Οι ερευνητές ασφάλειας Dennis Giese και Braelynn Luedtke αποκάλυψαν στο συνέδριο Def Con 2024 ότι οι συσκευές αυτές είναι ευάλωτες μέσω Bluetooth συνδεσιμότητας, η οποία ενεργοποιείται για συγκεκριμένη χρονική διάρκεια μετά το reboot (ή παραμένει συνεχώς ενεργή σε άλλα μοντέλα). Η ευπάθεια αυτή επιτρέπει σε επιτιθέμενους να εισάγουν κακόβουλο payload από απόσταση έως και περίπου 130 μ., αποκτώντας ριζική πρόσβαση στο λειτουργικό σύστημα Linux των συσκευών [31]. Ταυτόχρονα, αναδεικνύονται σοβαρά λάθη στην πραγματοποίηση μηχανισμού προστασίας μέσω τετραψήφιου PIN, η οποία ελέγχεται μόνο στην εφαρμογή (client-side) και όχι στον server. Αυτό σημαίνει ότι ο επιτιθέμενος μπορεί να παρακάμψει την προστασία απλώς χειραγωγώντας την εφαρμογή ή τις κλήσεις της στο backend. Επίσης, διαπιστώθηκε ότι τα δεδομένα — συμπεριλαμβανομένων των αρχείων εικόνας, φωνητικών εγγραφών ακόμα και των διαγραμμένων αρχείων — αποθηκεύονται στο Cloud της Ecovacs και παραμένουν προσβάσιμα ακόμη και μετά από διαγραφή λογαριασμού.

Τα περιστατικά αυτά δεν είναι μεμονωμένα. Σύμφωνα με αναλύσεις, οι ρομποτικές συσκευές καθίστανται στόχοι μεγάλης κλίμακας, καθώς λειτουργούν ως πλήρεις υπολογιστές (Linux), συνδεδεμένοι στο Internet, με ενδεχόμενο διάδοσης δικτυακού malware παρόμοιου με το Mirai. Επιπλέον, μελέτες πεδίου απέδειξαν ότι ακόμα και τα metadata των μεταδόσεων (header info) επαρκούν για την αναγνώριση προσωπικών συνηθειών — π.χ. ώρα και διάρκεια εργασίας της σκούπας — θέτοντας σε κίνδυνο και αυτή καθ’ αυτήν την ιδιωτικότητα των χρηστών.

Συμπερασματικά, η συγκεκριμένη μελέτη περίπτωσης αναδεικνύει τόσο τα τεχνικά όσο και τα κοινωνικά ζητήματα που εγείρονται από την ανεπαρκή ασφάλεια IoT συσκευών, θέτοντάς τις ως παράγοντες δυναμικής απειλής για τους ίδιους τους χρήστες αλλά και για το οικοσύστημα γενικότερα.

6.2 Περιγραφή συσκευής (hardware, software, interfaces)

Η συσκευή που μελετάται εν προκειμένω αποτελεί ένα σύνθετο IoT endpoint, δηλαδή έναν κόμβο που συνδυάζει στοιχεία ρομποτικής, αισθητήρων, επικοινωνιακών διεπαφών και cloud υπηρεσιών. Στην κατηγορία αυτή περιλαμβάνονται τόσο οι οικιακές ρομποτικές σκούπες (π.χ. Ecovacs Deebot X-series) όσο και τα ρομπότ υπηρεσιών (π.χ. temi).

Το υλικό hardware των συσκευών αυτών βασίζονται σε ένα embedded σύστημα αρχιτεκτονικής ARM που τρέχει Linux, προσφέροντας την απαραίτητη υπολογιστική ισχύ για την ταυτόχρονη εκτέλεση πλοήγησης, επεξεργασίας δεδομένων αισθητήρων και μετάδοσης streaming. Ο εξοπλισμός τους περιλαμβάνει πολλαπλούς αισθητήρες, όπως LIDAR και υπέρυθρες κάμερες για χαρτογράφηση χώρου, υπερηχητικούς αισθητήρες για αποφυγή εμποδίων, καθώς και gyroscope και accelerometer για ισορροπία και ακριβή προσανατολισμό. Για την υποστήριξη οπτικοακουστικών λειτουργιών, διαθέτουν κάμερα υψηλής ανάλυσης (HD ή 4K, ανάλογα με το μοντέλο), μικρόφωνο και ηχεία για αμφίδρομη επικοινωνία. Το κινητήριο σύστημα αποτελείται από ηλεκτρικούς κινητήρες που επιτρέπουν κίνηση και ευελιξία μέσω τροχών ή αρθρωτών μηχανισμών. Επιπλέον, ενσωματώνεται μονάδα αποθήκευσης flash για το firmware, τις ρυθμίσεις του χρήστη και προσωρινά δεδομένα όπως χάρτες χώρου. Τέλος, η ενεργειακή αυτονομία εξασφαλίζεται μέσω μίας επαναφορτιζόμενης μπαταρίας ιόντων λιθίου, η οποία προσφέρει διάρκεια λειτουργίας αρκετών ωρών και δυνατότητα αυτόματης επιστροφής στη βάση φόρτισης για επαναφόρτιση.

Το λογισμικό που ενσωματώνουν οι συσκευές βασίζεται σε μια παραμετροποιημένη διανομή Linux, η οποία παρέχει το λειτουργικό υπόβαθρο για την εκτέλεση εξειδικευμένων modules. Σε αυτά περιλαμβάνονται μηχανισμοί real-time πλοήγησης μέσω αλγορίθμων SLAM (Simultaneous Localization and Mapping), οι οποίοι επιτρέπουν στον ρομποτικό μηχανισμό να χαρτογραφεί το περιβάλλον και να εντοπίζει τη θέση του σε πραγματικό χρόνο. Παράλληλα, υπάρχουν υποσυστήματα για τη διαχείριση αισθητήρων και κινητήρων, εξασφαλίζοντας συντονισμένη απόκριση στις συνθήκες του χώρου. Για τις οπτικοακουστικές λειτουργίες, υλοποιείται multimedia streaming που αξιοποιεί την κάμερα και το μικρόφωνο της συσκευής, επιτρέποντας αμφίδρομη επικοινωνία και απομακρυσμένη παρακολούθηση. Επιπλέον, παρέχονται cloud connectivity services, τα οποία συνδέουν τη συσκευή με τον κεντρικό server του κατασκευαστή για ενημερώσεις, αποθήκευση δεδομένων και απομακρυσμένο έλεγχο. Σε αυτό το πλαίσιο εντάσσεται και το Mobile App API, μέσω του οποίου οι χρήστες έχουν τη δυνατότητα να ελέγχουν τη συσκευή από απόσταση. Τέλος, υποστηρίζονται over-the-air (OTA) firmware updates, μια κρίσιμη λειτουργία που ενισχύει τη μακροχρόνια βιωσιμότητα και αναβάθμιση του συστήματος· ωστόσο, η διαδικασία αυτή δημιουργεί και νέες προκλήσεις ασφαλείας, καθώς σε περίπτωση ανεπαρκών μηχανισμών επαλήθευσης (όπως η απαίτηση για signed firmware), μπορεί να προκύψουν σοβαροί κίνδυνοι κυβερνοασφάλειας.

