ΔΙΕΘΝΕΣ
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΤΗΣ ΕΛΛΑΔΟΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«Κυβερνοασφάλεια σε Φορετές Ιατρικές Συσκευές»

Του φοιτητή
Γιαννούλη Γεώργιου
Αρ. Μητρώου: 2020025

Επιβλέπων
Καθηγητής
Ηλιούδης Χρήστος

Ημερομηνία 23/1/2026

Τίτλος Δ.Ε.: Κυβερνοασφάλεια σε Φορετές Ιατρικές Συσκευές
Κωδικός Δ.Ε. : 25195
Ονοματεπώνυμο φοιτητή: Γεώργιος Γιαννούλης
Ονοματεπώνυμο εισηγητή : Χρήστος Ηλιούδης
Ημερομηνία ανάληψης Δ.Ε. : 20/3/2025
Ημερομηνία περάτωσης Δ.Ε.: 23/1/2026

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.

«Σε όσους έδωσαν χρόνο σε ό,τι είχε αξία.»

Πρόλογος

Η ραγδαία ανάπτυξη των ψηφιακών τεχνολογιών στον τομέα της υγείας και η αυξανόμενη χρήση φορητών και δικτυωμένων ιατρικών συσκευών έχουν αναδείξει σημαντικές προκλήσεις στον τομέα της κυβερνοασφάλειας. Η συνεχής συλλογή, μετάδοση και διαχείριση ευαίσθητων ιατρικών δεδομένων, ιδιαίτερα σε νοσοκομειακά και κλινικά περιβάλλοντα, καθιστούν αναγκαία τη συστηματική μελέτη των κινδύνων που σχετίζονται με την ασφάλεια, την αξιοπιστία και τη διαθεσιμότητα των συστημάτων αυτών.

Η επιλογή του συγκεκριμένου θέματος πραγματοποιήθηκε με στόχο την ενασχόληση με σύγχρονα και ιδιαίτερα επίκαιρα ζητήματα κυβερνοασφάλειας που αφορούν τις φορητές ιατρικές συσκευές και το Διαδίκτυο των Ιατρικών Πραγμάτων (IoMT). Στο πλαίσιο της παρούσας εργασίας αξιοποιήθηκε προσομοιωτικό περιβάλλον, το οποίο επέτρεψε τη συστηματική μελέτη σεναρίων κανονικής λειτουργίας και κυβερνοαπειλών, προσφέροντας μια ολοκληρωμένη και ελεγχόμενη προσέγγιση στο αντικείμενο.

Η εκπόνηση της παρούσας διπλωματικής εργασίας συνέβαλε ουσιαστικά στην εμβάθυνση γνώσεων στον τομέα της κυβερνοασφάλειας και στην κατανόηση της πολυπλοκότητας των σύγχρονων συστημάτων ψηφιακής υγείας. Παράλληλα, αποτέλεσε ένα σημαντικό ακαδημαϊκό εφόδιο και ενίσχυσε το ενδιαφέρον μου για περαιτέρω ενασχόληση με τον συγκεκριμένο επιστημονικό και ερευνητικό χώρο.

Περίληψη

Η παρούσα διπλωματική εργασία εξετάζει την κυβερνοασφάλεια στο οικοσύστημα του Internet of Medical Things (IoMT), με έμφαση στις φορητές ιατρικές συσκευές και στις προκλήσεις που προκύπτουν από την αυξανόμενη διασύνδεσή τους με δίκτυα και πληροφοριακά συστήματα υγείας. Η εκτεταμένη χρήση των συσκευών αυτών σε κλινικά και νοσοκομειακά περιβάλλοντα καθιστά κρίσιμη την προστασία της ακεραιότητας, της εμπιστευτικότητας και της αξιοπιστίας των ιατρικών δεδομένων.

Στο θεωρητικό και ερευνητικό μέρος της εργασίας παρουσιάζεται συστηματική ανάλυση των IoMT συστημάτων, εστιάζοντας στην αρχιτεκτονική τους, στην εγγενή πολυπλοκότητα ασφάλειας και στις κύριες κατηγορίες απειλών και κυβερνοεπιθέσεων που τα στοχεύουν. Παράλληλα, πραγματοποιείται ερευνητική μελέτη περίπτωσης, βασισμένη στη μελέτη πιέσεων, ευπαθειών και επιπτώσεων κυβερνοεπιθέσεων, σε συνδυασμό με τη διερεύνηση διεθνών προτύπων και κανονιστικών πλαισίων ασφάλειας, όπως τα MDR, ISO 14971, ISO 27001, καθώς και οι κατευθυντήριες οδηγίες των οργανισμών FDA και NIST. Η ανάλυση αυτή αναδεικνύει τη σημασία της διαχείρισης κινδύνων και της κανονιστικής συμμόρφωσης στον κύκλο ζωής των ιατρικών συσκευών.

Στο ίδιο κεφάλαιο εντάσσεται και η πρακτική μελέτη περίπτωσης της εργασίας, η οποία υλοποιείται μέσω προσομοίωσης σε περιβάλλον SIMUL8. Στο πλαίσιο αυτό, αναπτύσσεται ένα σύστημα ανίχνευσης εισβολών (Intrusion Detection System – IDS) βασισμένο σε κανόνες, το οποίο επεξεργάζεται δεδομένα από φορητές ιατρικές συσκευές. Η προσομοίωση επιτρέπει την πρακτική αξιολόγηση της συμπεριφοράς του συστήματος σε συνθήκες κανονικής λειτουργίας, αλλοίωσης, ελλιπών μετρήσεων και συνδυασμένων ανωμαλιών, καταδεικνύοντας τη δυνατότητα έγκαιρης και ερμηνεύσιμης ανίχνευσης μη φυσιολογικών δεδομένων.

Τέλος, η εργασία συνοψίζει τα συμπεράσματα, αναδεικνύει τους περιορισμούς της προσέγγισης και προτείνει μελλοντικές επεκτάσεις, με έμφαση στην αξιοποίηση τεχνικών μηχανικής μάθησης και υβριδικών συστημάτων ανίχνευσης. Συνολικά, η διπλωματική προσφέρει ένα συνεκτικό πλαίσιο θεωρητικής ανάλυσης, ερευνητικής μελέτης και πρακτικής αξιολόγησης της κυβερνοασφάλειας στο IoMT.

«Cybersecurity in Wearable Medical Devices»

«Georgios Giannoulis»

Abstract

This diploma thesis investigates cybersecurity issues within the Internet of Medical Things (IoMT) ecosystem, with particular emphasis on wearable medical devices and the challenges arising from their increasing interconnection with healthcare information systems and networks. The widespread deployment of such devices in clinical and hospital environments makes the protection of data integrity, confidentiality, and reliability a critical requirement.

In the theoretical and research-oriented part of the thesis, a systematic analysis of IoMT systems is presented, focusing on their architecture, inherent security complexity, and the main categories of cyber threats and attacks targeting them. Within this context, a research case study is conducted, based on the analysis of security pressures, vulnerabilities, and the potential impacts of cyberattacks on IoMT infrastructures. This analysis is complemented by an examination of international security standards and regulatory frameworks, including MDR, ISO 14971, ISO 27001, as well as guidelines issued by the FDA and NIST. The study highlights the importance of risk management and regulatory compliance throughout the lifecycle of medical devices.

In the same chapter, a distinct practical case study is presented, implemented through simulation using the SIMUL8 software environment. In this practical study, a rule-based Intrusion Detection System (IDS) is developed and evaluated, processing data originating from wearable medical devices. The simulation enables the practical assessment of system behavior under normal operating conditions, data tampering scenarios, missing measurements, and combined anomalies. The results demonstrate the capability of the IDS to detect abnormal data patterns in a timely and interpretable manner, assigning corresponding severity levels.

Finally, the thesis summarizes the overall findings, discusses the limitations of the proposed approach, and outlines directions for future work, with particular emphasis on the integration of machine learning techniques and hybrid intrusion detection systems. Overall, the thesis provides a coherent framework combining theoretical analysis, research case study, and practical evaluation for the study of cybersecurity in IoMT environments.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω την οικογένειά μου και ιδιαίτερα τους γονείς μου για τη συνεχή υποστήριξη τους καθ' όλη τη διάρκεια των σπουδών μου. Επιπλέον, ευχαριστώ θερμά τον επιβλέποντα καθηγητή μου κ. Ηλιούδη για την καθοδήγηση, τη στήριξη και τη συμβολή του στα πρώτα μου βήματα στον τομέα της κυβερνοασφάλειας.

Περιεχόμενα

Κατάλογος Σχημάτων

Κατάλογος Πινάκων

Κεφάλαιο 1ο: Εισαγωγή

1.1 Αντικείμενο της Διπλωματικής και Μέγεθος του Προβλήματος

Το Διαδίκτυο των Ιατρικών Πραγμάτων (Internet of Medical Things – IoMT) περιγράφει το οικοσύστημα διασυνδεδεμένων ιατρικών συσκευών (φορητών/wearables, εμφυτεύσιμων, οικιακών, κλινικών), λογισμικού και δικτύων που συλλέγουν, μεταδίδουν και αναλύουν ευαίσθητα βιοϊατρικά δεδομένα σε πραγματικό χρόνο [2], [5]. Στο πλαίσιο της εργασίας αυτής, εστιάζουμε ειδικά στο IoT for Medical Devices (IoTMD), δηλαδή στο υποσύνολο των συσκευών που μετρούν, επεξεργάζονται ή ενεργούν πάνω σε κλινικά κρίσιμες παραμέτρους (π.χ. καρδιοαναπνευστικά σήματα, γλυκόζη, δοσομέτρηση ινσουλίνης), και συνδέονται με πλατφόρμες τηλεπαρακολούθησης και ηλεκτρονικούς φακέλους υγείας [1], [2]. Η επιχειρησιακή αξία είναι μεγάλη: βελτίωση συμμόρφωσης θεραπείας, μείωση κόστους νοσηλείας, έγκαιρες κλινικές παρεμβάσεις και εξατομικευμένη φροντίδα [1].

Παράλληλα, η ραγδαία διείσδυση των IoTMD φέρνει μια εκθετική αύξηση επιφάνειας επίθεσης: περισσότερα τελικά σημεία, ετερογενή πρωτόκολλα (BLE, Zigbee, Wi-Fi/6, 5G), διαφορετικά firmware/OS, ποικίλοι προμηθευτές με ανόμοια κύκλα ενημερώσεων [2], [5]. Το πολυεπίπεδο μοντέλο του IoMT (Perception–Network–Application) συνεπάγεται ότι επιθέσεις μπορούν να εκδηλωθούν σε κάθε επίπεδο της αρχιτεκτονικής:

- Perception/Device: ανεπαρκής κρυπτογράφηση, αδύναμοι/επαναχρησιμοποιούμενοι κωδικοί, μη υπογεγραμμένα firmware, φυσικός χειρισμός/πλαστογράφηση αισθητήρων.
- Network: υποκλοπή (eavesdropping), MITM, δρομολόγηση μη ασφαλών API, πλαστογράφηση πακέτων.
- Application/Cloud: ελλιπής έλεγχος πρόσβασης/ρόλων, κακή διαχείριση μυστικών, ευπάθειες σε web services [2], [5].

Οι κυβερνοαπειλές που εκμεταλλεύονται τα παραπάνω κυμαίνονται από επιθέσεις εμπιστευτικότητας (παραβίαση απορρήτου, διαρροή ιατρικών δεδομένων), ακεραιότητας (αλλοίωση μετρήσεων – data tampering) έως διαθεσιμότητας (DoS/DDoS, ransomware με κρυπτογράφηση κρίσιμων συστημάτων) [2], [3]. Ιδίως το ransomware έχει αποδειχθεί καταστροφικό για οργανισμούς υγείας: διακοπή τηλεπαρακολούθησης, καθυστερήσεις σε διαγνώσεις/επεμβάσεις, απώλεια πρόσβασης σε EHR, επιχειρησιακός αντίκτυπος και κίνδυνος για την ασφάλεια ασθενών [3], [4]. Επιπλέον, επιθέσεις κοινωνικής μηχανικής (phishing/baiting) λειτουργούν συχνά ως αρχικός φορέας μόλυνσης, εκμεταλλευόμενες τον ανθρώπινο παράγοντα σε περιβάλλοντα υψηλής πίεσης χρόνου, όπως τα νοσοκομεία [4].

Το μέγεθος του προβλήματος δεν είναι μόνο τεχνικό αλλά και κλινικό και κανονιστικό: αλλοίωση δεδομένων αισθητήρα μπορεί να οδηγήσει σε λανθασμένες θεραπευτικές αποφάσεις, ενώ παραβιάσεις απορρήτου υπονομεύουν εμπιστοσύνη ασθενών και επιφέρουν ρυθμιστικές/νομικές συνέπειες (GDPR/HIPAA). Παρά την ύπαρξη διεθνών πλαισίων (λ.χ. ISO/IEC 27001, NIST SP 800-53), η ετερογένεια των IoTMD και η ανισομερής ωριμότητα διαδικασιών κυβερνοασφάλειας μεταξύ παρόχων/προμηθευτών δυσχεραίνουν την ομοιόμορφη συμμόρφωση και τη συνεχή διαχείριση κινδύνων [1], [5]. Η βιβλιογραφία αναδεικνύει ότι η έλλειψη τυποποιημένων ελέγχων στην αρχιτεκτονική των IoTMD, καθώς και ασυνεπείς πρακτικές ενημέρωσης (patching), αυξάνουν σημαντικά την πιθανότητα επιτυχούς επίθεσης [1], [2].

Συνοψίζοντας, το αντικείμενο της παρούσας εργασίας είναι η ολιστική μελέτη κυβερνοασφάλειας στα IoTMD/IoMT: χαρτογράφηση απειλών & ευπαθειών, εκτίμηση κινδύνου και ευθυγράμμιση με πρότυπα, με στόχο πρακτικές κατευθύνσεις που βελτιώνουν ανθεκτικότητα και κλινική ασφάλεια. Η ανάλυση που ακολουθεί στηρίζεται σε καθιερωμένες ταξινομίες και μεθοδολογίες ανάλυσης κινδύνων [2], πρόσφατες μελέτες για ransomware σε IoMT δίκτυα [3], πραγματικά περιστατικά/μελέτες

περίπτωσης [4], καθώς και προτάσεις ενοποίησης προτύπων σε περιβάλλοντα AI-ενισχυμένης υγείας [5].

1.2 Στόχοι της Διπλωματικής Εργασίας

Σύμφωνα με τους Alegría et al. [1] και Yasir & Iqbal [5], τα δίκτυα του Internet of Medical Things (IoMT) αποτελούν σύνθετα συστήματα όπου η ασφάλεια δεν αφορά μόνο την τεχνολογία αλλά και τη διασφάλιση της κλινικής αξιοπιστίας. Με βάση αυτήν την παραδοχή, ο κύριος στόχος της παρούσας διπλωματικής είναι η συστηματική μελέτη των απειλών, των ευπαθειών και των μηχανισμών προστασίας που αφορούν το IoMT και ειδικότερα τις φορητές ιατρικές συσκευές (IoTMD).

Η ανάλυση που ακολουθεί στηρίζεται σε καθιερωμένες ταξινομίες και μεθοδολογίες ανάλυσης κινδύνων για το Διαδίκτυο των Ιατρικών Πραγμάτων, όπως αυτές παρουσιάζονται στη σχετική βιβλιογραφία [2]. Παράλληλα, στοχεύει στην αξιολόγηση υφιστάμενων προτύπων ασφάλειας, προτείνοντας την ενοποίηση διεθνών πλαισίων (ISO/IEC 27001, NIST SP 800-53, GDPR, HIPAA) με σύγχρονες τεχνικές AI-based ανίχνευσης απειλών, σύμφωνα με τις προτάσεις των Yasir & Iqbal [5].

Οι επιμέρους στόχοι της εργασίας συνοψίζονται ως εξής:

1. Καταγραφή και ταξινόμηση απειλών που στοχεύουν συσκευές και υποδομές IoMT, όπως malware, phishing, ransomware και DoS επιθέσεις.
2. Εντοπισμός ευπαθειών σε επίπεδο hardware, δικτύου και λογισμικού, λαμβάνοντας υπόψη τη διαλειτουργικότητα και ετερογένεια των συσκευών IoTMD.
3. Αξιολόγηση κινδύνων (Risk Assessment) με τη χρήση συγκριτικών μεθοδολογιών (OCTAVE, ISO 31000, NIST 800-30).
4. Μελέτη διεθνών προτύπων ασφάλειας (ISO 27001, 27799, NIST SP 800-53, GDPR, HIPAA) και αξιολόγηση του βαθμού εφαρμογής τους σε IoMT περιβάλλοντα.
5. Επισκόπηση σύγχρονων τεχνικών άμυνας που αξιοποιούν Τεχνητή Νοημοσύνη και Μηχανική Μάθηση για ανίχνευση ανωμαλιών και πρόληψη επιθέσεων.
6. Ανάπτυξη μοντέλου προσομοίωσης για την αποτύπωση των επιπτώσεων κυβερνοεπιθέσεων σε φορητές ιατρικές συσκευές μέσω του SIMUL8 στο πλαίσιο μελέτης ransomware σε IoMT δίκτυα.

Η επιδίωξη είναι να διαμορφωθεί ένα πλαίσιο κυβερνοασφάλειας ειδικά προσαρμοσμένο στο IoTMD, το οποίο θα συνδυάζει τεχνικές και οργανωτικές πρακτικές με διεθνή πρότυπα και έξυπνους αλγορίθμους παρακολούθησης. Όπως επισημαίνουν οι Yasir & Iqbal [5], μόνο μέσα από ένα τέτοιο ενοποιημένο πλαίσιο είναι δυνατή η αποτελεσματική αντιμετώπιση των σύγχρονων κυβερνοαπειλών στο χώρο της υγείας.