Οι σύγχρονες έξυπνες συσκευές ενσωματώνουν ένα ευρύ φάσμα διεπαφών επικοινωνίας (interfaces), που καλύπτουν τόσο τοπικές όσο και απομακρυσμένες ανάγκες διασύνδεσης. Η βασική συνδεσιμότητα εξασφαλίζεται μέσω Wi-Fi (2.4GHz/5GHz), το οποίο επιτρέπει την απευθείας επικοινωνία με το οικιακό router και κατ’ επέκταση με το cloud, αξιοποιώντας REST APIs και HTTPS για την ασφαλή μεταφορά δεδομένων. Συμπληρωματικά, υποστηρίζεται Bluetooth Low Energy (BLE) για pairing με κινητά ή άλλες συσκευές, αν και συχνά αναφέρεται στη βιβλιογραφία ως πιθανή πηγή ευπάθειας, λόγω ανεπαρκών μηχανισμών authentication ή αδύναμων υλοποιήσεων στο firmware. Επιπλέον, οι κατασκευαστές παρέχουν native mobile εφαρμογές (iOS/Android), οι οποίες προσφέρουν στον χρήστη τη δυνατότητα τηλεχειρισμού, αποθήκευσης χαρτών, δημιουργίας χρονοδιαγραμμάτων λειτουργίας αλλά και πρόσβασης σε live video feed από την κάμερα της συσκευής. Η λειτουργία των

cloud services είναι επίσης κομβικής σημασίας, καθώς οι servers του κατασκευαστή αποθηκεύουν δεδομένα χρηστών (π.χ. χάρτες σπιτιού, εγγραφές, εικόνες), με πρόσβαση μέσω RESTful APIs ή WebSocket για αμφίδρομη real-time επικοινωνία. Τέλος, σημαντικό ρόλο έχει η δυνατότητα third-party integration, με τη συσκευή να είναι συμβατή με πλατφόρμες όπως το Amazon Alexa και το Google Assistant, προσφέροντας φωνητικό έλεγχο και διευκολύνοντας την απρόσκοπτη διασύνδεσή της με τα υπόλοιπα στοιχεία ενός ευρύτερου smart home οικοσυστήματος.

Ως IoT node, η συσκευή αναλαμβάνει ταυτόχρονα πολλαπλές κρίσιμες λειτουργίες που την καθιστούν αναπόσπαστο τμήμα του ευρύτερου οικοσυστήματος του Internet of Things. Σε πρώτο επίπεδο, υλοποιεί συλλογή και μετάδοση δεδομένων (telemetry), παρέχοντας πληροφορίες όπως χάρτες χώρου, στατιστικά χρήσης και εντολές που αποστέλλονται από τον χρήστη. Παράλληλα, υποστηρίζει αμφίδρομη επικοινωνία πολυμέσων, επιτρέποντας τη μετάδοση ζωντανού βίντεο και ήχου τόσο για σκοπούς παρακολούθησης όσο και για αλληλεπίδραση σε πραγματικό χρόνο. Μέσω της σύνδεσης με το cloud και της αντίστοιχης εφαρμογής, καθίσταται εφικτό το remote control, δηλαδή η εκτέλεση εντολών με χαμηλή καθυστέρηση και η άμεση ανταπόκριση της συσκευής. Επιπλέον, σημαντικό ρόλο διαδραματίζει το edge processing, καθώς η συσκευή επεξεργάζεται τοπικά κρίσιμα δεδομένα, όπως για παράδειγμα στο πλαίσιο του SLAM (Simultaneous Localization and Mapping), μειώνοντας την ανάγκη συνεχούς αποστολής δεδομένων στο cloud και βελτιώνοντας τόσο την απόδοση όσο και την ιδιωτικότητα.

6.3 Αρχιτεκτονική επικοινωνίας & πρωτόκολλα

Η αρχιτεκτονική επικοινωνίας μιας έξυπνης IoT συσκευής βασίζεται σε ένα πολυεπίπεδο σύνολο πρωτοκόλλων που καλύπτουν τόσο την τοπική συνδεσιμότητα όσο και την απομακρυσμένη πρόσβαση μέσω cloud υπηρεσιών. Τα κύρια κανάλια επικοινωνίας περιλαμβάνουν διαφορετικές τεχνολογίες και μηχανισμούς ασφαλείας, με στόχο την αδιάλειπτη και αξιόπιστη λειτουργία. Συγκεκριμένα, το Wi-Fi (2.4/5GHz) χρησιμοποιείται ως κύριο μέσο σύνδεσης στο οικιακό δίκτυο και λειτουργεί ως αγωγός για επικοινωνία με τον απομακρυσμένο cloud server, όπου εφαρμόζονται πρωτόκολλα όπως το HTTPS/REST για τυπικές κλήσεις API (π.χ. τηλεχειρισμός, λήψη στατιστικών) και WebSocket για αμφίδρομη επικοινωνία σε πραγματικό χρόνο, όπως το live video streaming ή η άμεση μετάδοση εντολών. Για τη διαδικασία pairing και commissioning, οι συσκευές συχνά αξιοποιούν Bluetooth Low Energy (BLE), το οποίο επιτρέπει στον χρήστη να πραγματοποιήσει την αρχική παραμετροποίηση μέσω της εφαρμογής κινητού (mobile app). Ωστόσο, σε αρκετές περιπτώσεις το BLE υλοποιείται χωρίς ισχυρούς μηχανισμούς πιστοποίησης ή με απλοϊκά PINs, αυξάνοντας τον κίνδυνο μη εξουσιοδοτημένης πρόσβασης κατά το στάδιο αρχικής ρύθμισης.

Η επικοινωνία μεταξύ mobile app και cloud βασίζεται συνήθως σε API authentication mechanisms, όπως bearer tokens ή OAuth 2.0, που επιτρέπουν την ταυτοποίηση του χρήστη. Παρ' όλα αυτά, έχουν παρατηρηθεί υλοποιήσεις όπου η επαλήθευση των διαπιστευτηρίων (π.χ. PIN για live feed) πραγματοποιείται σε επίπεδο client-side, δηλαδή αποκλειστικά από την εφαρμογή, αντί να γίνεται κεντρικά στον server. Αυτό δημιουργεί σοβαρές ευπάθειες, καθώς ο επιτιθέμενος μπορεί να τροποποιήσει τον κώδικα της εφαρμογής (reverse engineering, APK modification) και να παρακάμψει τον μηχανισμό ελέγχου. Επιπλέον, σε συσκευές που ενσωματώνουν κάμερα, είναι πιθανό να υποστηρίζονται και παραδοσιακά πρωτόκολλα βίντεο όπως RTSP (Real-Time Streaming Protocol) ή ONVIF, τα οποία χρησιμοποιούνται ευρέως στη βιομηχανία IP καμερών. Αν και αυτά τα πρωτόκολλα παρέχουν υψηλή διαλειτουργικότητα, σε αρκετές περιπτώσεις δεν εφαρμόζουν επαρκή κρυπτογράφηση ή χρησιμοποιούν προεπιλεγμένα διαπιστευτήρια, κάτι που τα καθιστά ευάλωτα σε επιθέσεις υποκλοπής (eavesdropping) ή μη εξουσιοδοτημένης πρόσβασης.

Συνολικά, η αρχιτεκτονική επικοινωνίας των IoT συσκευών χαρακτηρίζεται από πολυπλοκότητα λόγω της παράλληλης χρήσης διαφορετικών καναλιών και πρωτοκόλλων. Ωστόσο, η ασφάλεια εξαρτάται σε μεγάλο βαθμό από το κατά πόσο οι μηχανισμοί πιστοποίησης, κρυπτογράφησης και διαχείρισης ταυτότητας υλοποιούνται με συνέπεια σε όλα τα επίπεδα —από το BLE commissioning μέχρι την cloud επικοινωνία.

6.4 Ευπάθεια / exploit (τεχνική ανάλυση, attack flow)

Η τεχνική ανάλυση των ευπαθειών ανέδειξε μια σειρά από αδυναμίες στα διαφορετικά επίπεδα επικοινωνίας της συσκευής, οι οποίες επέτρεψαν την εκμετάλλευση (exploit) από επιτιθέμενους. Ένα από τα πιο συνηθισμένα σενάρια ήταν το credential stuffing, δηλαδή η χρήση διαρρευσάντων συνδυασμών χρηστών/κωδικών από άλλα περιστατικά παραβίασης δεδομένων. Δεδομένου ότι πολλοί χρήστες επαναχρησιμοποιούν τους ίδιους κωδικούς πρόσβασης, οι επιτιθέμενοι μπορούσαν να αποκτήσουν πρόσβαση στους λογαριασμούς cloud της συσκευής χωρίς να χρειάζεται άμεση παραβίαση του ίδιου του συστήματος.

Σε επίπεδο δικτύου, παρατηρήθηκαν περιπτώσεις έκθεσης tokens (π.χ. bearer tokens ή session cookies) που μεταδίδονταν χωρίς ισχυρή κρυπτογράφηση ή σε περιβάλλοντα όπου οι χρήστες χρησιμοποιούσαν μη ασφαλή Wi-Fi (π.χ. δημόσια hotspots). Μέσω τεχνικών packet sniffing ή Man-in-the-Middle (MitM) επιθέσεων, οι επιτιθέμενοι μπορούσαν να υποκλέψουν αυτά τα tokens και να τα χρησιμοποιήσουν για να αναπαράγουν (replay) αυθεντικοποιημένα αιτήματα προς τον server.

Στο τοπικό επίπεδο, ευπάθειες στο Bluetooth Low Energy (BLE) commissioning αποκάλυψαν ότι ορισμένα μοντέλα δεν απαιτούσαν σωστή επαλήθευση κατά την αρχική ζευγοποίηση. Αυτό έδινε τη δυνατότητα σε επιτιθέμενο με φυσική εγγύτητα να «παγιδεύσει» τη διαδικασία pairing και να αποκτήσει πρόσβαση στον έλεγχο της συσκευής ή στις ρυθμίσεις της. Σε ακόμα πιο κρίσιμες περιπτώσεις, το PIN που προστάτευε το βίντεο stream ελέγχονταν αποκλειστικά από την πλευρά του client (mobile app) αντί για τον server, επιτρέποντας στους ερευνητές να πραγματοποιήσουν reverse engineering στο APK, να τροποποιήσουν τον κώδικα και να παρακάμψουν πλήρως τον μηχανισμό προστασίας. Με αυτόν τον τρόπο ήταν εφικτό να αποκτήσουν πλήρη πρόσβαση στο live feed (βίντεο και ήχο), με δυνατότητα καταγραφής ή ακόμα και απομακρυσμένης παρακολούθησης του χώρου.

Το συνολικό attack flow μπορεί να περιγραφεί ως εξής:

1. Reconnaissance: Ο επιτιθέμενος εντοπίζει ενεργές συσκευές μέσω scanning στο Wi-Fi ή παρακολουθώντας τις κλήσεις προς το cloud API.
2. Credential/Token Acquisition: Χρήση credential stuffing, υποκλοπής tokens ή exploitation του BLE για απόκτηση αρχικών διαπιστευτηρίων.
3. Bypass of Authentication: Εκμετάλλευση του client-side PIN validation μέσω reverse engineering για άμεση παράκαμψη των ελέγχων.
4. Access & Control: Απόκτηση απομακρυσμένης πρόσβασης στο live video/audio stream και πιθανή εκτέλεση εντολών προς τη συσκευή.
5. Persistence: Δημιουργία δευτερευόντων tokens ή session hijacking ώστε να διατηρείται η πρόσβαση ακόμη και μετά από reset του χρήστη.

Η ύπαρξη αυτών των αδυναμιών αποδεικνύει ότι η ασφάλεια δεν μπορεί να βασίζεται μόνο σε client-side μηχανισμούς και ότι είναι απαραίτητη η υιοθέτηση end-to-end κρυπτογράφησης, server-side validation και ισχυρής διαχείρισης ταυτοτήτων ώστε να αποτραπεί η εκμετάλλευση τέτοιων κενών.

6.5 Επιπτώσεις (privacy, safety, physical effects) και Αντιμετώπιση (reactive vs proactive)

Η εκμετάλλευση των ευπαθειών είχε πολυδιάστατες συνέπειες. Στο επίπεδο ιδιωτικότητας (privacy), η μη εξουσιοδοτημένη πρόσβαση σε live βίντεο και ήχο επέτρεψε την παρακολούθηση εσωτερικών χώρων, με σοβαρούς κινδύνους αποκάλυψης προσωπικών στιγμών και καθημερινών συνηθειών των χρηστών. Από την πλευρά της ασφάλειας (safety), ο έλεγχος της συσκευής από τρίτους μπορούσε να οδηγήσει σε ανεπιθύμητες ενέργειες — π.χ. ξαφνική κίνηση ή παρεμπόδιση λειτουργιών, που σε περιβάλλοντα με παιδιά ή ηλικιωμένους θα μπορούσε να δημιουργήσει κινδύνους τραυματισμού. Στο επίπεδο φυσικών επιπτώσεων (physical effects), η δυνατότητα παρακολούθησης και χαρτογράφησης του χώρου θα μπορούσε να χρησιμοποιηθεί ως προεργασία για φυσική διάρρηξη (π.χ. γνώση πότε λείπουν οι ένοικοι, διάταξη σπιτιού). Συνολικά, το impact δεν περιορίζεται μόνο στο κυβερνοχώρο αλλά επεκτείνεται στην καθημερινή ζωή και φυσική ασφάλεια των χρηστών.