1.3 Επιτεύγματα της Εργασίας

Η παρούσα διπλωματική εργασία επιτυγχάνει μια ολοκληρωμένη και πολυεπίπεδη προσέγγιση της κυβερνοασφάλειας στο οικοσύστημα του IoMT, συνδυάζοντας θεωρητική ανάλυση, κανονιστικό πλαίσιο και πρακτική αξιολόγηση. Αρχικά, πραγματοποιείται συστηματική αποτύπωση της αρχιτεκτονικής και της εγγενούς πολυπλοκότητας των IoMT συστημάτων, αναδεικνύοντας τα βασικά σημεία ευπάθειας σε επίπεδο συσκευών, δικτύων και εφαρμογών.

Στη συνέχεια, η εργασία συγκεντρώνει, αναλύει και συγκρίνει διεθνή πρότυπα και κανονιστικά πλαίσια ασφάλειας ιατρικών συσκευών, όπως το MDR της Ευρωπαϊκής Ένωσης, το ISO 14971, οι οδηγίες του FDA και τα τεχνικά πλαίσια του NIST, αναδεικνύοντας ομοιότητες, διαφορές και κενά εφαρμογής. Ιδιαίτερη έμφαση δίνεται στη συσχέτιση των απαιτήσεων αυτών με τον κύκλο ζωής των ιατρικών συσκευών και τη διαχείριση κινδύνου.

Επιπλέον, η εργασία ενσωματώνει πρακτική μελέτη περίπτωσης μέσω προσομοίωσης σε περιβάλλον Simul8, με στόχο την κατανόηση της επίδρασης κυβερνοεπιθέσεων και μηχανισμών αντιμετώπισης σε συστήματα IoMT. Μέσω της σύνδεσης θεωρίας, προτύπων και προσομοίωσης, η εργασία συμβάλλει

στην ουσιαστική κατανόηση της ασφάλειας των ιατρικών συσκευών σε σύγχρονα, σύνθετα ψηφιακά περιβάλλοντα.

1.4 Διάρθρωση της Εργασίας

Η παρούσα διπλωματική εργασία διαρθρώνεται σε επτά κεφάλαια, τα οποία ακολουθούν μια λογική κλιμάκωση από την ανάδειξη των προβλημάτων ασφάλειας έως την πρακτική αξιολόγηση και τη συνολική αποτίμηση των αποτελεσμάτων.

Στο Κεφάλαιο 1 παρουσιάζεται η εισαγωγή στο αντικείμενο της κυβερνοασφάλειας στο Internet of Medical Things (IoMT), ο σκοπός και οι στόχοι της εργασίας, καθώς και η συνολική διάρθρωσή της.

Το Κεφάλαιο 2 αναλύει τα βασικά προβλήματα και την αυξημένη πολυπλοκότητα ασφάλειας που χαρακτηρίζουν τις φορητές ιατρικές συσκευές, εξετάζοντας τεχνολογικούς, λειτουργικούς και οργανωτικούς παράγοντες που αυξάνουν την επιφάνεια επίθεσης στο περιβάλλον του IoMT.

Στο Κεφάλαιο 3 παρουσιάζονται τα διεθνή πρότυπα και οι βέλτιστες πρακτικές ασφάλειας που εφαρμόζονται σε συστήματα IoMT, με έμφαση σε αρχές ασφαλούς σχεδιασμού, διαχείρισης κινδύνου και προστασίας ιατρικών δεδομένων.

Το Κεφάλαιο 4 εξετάζει το κανονιστικό και νομοθετικό πλαίσιο ασφάλειας ιατρικών συσκευών, συμπεριλαμβανομένων των MDR, ISO 14971, ISO/IEC 27001, FDA και NIST, αναλύοντας τον ρόλο τους στη συμμόρφωση και τη διαχείριση κινδύνων στο IoMT.

Στο Κεφάλαιο 5 πραγματοποιείται αξιολόγηση ευπαθειών και των επιπτώσεών τους σε IoMT συσκευές, αναλύοντας σενάρια επιθέσεων, τεχνικές αδυναμίες και τις πιθανές συνέπειες για την ασφάλεια, τη λειτουργικότητα και την προστασία των ασθενών.

Το Κεφάλαιο 6 περιλαμβάνει τη θεωρητική μελέτη περίπτωσης και την πρακτική αξιολόγηση μέσω προσομοίωσης, παρουσιάζοντας την υλοποίηση και τον έλεγχο ενός συστήματος ανίχνευσης εισβολών (IDS) για δεδομένα φορητών ιατρικών συσκευών, καθώς και τα πειραματικά αποτελέσματα και τους περιορισμούς της προσέγγισης.

Τέλος, το Κεφάλαιο 7 συνοψίζει τα κύρια συμπεράσματα της διπλωματικής εργασίας και παρουσιάζει τις μελλοντικές επεκτάσεις, με έμφαση στις σύγχρονες τεχνικές άμυνας που αξιοποιούν Τεχνητή Νοημοσύνη και Μηχανική Μάθηση για την ανίχνευση ανωμαλιών και την πρόληψη επιθέσεων σε IoMT συστήματα.

1.5 Συμπεράσματα του Κεφαλαίου

Η παρούσα διπλωματική εργασία απευθύνεται σε φοιτητές, ερευνητές και επαγγελματίες του χώρου της Πληροφορικής, της Ηλεκτρονικής και των Συστημάτων Υγείας, οι οποίοι επιθυμούν να αποκτήσουν σφαιρική κατανόηση της κυβερνοασφάλειας στο Διαδίκτυο των Ιατρικών Πραγμάτων (IoMT). Όπως επισημαίνουν οι Yasir και Iqbal [5], η σύγχρονη υγειονομική τεχνολογία συνδυάζει πλέον ιατρικές συσκευές, τεχνητή νοημοσύνη και δικτυακές υποδομές, απαιτώντας διατομεακή γνώση που εκτείνεται από την ασφάλεια πληροφοριών έως τη ρυθμιστική συμμόρφωση.
Η εργασία μπορεί να αξιοποιηθεί από:

- Ακαδημαϊκούς και ερευνητές, οι οποίοι επιθυμούν να επεκτείνουν τη μελέτη τους σε θέματα κυβερνοασφάλειας υγείας, λαμβάνοντας υπόψη τις τεχνολογίες IoTMD και τα διεθνή πρότυπα ISO/NIST [1] [5].

- Μηχανικούς πληροφορικής και δικτύων, που εμπλέκονται στον σχεδιασμό και τη διαχείριση IoMT υποδομών, παρέχοντας πρακτικές οδηγίες για προστασία δεδομένων, έλεγχο πρόσβασης και αξιολόγηση κινδύνων [3] [6].
- Επαγγελματίες και διοικητικά στελέχη οργανισμών υγείας, οι οποίοι χρειάζονται τεκμηριωμένες πληροφορίες για την εφαρμογή προτύπων ασφαλείας και τη βελτίωση της ανθεκτικότητας των ιατρικών συστημάτων σε κυβερνοεπιθέσεις [4] [5].

Σύμφωνα με τους Alegría et al. [1], η κατανόηση των προτύπων ISO/IEC 27001 και ISO/IEC 27799 είναι κρίσιμη για την ορθή διαχείριση πληροφοριών υγείας, ενώ η ανάλυση των Malamas et al. [6] υπογραμμίζει τη σημασία της σωστής εκτίμησης κινδύνων (risk assessment) για τη διασφάλιση της συνεχούς λειτουργίας. Παράλληλα, οι Tariq et al. [3] δείχνουν ότι η έλλειψη εκπαίδευσης και προληπτικών μέτρων οδηγεί σε αυξημένη ευπάθεια έναντι ransomware επιθέσεων σε νοσοκομειακά δίκτυα, στοιχείο που καταδεικνύει τη χρησιμότητα της εργασίας και στο πρακτικό επίπεδο.

Η παρούσα διπλωματική συμβάλλει επομένως:

- στη θεωρητική κατανόηση των αρχών κυβερνοασφάλειας σε IoMT συστήματα,
- στην τεκμηριωμένη καταγραφή επιθέσεων και ευπαθειών βάσει σύγχρονης βιβλιογραφίας,
- και στην παρουσίαση πρακτικών προτάσεων και προτύπων που μπορούν να εφαρμοστούν σε πραγματικές ιατρικές υποδομές.

Επιπλέον, η εργασία αναδεικνύει τη χρησιμότητα της προσομοίωσης ως εργαλείου ανάλυσης και κατανόησης της συμπεριφοράς συστημάτων κυβερνοασφάλειας σε περιβάλλοντα IoMT, ενισχύοντας τη σύνδεση θεωρίας και πράξης και προσφέροντας μια ολοκληρωμένη θεώρηση της ασφάλειας στον χώρο των ιατρικών συσκευών.

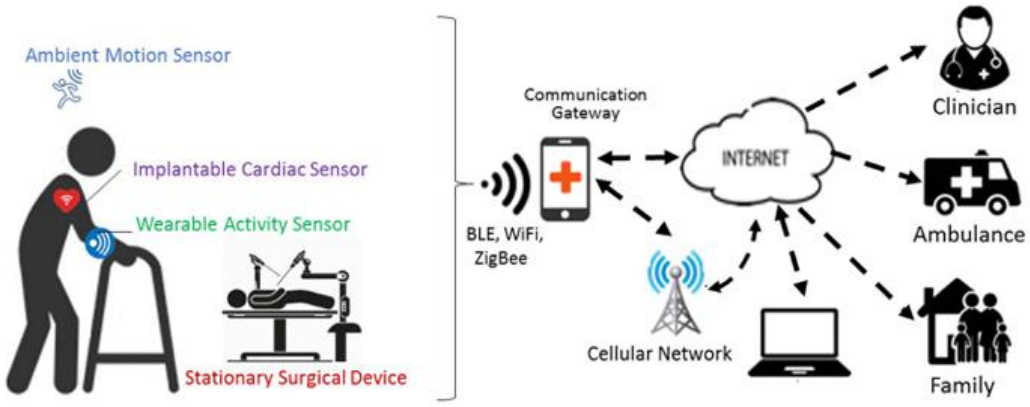
Κεφάλαιο 2ο: Προβλήματα και Πολυπλοκότητα Ασφάλειας στις Φορητές Ιατρικές Συσκευές

2.1 Εισαγωγή στο IOMT και στο θεωρητικό υπόβαθρο

Το Διαδίκτυο των Ιατρικών Πραγμάτων (Internet of Medical Things – IoMT) ορίζεται ως το δίκτυο διασυνδεδεμένων ιατρικών συσκευών, αισθητήρων, λογισμικών και πληροφοριακών συστημάτων, που συλλέγουν και ανταλλάσσουν ευαίσθητα ιατρικά δεδομένα με σκοπό τη βελτίωση της διάγνωσης, της πρόληψης και της παροχής φροντίδας υγείας [2]. Όπως επισημαίνουν οι Alegría et al. [1], το IoMT αποτελεί εξέλιξη του κλασικού Internet of Things (IoT) και προσαρμόζεται ειδικά στις απαιτήσεις του τομέα της υγείας, συνδέοντας φορητές συσκευές, εμφυτεύσιμα όργανα, ιατρικά μηχανήματα, πλατφόρμες τηλεϊατρικής και νοσοκομειακά πληροφοριακά συστήματα.

Σύμφωνα με τους Alsubaei et al. [2], η αρχιτεκτονική του IoMT οργανώνεται σε τρία διακριτά επίπεδα:

- Το επίπεδο αντίληψης (Perception Layer), που περιλαμβάνει τις συσκευές και τους αισθητήρες που συλλέγουν δεδομένα φυσιολογικών μετρήσεων (π.χ. καρδιακός παλμός, πίεση, θερμοκρασία).
- Το επίπεδο δικτύου (Network Layer), μέσω του οποίου τα δεδομένα μεταφέρονται σε πραγματικό χρόνο, χρησιμοποιώντας ποικιλία πρωτοκόλλων επικοινωνίας όπως Bluetooth Low Energy (BLE), Zigbee, Wi-Fi και 5G.
- Το επίπεδο εφαρμογής (Application Layer), όπου τα δεδομένα αποθηκεύονται και αναλύονται σε πλατφόρμες cloud ή σε νοσοκομειακά πληροφοριακά συστήματα (HIS, EHR), προσφέροντας δυνατότητες τηλεπαρακολούθησης και έξυπνων ειδοποιήσεων.



Σχήμα 2.1 : Σύστημα απομακρυσμένης παρακολούθησης ασθενών (IoMT) [2]

Το σχήμα απεικονίζει τη λειτουργική αρχιτεκτονική ενός συστήματος IoMT με φορητές, εμφυτεύσιμες και σταθερές ιατρικές συσκευές που μεταδίδουν δεδομένα μέσω BLE/Wi-Fi/ZigBee σε cloud πλατφόρμες και κατόπιν σε γιατρούς, οικογένεια και υπηρεσίες υγείας.Οι Yasir και Iqbal [5] αναφέρουν ότι το IoMT μπορεί να θεωρηθεί ως ένα σύστημα δυναμικής αλληλεπίδρασης μεταξύ φυσικών και ψηφιακών οντοτήτων, το οποίο βασίζεται σε αυτοματοποιημένες διαδικασίες λήψης αποφάσεων. Παράλληλα, η χρήση αλγορίθμων τεχνητής νοημοσύνης σε επίπεδο εφαρμογής έχει καταστήσει δυνατή την προγνωστική ανάλυση δεδομένων, επιτρέποντας τη δημιουργία έξυπνων συστημάτων διάγνωσης και υποστήριξης κλινικών αποφάσεων.

Ωστόσο, όπως επισημαίνουν οι Alsubaei et al. [2], η σύνθετη αυτή αρχιτεκτονική συνεπάγεται και πολλαπλά σημεία ευπάθειας. Κάθε επίπεδο του IoMT παρουσιάζει ξεχωριστές απειλές: στο επίπεδο αντίληψης οι συσκευές είναι εκτεθειμένες σε φυσική παραβίαση και υποκλοπή δεδομένων· στο

επίπεδο δικτύου οι επιθέσεις τύπου man-in-the-middle (MITM) και packet sniffing απειλούν την ακεραιότητα και την εμπιστευτικότητα· ενώ στο επίπεδο εφαρμογής, μη ασφαλείς διεπαφές (API) ή αδύναμη διαχείριση πρόσβασης επιτρέπουν τη μη εξουσιοδοτημένη πρόσβαση σε ιατρικά δεδομένα [2] [5].

Σύμφωνα με τους Alegría et al. [1], η έλλειψη ομοιογενών προτύπων ασφάλειας και ελέγχου συμμόρφωσης δυσχεραίνει τη δημιουργία ενός ενιαίου πλαισίου προστασίας. Παράλληλα, οι Yasir και Iqbal [5] υπογραμμίζουν ότι στα AI-based δίκτυα υγείας, ακόμη και μια μικρή αλλοίωση δεδομένων μπορεί να προκαλέσει εσφαλμένες προβλέψεις ή λάθος ιατρικές αποφάσεις, καθιστώντας την κυβερνοασφάλεια κρίσιμο παράγοντα για την ασφάλεια των ασθενών.

Καθώς το IoMT συνδέει την τεχνολογία με τον ανθρώπινο οργανισμό, η προστασία της ακεραιότητας, εμπιστευτικότητας και διαθεσιμότητας των δεδομένων καθίσταται ζήτημα όχι μόνο ψηφιακής αλλά και βιολογικής ασφάλειας. Η ανάλυση που ακολουθεί επικεντρώνεται στις βασικές κατηγορίες επιθέσεων και στα είδη απειλών που επηρεάζουν τα συστήματα IoMT, θέτοντας τα θεμέλια για τη συζήτηση των ευπαθειών και των μηχανισμών προστασίας στα επόμενα τμήματα.

2.2 Κατηγορίες επιθέσεων στο IOMT

Το οικοσύστημα του Internet of Medical Things (IoMT) αποτελείται από εκατοντάδες ετερογενείς συσκευές – φορητές, εμφυτεύσιμες και νοσοκομειακές – που επικοινωνούν μέσω ποικιλίας πρωτοκόλλων και λογισμικών περιβαλλόντων. Αυτή η πολυπλοκότητα δημιουργεί πλήθος σημείων πρόσβασης για κυβερνοεπιθέσεις, καθιστώντας τα συστήματα υγείας έναν από τους πιο ευάλωτους τομείς παγκοσμίως [12]. Οι επιθέσεις στο IoMT παρουσιάζουν μεγάλη ποικιλία ως προς τη φύση, το κίνητρο και το τεχνολογικό τους βάθος [2].

2.2.1 Επιθέσεις στην εμπιστευτικότητα (Confidentiality)

Η εμπιστευτικότητα αφορά τη διασφάλιση ότι τα ιατρικά δεδομένα παραμένουν προσιτά μόνο σε εξουσιοδοτημένα μέρη. Όπως επισημαίνουν οι Alsubaei et al. [2], συνηθισμένες τεχνικές παραβίασης είναι η υποκλοπή επικοινωνίας (eavesdropping) σε κανάλια BLE ή Wi-Fi, οι Man-in-the-Middle (MITM) επιθέσεις και η εκμετάλλευση μη κρυπτογραφημένων API στο cloud. Σύμφωνα με τους Koutras et al. [9], το περιβάλλον του IoMT πάσχει συχνά από ασυνεπείς υλοποιήσεις πρωτοκόλλων και έλλειψη κοινών μηχανισμών αυθεντικοποίησης μεταξύ συσκευών και πλατφορμών. Οι παραβιάσεις αυτές οδηγούν σε διαρροή ευαίσθητων δεδομένων ασθενών, παραβίαση του GDPR και απώλεια εμπιστοσύνης προς τους παρόχους υγείας [7].