Οι πρώτες ενέργειες (reactive measures) περιλάμβαναν επείγοντα patches από τον κατασκευαστή: ενημέρωση firmware με διορθωμένα modules, αναβάθμιση της mobile εφαρμογής, επανασχεδιασμό του authentication flow ώστε οι έλεγχοι (π.χ. PIN validation) να εκτελούνται αποκλειστικά server-side, καθώς και forced password resets για όλους τους χρήστες. Επιπλέον, έγινε αποκλεισμός ύποπτων IPs μέσω firewall rules στο cloud, ενώ οι χρήστες έλαβαν οδηγίες για αλλαγή κωδικών, χρήση WPA2/3 στο Wi-Fi και απομόνωση της συσκευής σε IoT VLAN για περιορισμό lateral movement.

Σε πιο μακροπρόθεσμο επίπεδο (proactive measures), προτάθηκαν:

- Ισχυρή αυθεντικοποίηση με ενεργοποίηση 2FA (π.χ. μέσω TOTP ή push notification).
- Ελαχιστοποίηση επιφάνειας επίθεσης με απενεργοποίηση μη απαραίτητων υπηρεσιών, κλείσιμο αχρησιμοποίητων θυρών (port hardening) και περιορισμό του debugging mode.
- Privacy by design: προαιρετική απενεργοποίηση/φυσικό κάλυμμα κάμερας όταν δεν χρησιμοποιείται, καθώς και local-only λειτουργία όπου είναι εφικτό (edge mode).
- Network segmentation & monitoring: τοποθέτηση IoT συσκευών σε ξεχωριστό VLAN, χρήση IDS/IPS για ανίχνευση ανωμαλιών, και εφαρμογή rate limiting σε API calls.
- Secure update mechanisms: OTA firmware με υπογραφή (signed firmware), ώστε να αποτρέπεται η εισαγωγή κακόβουλων images.

Με αυτό τον τρόπο, η αντιμετώπιση δεν περιορίζεται σε ad-hoc αντιδράσεις μετά από περιστατικά, αλλά υιοθετείται μια ολοκληρωμένη στρατηγική ασφαλείας που ενισχύει την ανθεκτικότητα (resilience) των IoT συστημάτων απέναντι σε μελλοντικές επιθέσεις.

6.6 Μαθήματα & βέλτιστες πρακτικές (σύνδεση με πρότυπα/πρωτόκολλα)

Τα περιστατικά που αναλύθηκαν καταδεικνύουν ότι τα ρομποτικά IoT endpoints, ειδικά εκείνα που ενσωματώνουν κάμερες και μικρόφωνα, αποτελούν κρίσιμα σημεία υψηλού ρίσκου για την ιδιωτικότητα και την ασφάλεια των χρηστών. Από τεχνική σκοπιά, η παρουσία client-side validation, αδύναμου BLE pairing και ανεπαρκούς κρυπτογράφησης ενίσχυσε τις πιθανότητες επιτυχίας επιθέσεων, αναδεικνύοντας τις αδυναμίες στον σχεδιασμό πρωτοκόλλων επικοινωνίας. Με βάση αυτά τα μαθήματα, η βέλτιστη πρακτική περιλαμβάνει την αναλυτική τεκμηρίωση του authentication flow και των επικοινωνιακών πρωτοκόλλων σε κάθε στάδιο του design, ώστε να εντοπίζονται τυχόν αδύναμοι κρίκοι. Επιπλέον, η παρουσίαση της ευπάθειας ως παράδειγμα—όπως η client-side validation

ή η μη ασφαλής BLE ζεύξη—μπορεί να λειτουργήσει ως case study για την αξιολόγηση και δοκιμή των συστημάτων.

Σε επίπεδο εφαρμογής, προτείνονται τεχνικά και διαχειριστικά μέτρα τα οποία συνδέονται άμεσα με διεθνή πρότυπα ασφάλειας και κρυπτογράφησης:

- Signed firmware και secure OTA updates (σύμφωνα με best practices NIST SP 800-193, ISO/IEC 27001), ώστε να διασφαλίζεται η ακεραιότητα του λογισμικού.
- Server-side PIN verification και κρυπτογράφηση δεδομένων end-to-end (TLS/DTLS, OSCORE), προκειμένου να αποφευχθεί η παραβίαση μέσω client-side αδυναμιών.
- Διαχείριση ταυτοτήτων και πρόσβασης (Identity & Access Management) με χρήση token-based authentication, 2FA και περιορισμούς βάσει ρόλων, ώστε να ελαχιστοποιείται η πιθανότητα κακόβουλης χρήσης.
- Segmentation δικτύου και περιορισμός υπηρεσιών (close unused ports, IoT VLAN), με σκοπό τη μείωση της επιφάνειας επίθεσης.

Η υιοθέτηση αυτών των μέτρων δεν ενισχύει μόνο την ασφάλεια αλλά και τη συμμόρφωση με πρότυπα όπως ISO/IEC 27001, NIST CSF και ETSI TS 103 645 για consumer IoT security. Ταυτόχρονα, η ενσωμάτωση αυτών των πρακτικών από το στάδιο του σχεδιασμού (security by design) εξασφαλίζει μια προληπτική προσέγγιση, μειώνοντας την πιθανότητα επαναλαμβανόμενων ευπαθειών και ενισχύοντας την αξιοπιστία και ανθεκτικότητα των IoT συσκευών.

6.7 Εφαρμογή Self-Healing με OpenC² για τη βελτίωση της συσκευής

Όπως είδαμε στις προηγούμενες ενότητες της μελέτης περίπτωσης αναδείχθηκαν οι ευπάθειες που εντοπίστηκαν στις συσκευές, ενώ αναλύθηκαν οι συνέπειες των παραβιάσεων που σχετίζονται τόσο με την ιδιωτικότητα όσο και με την ασφάλεια των χρηστών. Παράλληλα, παρουσιάστηκαν αντιδραστικές και προληπτικές προσεγγίσεις που θα μπορούσαν να μειώσουν τον κίνδυνο, καθώς και βέλτιστες πρακτικές που συνδέονται με διεθνή πρότυπα και πρωτόκολλα.

Η ενσωμάτωση των μηχανισμών self-healing θα έδιναν μια περαιτέρω ενίσχυση της ανθεκτικότητας των συσκευών αυτών και πιθανόν δε θα είχε προσβληθεί σε τόσα επίπεδα αποτρέποντας όλες τις προαναφερθείσες παραβιάσεις. Παρακάτω θα αναλυθούν τα μοντέλα αυτοΐασης, οι αρχιτεκτονικές, τα πρότυπα και πρωτόκολλα που θα προσδίδανε μια καλύτερη και αποδοτικότερη λειτουργία στη συγκεκριμένη περίπτωση με τις smart ηλεκτρικές σκούπες :

Όσον αφορά τα Μοντέλα Αυτοΐασης, η εφαρμογή self-healing θα μπορούσε να αξιοποιήσει διαφορετικά μοντέλα, όπως:

- Ανίχνευση και Ανάκαμψη: Με τη συνεχή παρακολούθηση θα εντοπιζόταν οι τυχόν αλλαγές που υπήρξαν και θα υπήρχε άμεση αποκατάσταση (π.χ. διακοπή κακόβουλης σύνδεσης).
- Πρόβλεψη και Πρόληψη: χρήση τεχνικών μηχανικής μάθησης για πρόβλεψη ανώμαλης συμπεριφοράς πριν εξελιχθεί σε επίθεση.
- Ενισχυτική Μάθηση (Reinforcement Learning): δυναμική βελτίωση πολιτικών ασφαλείας ανάλογα με το εκάστοτε περιβάλλον.
- Υβριδικά Μοντέλα: συνδυασμός ανίχνευσης ανωμαλιών με προληπτικά μέτρα, ώστε το σύστημα να επιτυγχάνει ταυτόχρονα ταχεία αντίδραση και πρόληψη.

Όσον αφορά τις Αρχιτεκτονικές Εφαρμογής, η εφαρμογή self-healing θα μπορούσε να υλοποιηθεί μέσω διαφορετικών αρχιτεκτονικών:

- Edge-based self-healing: εντοπισμός και αντίδραση απευθείας στη συσκευή για ελαχιστοποίηση καθυστερήσεων.
- Cloud-native υποδομές: συγκεντρωτική ανάλυση δεδομένων και εφαρμογή διορθωτικών ενεργειών μέσω OTA ενημερώσεων.
- Κατανεμημένα Multi-Agent Systems (MAS): συνεργασία μεταξύ συσκευών για εντοπισμό και απομόνωση κοινών απειλών.
- Autonomic Computing (MAPE-K loop**)**: αυτόνομη λειτουργία με βρόχο *Monitor–Analyze–Plan–Execute–Knowledge*, που επιτρέπει συνεχή αυτορρύθμιση.

Επίσης, όσον αφορά τα Πρότυπα και Πρωτόκολλα, η αποτελεσματική εφαρμογή self-healing προϋποθέτει την αξιοποίηση διεθνών προτύπων και ασφαλών πρωτοκόλλων επικοινωνίας:

- Πρότυπα Ασφαλείας: ISO/IEC 27000, NIST Cybersecurity Framework, ETSI, ENISA για ολιστική διαχείριση κινδύνων.
- Πρωτόκολλα Επικοινωνίας IoT: MQTT, CoAP και AMQP, ενισχυμένα με μηχανισμούς ασφαλείας (π.χ. OSCORE).
- Πρωτόκολλα Κρυπτογράφησης: TLS/DTLS, lightweight cryptography (NIST LWC) για συσκευές περιορισμένων πόρων.
- Μηχανισμοί Εξουσιοδότησης και Ταυτοποίησης: End-to-End Encryption και Identity Management για αποφυγή καταχρήσεων διαπιστευτηρίων.

Υψίστης σημασίας παράγοντα αποτελεί ότι δεν υπήρχε ενσωμάτωση του προτύπου OpenC² με αποτέλεσμα να εκδηλωθεί η πολυεπίπεδη παραβίαση στην συσκευή. Τα μέτρα πρόβλεψης, πρόληψης και επιδιόρθωσης φάνηκε πως δεν ήταν επαρκή ή ήταν λάθος σχεδιασμένα και η υιοθέτηση του προτύπου OpenC² θα μπορούσε να προσφέρει ουσιαστικά πλεονεκτήματα στην αντιμετώπιση των επιθέσεων που αναλύθηκαν στη μελέτη περίπτωσης. Το OpenC² αποτελεί ένα διεθνώς αναγνωρισμένο πρότυπο, το οποίο καθιερώνει έναν τυποποιημένο τρόπο επικοινωνίας εντολών αντίδρασης σε περιστατικά ασφαλείας, ανεξαρτήτως κατασκευαστή ή τεχνολογικής πλατφόρμας, εξαλείφοντας έτσι το στοιχείο της ετερογένειας..

Στη συγκεκριμένη περίπτωση, όπου οι. έξυπνες ρομποτικές σκούπες παρουσίασαν ευπάθειες που οδήγησαν σε παραβίαση της ιδιωτικότητας μέσω μη εξουσιοδοτημένης πρόσβασης σε κάμερα και μικρόφωνο, η υιοθέτηση ενός self-healing μηχανισμού βασισμένου στο OpenC² θα μπορούσε να λειτουργήσει ως καταλύτης αυτόματης και ενοποιημένης απόκρισης, επιτρέποντας την άμεση ανίχνευση, απομόνωση και αποκατάσταση του προβλήματος, με στόχο τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της ανθεκτικότητας της συσκευής. .

Πιο αναλυτικά, η εφαρμογή του OpenC² θα παρείχε τα ακόλουθα οφέλη:

1. Τυποποιημένες εντολές άμεσης αντίδρασης

   Στην περίπτωση ανίχνευσης κακόβουλης δραστηριότητας, όπως Man-in-the-Middle επίθεσης, Duffie – Helman attack, certification forgety ή παράνομης αναμετάδοσης δεδομένων, το self-healing σύστημα θα μπορούσε να εκδώσει εντολές όπως:

- ✓ deny: άμεση διακοπή της ύποπτης σύνδεσης με τον κακόβουλο κόμβο.
- ✓ quarantine: απομόνωση της ευάλωτης συσκευής από το δίκτυο για περιορισμό της εξάπλωσης της επίθεσης.
- ✓ restore: επαναφορά των κρίσιμων ρυθμίσεων ασφαλείας ή του firmware από ασφαλή αποθηκευτική τοποθεσία.
- ✓ update: εφαρμογή διορθωτικών ενημερώσεων (patches) χωρίς ανθρώπινη παρέμβαση.

2. Διαλειτουργικότητα σε ετερογενές IoT οικοσύστημα

   Δεδομένου ότι οι συσκευές IoT προέρχονται από διαφορετικούς κατασκευαστές και συχνά χρησιμοποιούν διαφορετικά APIs, το OpenC² προσφέρει ένα κοινό λεξιλόγιο εντολών. Έτσι, σε ένα σενάριο όπου εντοπίζεται παραβίαση, ένας κεντρικός ελεγκτής θα μπορούσε να εκδώσει ενιαίες εντολές προς όλες τις συσκευές του οικοσυστήματος, εξασφαλίζοντας ταυτόχρονη και συντονισμένη απόκριση.

3. Συνδυασμός με Μοντέλα Μηχανικής Μάθησης

   Η συνεργασία του OpenC² με μοντέλα ανίχνευσης ανωμαλιών - anomaly detection και πρόβλεψης βλαβών θα επέτρεπε την υλοποίηση ενός πλήρους κύκλου αυτόνομης άμυνας. Πιο συγκεκριμένα, τα μοντέλα ML θα αναγνώριζαν έγκαιρα ύποπτα μοτίβα συμπεριφοράς, ενώ το OpenC² θα λειτουργούσε ως το «κανάλι δράσης», επιτρέποντας έτσι την άμεση εκτέλεση των απαραίτητων ενεργειών χωρίς να υπάρξει ανθρώπινη παρέμβαση που συνήθως είναι μια χρονοβόρα διαδικασία.