2.2.2 Επιθέσεις στην ακεραιότητα (Integrity)

Οι επιθέσεις στην ακεραιότητα επιδιώκουν την αλλοίωση ή παραποίηση των δεδομένων που παράγουν οι συσκευές IoMT. Όπως επισημαίνεται στη σχετική βιβλιογραφία, επιθέσεις όπως το data tampering και τα replay attacks μπορούν να μεταβάλουν τιμές κρίσιμων βιοϊατρικών μετρήσεων, οδηγώντας σε λανθασμένες διαγνώσεις ή λήψη εσφαλμένων θεραπευτικών αποφάσεων [2]. Οι Alsubaei et al. [2] τονίζουν ότι οι επιθέσεις αυτές καθίστανται ιδιαίτερα επικίνδυνες όταν συνδυάζονται με ανεπαρκείς μηχανισμούς επαλήθευσης, όπως η απουσία ψηφιακής υπογραφής σε ενημερώσεις λογισμικού ή μεταφορές αρχείων. Επιπλέον, η πολυπλοκότητα των αλυσίδων εξαρτήσεων μεταξύ λογισμικού και αισθητήρων μπορεί να οδηγήσει σε αλυσιδωτές επιπτώσεις, όπου μία μικρή τροποποίηση σε ένα υποσύστημα προκαλεί σοβαρές αστοχίες στην επεξεργασία δεδομένων [12].

2.2.3 Επιθέσεις στη διαθεσιμότητα (Availability)

Η διαθεσιμότητα είναι κρίσιμη σε περιβάλλοντα υγείας· η παύση λειτουργίας μπορεί να κοστίσει ζωές. Οι DoS και DDoS επιθέσεις αποτελούν τον πιο συχνό μηχανισμό παραβίασης της αρχής αυτής [12]. Οι επιθέσεις τύπου botnet εκμεταλλεύονται την ελλιπή ενημέρωση συσκευών και τη διασπορά τους σε διαφορετικά δίκτυα, γεγονός που αυξάνει εκθετικά την πολυπλοκότητα της αντιμετώπισης. Όπως αναφέρει η ENISA [12], το ransomware παραμένει μία από τις πιο καταστροφικές μορφές επίθεσης στον τομέα της υγείας, προκαλώντας διακοπές παρακολούθησης και αναστολή λειτουργίας νοσοκομειακών συστημάτων. Οι Tariq et al. [3] περιγράφουν τον κύκλο ζωής τέτοιων επιθέσεων με την σειρά: διείσδυση, εξάπλωση, κρυπτογράφηση δεδομένων, εκβιασμός.

2.2.4 Κοινωνική μηχανική και ανθρώπινος παράγοντας

Πέρα από τις τεχνικές απειλές, ο ανθρώπινος παράγοντας παραμένει η «αδύναμη αλυσίδα». Οι επιθέσεις κοινωνικής μηχανικής (social engineering) όπως το phishing, το pretexting και το baiting χρησιμοποιούνται για την εγκατάσταση malware ή τη διαρροή διαπιστευτηρίων [4]. Σε πολλά νοσοκομεία, το προσωπικό έχει περιορισμένη εκπαίδευση σε ζητήματα ασφάλειας, γεγονός που ενισχύει τη συστημική πολυπλοκότητα της προστασίας [12]. Η ενσωμάτωση προγραμμάτων εκπαίδευσης και πολιτικών πολλαπλής επαλήθευσης (MFA) είναι ουσιώδης για την ελαχιστοποίηση τέτοιων κινδύνων.

2.2.5 Συνθετική ανάλυση και συσχέτιση με πολυπλοκότητα

Η ταξινομία των Alsubaei et al. [2] και Rasool et al. [7] δείχνει ότι η πολυπλοκότητα στο IoMT προκύπτει από τη συνύπαρξη πολλών επιπέδων και παικτών στο οικοσύστημα: κατασκευαστές, πάροχοι λογισμικού, cloud operators και νοσοκομεία. Η έλλειψη ενιαίων πρωτοκόλλων διαχείρισης ασφάλειας καθιστά δυσχερή την αντιμετώπιση συνδυαστικών επιθέσεων, όπου ένα σφάλμα σε χαμηλό επίπεδο μπορεί να εκμεταλλευθεί μια λογική ευπάθεια σε ανώτερο. Όπως παρατηρεί η ENISA [12], η διασύνδεση με cloud και mobile εφαρμογές έχει πολλαπλασιάσει την «επιφάνεια επίθεσης», ενώ η αυξανόμενη εξάρτηση από AI προσθέτει νέες διαστάσεις κινδύνου (π.χ. model poisoning, adversarial attacks).

2.3 Ευπάθειες και πολυπλοκότητα στο IOMT

Η ασφάλεια στο οικοσύστημα του Internet of Medical Things (IoMT) καθορίζεται από ένα πλέγμα αλληλεξαρτήσεων μεταξύ συσκευών, λογισμικών, πρωτοκόλλων και κανονιστικών απαιτήσεων. Η πολυπλοκότητα αυτών των συστημάτων αποτελεί εγγενές χαρακτηριστικό και, ταυτόχρονα, βασική πηγή ευπαθειών [6]. Όπως επισημαίνουν οι Alsubaei et al. [2], κάθε επίπεδο της αρχιτεκτονικής του IoMT — από το perception έως το application — παρουσιάζει μοναδικές τεχνικές αδυναμίες, οι οποίες εντείνονται από τη συνεχή αλληλεπίδραση πολλών φορέων (κατασκευαστών, προγραμματιστών, παρόχων cloud, νοσοκομείων).

2.3.1 Τεχνικές Ευπάθειες ανά Επίπεδο

Στο επίπεδο αντίληψης (Perception Layer), το οποίο περιλαμβάνει αισθητήρες, φορητές και εμφυτεύσιμες συσκευές, οι ευπάθειες σχετίζονται με αδύναμους μηχανισμούς ταυτοποίησης, ανεπαρκή κρυπτογράφηση και έλλειψη ενημερώσεων firmware [2]. Οι Koutras et al. [9] επισημαίνουν ότι το Bluetooth Low Energy (BLE), αν και ενεργειακά αποδοτικό, είναι ιδιαίτερα ευάλωτο σε επιθέσεις υποκλοπής και spoofing, ειδικά όταν χρησιμοποιούνται προεπιλεγμένα ή κοινόχρηστα κλειδιά.

Στο επίπεδο δικτύου (Network Layer), η πολυπλοκότητα αυξάνεται λόγω της χρήσης πολλαπλών πρωτοκόλλων (Wi-Fi, Zigbee, 5G) και ετερογενών συστημάτων μετάδοσης δεδομένων. Αυτή η

ετερογένεια δημιουργεί ευπάθειες διαλειτουργικότητας (interoperability vulnerabilities), όπου η μία συσκευή δεν μπορεί να επιβεβαιώσει την ταυτότητα της άλλης, καθιστώντας δυνατές επιθέσεις Man-in-the-Middle (MITM) και Replay [9]. Οι Rasool et al. [7] αναφέρουν ότι ο κατακερματισμός των δικτυακών προτύπων οδηγεί σε μη ενοποιημένη διαχείριση κλειδιών και ασυμβατότητα πιστοποιητικών, προσθέτοντας σημαντική λειτουργική πολυπλοκότητα.

Στο επίπεδο εφαρμογής (Application Layer), οι ευπάθειες εντοπίζονται στις cloud πλατφόρμες και στα APIs των εφαρμογών τηλεϊατρικής. Ανεπαρκής έλεγχος ταυτότητας χρηστών, μη ασφαλής διαχείριση συνεδριών και κακή αποθήκευση διαπιστευτηρίων οδηγούν σε παραβιάσεις εμπιστευτικότητας και αλλοίωση δεδομένων [2]. Η ENISA [12] καταγράφει ότι τα περισσότερα περιστατικά στον τομέα υγείας τα τελευταία χρόνια σχετίζονται με διαρροές δεδομένων μέσω cloud misconfigurations και ransomware επιθέσεων.

2.4 Μεθοδολογίες εκτίμησης κινδύνου στο IOMT

Η αυξανόμενη πολυπλοκότητα του οικοσυστήματος IoMT απαιτεί την εφαρμογή δομημένων μεθοδολογιών εκτίμησης κινδύνου, ώστε να εντοπίζονται οι πιο κρίσιμες ευπάθειες και να καθορίζονται οι κατάλληλες στρατηγικές μετριασμού. Σε αντίθεση με τις παραδοσιακές προσεγγίσεις ασφάλειας πληροφοριακών συστημάτων, τα συστήματα IoMT συνδυάζουν τεχνικά, οργανωτικά και κανονιστικά στοιχεία, τα οποία καθιστούν αναγκαία μια ολιστική αξιολόγηση [6].

2.4.1 Ανάγκη για συστηματική εκτίμηση κινδύνου

Όπως επισημαίνουν οι Malamas et al. [6], η εκτίμηση κινδύνου στο IoMT πρέπει να λαμβάνει υπόψη τη δυναμική φύση των συσκευών, την ετερογένεια των πρωτοκόλλων και τη διαφορετικότητα των περιβαλλόντων χρήσης. Η απουσία ενιαίων μεθοδολογιών οδηγεί σε αποσπασματική αξιολόγηση και δυσκολία στην ιεράρχηση απειλών. Οι Rasool et al. [7] τονίζουν ότι οι αλληλεπιδράσεις πολλών εμπλεκόμενων φορέων αυξάνουν τη συστημική πολυπλοκότητα, καθιστώντας αναγκαία τη χρήση πολυεπίπεδων εργαλείων αξιολόγησης. Επιπλέον, η ENISA [12] αναγνωρίζει ότι ο τομέας της υγείας αποτελεί έναν από τους πλέον ευάλωτους κλάδους, προτείνοντας την υιοθέτηση risk-driven στρατηγικών βασισμένων σε ποσοτικοποιημένους δείκτες κινδύνου.

2.4.2 Βασικά πλαίσια και πρότυπα εκτίμησης κινδύνου

Σύμφωνα με τους Malamas et al. [6], μεταξύ των πιο ευρέως χρησιμοποιούμενων μεθοδολογιών για την αξιολόγηση κινδύνου στο IoMT αποτελούν τα παρακάτω τέσσερα θεσμικά πλαίσια:

1. NIST SP 800-30 (Risk Management Guide for Information Systems)

Το πρότυπο του National Institute of Standards and Technology (NIST) καθορίζει μια διαδικασία τεσσάρων βημάτων ανάλυσης:

i. Προσδιορισμός απειλών και ευπαθειών,
ii. Εκτίμηση πιθανοτήτων και επιπτώσεων,
iii. Υπολογισμός επιπέδου κινδύνου,
iv. Καθορισμός ελέγχων μετριασμού.

Το NIST συνιστά τη χαρτογράφηση των απειλών στις CIA παραμέτρους (Confidentiality, Integrity, Availability) και προτείνει την παρακολούθηση των κινδύνων καθ’ όλη τη διάρκεια ζωής του προϊόντος.

2. ISO 31000 – Risk Management Framework

Το πρότυπο ISO 31000 παρέχει ένα γενικό πλαίσιο διαχείρισης κινδύνων για όλους τους οργανισμούς. Στο IoMT εφαρμόζεται ως δομή συντονισμού μεταξύ τεχνικών ομάδων, νοσοκομείων και ρυθμιστικών φορέων. Εστιάζει στη συνεχή αξιολόγηση και την επικαιροποίηση των κινδύνων με βάση επιχειρησιακές αλλαγές.

3. OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)

Αναπτύχθηκε από το Carnegie Mellon University και χρησιμοποιείται για ποιοτική εκτίμηση κινδύνου σε κρίσιμες υποδομές. Οι Malamas et al. [6] προτείνουν την προσαρμογή του OCTAVE σε περιβάλλοντα IoMT, εστιάζοντας στην ανάλυση περιουσιακών στοιχείων (assets) όπως ιατρικές συσκευές, εφαρμογές και δεδομένα ασθενών.

4. NISTIR 8259 – Device Cybersecurity Capabilities

Το NISTIR 8259 [10] αποτελεί θεμέλιο για την ενσωμάτωση ασφάλειας στον σχεδιασμό συσκευών. Ορίζει έξι βασικές δυνατότητες (π.χ. ταυτοποίηση, ενημερώσεις, προστασία δεδομένων, logging) και συνιστά την ενσωμάτωσή τους στον κύκλο ζωής κάθε IoMT προϊόντος. Έτσι, η εκτίμηση κινδύνου δεν περιορίζεται στη λειτουργική φάση αλλά ξεκινά ήδη από το στάδιο της ανάπτυξης.

2.4.3 Προσαρμογή στις ρυθμιστικές απαιτήσεις

Η FDA [11] έχει ενσωματώσει στις οδηγίες της (2023) μια προσέγγιση “Security by Design and by Lifecycle”, απαιτώντας από τους κατασκευαστές να εφαρμόζουν συνεχή risk monitoring, vulnerability reporting και patch management. Οι κανονισμοί αυτοί συνδέουν τις τεχνικές εκτιμήσεις κινδύνου με τη νομοθετική συμμόρφωση, καθιστώντας την ασφάλεια των συσκευών διαρκή διαδικασία και όχι εφάπαξ ενέργεια.

Παράλληλα, η ENISA [12] υπογραμμίζει ότι η εκτίμηση κινδύνου πρέπει να επεκτείνεται πέρα από τα τεχνικά μέτρα, λαμβάνοντας υπόψη ανθρώπινους και οργανωτικούς παράγοντες, όπως εκπαίδευση προσωπικού, πολιτικές πρόσβασης και διαχείριση συμβάντων. Έτσι, επιτυγχάνεται πολυεπίπεδη προσέγγιση ασφάλειας, η οποία μειώνει τις αβεβαιότητες που προκύπτουν από την πολυπλοκότητα του IoMT.

2.4.4 Ενσωμάτωση Εκτίμησης Κινδύνου στη Διαχείριση Πολυπλοκότητας

Η αξιολόγηση κινδύνου στο IoMT δεν αποτελεί μεμονωμένο βήμα αλλά συνεχή δραστηριότητα μέσα σε ένα κύκλο ζωής (lifecycle) που περιλαμβάνει σχεδίαση, λειτουργία, συντήρηση και απόσυρση συσκευών. Οι Malamas et al. [6] και το NIST [10] τονίζουν ότι η διαχείριση της πολυπλοκότητας απαιτεί τυποποιημένη τεκμηρίωση και συνεχή ενημέρωση των μηχανισμών ανάλυσης. Η δημιουργία ενιαίου risk registry για όλα τα υποσυστήματα επιτρέπει την ανίχνευση αλληλεπιδράσεων μεταξύ επιπέδων και βοηθά στον έγκαιρο εντοπισμό κρίσιμων σημείων ευπάθειας.

Στο πλαίσιο αυτό, η συνεργασία μεταξύ τεχνικών ομάδων, ιατρικού προσωπικού και ρυθμιστικών αρχών είναι καθοριστική. Η συνδυαστική εφαρμογή των προτύπων NIST, ISO και FDA δημιουργεί μια πολυεπίπεδη ασπίδα προστασίας, που επιτρέπει την εξισορρόπηση ανάμεσα στην καινοτομία και την ασφάλεια. Η κατανόηση και διαχείριση της πολυπλοκότητας μέσω δομημένων risk frameworks αποτελεί τη βάση για τη συνεχή βελτίωση της ασφάλειας στα δίκτυα IoMT.

Κεφάλαιο 3ο: Πρότυπα και Βέλτιστες Πρακτικές Ασφάλειας

3.1 Εισαγωγή στα πρότυπα ασφάλειας του IoMT

Η ανάλυση του Κεφαλαίου 2 κατέδειξε ότι η ασφάλεια στο οικοσύστημα του Internet of Medical Things (IoMT) διαμορφώνεται από μια σύνθετη αλληλεξάρτηση συσκευών, πρωτοκόλλων, υπηρεσιών cloud/edge και οργανωτικών διαδικασιών. Η πολυπλοκότητα αυτή επιβάλλει την υιοθέτηση τυποποιημένων πλαισίων ασφάλειας που προσφέρουν κοινό λεξιλόγιο, σαφείς ελάχιστες απαιτήσεις και επαναλήψιμες διαδικασίες αξιολόγησης και ελέγχου. Τα πρότυπα λειτουργούν ως «γέφυρα» ανάμεσα στις τεχνικές πρακτικές και στις κανονιστικές υποχρεώσεις των οργανισμών υγείας, μειώνοντας την αβεβαιότητα και επιτρέποντας συστηματική διαχείριση κινδύνων σε όλο τον κύκλο ζωής των ιατρικών συσκευών [6], [10], [11], [12].

Σε επιχειρησιακό επίπεδο, η συμμόρφωση με συστήματα διαχείρισης ασφάλειας πληροφοριών (π.χ. ISO/IEC 27001) θέτει τις βάσεις για πολιτικές, ρόλους, διαδικασίες και τεχνικούς ελέγχους που αφορούν τα δεδομένα υγείας και τις υποδομές. Στο πλαίσιο του IoMT, η βιβλιογραφία δείχνει ότι η αρχιτεκτονική και οι ροές δεδομένων μπορούν να χαρτογραφηθούν πάνω σε τέτοια συστήματα, ώστε οι έλεγχοι να «δένονται» με συγκεκριμένες διεργασίες τηλεπαρακολούθησης και διαλειτουργικότητας [1], [6], [12]. Παράλληλα, η προσέγγιση βασισμένη στον κίνδυνο (risk-based) που περιγράφεται σε διεθνή πλαίσια επιτρέπει ιεράρχηση ευπαθειών και στοχευμένη κατανομή πόρων, κάτι κρίσιμο σε ετερογενή περιβάλλοντα IoMT [6].

Σε τεχνικο-ρυθμιστικό επίπεδο, το NISTIR 8259 ορίζει baseline δυνατότητες κυβερνοασφάλειας για IoT/IoMT συσκευές (ταυτοποίηση, ασφαλείς ενημερώσεις, προστασία δεδομένων, καταγραφή γεγονότων κ.ά.), προωθώντας την αρχή “security by design” από τη φάση της σχεδίασης έως την απόσυρση [10]. Συμπληρωματικά, οι οδηγίες της FDA μεταφράζουν αυτή τη φιλοσοφία σε συγκεκριμένες απαιτήσεις κύκλου ζωής (premarket/postmarket) για ιατρικές συσκευές: τεκμηριωμένο risk management, διαδικασίες ενημερώσεων/patching, ευπάθειες και υπεύθυνη γνωστοποίηση (coordinated vulnerability disclosure) [11]. Η σύγκλιση αυτών των πλαισίων επιδιώκει να περιορίσει συστημικές ασυνέπειες, που όπως είδαμε, τροφοδοτούν την πολυπλοκότητα (π.χ. ανομοιόμορφα firmware, ασυμβατότητες πρωτοκόλλων) [6], [10], [11].

Τέλος, το απειλητικό τοπίο του υγειονομικού τομέα, όπως αποτυπώνεται σε ENISA threat reports, προσδίδει εμπειρικό βάρος στην αναγκαιότητα των προτύπων: η κλιμάκωση περιστατικών ransomware/DoS, οι αδυναμίες σε cloud/misconfigurations και οι αλυσίδες προμηθευτών υπαγορεύουν πλαισιοθετημένη άμυνα με πολιτικές, τεχνικά μέτρα και συνεχή παρακολούθηση [12]. Η βιβλιογραφία αναδεικνύει επίσης τον ρόλο αναδυόμενων τεχνολογιών (AI για ανίχνευση ανωμαλιών, ασφαλείς αρχιτεκτονικές διαλειτουργικότητας) οι οποίες, όταν εντάσσονται σε τυποποιημένες διαδικασίες, ενισχύουν την αποτελεσματικότητα ελέγχων χωρίς να προσθέτουν ανεξέλεγκτη πολυπλοκότητα [5], [6], [12].

Συνοψίζοντας, τα πρότυπα και τα πλαίσια ασφάλειας λειτουργούν ως οργανωτική και τεχνική «ραχοκοκαλιά» για το IoMT: καθορίζουν τι πρέπει να προστατευθεί, πώς θα ελέγχεται διαρκώς και πότε/από ποιον λαμβάνονται αποφάσεις μετριασμού. Στις επόμενες ενότητες του Κεφαλαίου 3 θα παρουσιαστούν συστηματικά τα καίρια πρότυπα και κανονιστικά πλαίσια, καθώς και οι αντίστοιχες τεχνολογίες άμυνας που τα υλοποιούν στην πράξη, με άμεση αντιστοίχιση στα ευρήματα πολυπλοκότητας του Κεφαλαίου 2 [1], [5], [6], [10], [11], [12].

3.2 Διεθνή Πρότυπα και Κανονιστικά Πλαίσια για την Ασφάλεια στο IoMT

Η αυξανόμενη πολυπλοκότητα των συστημάτων Internet of Medical Things (IoMT), σε συνδυασμό με την ευαισθησία των ιατρικών δεδομένων, καθιστά απαραίτητη τη συμμόρφωση με ένα σύνολο διεθνών προτύπων και κανονιστικών πλαισίων που ορίζουν ελάχιστες απαιτήσεις ασφάλειας, ιδιωτικότητας και διαχείρισης κινδύνων. Τα πρότυπα αυτά προσφέρουν ένα κοινό σημείο αναφοράς για την ενοποίηση τεχνικών, οργανωτικών και νομικών απαιτήσεων, διασφαλίζοντας ότι οι ιατρικές συσκευές συμμορφώνονται τόσο με τεχνικά όσο και με θεσμικά κριτήρια [6], [10], [11], [12].

3.2.1 ISO/IEC 27001:2022 – Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών

Το ISO/IEC 27001:2022 αποτελεί το βασικό διεθνές πρότυπο για την ανάπτυξη, υλοποίηση και συντήρηση ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISMS) [13]. Βασίζεται στην αρχή της συνεχούς βελτίωσης (Plan–Do–Check–Act) και καθορίζει τις διαδικασίες για τον εντοπισμό κινδύνων, τον σχεδιασμό ελέγχων και την παρακολούθηση της αποτελεσματικότητας των μέτρων ασφαλείας.

Στο πλαίσιο του IoMT, η εφαρμογή του ISO 27001 συμβάλλει στη δημιουργία ενιαίας πολιτικής ασφάλειας που καλύπτει δεδομένα ασθενών, συσκευές και υποδομές.

Οι έλεγχοι του Annex A (όπως κρυπτογράφηση, διαχείριση πρόσβασης, ασφάλεια δικτύου και διαχείριση προμηθευτών) μπορούν να προσαρμοστούν σε φορητές και εμφυτεύσιμες συσκευές, εξασφαλίζοντας ομοιομορφία πρακτικών ανεξάρτητα από τον κατασκευαστή ή το νοσοκομείο [13], [6].

Η πιστοποίηση κατά ISO 27001 λειτουργεί επίσης ως μέσο αξιοπιστίας και κανονιστικής συμμόρφωσης απέναντι σε οργανισμούς όπως ο FDA και η ENISA.

3.2.2 NIST Cybersecurity Framework (CSF)

Το NIST Cybersecurity Framework (CSF), που αναπτύχθηκε από το National Institute of Standards and Technology, παρέχει ένα πλαίσιο αναφοράς πέντε λειτουργιών: Identify, Protect, Detect, Respond, και Recover [14].

Κάθε λειτουργία αντιστοιχεί σε επιμέρους κατηγορίες και υποκατηγορίες ελέγχων που καθοδηγούν τους οργανισμούς στη διαχείριση κινδύνων με βάση την προτεραιότητα και τον αντίκτυπο.

Στο IoMT, το πλαίσιο του NIST υποστηρίζει την προσαρμοστικότητα των ελέγχων σε διαφορετικά επίπεδα ωριμότητας:

- Η λειτουργία Identify επιτρέπει την καταγραφή όλων των ιατρικών συσκευών ως assets·
- Η Protect καλύπτει μέτρα πρόσβασης, awareness training και προστασία δεδομένων·
- Η Detect αφορά συστήματα ανίχνευσης εισβολών (IDS/IPS) και monitoring σε πραγματικό χρόνο·
- Οι Respond και Recover καθορίζουν διαδικασίες αντιμετώπισης περιστατικών και αποκατάστασης λειτουργιών [14], [10].

Η ευελιξία του NIST CSF το καθιστά ιδανικό για το risk-based management που απαιτείται στα περιβάλλοντα υγείας, επιτρέποντας τη συνεχή ευθυγράμμιση τεχνικών πρακτικών με ρυθμιστικές απαιτήσεις [6].

3.2.3 HIPAA – Health Insurance Portability and Accountability Act (Ηνωμένες Πολιτείες)

Η HIPAA, που θεσπίστηκε από το U.S. Department of Health and Human Services, καθορίζει τις ελάχιστες απαιτήσεις προστασίας των δεδομένων υγείας (Protected Health Information – PHI) για οργανισμούς που δραστηριοποιούνται στις Ηνωμένες Πολιτείες [15].

Παρά το γεωγραφικό της πεδίο εφαρμογής, θεωρείται παγκόσμιο πρότυπο αναφοράς για την οργάνωση πολιτικών ασφάλειας και ελέγχων σε φορείς υγείας.

Η HIPAA οργανώνεται σε τρεις βασικές κατηγορίες μέτρων:

- Administrative safeguards (πολιτικές, risk analysis, awareness training),
- Physical safeguards (έλεγχος εγκαταστάσεων, πρόσβαση σε συσκευές, προστασία αποθηκευτικών μέσων),
- Technical safeguards (access control, audit logs, encryption).

Η δομή αυτή έχει αποτελέσει τη βάση για την ανάπτυξη πολλών διεθνών προτύπων, συμπεριλαμβανομένων διατάξεων του ISO 27799 (Health Informatics Security Management) και των κατευθυντήριων γραμμών του FDA για ιατρικές συσκευές [11], [15].

Στο πλαίσιο της εργασίας, η HIPAA εξετάζεται συγκριτικά με τον GDPR ως παράδειγμα της αμερικανικής προσέγγισης προστασίας δεδομένων, η οποία δίνει έμφαση στη λειτουργική ασφάλεια και όχι μόνο στη νομική συμμόρφωση.

3.2.4 GDPR – General Data Protection Regulation (Ευρωπαϊκή Ένωση)

Ο GDPR (Κανονισμός (ΕΕ) 2016/679) αποτελεί το νομικό πλαίσιο προστασίας προσωπικών δεδομένων στην Ευρωπαϊκή Ένωση και το πλέον αυστηρό διεθνώς ως προς τη διαχείριση ευαίσθητων δεδομένων υγείας [16].

Σε αντίθεση με τη HIPAA, ο GDPR είναι principle-based, βασισμένος στις αρχές νομιμότητας, διαφάνειας, ελαχιστοποίησης δεδομένων, ακεραιότητας και λογοδοσίας.

Στον τομέα του IoMT, ο GDPR επιβάλλει στους υπεύθυνους επεξεργασίας και τους κατασκευαστές ιατρικών συσκευών να αποδεικνύουν την ενσωμάτωση της προστασίας δεδομένων εξ ορισμού και εξ αρχής (privacy by design & by default), καθώς και την εφαρμογή Privacy Impact Assessments (PIAs) για κάθε νέα τεχνολογική υλοποίηση.

Ο κανονισμός θέτει επίσης αυστηρές απαιτήσεις για διασυνοριακές μεταφορές δεδομένων, συγκατάθεση ασθενών, και διαχείριση περιστατικών παραβίασης.

Η εφαρμογή του GDPR στα συστήματα IoMT προσφέρει ένα πλαίσιο νομικής συμμόρφωσης που συμπληρώνει τα τεχνικά πρότυπα ISO και NIST, δημιουργώντας μια πολυεπίπεδη προσέγγιση ασφάλειας και ιδιωτικότητας [16], [12].

3.2.5 Συνδυαστική Ανάλυση και Εννοιολογική Σύγκλιση Προτύπων

Η σύγκριση των προτύπων ISO 27001, NIST CSF, HIPAA και GDPR αποκαλύπτει ότι, παρά τις διαφοροποιήσεις τους, μοιράζονται κοινές αρχές:

1. Risk-based προσέγγιση,
2. Συνεχής παρακολούθηση και βελτίωση,
3. Αναγνώριση και διαχείριση ευπαθειών,
4. Διασφάλιση ιδιωτικότητας και διαφάνειας.

Ενώ η HIPAA παρέχει λειτουργικές απαιτήσεις, ο GDPR καθορίζει νομικές υποχρεώσεις· το ISO 27001 προσφέρει διαχειριστική δομή, ενώ το NIST CSF συνδέει όλα τα παραπάνω σε ένα λειτουργικό κύκλο ασφάλειας.

Μαζί, συνθέτουν το θεσμικό πλαίσιο πάνω στο οποίο βασίζονται οι τεχνολογίες άμυνας και οι μηχανισμοί συμμόρφωσης που θα παρουσιαστούν στις επόμενες ενότητες [13]–[16].

3.3 Τεχνολογίες Ασφάλειας και Άμυνας στο IoMT

Η προστασία των συστημάτων Internet of Medical Things (IoMT) δεν εξαρτάται μόνο από τη συμμόρφωση με πρότυπα και κανονισμούς, αλλά απαιτεί την εφαρμογή συγκεκριμένων τεχνολογιών άμυνας που υλοποιούν στην πράξη τις αρχές των πλαισίων ISO, NIST και GDPR.

Η φύση των IoMT συσκευών – με περιορισμένους πόρους, συνεχή διασύνδεση και μετάδοση ευαίσθητων δεδομένων – επιβάλλει την υιοθέτηση μέτρων ασφάλειας σε πολλαπλά επίπεδα: από το υλικό (hardware) έως το cloud [6], [10], [12], [17].

3.3.1 Κρυπτογράφηση και Έλεγχος Πρόσβασης

Η κρυπτογράφηση αποτελεί θεμελιώδη μηχανισμό προστασίας της εμπιστευτικότητας των δεδομένων στο IoMT. Η χρήση αλγορίθμων AES, RSA ή ECC (Elliptic Curve Cryptography) επιτρέπει την ασφαλή αποθήκευση και μετάδοση δεδομένων από φορητές ή εμφυτεύσιμες συσκευές προς cloud ή νοσοκομειακούς διακομιστές. Σύμφωνα με την ENISA [17], η end-to-end κρυπτογράφηση και η ψηφιακή υπογραφή των δεδομένων συμβάλλουν ουσιαστικά στη διατήρηση της ακεραιότητας και στην αποτροπή παραποίησης ή υποκλοπής. Ο έλεγχος πρόσβασης (Access Control) είναι εξίσου κρίσιμος. Τα συστήματα RBAC (Role-Based Access Control) και ABAC (Attribute-Based Access Control) καθορίζουν ποιοι χρήστες ή εφαρμογές έχουν πρόσβαση σε δεδομένα ή συσκευές, ανάλογα με τον ρόλο ή τα χαρακτηριστικά τους. Η πολυπαραγοντική ταυτοποίηση (MFA), όπως προτείνεται από το NIST [10], ενισχύει περαιτέρω την ασφάλεια, περιορίζοντας τον κίνδυνο μη εξουσιοδοτημένης πρόσβασης, ειδικά σε περιπτώσεις απομακρυσμένης διαχείρισης IoMT συσκευών.

3.3.2 Firewall, IDS/IPS και SIEM

Η προστασία των δικτύων IoMT απαιτεί συνδυασμό προληπτικών και ανιχνευτικών μηχανισμών. Τα firewalls λειτουργούν ως φίλτρα εισερχόμενης και εξερχόμενης κυκλοφορίας, επιτρέποντας μόνο τις εξουσιοδοτημένες συνδέσεις μεταξύ συσκευών και διακομιστών.

Η ENISA [17] προτείνει τη χρήση micro-segmentation σε νοσοκομειακά δίκτυα, ώστε κάθε κατηγορία ιατρικών συσκευών (π.χ. απινιδωτές, αντλίες ινσουλίνης, monitors) να απομονώνεται λογικά σε ξεχωριστό υποδίκτυο. Τα συστήματα ανίχνευσης και πρόληψης εισβολών (IDS/IPS) προσφέρουν τη δυνατότητα εντοπισμού ανωμαλιών σε πραγματικό χρόνο. Τα Network-based IDS επιβλέπουν την κυκλοφορία του δικτύου, ενώ τα Host-based IDS (HIDS) παρακολουθούν μεμονωμένες συσκευές ή servers για ύποπτες ενέργειες.

Η εφαρμογή AI/ML αλγορίθμων στα IDS, όπως περιγράφουν οι Hassija et al. [18], βελτιώνει σημαντικά την ανίχνευση επιθέσεων μηδενικής ημέρας (zero-day) και τη συμπεριφορική ανάλυση (behavioral analysis) χρηστών και συσκευών.

Τα Συστήματα Διαχείρισης Πληροφοριών και Συμβάντων Ασφαλείας (SIEM) συλλέγουν και συσχετίζουν δεδομένα από πολλαπλές πηγές (firewalls, IDS, servers), επιτρέποντας την κεντρική εποπτεία και έγκαιρη ειδοποίηση για περιστατικά ασφάλειας [17].

3.3.3 Προστασία Δεδομένων και Endpoint Security

Η προστασία των τελικών σημείων (endpoints) αποτελεί κρίσιμο στοιχείο άμυνας στο IoMT.

Οι ENISA [17] και Malamas et al. [6] προτείνουν την εγκατάσταση αντι-malware και endpoint protection platforms (EPP) σε servers και σταθμούς εργασίας, ενώ για φορητές συσκευές και tablets προτείνεται η χρήση Mobile Device Management (MDM) για τον έλεγχο πρόσβασης, την κρυπτογράφηση τοπικών δεδομένων και την απομακρυσμένη διαγραφή σε περίπτωση απώλειας. Η

πρόληψη απώλειας δεδομένων (Data Loss Prevention – DLP) ελέγχει τη ροή ευαίσθητων πληροφοριών και εμποδίζει τη μη εξουσιοδοτημένη αποστολή ή αντιγραφή αρχείων.

Η ενσωμάτωση τεχνολογιών καταγραφής (logging) και συνεχούς επιτήρησης (continuous monitoring) επιτρέπει την έγκαιρη ανίχνευση ύποπτης δραστηριότητας, συνδέοντας τεχνικά την έννοια του "Detect" από το πλαίσιο NIST CSF με τις λειτουργικές απαιτήσεις της HIPAA και του GDPR [14]–[16].

3.3.4 VPN, Cloud Security και Δικτυακή Απομόνωση

Οι απομακρυσμένες ιατρικές εφαρμογές και τα συστήματα τηλεπαρακολούθησης απαιτούν ασφαλή κανάλια επικοινωνίας. Τα Virtual Private Networks (VPNs) προσφέρουν κρυπτογράφηση end-to-end μεταξύ των IoMT συσκευών και των νοσοκομειακών servers, μειώνοντας τον κίνδυνο υποκλοπής δεδομένων. Η χρήση TLS 1.3 και IPsec tunnels είναι πλέον βασική πρακτική στα περιβάλλοντα αυτά [17]. Παράλληλα, οι cloud-based υπηρεσίες που φιλοξενούν δεδομένα ασθενών πρέπει να υιοθετούν ασφαλή APIs, πολιτικές least-privilege, και μηχανισμούς auditing.

Η ENISA [17] επισημαίνει ότι ο διαχωρισμός των cloud tenants (multi-tenant isolation) και η εφαρμογή zero-trust αρχιτεκτονικής αποτελούν σύγχρονες τεχνικές αντιμετώπισης της πολυπλοκότητας, επιτρέποντας granular έλεγχο πρόσβασης σε κάθε επίπεδο επικοινωνίας.

3.3.5 Ενοποίηση Τεχνολογιών και Διαχείριση Πολυπλοκότητας

Η εφαρμογή πολλών και διαφορετικών μηχανισμών ασφάλειας στο IoMT δημιουργεί ένα περιβάλλον με υψηλή τεχνική πολυπλοκότητα.

Για την αντιμετώπιση αυτού του φαινομένου, η ENISA [17] προτείνει τη χρήση ενοποιημένων πλατφορμών ασφαλείας (Security Orchestration, Automation and Response – SOAR), που συγκεντρώνουν δεδομένα από SIEM, IDS/IPS και DLP συστήματα, επιτρέποντας αυτοματοποιημένη αντίδραση και μείωση του χρόνου απόκρισης σε περιστατικά.