4. Ασφάλεια και ιχνηλασιμότητα

   Οι εντολές OpenC² δύνανται να μεταδίδονται μέσω ασφαλών πρωτοκόλλων, όπως TLS/DTLS, CoAP bindings, διασφαλίζοντας με αυτόν τον τρόπο την εμπιστευτικότητα και την ακεραιότητα της επικοινωνίας. Επιπλέον, κάθε εντολή και ενέργεια καταγράφεται, παρέχοντας ένα πλήρες audit trail που ενισχύει τη διαφάνεια και την αξιοπιστία του συστήματος.

Συνεπώς, αν οι συσκευές της μελέτης περίπτωσης είχαν ενσωματώσει μηχανισμούς self-healing με βάση το OpenC², η διαδικασία απόκρισης θα ήταν αυτόματη, ταχύτερη και αποτελεσματικότερη. Για παράδειγμα, κατά τη στιγμή της παραβίασης, η συσκευή θα μπορούσε να εντοπίσει την ανώμαλη συμπεριφορά, να διακόψει άμεσα την ανεπιθύμητη σύνδεση και να αποκαταστήσει την ομαλή λειτουργία μέσω rollback του firmware, περιορίζοντας σημαντικά τον χρόνο έκθεσης και τις συνέπειες της επίθεσης.

Η ενσωμάτωση του OpenC² θα αποτελούσε, επομένως, ένα ισχυρό εργαλείο για την ενίσχυση της ανθεκτικότητας, της ιδιωτικότητας, της απρόσκοπτης λειτουργίας και της αυτονομίας των IoT συσκευών, σε πλήρη εναρμόνιση με τις διεθνείς κατευθυντήριες οδηγίες και καλές πρακτικές, όπως αυτές των NIST, ENISA, ISO, που συμβάλλουν τόσο στην αυτοΐαση όσο και στην προληπτική ασφάλεια.

Κεφάλαιο 7ο: Συμπεράσματα

Το κεφάλαιο αυτό συνοψίζει τα κύρια ευρήματα της διπλωματικής εργασίας, αναδεικνύοντας τα διδάγματα που προέκυψαν από την ανάλυση των συστημάτων αυτοΐασης, των προτύπων και πρωτοκόλλων ασφάλειας, καθώς και από τη μελέτη περίπτωσης σε IoT συσκευές. Τα συμπεράσματα αυτά συνδέουν τη θεωρία με την πράξη και προσφέρουν κατευθύνσεις για μελλοντικές επεκτάσεις, βελτιώνοντας την αξιοπιστία, την ασφάλεια και τη βιωσιμότητα των εφαρμογών αυτοΐασης και των έξυπνων συστημάτων.

7.1 Αυτοΐαση και Εφαρμογές της

Η αυτοΐαση (self-healing) αναδεικνύεται ως μια κρίσιμη τεχνολογία για την ενίσχυση της αξιοπιστίας, της ασφάλειας και της αποδοτικότητας σε πληθώρα τομέων, από τα δίκτυα ενέργειας, τις τηλεπικοινωνίες, την αυτοκινητοβιομηχανία και την αεροναυπηγική. Η ικανότητα ανίχνευσης, απομόνωσης και αυτόματης αποκατάστασης βλαβών μειώνει σημαντικά το λειτουργικό κόστος, το χρόνο διακοπής υπηρεσιών και τις επιπτώσεις από ανθρώπινα λάθη, επιτρέποντας παράλληλα τη συνεχή και ασφαλή λειτουργία των συστημάτων. Οι προκλήσεις που παραμένουν αφορούν κυρίως την ασφάλεια και την ολοκλήρωση των συστημάτων αυτοΐασης με υπάρχουσες υποδομές, καθώς και την ανάπτυξη ευφυών αλγορίθμων που θα μπορούν να ανταποκρίνονται σε ποικίλα και απρόβλεπτα σενάρια βλαβών. Επιπλέον, η ευρύτερη εφαρμογή της τεχνολογίας απαιτεί πρότυπα και κανονισμούς που να διασφαλίζουν την ομοιογένεια, τη διαλειτουργικότητα και την προστασία των χρηστών.

Ένα από τα σημαντικότερα συμπεράσματα της παρούσας μελέτης προκύπτει από το Κεφάλαιο 5, όπου αναλύθηκαν εκτενώς τα μοντέλα αυτοΐασης που στηρίζονται στη Μηχανική Μάθηση. Φάνηκε ότι η αξιοποίηση αλγορίθμων ανίχνευσης ανωμαλιών, πρόβλεψης βλαβών και ενισχυτικής μάθησης μπορεί να προσδώσει στα IoT οικοσυστήματα υψηλό βαθμό αυτονομίας, ανθεκτικότητας και προσαρμοστικότητας. Οι εφαρμογές σε κρίσιμους τομείς, όπως τα έξυπνα δίκτυα ενέργειας, η υγεία και το βιομηχανικό IoT, αποδεικνύουν ότι η ML δεν αποτελεί απλώς ένα εργαλείο βελτιστοποίησης, αλλά τον βασικό καταλύτη για τη μετάβαση σε πραγματικά αυτοΐατα συστήματα. Παράλληλα, οι προκλήσεις που αναλύθηκαν στο ίδιο κεφάλαιο – επεξηγησιμότητα, κατανάλωση πόρων, ασφάλεια, διαλειτουργικότητα και ιδιωτικότητα – δείχνουν τον δρόμο για περαιτέρω έρευνα και εξέλιξη, ώστε τα μοντέλα αυτά να μπορέσουν να υιοθετηθούν σε ευρεία κλίμακα.

Σε επίπεδο εφαρμογών, οι τομείς της ενέργειας και των έξυπνων δικτύων προβλέπεται να πρωτοστατήσουν, δεδομένης της αυξανόμενης ανάγκης για ευελιξία και ανθεκτικότητα σε συνθήκες αυξανόμενης ζήτησης και ενσωμάτωσης Ανανεώσιμων Πηγών Ενέργειας (ΑΠΕ). Παράλληλα, η αυτοΐαση στα αυτόνομα οχήματα και τα συστήματα υγείας προσφέρει σημαντικές δυνατότητες για ασφαλέστερες και πιο αξιόπιστες υπηρεσίες, με ταυτόχρονη μείωση κόστους και βελτίωση της εμπειρίας του χρήστη. Η μελλοντική εξέλιξη της αυτοΐασης αναμένεται να επηρεαστεί καθοριστικά από τις προόδους στην τεχνητή νοημοσύνη, τα δίκτυα 5G/6G και την ανάλυση μεγάλων δεδομένων (big data), που θα επιτρέψουν τη δημιουργία πιο ευέλικτων, προγνωστικών και αυτόνομων συστημάτων. Οι συνδυαστικές αυτές τεχνολογίες μπορούν να προσδώσουν νέα χαρακτηριστικά, όπως την πρόβλεψη βλαβών σε πραγματικό χρόνο, την αυτό-βελτιστοποίηση και την προσαρμογή σε πολυπλοκότερα περιβάλλοντα λειτουργίας.