Επιπλέον, η ενσωμάτωση Blockchain τεχνολογιών, όπως παρουσιάζουν οι Hassija et al. [18], επιτρέπει αποκεντρωμένη αποθήκευση και πιστοποίηση δεδομένων, μειώνοντας τον κίνδυνο αλλοίωσης ή απώλειας. Το blockchain μπορεί να λειτουργήσει ως audit trail για όλες τις συναλλαγές μεταξύ συσκευών, δημιουργώντας ένα επαληθεύσιμο και αδιάβλητο ιστορικό ανταλλαγής δεδομένων.

Συνοψίζοντας, οι τεχνολογίες ασφάλειας και άμυνας στο IoMT συνιστούν ένα πολυεπίπεδο σύστημα προστασίας που καλύπτει τεχνικούς, λειτουργικούς και οργανωτικούς άξονες. Η αποτελεσματική τους εφαρμογή προϋποθέτει τυποποίηση, διαλειτουργικότητα και συνεχή παρακολούθηση, όπως επιτάσσουν τα πλαίσια ISO, NIST και GDPR. Η κατανόηση και διαχείριση της τεχνικής πολυπλοκότητας μέσω αυτών των τεχνολογιών αποτελεί κρίσιμο βήμα για την ενίσχυση της εμπιστοσύνης, της διαθεσιμότητας και της ανθεκτικότητας των συστημάτων υγείας [6], [10]–[12], [17], [18].

3.4 Καινοτόμες Προσεγγίσεις: AI και Blockchain στο IoMT

3.4.1 Εφαρμογές Τεχνητής Νοημοσύνης (AI) και Μηχανικής Μάθησης (ML) στην Ασφάλεια του IoMT

Η αυξανόμενη πολυπλοκότητα και η δυναμική φύση των συστημάτων Internet of Medical Things (IoMT) καθιστούν τις παραδοσιακές μεθόδους ασφάλειας ανεπαρκείς. Η Τεχνητή Νοημοσύνη (AI) και η Μηχανική Μάθηση (Machine Learning – ML) προσφέρουν νέα εργαλεία για ανίχνευση απειλών, πρόληψη επιθέσεων και ενίσχυση της εμπιστευτικότητας και ακεραιότητας των δεδομένων.

Οι τεχνολογίες αυτές λειτουργούν προσαρμοστικά, μαθαίνοντας από τη ροή δεδομένων και εντοπίζοντας ανωμαλίες που υποδηλώνουν κυβερνοεπιθέσεις ή παραβιάσεις συστημάτων [5], [12].

A. AI-driven ανίχνευση ανωμαλιών και επιθέσεων

Σύμφωνα με τους Yasir & Iqbal [5], τα AI μοντέλα βασισμένα σε supervised και unsupervised learning μπορούν να ανιχνεύουν ανωμαλίες σε πραγματικό χρόνο, παρακολουθώντας δεδομένα από αισθητήρες, δίκτυα και cloud υπηρεσίες. Τα deep learning συστήματα, όπως τα Convolutional Neural Networks (CNNs) και Recurrent Neural Networks (RNNs), έχουν αποδειχθεί αποτελεσματικά στην ανίχνευση DoS, data tampering και malware injection επιθέσεων. Η δυνατότητα εκμάθησης προτύπων συμπεριφοράς επιτρέπει την αυτόματη προσαρμογή σε νέες απειλές χωρίς ανθρώπινη παρέμβαση [5], [6]. Στο πλαίσιο του IoMT, η AI συμβάλλει στη δημιουργία έξυπνων IDS/IPS συστημάτων (Intelligent Intrusion Detection/Prevention Systems), τα οποία βασίζονται σε behavioral analytics. Οι ENISA [12] και Malamas et al. [6] τονίζουν ότι τα συστήματα αυτά μπορούν να λειτουργούν ακόμη και σε περιορισμένες υπολογιστικές πλατφόρμες, π.χ. σε edge συσκευές, μειώνοντας την καθυστέρηση (latency) και διασφαλίζοντας τοπική απόκριση σε πραγματικό χρόνο.

B. AI για προστασία ιδιωτικότητας και ανωνυμοποίηση δεδομένων

Η AI δεν περιορίζεται στην ανίχνευση απειλών. Μπορεί επίσης να υποστηρίξει την προστασία της ιδιωτικότητας μέσω τεχνικών differential privacy και federated learning. Το federated learning, που εφαρμόζεται ήδη σε έξυπνα νοσοκομεία, επιτρέπει τη συλλογική εκπαίδευση μοντέλων AI χωρίς τη μεταφορά ευαίσθητων δεδομένων ασθενών εκτός του τοπικού νοσοκομειακού περιβάλλοντος. Έτσι, ενισχύεται η συμμόρφωση με τον GDPR και τις αρχές privacy by design, καθώς οι υπολογισμοί πραγματοποιούνται τοπικά και μόνο τα στατιστικά βάρη του μοντέλου κοινοποιούνται [5], [16]. Η ENISA [12] αναγνωρίζει ότι οι AI τεχνικές ανωνυμοποίησης και τα AI-based access controls μπορούν να μειώσουν δραστικά τα περιστατικά διαρροών δεδομένων, ειδικά σε περιβάλλοντα όπου πολλοί φορείς υγείας ανταλλάσσουν πληροφορίες (π.χ. διασυνδεδεμένα νοσοκομεία, φορητές πλατφόρμες IoMT).

C. Συστήματα πρόβλεψης και διαχείρισης κινδύνου

Η τεχνητή νοημοσύνη αξιοποιείται και για προγνωστικά συστήματα κινδύνου, όπου τα μοντέλα ML αναλύουν ιστορικά δεδομένα ασφάλειας και επιθέσεων, εκτιμώντας την πιθανότητα μελλοντικών παραβιάσεων. Οι Malamas et al. [6] προτείνουν τη χρήση AI-based risk scoring, το οποίο ενσωματώνεται στα πλαίσια ISO 27001 και NIST CSF, επιτρέποντας τη δυναμική ιεράρχηση κινδύνων και την αυτόματη ενεργοποίηση μέτρων άμυνας (π.χ. αποκλεισμός θυρών, επιβολή πολιτικών πρόσβασης). Η προσέγγιση αυτή ενισχύει τη λειτουργική ευφυΐα των συστημάτων ασφάλειας, μετατρέποντάς τα από παθητικούς μηχανισμούς σε προγνωστικά και προσαρμοστικά συστήματα.

D. Προκλήσεις και περιορισμοί

Παρά τα οφέλη, η εφαρμογή της AI στο IoMT συνοδεύεται από προκλήσεις. Η έλλειψη διαλειτουργικότητας μεταξύ συσκευών, η έλλειψη επαρκών δεδομένων εκπαίδευσης και η ευπάθεια σε adversarial attacks περιορίζουν την αξιοπιστία των συστημάτων [12]. Η βιβλιογραφία επισημαίνει ότι οι μελλοντικές έρευνες πρέπει να επικεντρωθούν σε επεξηγήσιμα (explainable) AI μοντέλα, τα οποία να παρέχουν διαφάνεια στις αποφάσεις των αλγορίθμων, στοιχείο κρίσιμο για τον τομέα της υγείας όπου απαιτείται τεκμηριωμένη λήψη αποφάσεων [5], [6].

Συνοψίζοντας, η χρήση της Τεχνητής Νοημοσύνης και της Μηχανικής Μάθησης στο IoMT επιτρέπει τη μετάβαση από αντιδραστικά σε προληπτικά και αυτοπροσαρμοζόμενα συστήματα ασφάλειας.

Η AI μπορεί να ενισχύσει τόσο την ανίχνευση και πρόληψη επιθέσεων, όσο και την προστασία ιδιωτικότητας και συμμόρφωση με κανονισμούς όπως ο GDPR.

Η επόμενη ενότητα (3.4.2) θα επικεντρωθεί στο Blockchain, το οποίο συμπληρώνει τις δυνατότητες της AI μέσω αδιάβλητης αποθήκευσης και αποκεντρωμένης διαχείρισης εμπιστοσύνης.

3.4.2 Blockchain και Αποκεντρωμένες Λύσεις για το IoMT

Η τεχνολογία Blockchain έχει αναδειχθεί ως μια από τις πιο καινοτόμες προσεγγίσεις για την ενίσχυση της ασφάλειας και της εμπιστοσύνης στα συστήματα Internet of Medical Things (IoMT). Χάρη στα χαρακτηριστικά της αποκέντρωσης, διαφάνειας και αμεταβλητότητας, το Blockchain προσφέρει μηχανισμούς που αντιμετωπίζουν εγγενείς αδυναμίες των παραδοσιακών κεντρικών συστημάτων, όπως η αλλοίωση δεδομένων, η μη εξουσιοδοτημένη πρόσβαση και οι single points of failure [18], [19].

A. Αρχές και λειτουργικά χαρακτηριστικά του Blockchain στο IoMT

Σύμφωνα με τους Hassija et al. [18], το Blockchain λειτουργεί ως ένα κατανεμημένο καθολικό (distributed ledger), όπου κάθε συναλλαγή επαληθεύεται μέσω κρυπτογραφικών συναρτήσεων και αποθηκεύεται σε μπλοκ που συνδέονται αμετάκλητα μεταξύ τους. Αυτό σημαίνει ότι οποιαδήποτε προσπάθεια αλλοίωσης ή διαγραφής δεδομένων καθίσταται πρακτικά αδύνατη χωρίς την τροποποίηση ολόκληρης της αλυσίδας. Στο περιβάλλον του IoMT, η τεχνολογία αυτή χρησιμοποιείται για την καταγραφή ιατρικών δεδομένων, την επαλήθευση ταυτότητας συσκευών και τη διασφάλιση της ιχνηλασιμότητας (traceability) σε κάθε στάδιο μετάδοσης πληροφορίας [18]. Η αποκέντρωση εξαλείφει την ανάγκη για έναν κεντρικό διαχειριστή δεδομένων, γεγονός που μειώνει σημαντικά τον κίνδυνο επιθέσεων σε κεντρικά συστήματα ή παραβίασης βάσεων δεδομένων [19].

B. Εφαρμογές του Blockchain στην ασφάλεια δεδομένων και πρόσβασης

Οι εφαρμογές του Blockchain στο IoMT εκτείνονται από τη διαχείριση πρόσβασης έως την επικύρωση δεδομένων. Η χρήση Smart Contracts επιτρέπει την αυτόματη εκτέλεση πολιτικών ασφάλειας — όπως η εξουσιοδότηση χρηστών, η ανταλλαγή δεδομένων μεταξύ φορέων υγείας και η λήψη συγκατάθεσης ασθενών — χωρίς ανθρώπινη παρέμβαση [18]. Έτσι, κάθε πρόσβαση σε ιατρικά δεδομένα καταγράφεται ως αδιάβλητη συναλλαγή, διασφαλίζοντας πλήρη λογοδοσία (accountability). Παράλληλα, η χρήση Blockchain για την αποθήκευση hash τιμών των αρχείων ασθενών επιτρέπει την επαλήθευση ακεραιότητας χωρίς την αποκάλυψη του ίδιου του περιεχομένου, προσφέροντας έναν συνδυασμό εμπιστευτικότητας και διαφάνειας. Οι Ali et al. [19] προτείνουν την ενσωμάτωση lightweight blockchain μοντέλων, όπως Hyperledger Fabric και IOTA Tangle, τα οποία είναι σχεδιασμένα για περιβάλλοντα περιορισμένων πόρων, όπως τα ιατρικά αισθητήρια δίκτυα.

C. Blockchain για διαλειτουργικότητα και auditability στο IoMT

Ένα από τα σημαντικότερα πλεονεκτήματα του Blockchain είναι η δυνατότητα βελτίωσης της διαλειτουργικότητας μεταξύ συσκευών και οργανισμών. Οι Hassija et al. [18] αναφέρουν ότι η αποθήκευση metadata σχετικά με ιατρικές συσκευές (ID, timestamps, calibration data) στο Blockchain μπορεί να λειτουργήσει ως μηχανισμός πιστοποίησης γνησιότητας, αποτρέποντας τη χρήση μη εγκεκριμένων ή παραποιημένων συσκευών. Επιπλέον, τα Blockchain audit trails προσφέρουν ιστορικό κάθε ενέργειας (data logging, ενημερώσεις, μεταφορές), κάτι που υποστηρίζει τη συμμόρφωση με κανονισμούς όπως ο GDPR και οι οδηγίες της FDA [11], [16], [18]. Η αποκεντρωμένη φύση της τεχνολογίας καθιστά δυνατή την επαλήθευση των ενεργειών όλων των συμμετεχόντων χωρίς την ανάγκη εμπιστοσύνης σε έναν ενδιάμεσο φορέα (trustless environment).

D. Συνδυασμός Blockchain με AI και IoMT Analytics

Η συνδυαστική αξιοποίηση Blockchain και AI αποτελεί το επόμενο βήμα στην ασφάλεια του IoMT. Ενώ η AI προσφέρει προβλεπτική ανάλυση και ανίχνευση ανωμαλιών, το Blockchain εξασφαλίζει την ακεραιότητα των δεδομένων που χρησιμοποιούνται για εκπαίδευση και λήψη αποφάσεων [5], [18], [19]. Για παράδειγμα, σε σενάρια federated learning, όπου τα μοντέλα εκπαιδεύονται κατανεμημένα, το Blockchain μπορεί να αποθηκεύει και να επαληθεύει τις ενημερώσεις μοντέλων, αποτρέποντας κακόβουλες παρεμβολές (model poisoning). Οι ENISA [12] και Malamas et al. [6] επισημαίνουν ότι

τέτοιες αρχιτεκτονικές μπορούν να υποστηρίξουν ένα ολοκληρωμένο οικοσύστημα εμπιστοσύνης, όπου η διαχείριση ταυτότητας, η ανταλλαγή δεδομένων και η απόδειξη προέλευσης πραγματοποιούνται αυτόματα και με ασφάλεια.

Ε. Προκλήσεις και περιορισμοί εφαρμογής

Παρά τα πλεονεκτήματά του, το Blockchain αντιμετωπίζει ορισμένες προκλήσεις όταν εφαρμόζεται στο IoMT. Η υπολογιστική επιβάρυνση, η καθυστέρηση συναλλαγών (latency) και η ενεργειακή κατανάλωση αποτελούν εμπόδια για φορητές ή εμφυτεύσιμες συσκευές. Επιπλέον, ζητήματα προστασίας ιδιωτικότητας και συμμόρφωσης με κανονισμούς (όπως το δικαίωμα διαγραφής δεδομένων του GDPR) απαιτούν ειδική αντιμετώπιση, όπως η χρήση off-chain αποθήκευσης και zero-knowledge proofs [18], [19]. Ωστόσο, οι τρέχουσες ερευνητικές τάσεις επικεντρώνονται στην ανάπτυξη lightweight blockchains, hybrid architectures και sidechains, που μειώνουν το ενεργειακό αποτύπωμα και επιτρέπουν ευρεία υιοθέτηση στο IoMT [19].

Συνοψίζοντας, η τεχνολογία Blockchain προσφέρει στο IoMT μια αξιόπιστη και αδιάβλητη υποδομή εμπιστοσύνης, ικανή να διασφαλίσει την ακεραιότητα, τη διαφάνεια και την ιχνηλασιμότητα των ιατρικών δεδομένων.

Η συνδυαστική χρήση της με την Τεχνητή Νοημοσύνη μπορεί να οδηγήσει στη δημιουργία αυτορρυθμιζόμενων και επεξηγήσιμων συστημάτων ασφάλειας, όπου οι αποφάσεις βασίζονται σε επαληθευμένα δεδομένα και μη αλλοιώσιμα αρχεία συναλλαγών.

Η ενότητα αυτή θέτει το υπόβαθρο για την τελική σύνοψη του Κεφαλαίου 3, όπου θα συνδεθούν τα πρότυπα, οι τεχνολογίες και οι καινοτόμες λύσεις σε ένα ενιαίο μοντέλο διαχείρισης ασφάλειας για το IoMT.

3.4.3 Σύνοψη Κεφαλαίου 3 – Πρότυπα, Πλαίσια και Τεχνολογίες Ασφάλειας στο IoMT

Το Κεφάλαιο 3 ανέπτυξε τη θεμελιώδη δομή ασφάλειας του οικοσυστήματος Internet of Medical Things (IoMT), παρουσιάζοντας τα διεθνή πρότυπα, τα κανονιστικά πλαίσια και τις τεχνολογικές λύσεις που καθορίζουν την κυβερνοασφάλεια σε φορετές ιατρικές συσκευές και δικτυωμένες υποδομές υγείας.

Στην αρχή, αναλύθηκε η ανάγκη για τυποποιημένες προσεγγίσεις μέσω του ISO/IEC 27001, του NIST Cybersecurity Framework, καθώς και των νομικών πλαισίων HIPAA και GDPR, τα οποία καθορίζουν αντίστοιχα λειτουργικές και νομικές απαιτήσεις προστασίας δεδομένων. Οι συνδυασμοί αυτών των προτύπων προσφέρουν ένα πολυεπίπεδο σύστημα διακυβέρνησης της ασφάλειας, που ευθυγραμμίζει τεχνικά, οργανωτικά και κανονιστικά μέτρα [13]–[16].

Στη συνέχεια, εξετάστηκαν οι τεχνολογίες άμυνας που υλοποιούν στην πράξη τις αρχές των προτύπων: κρυπτογράφηση, έλεγχος πρόσβασης, firewall, IDS/IPS, SIEM, VPN, DLP και MDM.

Η βιβλιογραφία έδειξε ότι η εφαρμογή αυτών των τεχνολογιών σε συνδυασμό με αρχιτεκτονικές cloud και edge computing ενισχύει σημαντικά την ανθεκτικότητα των IoMT δικτύων, περιορίζοντας την επιφάνεια επίθεσης και τη λειτουργική πολυπλοκότητα [6], [10]–[12], [17].

Τέλος, παρουσιάστηκαν οι καινοτόμες προσεγγίσεις που αξιοποιούν Τεχνητή Νοημοσύνη (AI) και Blockchain για την προληπτική προστασία των δεδομένων και την ενίσχυση της εμπιστοσύνης.

Η AI επιτρέπει αυτόματη ανίχνευση απειλών, πρόβλεψη κινδύνων και ανωνυμοποίηση δεδομένων μέσω τεχνικών federated learning και differential privacy [5], [12], [16], ενώ το Blockchain προσφέρει αδιάβλητη ιχνηλασιμότητα, έλεγχο πρόσβασης μέσω smart contracts και διαλειτουργικότητα μεταξύ οργανισμών υγείας [18], [19]. Ο συνδυασμός των δύο τεχνολογιών δημιουργεί αυτορρυθμιζόμενα και

επεξηγήσιμα συστήματα ασφάλειας, ικανά να λειτουργούν σε πραγματικό χρόνο με υψηλό επίπεδο αξιοπιστίας.

Συνολικά, το Κεφάλαιο 3 απέδειξε ότι η αποτελεσματική ασφάλεια στο IoMT επιτυγχάνεται μέσω της ολοκληρωμένης ενσωμάτωσης προτύπων, κανονισμών και τεχνολογιών, που λειτουργούν συνδυαστικά για την προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των ιατρικών δεδομένων.

Η προσέγγιση αυτή θέτει το υπόβαθρο για το Κεφάλαιο 4, όπου θα εξεταστούν οι πρακτικές εφαρμογές, πρότυπα συμμόρφωσης και μελέτες περίπτωσης που αποδεικνύουν την υλοποίηση των παραπάνω θεωρητικών αρχών στην πράξη.

Κεφάλαιο 4ο: Πρότυπα και Κανονιστικό Πλαίσιο Ασφάλειας Ιατρικών Συσκευών

4.1 Εισαγωγή στα πρότυπα ασφάλειας ιατρικών συσκευών

Το οικοσύστημα των ιατρικών συσκευών και ιδιαίτερα των διασυνδεδεμένων συστημάτων Internet of Medical Things (IoMT) λειτουργεί μέσα σε ένα σύνθετο περιβάλλον κανονιστικών απαιτήσεων και προτύπων ασφάλειας. Η αυξανόμενη εξάρτηση από λογισμικό, ασύρματες επικοινωνίες και υπηρεσίες cloud έχει ενισχύσει τη σημασία της κυβερνοασφάλειας ως βασικού στοιχείου της ασφάλειας και απόδοσης μιας συσκευής· δεν πρόκειται πλέον μόνο για τεχνικό ζήτημα πληροφορικής, αλλά για κρίσιμο παράγοντα κλινικής ασφάλειας και προστασίας της ανθρώπινης ζωής [6], [7], [12].

Για τον λόγο αυτό, διεθνείς οργανισμοί τυποποίησης και ρυθμιστικές αρχές έχουν αναπτύξει ένα πλέγμα προτύπων και κατευθυντήριων γραμμών που καθορίζουν πώς πρέπει να ενσωματώνεται η διαχείριση κινδύνων και η κυβερνοασφάλεια σε όλο τον κύκλο ζωής των ιατρικών συσκευών. Στην Ευρωπαϊκή Ένωση, ο Κανονισμός (ΕΕ) 2017/745 (MDR) εισάγει αυστηρές απαιτήσεις για την ασφάλεια λογισμικού, τη διαχείριση κινδύνου και την προστασία δεδομένων, επηρεάζοντας άμεσα και τις IoMT συσκευές [20]. Συμπληρωματικά, το πρότυπο ISO 14971 παρέχει ένα δομημένο πλαίσιο για τη συστηματική αναγνώριση, αξιολόγηση και έλεγχο κινδύνων, το οποίο οι κατασκευαστές καλούνται να εφαρμόσουν ως βάση του συστήματος ποιότητάς τους [21], [22], [24].

Στις Ηνωμένες Πολιτείες, ο Οργανισμός Τροφίμων και Φαρμάκων (FDA) έχει εκδώσει εξειδικευμένες οδηγίες για την κυβερνοασφάλεια τόσο στο στάδιο της προέγκρισης (premarket) όσο και μετά την κυκλοφορία (postmarket) των ιατρικών συσκευών. Οι οδηγίες αυτές περιγράφουν τις αναμενόμενες λειτουργίες ασφάλειας (π.χ. ελέγχους πρόσβασης, ασφαλείς ενημερώσεις λογισμικού, καταγραφή συμβάντων) και τον τρόπο με τον οποίο τεκμηριώνονται στα συνοδευτικά έγγραφα των συσκευών [11], [23]. Παράλληλα, οργανισμοί όπως το NIST έχουν προτείνει βασικές δυνατότητες κυβερνοασφάλειας για συσκευές IoT/IoMT (NISTIR 8259 και 8259A), οι οποίες λειτουργούν ως baseline για τον σχεδιασμό, την υλοποίηση και τη διαχείριση ασφαλών συσκευών [10], [25], [25a].

Η συνύπαρξη αυτών των πλαισίων δημιουργεί ένα πολυεπίπεδο περιβάλλον συμμόρφωσης. Ο κάθε φορέας (ΕΕ, ΗΠΑ, διεθνείς οργανισμοί τυποποίησης) εστιάζει σε διαφορετική οπτική –κανονιστική συμμόρφωση, διαχείριση κινδύνου, τεχνικές δυνατότητες ασφαλείας– αλλά όλα τα πλαίσια συγκλίνουν στον στόχο της μείωσης των κυβερνοκινδύνων και της προστασίας των ασθενών. Πρόσφατες μελέτες συγκριτικής ανάλυσης δείχνουν ότι, παρότι υπάρχουν διαφορές στη δομή και τη φρασεολογία των κανονισμών, εντοπίζονται σημαντικά σημεία σύγκλισης στις βασικές αρχές ασφαλούς σχεδίασης και αξιολόγησης ιατρικών συσκευών [6], [23], [27].

Στο παρόν κεφάλαιο παρουσιάζονται αναλυτικά τα βασικά πρότυπα και κατευθυντήριες γραμμές που επηρεάζουν την κυβερνοασφάλεια των IoMT συστημάτων: ο MDR ως κεντρικό ρυθμιστικό πλαίσιο της ΕΕ, το ISO 14971 ως πρότυπο διαχείρισης κινδύνου, οι οδηγίες του FDA για την κυβερνοασφάλεια ιατρικών συσκευών και τα έγγραφα NISTIR 8259/8259A για τις ελάχιστες δυνατότητες ασφάλειας των IoT συσκευών. Στη συνέχεια, πραγματοποιείται συγκριτική ανάλυση των πλαισίων αυτών και διερευνάται πώς μπορούν να αξιοποιηθούν συνδυαστικά για την αντιμετώπιση των ευπαθειών που αναδείχθηκαν στα προηγούμενα κεφάλαια.

4.2 MDR – Κανονιστικό πλαίσιο της ΕΕ για την ασφάλεια ιατρικών συσκευών

Ο Κανονισμός (ΕΕ) 2017/745 για τις ιατρικές συσκευές (Medical Device Regulation – MDR) αποτελεί το κεντρικό ρυθμιστικό πλαίσιο της Ευρωπαϊκής Ένωσης για τη διασφάλιση της ποιότητας,

της ασφάλειας και της κλινικής αποτελεσματικότητας των ιατρικών προϊόντων. Ο MDR εισάγει αυστηρότερες απαιτήσεις σε σχέση με την προηγούμενη οδηγία (MDD), ιδίως ως προς τη διαχείριση κινδύνων, τη διαφάνεια, την ανιχνευσιμότητα και τον έλεγχο των κατασκευαστών. Η σημασία του MDR καθίσταται ακόμη μεγαλύτερη για τα διασυνδεδεμένα συστήματα και τις IoMT συσκευές, όπου η κυβερνοασφάλεια συνδέεται άμεσα με την ασφάλεια των ασθενών [20].

Σύμφωνα με τον Greser [20], ο MDR δεν είναι εξειδικευμένο πρότυπο κυβερνοασφάλειας, αλλά λειτουργεί ως οριζόντιο πλαίσιο που επιβάλλει σαφείς υποχρεώσεις στους κατασκευαστές λογισμικού και έξυπνων ιατρικών συσκευών. Ενδεικτικά, απαιτεί:

- τεκμηριωμένη διαχείριση κινδύνων καθ' όλη τη διάρκεια ζωής του προϊόντος,
- εξασφάλιση ασφαλούς σχεδίασης, ανάπτυξης και επικύρωσης λογισμικού,
- ενσωμάτωση διαδικασιών προστασίας δεδομένων,
- αξιολόγηση αλληλεπιδράσεων με άλλα συστήματα, όπως δίκτυα, αισθητήρες και cloud πλατφόρμες,
- εφαρμογή μηχανισμών για την ανίχνευση και αντιμετώπιση περιστατικών ασφάλειας.

Ένα βασικό σημείο που επισημαίνει ο Ostermann et al. [27] είναι ότι ο MDR αντιμετωπίζει την κυβερνοασφάλεια κυρίως ως ζήτημα διαχείρισης κινδύνου, συνδέοντας καθαρά το τεχνικό σκέλος με την κλινική ασφάλεια. Με άλλα λόγια, τυχόν ευπάθειες λογισμικού, σφαλμάτων διαμόρφωσης ή ανεπαρκών ενημερώσεων θεωρούνται πιθανοί κίνδυνοι που μπορούν να επηρεάσουν άμεσα την υγεία του ασθενούς.

Επιπλέον, ο MDR απαιτεί τεκμηρίωση για:

- συμβατότητα και διαλειτουργικότητα,
- κυβερνοασφάλεια δικτύου (network & software security),
- μηχανισμούς πρόσβασης και αυθεντικοποίησης,
- ασφαλείς αναβαθμίσεις και patches,
- διασφάλιση εμπιστευτικότητας και ακεραιότητας δεδομένων.

Ο Greser [20] υπογραμμίζει επίσης ότι, παρότι ο MDR δεν καθορίζει συγκεκριμένες τεχνικές λύσεις, αναμένει από τον κατασκευαστή να εφαρμόζει διεθνή πρότυπα όπως το ISO 14971, τα οποία λειτουργούν συμπληρωματικά και υποχρεωτικά για την πλήρη συμμόρφωση.

Ο Ostermann et al. [27] σημειώνουν ότι, σε σύγκριση με τις απαιτήσεις του FDA, ο MDR εστιάζει περισσότερο στις διαδικασίες (process-based compliance), παρά στις τεχνικές απαιτήσεις, κάτι που δημιουργεί διαφορές αλλά και σημαντικά κοινά σημεία που θα συζητηθούν αναλυτικά στη συγκριτική ανάλυση της ενότητας 5.6.

Συνολικά, ο MDR αποτελεί θεμέλιο πλαίσιο για την κυβερνοασφάλεια των IoMT συσκευών στην Ευρώπη, καθώς μεταφέρει την ευθύνη ασφάλειας στον κατασκευαστή και επιβάλλει συνεχείς διαδικασίες ελέγχου, διαχείρισης κινδύνου και τεκμηρίωσης από το στάδιο του σχεδιασμού έως και τη μετα-κυκλοφοριακή παρακολούθηση.

4.3 ISO 14971 – Πρότυπο Διαχείρισης Κινδύνου για Ιατρικές Συσκευές

Το ISO 14971 αποτελεί το διεθνώς αναγνωρισμένο πρότυπο για τη διαχείριση κινδύνου σε ιατρικές συσκευές και λογισμικό υγείας, συμπεριλαμβανομένων των συστημάτων IoMT. Σύμφωνα με τον Yang [21], το ISO 14971 λειτουργεί ως το θεμέλιο πάνω στο οποίο οι κατασκευαστές οργανώνουν, εφαρμόζουν και τεκμηριώνουν μια συστηματική διαδικασία αναγνώρισης, αξιολόγησης και ελέγχου κινδύνων σε όλο τον κύκλο ζωής της συσκευής — από τον σχεδιασμό έως τη μετα-κυκλοφοριακή παρακολούθηση.

Ο Flood et al. [22] επισημαίνουν ότι το ISO 14971 δεν περιορίζεται σε τεχνικές προδιαγραφές, αλλά περιγράφει μια ολιστική προσέγγιση διαχείρισης κινδύνου, η οποία περιλαμβάνει ιατρικούς,

τεχνικούς, κλινικούς και λειτουργικούς κινδύνους. Αυτό το χαρακτηριστικό το καθιστά ιδιαίτερα σημαντικό για συσκευές IoMT, όπου η κυβερνοασφάλεια συνδέεται άμεσα με την ασφάλεια του ασθενούς και μπορεί να επηρεάσει τόσο την ακεραιότητα των δεδομένων όσο και την ακρίβεια των κλινικών αποφάσεων.

4.3.1 Βασικά στοιχεία της διαδικασίας ISO 14971

Όπως αναλύεται στη λευκή βίβλο του BSI [24], το πρότυπο καθορίζει μια σειρά από διαδοχικά βήματα που πρέπει να ακολουθούνται αυστηρά από τον κατασκευαστή:

1. Ανάλυση κινδύνου (Risk Analysis)
   - Αναγνώριση πιθανών κινδύνων σχετικών με τη συσκευή (τεχνικά, λειτουργικά, κλινικά).
   - Αναγνώριση απειλών κυβερνοασφάλειας, ιδίως για συσκευές IoMT που χρησιμοποιούν δίκτυα, ασύρματα πρωτόκολλα ή cloud.
2. Αξιολόγηση κινδύνου (Risk Evaluation)
   - Εκτίμηση σοβαρότητας και πιθανότητας εμφάνισης.
   - Σύγκριση των κινδύνων με τα αποδεκτά όρια ασφαλείας.
3. Έλεγχος κινδύνου (Risk Control)
   - Επιλογή τεχνικών και οργανωτικών μέτρων για τη μείωση των κινδύνων σε ανεκτό επίπεδο.
   - Για συσκευές IoMT, τα μέτρα μπορεί να περιλαμβάνουν: κρυπτογράφηση, έλεγχο πρόσβασης, ασφαλείς ενημερώσεις λογισμικού, μηχανισμούς ανίχνευσης ανωμαλιών.
4. Αξιολόγηση υπολειπόμενου κινδύνου (Residual Risk)
   - Επιβεβαίωση ότι οι κίνδυνοι που απομένουν μετά τα μέτρα μετριασμού είναι αποδεκτοί και τεκμηριωμένοι.
5. Παρακολούθηση μετά την κυκλοφορία (Post-market Surveillance)
   - Συλλογή δεδομένων για περιστατικά, ευπάθειες, καινοφανείς απειλές κ.λπ.
   - Για το IoMT, αυτό περιλαμβάνει την παρακολούθηση νέων κυβερνοεπιθέσεων ή ενημερώσεων λογισμικού που μπορεί να προκαλέσουν νέες ευπάθειες.

Ο Yang [21] τονίζει ότι το ISO 14971 δεν παρέχει μόνο διαδικαστικές οδηγίες, αλλά απαιτεί από τους κατασκευαστές να μπορούν να αποδείξουν τη συνεχή εφαρμογή της διαδικασίας με τεκμηριωμένο και αναγνώσιμο τρόπο. Γι' αυτό, οργανισμοί όπως ο BSI [24] παρέχουν αναλυτική καθοδήγηση για τον τρόπο ενσωμάτωσης του προτύπου σε ένα σύστημα ποιότητας.

Σύμφωνα με το ISO 14971, η διαδικασία διαχείρισης κινδύνου υλοποιείται ως μία κυκλική και επαναλαμβανόμενη ροή ενεργειών, όπου κάθε στάδιο επηρεάζει άμεσα το επόμενο και τροφοδοτείται από δεδομένα που συλλέγονται σε όλο τον κύκλο ζωής της συσκευής. Η συνολική διαδικασία ξεκινά με τον σχεδιασμό και την τεκμηρίωση του πλάνου διαχείρισης κινδύνου και συνεχίζεται με την ανάλυση, αξιολόγηση και έλεγχο των κινδύνων, έως την αξιολόγηση του υπολειπόμενου κινδύνου και τη συνεχή συλλογή πληροφοριών μετά την κυκλοφορία. Η ροή αυτών των βημάτων παρουσιάζεται στο Σχήμα 5.1, το οποίο απεικονίζει συνοπτικά την πλήρη διαδικασία διαχείρισης κινδύνου όπως ορίζεται στο ISO 14971.

Σχήμα 5.1: Διαδικασία διαχείρισης κινδύνου κατά ISO 14971 [24]

4.3.2 Σχέση ISO 14971 με τον MDR και την ασφάλεια IoMT

Το ISO 14971 χρησιμοποιείται υποχρεωτικά από τους κατασκευαστές στην ΕΕ ως εργαλείο συμμόρφωσης με τον MDR, όπως σημειώνεται από τους Flood et al. [22].

Για τις IoMT συσκευές, το πρότυπο:

- επιτρέπει τη συστηματική τεκμηρίωση κινδύνων κυβερνοασφάλειας,
- συνδέει άμεσα τις τεχνικές ευπάθειες με την κλινική ασφάλεια,
- βοηθά στον εντοπισμό κινδύνων που σχετίζονται με διαλειτουργικότητα, ενημερώσεις λογισμικού, εφαρμογές cloud ή προσβάσεις τρίτων,
- λειτουργεί ως βάση για την εναρμόνιση με τις παραμέτρους που θέτει ο MDR όσον αφορά την ανάλυση κινδύνου.

Η λευκή βίβλος του BSI [24] τονίζει ότι το ISO 14971 έχει εναρμονιστεί με τον MDR, επιτρέποντας μια συνεκτική και επαναλήψιμη διαδικασία διαχείρισης κινδύνου για προϊόντα που περιλαμβάνουν λογισμικό, αισθητήρες και συνδεσιμότητα.

4.3.3 Η σημασία του ISO 14971 για το IoMT

Οι συσκευές IoMT έχουν πολύ υψηλότερη πολυπλοκότητα και πιο δυναμικό κύκλο ζωής από τις παραδοσιακές ιατρικές συσκευές.