Τέλος, η ενσωμάτωση της αυτοΐασης με τις αρχές βιωσιμότητας και κυκλικής οικονομίας προωθεί τη δημιουργία πιο αποδοτικών και φιλικών προς το περιβάλλον συστημάτων, βελτιώνοντας τη συνολική απόδοση των υποδομών. Συνολικά , η αυτοΐαση αποτελεί μια τεχνολογική κατεύθυνση με ισχυρή δυναμική, η οποία με την κατάλληλη υποστήριξη σε επίπεδο έρευνας, ανάπτυξης και πολιτικών,

μπορεί να μετασχηματίσει σημαντικά βιομηχανικούς και κοινωνικούς τομείς, καθιστώντας τα συστήματα πιο ανθεκτικά, έξυπνα και φιλικά προς τον χρήστη.

7.2 Τυποποίηση και Πρωτόκολλα για Αυτοΐατα Συστήματα

Η ανάλυση που προηγήθηκε ανέδειξε τη σημασία των διεθνών προτύπων, των πρωτοκόλλων επικοινωνίας και των θεσμικών πλαισίων στη διαμόρφωση ενός ασφαλούς, διαλειτουργικού και βιώσιμου οικοσυστήματος. Από την αυτοκινητοβιομηχανία και την αεροναυπηγική έως τον τομέα της υγείας, των έξυπνων πόλεων και των ενεργειακών δικτύων, τα πρότυπα δεν αποτελούν απλώς κατευθυντήριες γραμμές, αλλά λειτουργούν ως καταλύτες για την καινοτομία, την ποιότητα και την προστασία των χρηστών. Η ανάπτυξη πρωτοκόλλων εντολών και ελέγχου (όπως OpenC², STIX, TAXII) και η ευρεία υιοθέτηση πρωτοκόλλων επικοινωνίας σε περιβάλλοντα IoT (MQTT, CoAP, REST APIs) αποδεικνύουν ότι η ασφάλεια και η αξιοπιστία μπορούν να συνδυαστούν με την ευελιξία και την αποδοτικότητα. Παράλληλα, οι μελλοντικές κατευθύνσεις που βασίζονται στη χρήση τεχνητής νοημοσύνης και μηχανικής μάθησης, καθώς και στην ενοποίηση προτύπων με γνώμονα τη βιωσιμότητα, αναδεικνύουν ότι το μέλλον της τυποποίησης δεν θα περιοριστεί στη συμμόρφωση, αλλά θα αποτελέσει θεμελιώδη μοχλό για την επίτευξη ανθεκτικών, ασφαλών και περιβαλλοντικά υπεύθυνων συστημάτων. Συνολικά, η ενσωμάτωση των προτύπων και των βέλτιστων πρακτικών συνιστά αναγκαιότητα για την αποτελεσματική αντιμετώπιση των σύγχρονων τεχνολογικών και κοινωνικών προκλήσεων, καθιστώντας σαφές ότι η τυποποίηση αποτελεί στρατηγικό παράγοντα ανάπτυξης και ασφάλειας σε παγκόσμια κλίμακα.

7.3 Μαθήματα από Πραγματικές Περιπτώσεις

Η μελέτη περίπτωσης ανέδειξε πραγματικές ευπάθειες σε ρομποτικά IoT endpoints, όπως client-side validation, αδύναμο Bluetooth pairing και μη ασφαλή διαχείριση tokens. Οι επιπτώσεις σε privacy, safety και physical security κατέδειξαν την ανάγκη συνδυασμού reactive και proactive μέτρων: ενημερώσεις firmware, server-side authentication, network segmentation και signed firmware. Τα μαθήματα αυτά συνδέουν τη θεωρία με την πράξη και προτείνουν βέλτιστες πρακτικές για ασφαλή, αυτοΐατα συστήματα IoT.

7.4 Μελλοντικές προοπτικές

Η μελλοντική ανάπτυξη των συστημάτων αυτοΐασης αναμένεται να καθοριστεί από την πρόοδο στην τεχνητή νοημοσύνη, τα δίκτυα νέας γενιάς και τις κατανεμημένες υπολογιστικές αρχιτεκτονικές. Οι τεχνολογίες αυτές θα ενισχύσουν τις δυνατότητες προληπτικής ανίχνευσης και αυτόνομης αντιμετώπισης σφαλμάτων, διευρύνοντας τα πεδία εφαρμογής σε κρίσιμες υποδομές και έξυπνα περιβάλλοντα. Παράλληλα, η τυποποίηση και η διαλειτουργικότητα θα αποτελέσουν προϋποθέσεις για την ευρεία υιοθέτηση, ενώ η ενσωμάτωση αρχών βιωσιμότητας θα καταστήσει τα αυτοΐατα συστήματα όχι μόνο πιο ασφαλή και ανθεκτικά, αλλά και περιβαλλοντικά υπεύθυνα. Συνολικά, η αυτοΐαση θα αποτελέσει τον βασικό άξονα των μελλοντικών ψηφιακών υποδομών και γι’ αυτό είναι ένας κλάδος με τεράστια προοπτική και δυναμική.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] IoT.Business.News, "State of IoT 2024: Number of Connected IoT Devices Growing 13% to 18.8 Billion Globally," IoT Business News, Sep. 4, 2024. [Online]. Available: iotbusinessnews.com [Accessed: Aug. 31, 2025].

[2] DemandSage, "Internet of Things (IoT) Statistics: Market & Growth Data," 2024. [Online]. Available: https://www.demandsage.com/internet-of-things-statistics [Accessed: Aug. 31, 2025].

[3] Β. Αμανατίδης, "Απότομη αύξηση των κυβερνοεπιθέσεων σε IoT συσκευές καταγράφει η έρευνα της Check Point σε παγκόσμιο επίπεδο," IT Security Pro, Apr. 17, 2023. [Online]. Available: www.itsecuritypro.gr.

[4] S. Li, et al., "The Internet of Things: A Security Point of View," Internet Research, vol. 26, no. 2, pp. 337–359, Apr. 2016. [Online]. Available: https://doi.org/10.1108/IntR-07-2014-0173.

[5] GeeksforGeeks, "Important Self-Healing Patterns for Distributed Systems," Aug. 14, 2024. [Online]. Available: www.geeksforgeeks.org [Accessed: Aug. 21, 2025].

[6] GeeksforGeeks, "Self-Healing Systems System Design," Aug. 5, 2024. [Online]. Available: www.geeksforgeeks.org [Accessed: Aug. 21, 2025].

[7] C. J. Green, "Protocols for a Self-Healing Network," Proc. IEEE, vol. 1, pp. 252–256, Nov. 2002. [Online]. Available: https://ieeexplore.ieee.org/document/483308. DOI: 10.1109/MILCOM.1995.483308 [Accessed: Aug. 21, 2025].