Για αυτό, το ISO 14971:

- αποτελεί βασικό εργαλείο τεκμηρίωσης κυβερνοκινδύνων,
- επιτρέπει τον προληπτικό σχεδιασμό ασφαλών αρχιτεκτονικών,
- ενισχύει τη διαφάνεια και την ανιχνευσιμότητα σε κάθε αλλαγή λογισμικού,
- υποστηρίζει την υιοθέτηση βέλτιστων πρακτικών ασφαλείας σε όλο το οικοσύστημα IoMT.

Έτσι, λειτουργεί ως κρίσιμη γέφυρα μεταξύ κανονισμών, τεχνικών απαιτήσεων και κλινικής ασφάλειας [21], [22], [24].

4.4 Οδηγίες FDA για την Κυβερνοασφάλεια Ιατρικών Συσκευών (Premarket & Postmarket)

Η Υπηρεσία Τροφίμων και Φαρμάκων των ΗΠΑ (FDA) αποτελεί έναν από τους σημαντικότερους διεθνείς ρυθμιστικούς φορείς στον χώρο των ιατρικών συσκευών. Οι κατευθυντήριες γραμμές του FDA για την κυβερνοασφάλεια καθορίζουν τις απαιτήσεις που πρέπει να πληρούν οι κατασκευαστές ώστε μια συσκευή να εγκριθεί για χρήση στην αγορά των Ηνωμένων Πολιτειών. Οι οδηγίες αυτές

έχουν ιδιαίτερη σημασία για τις διασυνδεδεμένες IoMT συσκευές, οι οποίες επιδρούν άμεσα στην ασφάλεια του ασθενούς και στη λειτουργική συνέχεια των κλινικών συστημάτων [11].

Το FDA αντιμετωπίζει την κυβερνοασφάλεια ως ενσωματωμένο στοιχείο της ασφάλειας και αποτελεσματικότητας της συσκευής. Όπως τονίζεται στην καθοδήγηση premarket του 2023 [11], η συσκευή οφείλει να επιδεικνύει:

- ασφαλή σχεδίαση (secure-by-design)
- ικανότητα ανθεκτικότητας σε κυβερνοεπιθέσεις
- μηχανισμούς διατήρησης της ασφάλειας σε όλα τα στάδια ζωής του προϊόντος

Η καθοδήγηση χωρίζεται σε δύο βασικά σκέλη:

4.4.1 Premarket Requirements (2023)

Στην καθοδήγηση FDA 2023 για premarket submissions, αναλύονται τέσσερις πυλώνες ασφάλειας που πρέπει να τεκμηριώνονται για κάθε IoMT συσκευή [11]:

1. Cybersecurity Risk Management

Ο κατασκευαστής πρέπει να παρουσιάζει λεπτομερή ανάλυση κινδύνων (threat modeling, vulnerability assessment, attack surface analysis). Απαιτείται χαρτογράφηση των κινδύνων σε controls και αξιολόγηση residual risk, σε απόλυτη ευθυγράμμιση με το ISO 14971.

2. Secure Product Development Framework (SPDF)

Το FDA απαιτεί τεκμηριωμένο SDLC με διαδικασίες για:

- ασφαλή ανάπτυξη λογισμικού
- code reviews
- penetration testing
- static & dynamic analysis

Η έννοια SPDF αποτελεί βασικό δομικό στοιχείο των premarket submissions.

3. Cybersecurity Controls & Device Architecture

Για κάθε συσκευή πρέπει να τεκμηριώνονται:

- έλεγχοι αυθεντικοποίησης (authentication)
- έλεγχος πρόσβασης
- προστασία ακεραιότητας (data integrity)
- κρυπτογράφηση δεδομένων
- secure boot
- logging & audit trails
- προστασία firmware και ασφαλείς ενημερώσεις (patchability)

Αυτά τα χαρακτηριστικά εντοπίζονται και εμπειρικά σε πραγματικές συσκευές, όπως δείχνει η μελέτη Stern et al. [23].

4. Software Bill of Materials (SBOM)

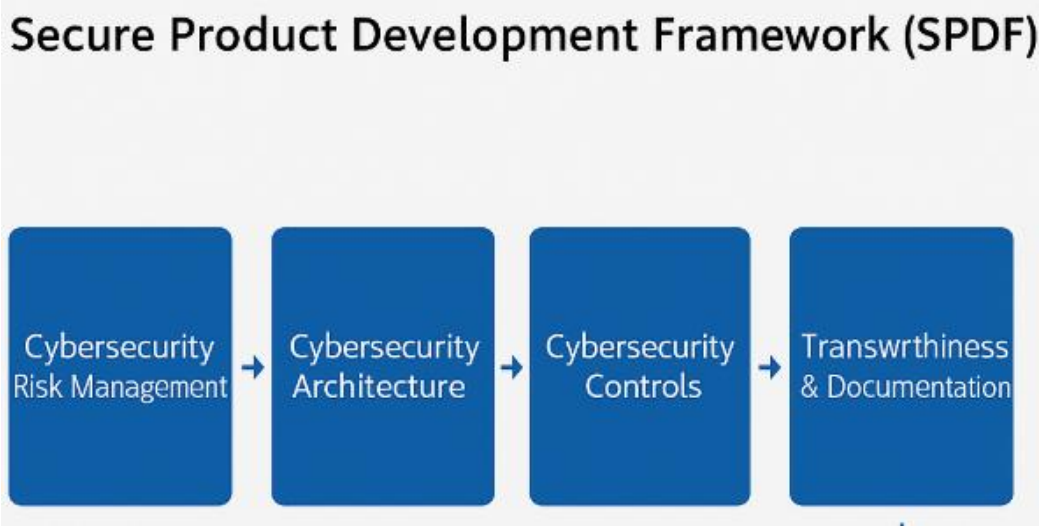
Απαιτείται πλήρης κατάλογος λογισμικού και βιβλιοθηκών που χρησιμοποιούνται στη συσκευή για:

- ανίχνευση ευπαθειών
- compliance
- εξασφάλιση δυνατότητας ενημερώσεων

Το Secure Product Development Framework (SPDF) αποτελεί τον βασικό μηχανισμό που εισάγει το FDA για τη συστηματική ενσωμάτωση της κυβερνοασφάλειας κατά την ανάπτυξη ιατρικών συσκευών. Το SPDF περιλαμβάνει ένα σύνολο αρχών και πρακτικών που πρέπει να εφαρμόζονται σε όλα τα στάδια του κύκλου ζωής της συσκευής, από τον αρχικό σχεδιασμό έως την τελική τεκμηρίωση. Σύμφωνα με το FDA, το SPDF διασφαλίζει ότι οι συσκευές IoMT σχεδιάζονται με γνώμονα την

ασφάλεια (secure-by-design), ενσωματώνοντας μηχανισμούς διαχείρισης κινδύνων, ασφαλή αρχιτεκτονική λογισμικού, ελέγχους προστασίας, διαφάνεια και πλήρη τεκμηρίωση.

Η οπτική αναπαράσταση του SPDF παρουσιάζεται στο Σχήμα 5.2, όπου συνοψίζονται τα κρίσιμα δομικά στοιχεία του πλαισίου και ο τρόπος με τον οποίο συνδέονται μεταξύ τους για την εξασφάλιση της αξιοπιστίας μιας ιατρικής συσκευής.



Σχήμα 5.2: Επισκόπηση του Secure Product Development Framework του FDA [11]

4.4.2 Postmarket Requirements (FDA 2018)

Η καθοδήγηση του FDA για την περίοδο μετά την κυκλοφορία των ιατρικών συσκευών δίνει έμφαση στην συνεχή παρακολούθηση και διαχείριση κυβερνοασφάλειας σε πραγματικό χρόνο [11]. Σε αντίθεση με την premarket αξιολόγηση, όπου ο κατασκευαστής τεκμηριώνει τις λειτουργίες ασφάλειας, το postmarket πλαίσιο επικεντρώνεται στη διατήρηση της ασφάλειας καθ' όλη τη διάρκεια ζωής του προϊόντος.

Συγκεκριμένα, ο κατασκευαστής οφείλει να διαθέτει:

- Σύστημα παρακολούθησης ευπαθειών (vulnerability monitoring)

Παρακολούθηση βάσεων δεδομένων ευπαθειών (NVD, ICS-CERT), καταγραφής incident reports, ενημερώσεων προμηθευτών λογισμικού και ανάλυση απειλών σε πραγματικό χρόνο.

- Μηχανισμό διάγνωσης και αναφοράς συμβάντων (incident detection & reporting)

Ανίχνευση ανωμαλιών λειτουργίας, επιθέσεων σε firmware ή ασυνήθιστης συμπεριφοράς συσκευής. Τα υπολειπόμενα ή μη ελεγχόμενα κυβερνοασφαλιστικά ρίσκα ("uncontrolled risks") οφείλουν να παρακολουθούνται και να αναφέρονται στον FDA στο πλαίσιο των postmarket απαιτήσεων ασφάλειας [11].

- Διαδικασίες ταχείας διόρθωσης (rapid patching & secure updates)

Το FDA απαιτεί τεχνικούς μηχανισμούς για ασφαλείς ενημερώσεις, επαλήθευση firmware, και μεθοδολογία αξιολόγησης της επίδρασης ενός patch στα χαρακτηριστικά ασφαλείας.

- Root Cause Analysis (RCA)

Ανάλυση των αιτιών που οδήγησαν σε παραβίαση ή αστοχία ασφάλειας, με τεκμηρίωση των corrective & preventive actions.

- Συνεχή αξιολόγηση κινδύνων στο πραγματικό περιβάλλον (continuous risk evaluation)

Η διαχείριση κινδύνων δεν ολοκληρώνεται στην premarket φάση αλλά αποτελεί διαρκή υποχρέωση, σύμφωνα με την αρχή “Cybersecurity Risk Management throughout the product life-cycle” [11].

Τα ευρήματα της μελέτης Stern et al. [23] υποστηρίζουν τη σημασία της postmarket εποπτείας, δείχνοντας ότι πολλές συσκευές που εγκρίθηκαν με επαρκή τεκμηρίωση παρουσιάζουν αδυναμίες μετά την κυκλοφορία τους, όπως:

- μη ασφαλή firmware updates,
- ανεπαρκή μηχανισμούς αυθεντικοποίησης,
- ελλείψεις στην κρυπτογράφηση και στο access control.

Επιπλέον, σύμφωνα με την ENISA [12], οι επιθέσεις ransomware και οι επιθέσεις σε ξεπερασμένες εκδόσεις firmware αποτελούν την κυριότερη αιτία επιπτώσεων ασφάλειας σε IoMT περιβάλλοντα την τελευταία πενταετία.

Τέλος, η πρόσφατη συγκριτική ανάλυση των Ostermann et al. [27] καταδεικνύει ότι η προσέγγιση του FDA στο postmarket στάδιο είναι περισσότερο τεχνικά προσανατολισμένη, ενώ το MDR υιοθετεί έναν πιο διαδικασιακό και οργανωτικό χαρακτήρα. Αυτό οδηγεί σε διαφορετική φιλοσοφία ως προς τη συμμόρφωση και τον τρόπο διαχείρισης συμβάντων στα δύο κανονιστικά πλαίσια.

4.4.3 Επιπλέον ευρήματα από τη βιβλιογραφία

Η εμπειρική μελέτη των Stern et al. [23], η οποία ανέλυσε εκατοντάδες FDA product summaries, ανέδειξε κρίσιμες αδυναμίες στην πρακτική εφαρμογή των απαιτήσεων κυβερνοασφάλειας από τους κατασκευαστές ιατρικών συσκευών. Τα ευρήματα αυτά επιβεβαιώνουν ότι, παρά την ύπαρξη σαφούς κανονιστικού πλαισίου, η ωριμότητα υλοποίησης διαφέρει σημαντικά μεταξύ των προϊόντων.

Συγκεκριμένα, η μελέτη κατέγραψε ότι:

- Υπάρχει έντονη ανομοιομορφία στην τεκμηρίωση και εφαρμογή βασικών cybersecurity controls.

Σε πολλές συσκευές απουσιάζουν στοιχεία όπως ασφαλής διαχείριση πρόσβασης, ακεραιότητα firmware ή συστηματική χρήση κρυπτογράφησης.

- Οι μηχανισμοί ασφαλούς ενημέρωσης λογισμικού (secure updates) παραμένουν αδύναμοι.

Ελλείπουν διαδικασίες ελέγχου ψηφιακής υπογραφής, επαλήθευσης πακέτων ενημέρωσης ή προστασίας έναντι rollback attacks—αδυναμίες που επισημαίνονται συστηματικά και σε αναφορές της ENISA [12].

- Ανεπαρκείς μηχανισμοί αυθεντικοποίησης (authentication) εντοπίστηκαν σε μεγάλο αριθμό συσκευών, ακόμη και σε νεότερα μοντέλα.

Οι συσκευές συχνά βασίζονται σε στατικά credentials, κοινά passwords ή χωρίς MFA, κάτι που αντιβαίνει στις premarket απαιτήσεις του FDA [11].

- Στα πιο σύγχρονα προϊόντα παρατηρείται βελτίωση, όπως ενσωμάτωση SBOM, secure boot, audit logging και αυστηρότερος έλεγχος ακεραιότητας.

Αυτές οι πρακτικές ευθυγραμμίζονται με τις πρόσφατες ανάγκες του FDA για τεκμηρίωση της αλυσίδας λογισμικού και αντιμετώπιση supply-chain απειλών.

Τα παραπάνω ευρήματα υπογραμμίζουν ότι, παρά την πρόοδο της βιομηχανίας, εξακολουθεί να υπάρχει σημαντική ασυνέπεια στον βαθμό συμμόρφωσης. Η βιβλιογραφία επιβεβαιώνει ότι η αδυναμία ενιαίας εφαρμογής των κατευθυντήριων οδηγιών αυξάνει την πιθανότητα παραβιάσεων και καθιστά τις IoMT συσκευές ελκυστικούς στόχους.

Επομένως, η ανάγκη για ενισχυμένη τυποποίηση, συνεχείς αξιολογήσεις και αυστηρή τεκμηρίωση καθίσταται θεμελιώδης, δημιουργώντας τη βάση για την ανάλυση που ακολουθεί στο πλαίσιο των NISTIR 8259/8259A.

4.5 NISTIR 8259 & 8259A για IoT/IoMT Συσκευές

Τα έγγραφα NISTIR 8259 και NISTIR 8259A αποτελούν βασικές αναφορές του NIST για την κυβερνοασφάλεια συσκευών Internet of Things (IoT) και, κατ' επέκταση, IoMT. Το NISTIR 8259 επικεντρώνεται στις θεμελιώδεις δραστηριότητες που οφείλουν να υλοποιούν οι κατασκευαστές IoT συσκευών, ενώ το NISTIR 8259A ορίζει ένα core baseline από συγκεκριμένες δυνατότητες ασφάλειας που πρέπει να ενσωματώνουν οι ίδιες οι συσκευές [25], [25a]. Τα κείμενα αυτά δεν είναι κανονιστικά με την αυστηρή έννοια, αλλά λειτουργούν ως πρακτικός οδηγός για τη σχεδίαση ασφαλών συστημάτων, ο οποίος μπορεί να αξιοποιηθεί συμπληρωματικά με το MDR, το ISO 14971 και τις οδηγίες του FDA.

4.5.1 Στόχοι και Ρόλος των NISTIR 8259 / 8259A

Σκοπός του NISTIR 8259 είναι να περιγράψει ένα σύνολο θεμελιωδών δραστηριοτήτων κυβερνοασφάλειας που πρέπει να ακολουθεί ο κατασκευαστής μιας IoT συσκευής, από τον αρχικό σχεδιασμό έως την υποστήριξη μετά την κυκλοφορία [25]. Οι δραστηριότητες αυτές καλύπτουν την αναγνώριση των αναγκών ασφάλειας, την ανάλυση κινδύνων, τη σχεδίαση, τις δοκιμές και τη διαχείριση ευπαθειών. Στόχος είναι να δημιουργηθεί ένα ελάχιστο επίπεδο ωριμότητας, ανεξάρτητα από τον κλάδο ή το είδος της συσκευής.

Το NISTIR 8259A συμπληρώνει τον σκοπό του NISTIR 8259, καθορίζοντας επιπλέον έξι βασικές κατηγορίες ικανοτήτων που πρέπει να διαθέτει η ίδια η συσκευή (device cybersecurity capability core baseline) [25a]. Ενώ το MDR και το ISO 14971 επικεντρώνονται στη διαχείριση κινδύνου σε επίπεδο συστήματος, τα NISTIR 8259/8259A εστιάζουν στο τι πρέπει να μπορεί να κάνει η συσκευή και πώς ο κατασκευαστής οργανώνει τις εσωτερικές του διαδικασίες ώστε να το επιτύχει.

4.5.2 Θεμελιώδεις Δραστηριότητες Κατασκευαστών (NISTIR 8259)

Το NISTIR 8259 περιγράφει ένα σύνολο Foundational Cybersecurity Activities for IoT Device Manufacturers, οι οποίες λειτουργούν ως εσωτερικό πλαίσιο οργάνωσης για τις εταιρείες που αναπτύσσουν IoT/IoMT συσκευές [25]. Ενδεικτικά, οι βασικές ομάδες δραστηριοτήτων είναι:

- Identify Expected Device Cybersecurity Capabilities

Ο κατασκευαστής πρέπει να προσδιορίσει ποιες από τις baseline ικανότητες (8259A) [25a] είναι απαραίτητες για τη συγκεκριμένη συσκευή, λαμβάνοντας υπόψη το περιβάλλον χρήσης, τα δεδομένα που διαχειρίζεται και τις απαιτήσεις των πελατών.

- Identify Customer Cybersecurity Needs and Goals

Η ανάλυση των αναγκών των οργανισμών-πελατών (π.χ. νοσοκομεία) είναι κρίσιμη: πολιτικές πρόσβασης, απαιτήσεις logging, integration με SIEM, κανονιστικά πλαίσια (MDR, HIPAA, GDPR κ.λπ.).