[8] D. D. Bhavani, et al., "Machine Learning for Predictive Maintenance Applications in Industrial Equipment and Manufacturing Processes," ITM Web of Conferences, vol. 76, p. 01008, Jan. 2025. [Online]. Available: https://doi.org/10.1051/itmconf/20257601008.

[9] J. Meah, "Self-Healing Networks: AI's Role in Autonomous Cybersecurity," Techopedia, Jul. 2, 2025. [Online]. Available: www.techopedia.com. COI: 20.500.12592/1vpc6vy. [Accessed: Aug. 21, 2025].

[10] X. Fang, et al., "Smart Grid — the New and Improved Power Grid: A Survey," IEEE Commun. Surveys & Tutorials, vol. 14, no. 4, pp. 944–980, 2012. [Online]. Available: https://doi.org/10.1109/SURV.2011.101911.00087. [Accessed: Sep. 18, 2019].

[11] A. Mok, "Utilities Are Modernizing the Grid with AI amid Growing Energy Demands," Business Insider, Jul. 3, 2025. [Online]. Available: https://www.businessinsider.com/utilities-modernize-energy-grid-generative-ai-predictive-maintenance-2025-7 .

[12] B. J. Santos, et al., "Cyber Security in Health," in Advances in Information Security, Privacy, and Ethics, Jan. 2020, pp. 313–329. [Online]. Available: https://doi.org/10.4018/978-1-6684-6311-6.ch012 [Accessed: Oct. 18, 2024].

[13] H. Lu, et al., "Integrating Circular Economy and Industry 4.0 for Sustainable Supply Chain Management: A Dynamic Capability View," Production Planning & Control, vol. 35, no. 2, pp. 1–17, May 2022. [Online]. Available: https://doi.org/10.1080/09537287.2022.2063198

[14] S. Scotis, "How to Build AI-Powered Cities Intelligently," The Australian, Apr. 22, 2025. [Online]. Available: www.theaustralian.com.au/business/cfo-journal/how-to-build-aipowered-cities-intelligently

[15] S. Benneet, et al., "A Study on Cyber Security's Impact on Sustainable Advancements and Challenges," Feb. 2025. [Online]. Available: www.researchgate.net/publication/388708354_A_Study_on_Cyber_security's_Impact_on_Sustainable_Advancements_and_Challenges .

[16] Unidel.edu.ng, "Principles of Information Security," 2025. [Online]. Available: https://unidel.edu.ng//books/Principles_of_Information_Security.pdf .

[17] ISO, "ISO/IEC 27001:2013(En) Information Technology — Security Techniques — Information Security Management Systems — Requirements," 2013. [Online]. Available: https://www.iso.org/standard/27001

[18] NIST, "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1," Apr. 16, 2018. [Online]. Available: www.nvlpubs.nist.gov/NIST.CSWP.04162018.pdf

[19] ETSI, "ETSI Standards," 2019. [Online]. Available: https://www.etsi.org/images/files/AnnualReports/etsi-annual-report-december-2020.pdf .

[20] ENISA, "ENISA Threat Landscape 2021," Oct. 27, 2021. [Online]. Available: https://www.enisa.europa.eu/ENISA_Threat_Landscape_2021.pdf .

[21] OpenC2, "OpenC2 Standards," 2025. [Online]. Available: openc2.org [Accessed: Aug. 21, 2025].

[22] ISACA, Governance and Management Objectives, 2019. [Online]. Available: https://www.isaca.org/resources/cobit .

[23] XMPP, "XMPP RFCs," 2015. [Online]. Available: xmpp.org/rfcs/ [Accessed: Aug. 31, 2025].

[24] A. Al-Fuqaha, et al., "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," IEEE Commun. Surveys & Tutorials, vol. 17, no. 4, pp. 2347–2376, Jun. 2015. [Online]. Available: https://doi.org/10.1109/COMST.2015.2444095

[25] HiveMQ Team, "Introducing the MQTT Protocol – MQTT Essentials: Part 1," HiveMQ Blog, Jan. 12, 2015. [Online]. Available: https://www.hivemq.com/blog/mqtt-essentials-part-1-introducing-mqtt/

[26] C. Pautasso, et al., "Restful Web Services vs. Big Web Services," Proc. WWW, 2008. [Online]. Available: https://doi.org/10.1145/1367497.1367606.

[27] D. Guinard and V. Trifa, Towards the Web of Things: Web Mashups for Embedded Devices, Jan. 2009. [Online]. Available: www.researchgate.net/Towards_the_Web_of_Things_Web_Mashups

[28] NXP, "Safety Mechanisms Using the DDS Middleware in Software-Defined Cars," 2021. [Online]. Available: www.nxp.com/about-nxp/BL-SAFETY-MECHANISMS [Accessed: Aug. 31, 2025].

[29] P. Arntz, "Robot Vacuum Cleaners Hacked to Spy On, Insult Owners," Malwarebytes, Oct. 14, 2024. [Online]. Available: https://www.malwarebytes.com/blog/news/2024/10/robot-vacuum-cleaners-hacked-to-spy-on-insult-owners [Accessed: Sep. 7, 2025].

[30] B. Cost, "Hacked Robot Vacuums Hurl Racial Slurs at Shocked Owners," New York Post, Oct. 17, 2024. [Online]. Available: https://nypost.com/2024/10/17/tech/hacked-robot-vacuums-hurl-racial-slurs-at-shocked-owners-who-react-with-fear-disgust/ [Accessed: Sep. 7, 2025].

[31] L. Franceschi-Bicchierai, "Ecovacs Home Robots Can Be Hacked to Spy on Their Owners, Researchers Say," TechCrunch, Aug. 9, 2024. [Online]. Available: www.techcrunch.com/ecovacs-home-robots-can-be-hacked-to-spy-on-their-owners-researchers-say [Accessed: Sep. 7, 2025].

[32] P. Rauba, N. Seedat, K. Kacprzyk, M. van der Schaar, "Self-Healing Machine Learning: A Framework for Autonomous Adaptation in Real-World Environments," Proceedings of the 38th International Conference on Neural Information Processing Systems (NeurIPS 2024), 2024. [Online]. Available: https://openreview.net/forum?id=f63DKIpx0I . [Accessed: 11-Sep-2025].

[33] P. Rauba, N. Seedat, K. Kacprzyk, M. van der Schaar, "Self-healing machine learning," ACM Digital Library, Proceedings of NeurIPS 2024, DOI: 10.5555/3737916.3739252 . [Online]. Available: https://dl.acm.org/doi/10.5555/3737916.3739252 . [Accessed: 11-Sep-2025].

[34] O. Johnphill, A. S. Sadiq, F. Al-Obeidat, H. Al-Khateeb, M. A. Taheir, O. Kaiwartya, M. Ali, "Self-Healing in Cyber–Physical Systems Using Machine Learning: A Critical Analysis of Theories and Tools," Future Internet, vol. 15, no. 7, Art. 244, Jul. 2023. DOI: 10.3390/fi15070244 . [Online]. Available: https://www.mdpi.com/1999-5903/15/7/244 . [Accessed: 11-Sep-2025].