- Design and Develop Securely

Το NISTIR 8259 προτείνει την ενσωμάτωση πρακτικών secure SDLC: threat modeling, code review, δοκιμές ασφάλειας, καθώς και την τεκμηρίωση των απαιτήσεων και των ελέγχων ασφάλειας καθ' όλη τη διάρκεια του κύκλου ανάπτυξης.

- Manufacture and Configure Securely

Περιλαμβάνει πρακτικές όπως ασφαλής ρύθμιση factory defaults, προστασία των production keys, έλεγχος της εφοδιαστικής αλυσίδας (supply chain security) και επαλήθευση της αυθεντικότητας hardware/firmware πριν από την παράδοση στον πελάτη.

- Manage Device Cybersecurity Over Time

Εδώ εντάσσονται οι διαδικασίες διαχείρισης ευπαθειών, παρακολούθησης αναφορών, δημοσίευσης advisories και παροχής patches ή αναβαθμίσεων. Οι δραστηριότητες αυτές ευθυγραμμίζονται με τις postmarket απαιτήσεις του FDA [11] και τις αρχές συνεχούς βελτίωσης κινδύνου.

Με αυτόν τον τρόπο, το NISTIR 8259 λειτουργεί ως ένας πρακτικός "οδικός χάρτης" για τις εταιρείες, δίνοντάς τους μια δομημένη μεθοδολογία για να ενσωματώσουν τις ικανότητες του 8259A σε διαδικασίες ανάπτυξης και υποστήριξης.

4.5.3 Απαιτήσεις Ασφάλειας για IoMT (NISTIR 8259A)

Στο NISTIR 8259A ορίζεται ένα IoT Device Cybersecurity Capability Core Baseline, το οποίο αποτελείται από έξι κατηγορίες ικανοτήτων [25a]:

1. Device Identification

Η συσκευή πρέπει να μπορεί να αναγνωρίζεται με μοναδικό τρόπο μέσα στο δίκτυο. Αυτό περιλαμβάνει σταθερά identifiers, certificates ή άλλα credentials που επιτρέπουν σε συστήματα διαχείρισης να την εντοπίζουν και να εφαρμόζουν πολιτικές ασφάλειας.

2. Device Configuration

Η δυνατότητα ασφαλούς διαμόρφωσης των παραμέτρων της συσκευής είναι κρίσιμη. Το baseline απαιτεί μηχανισμούς προστασίας των ρυθμίσεων (π.χ. role-based access, προστασία configuration interface) και δυνατότητα επαναφοράς σε ασφαλή προεπιλεγμένη κατάσταση.

3. Data Protection

Η συσκευή πρέπει να προστατεύει τα δεδομένα που αποθηκεύει, επεξεργάζεται ή μεταδίδει. Αυτό συνεπάγεται κρυπτογράφηση, έλεγχο πρόσβασης σε ευαίσθητες πληροφορίες και μηχανισμούς διασφάλισης ακεραιότητας (π.χ. χρήση MACs ή ψηφιακών υπογραφών).

4. Logical Access to Interfaces

Το NISTIR 8259A ορίζει ότι οι λογικές διεπαφές (network services, APIs, local ports) πρέπει να προστατεύονται με κατάλληλους μηχανισμούς αυθεντικοποίησης και authorization. Οι αχρείαστες διεπαφές πρέπει να απενεργοποιούνται, μειώνοντας το attack surface.

5. Software Update

Βασικό στοιχείο του baseline είναι η δυνατότητα ασφαλούς ενημέρωσης λογισμικού και firmware. Η συσκευή οφείλει να υποστηρίζει ελεγχόμενες, επαληθεύσιμες και, όπου είναι δυνατό, κρυπτογραφημένες ενημερώσεις, ώστε να διορθώνονται ευπάθειες χωρίς να εισάγονται νέοι κίνδυνοι.

6. Cybersecurity State Awareness

Η συσκευή πρέπει να μπορεί να παρέχει πληροφορίες για την κατάσταση ασφάλειας: logs, alerts και telemetry δεδομένα που επιτρέπουν στον οργανισμό να ανιχνεύει ανωμαλίες και να ερευνά περιστατικά.

Για τις IoMT συσκευές, οι παραπάνω ικανότητες συνδέονται άμεσα με τις κλινικές απαιτήσεις: π.χ. η ασφαλής ενημέρωση firmware συνδέεται με την πρόληψη βλαβών που θα μπορούσαν να επηρεάσουν τη θεραπεία, ενώ η δυνατότητα logging είναι κρίσιμη για την ιχνηλάτηση περιστατικών που σχετίζονται με ασφάλεια ασθενή.

4.5.4 Συσχέτιση των NISTIR 8259 / 8259A με IoMT και τα υπόλοιπα πρότυπα

Τα έγγραφα NISTIR 8259 και 8259A αποτελούν τεχνικές κατευθυντήριες γραμμές για την κυβερνοασφάλεια συσκευών IoT και, σύμφωνα με το NIST, μπορούν να χρησιμοποιηθούν σε συνδυασμό με κλαδικά ρυθμιστικά πλαίσια, όπως οι οδηγίες του FDA, το ISO 14971 και ο Κανονισμός MDR [25], [25a].

Το NISTIR 8259 προσδιορίζει έξι θεμελιώδεις δραστηριότητες για τους κατασκευαστές (foundational activities), οι οποίες ευθυγραμμίζονται άμεσα με τις απαιτήσεις τεκμηρίωσης και post-market monitoring του FDA. Ειδικότερα, το NIST επισημαίνει ότι οι κατασκευαστές πρέπει να ενσωματώνουν διαδικασίες για:

- προσδιορισμό των αναμενόμενων ικανοτήτων ασφάλειας,
- αναγνώριση των αναγκών κυβερνοασφάλειας των χρηστών,
- ασφαλή ανάπτυξη,
- προστασία της εφοδιαστικής αλυσίδας και
- συνεχή διαχείριση ευπαθειών [25].

Αντίστοιχες απαιτήσεις περιγράφονται και στο πλαίσιο FDA SPDF, το οποίο απαιτεί documented security processes, vulnerability handling και secure update mechanisms [11].

Το NISTIR 8259A, το οποίο ορίζει το IoT Device Cybersecurity Capability Core Baseline, καλύπτει ικανότητες όπως device identification, secure configuration, data protection, logical access control και secure update—στοιχεία τα οποία συνδέονται άμεσα με τους τεχνικούς ελέγχους (cybersecurity controls) που απαιτεί το FDA στις premarket υποβολές [25a], [11]. Επίσης, η απαίτηση “cybersecurity state awareness” ευθυγραμμίζεται με την ανάγκη logging και incident detection που αναφέρει η FDA στην postmarket καθοδήγησή της [11].

Σε ευρωπαϊκό επίπεδο, ο Κανονισμός MDR απαιτεί από τους κατασκευαστές τεκμηριωμένη διαδικασία διαχείρισης κινδύνου, ενσωμάτωση μέτρων κυβερνοασφάλειας και συνεχή αξιολόγηση της ασφάλειας του λογισμικού, κάτι που ευθυγραμμίζεται με τις δραστηριότητες του NISTIR 8259 περί “secure design and development” και “ongoing device cybersecurity management” [20], [25].

Τέλος, το ISO 14971 αποτελεί τη βάση για την ανάλυση και αξιολόγηση κινδύνου σε όλες τις ιατρικές συσκευές. Αν και το ISO 14971 επικεντρώνεται στο risk management και όχι σε συγκεκριμένες τεχνικές ικανότητες, η NISTIR 8259A baseline μπορεί να θεωρηθεί ως τεχνικό συμπλήρωμα που περιγράφει πώς υλοποιούνται στην πράξη τα controls που προκύπτουν από την αξιολόγηση κινδύνων [21], [24], [25a].

Συνολικά, τα NISTIR 8259 και 8259A δεν αντικαθιστούν τα MDR, ISO 14971 ή FDA, αλλά λειτουργούν ως τεχνικό υπόβαθρο που μπορεί να χρησιμοποιηθεί συμπληρωματικά για την ενίσχυση της ασφάλειας και της τεκμηρίωσης συσκευών IoMT.

4.6 Συγκριτική Ανάλυση Ρυθμιστικών Πλαισίων & Προτύπων Ασφάλειας IoMT

Η κυβερνοασφάλεια των IoMT συσκευών καθορίζεται από ένα σύνολο προτύπων και ρυθμιστικών πλαισίων που προέρχονται τόσο από τις Ηνωμένες Πολιτείες όσο και από την Ευρωπαϊκή Ένωση. Τα βασικά αυτά πλαίσια περιλαμβάνουν τον Κανονισμό MDR της ΕΕ, το πρότυπο ISO 14971, τις οδηγίες του FDA για premarket και postmarket ασφάλεια και τα έγγραφα NISTIR 8259/8259A. Κάθε ένα από αυτά τα πλαίσια προσεγγίζει την ασφάλεια των ιατρικών συσκευών από διαφορετική οπτική: ρυθμιστική, μεθοδολογική, τεχνική ή διαδικασιακή.

Σύμφωνα με τον Greser [20], ο MDR εστιάζει στη συνολική διαχείριση κινδύνου και στην τεκμηρίωση της συμμόρφωσης των ιατρικών συσκευών με απαιτήσεις ασφαλείας και απόδοσης. Αντίστοιχα, το ISO 14971, όπως περιγράφεται από τους Yang [21] και Flood et al. [22], παρέχει τη

μεθοδολογική βάση για την αναγνώριση, αξιολόγηση και έλεγχο κινδύνων σε όλο τον κύκλο ζωής της συσκευής.

Οι οδηγίες του FDA, σύμφωνα με τη μελέτη Stern et al. [23] και τα επίσημα έγγραφα premarket/postmarket [11], προσφέρουν μια περισσότερο τεχνική και συγκεκριμένη καθοδήγηση σχετικά με τον σχεδιασμό, την ενημέρωση λογισμικού, τις δυνατότητες auditing, την αυθεντικοποίηση και την προστασία firmware. Παράλληλα, όπως επισημαίνουν οι Ostermann et al. [27], το FDA δίνει έμφαση στην τεχνική τεκμηρίωση και στα αποδεικτικά στοιχεία για την κυβερνοασφάλεια, ενώ ο MDR υιοθετεί μια πιο διαδικασιοκεντρική και οργανωτική φιλοσοφία.

Τα έγγραφα NISTIR 8259 και NISTIR 8259A [25], [25a] λειτουργούν συμπληρωματικά, παρέχοντας ένα baseline τεχνικών ικανοτήτων και ένα σύνολο δραστηριοτήτων για την υλοποίηση ασφάλειας σε IoT/IoMT συσκευές. Αν και δεν αποτελούν νομικά δεσμευτικά πρότυπα, η δομή τους ευθυγραμμίζεται άμεσα με τις απαιτήσεις του FDA (secure updates, device identification, logging) και στις απαιτήσεις MDR/ISO 14971 για συνεχή διαχείριση κινδύνου.

Η συνδυαστική ανάλυση των παραπάνω πλαισίων επιτρέπει τη δημιουργία ενός ενιαίου μοντέλου κατανόησης της κυβερνοασφάλειας IoMT συσκευών, όπως θα παρουσιαστεί στις υποενότητες που ακολουθούν.

4.6.1 Σύγκριση MDR και ISO 14971 ως προς τη Διαχείριση Κινδύνου και την Κυβερνοασφάλεια

Ο Κανονισμός MDR (ΕΕ 2017/745) και το πρότυπο ISO 14971 αποτελούν δύο βασικά στοιχεία του ευρωπαϊκού πλαισίου για την ασφάλεια ιατρικών συσκευών, με άμεση εφαρμογή και στις IoMT συσκευές. Παρότι έχουν διαφορετικό χαρακτήρα —ο MDR είναι νομικά δεσμευτικό ρυθμιστικό πλαίσιο, ενώ το ISO 14971 αποτελεί διεθνές τεχνικό πρότυπο— λειτουργούν συμπληρωματικά.

Σύμφωνα με τον Greser [20], ο MDR ορίζει από τους κατασκευαστές να εφαρμόζουν μια τεκμηριωμένη διαδικασία διαχείρισης κινδύνου, η οποία καλύπτει τον πλήρη κύκλο ζωής της συσκευής, συμπεριλαμβανομένων θεμάτων ασφάλειας λογισμικού, διαλειτουργικότητας και κυβερνοασφάλειας. Ο MDR δεν καθορίζει συγκεκριμένη μεθοδολογία, αλλά αναμένει από τον κατασκευαστή να χρησιμοποιεί αναγνωρισμένα πρότυπα· το ISO 14971 αποτελεί την προτεινόμενη και ευρέως χρησιμοποιούμενη βάση για την εκπλήρωση αυτής της απαίτησης.

Το ISO 14971, όπως περιγράφεται από τους Yang [21] και Flood et al. [22], ορίζει μια συστηματική και επαναλαμβανόμενη διαδικασία για την αναγνώριση κινδύνων, την εκτίμηση σοβαρότητας και πιθανότητας, τον έλεγχο κινδύνων και την αξιολόγηση του υπολειπόμενου κινδύνου. Το πρότυπο επεκτείνεται και στη μετα-κυκλοφοριακή παρακολούθηση, στοιχείο που ευθυγραμμίζεται με τις απαιτήσεις του MDR για συνεχή αναθεώρηση και συνεχή συλλογή στοιχείων ασφάλειας.

Σε πρακτικό επίπεδο, ο MDR επιβάλλει στους κατασκευαστές να διασφαλίζουν ότι οι επιλεγμένοι μηχανισμοί ασφαλείας, συμπεριλαμβανομένων των μέτρων κυβερνοασφάλειας, τεκμηριώνονται επαρκώς και συνδέονται με τα αποτελέσματα της ανάλυσης κινδύνου. Αυτή η φιλοσοφία αντανακλάται άμεσα στις αρχές του ISO 14971, όπου ορίζεται ότι κάθε μέτρο ελέγχου κινδύνου πρέπει να αιτιολογείται και να αξιολογείται.

Συμπερασματικά, ο MDR αποτελεί το πλαίσιο υποχρεώσεων, ενώ το ISO 14971 παρέχει τη μεθοδολογία εφαρμογής της διαχείρισης κινδύνου. Και τα δύο θεωρούνται απαραίτητα για τη συμμόρφωση IoMT συσκευών με τις ευρωπαϊκές απαιτήσεις ασφάλειας.

4.6.2 Σύγκριση FDA – MDR

Ο Κανονισμός MDR και το ρυθμιστικό πλαίσιο του FDA επιδιώκουν και τα δύο τη διασφάλιση της ασφάλειας και της απόδοσης των ιατρικών συσκευών, ωστόσο διαφέρουν ως προς τη δομή, το πεδίο

εφαρμογής και τον τρόπο με τον οποίο ενσωματώνουν την κυβερνοασφάλεια. Ο Greser [20] επισημαίνει ότι ο MDR λειτουργεί ως οριζόντιο, νομικά δεσμευτικό πλαίσιο για την ευρωπαϊκή αγορά, καλύπτοντας όλες τις κατηγορίες ιατρικών συσκευών και απαιτώντας από τους κατασκευαστές τεκμηριωμένη διαχείριση κινδύνου, συμπεριλαμβανομένων κινδύνων που σχετίζονται με λογισμικό και συνδεσιμότητα. Αντίθετα, το FDA εκδίδει εξειδικευμένες κατευθυντήριες οδηγίες για την κυβερνοασφάλεια (premarket και postmarket), οι οποίες εστιάζουν σε συγκεκριμένες τεχνικές και διαδικαστικές απαιτήσεις για την έγκριση και παρακολούθηση συσκευών στην αγορά των ΗΠΑ [11].

Σύμφωνα με τους Ostermann et al. [27], η προσέγγιση του MDR είναι πιο διαδικασιοκεντρική και βασίζεται έντονα στην ενσωμάτωση της ανάλυσης κινδύνου (π.χ. μέσω ISO 14971) σε όλο το σύστημα διαχείρισης ποιότητας του κατασκευαστή, ενώ το FDA υιοθετεί μια πιο τεχνοκεντρική προσέγγιση, δίνοντας έμφαση στη λεπτομερή τεκμηρίωση συγκεκριμένων controls, όπως secure updates, authentication, logging και προστασία firmware [11], [23]. Η μελέτη Stern et al. [23] δείχνει πως τα FDA product summaries περιλαμβάνουν συχνά περιγραφές συγκεκριμένων μηχανισμών κυβερνοασφάλειας, αλλά ταυτόχρονα αναδεικνύει και ανομοιομορφίες στην πρακτική εφαρμογή τους, κάτι που υπογραμμίζει την ανάγκη για πιο συνεπή συμμόρφωση.

Επιπλέον, ο MDR απαιτεί από τους κατασκευαστές να αποδεικνύουν συμμόρφωση όχι μόνο με τεχνικές απαιτήσεις, αλλά και με κλινική αξιολόγηση, post-market surveillance και vigilance, ενσωματώνοντας την κυβερνοασφάλεια μέσα σε ένα ευρύτερο πλαίσιο ασφάλειας ασθενή [20]. Το FDA, μέσω των premarket και postmarket οδηγιών, εστιάζει ιδιαίτερα στη διαχείριση ευπαθειών, στην παρακολούθηση απειλών και στη δυνατότητα ταχείας διόρθωσης (rapid patching) [11]. Έτσι, ενώ τα δύο πλαίσια επιδιώκουν παρόμοιους στόχους, ο MDR θέτει κυρίως ρυθμιστικές και οργανωτικές υποχρεώσεις, ενώ το FDA παρέχει πιο λεπτομερή τεχνική καθοδήγηση για τη σχεδίαση και τη συντήρηση ασφαλών συσκευών.

4.6.3 Σύγκριση FDA – NISTIR 8259 / 8259A

Οι οδηγίες του FDA (premarket και postmarket) και τα τεχνικά έγγραφα NISTIR 8259 και NISTIR 8259A αποτελούν βασικά εργαλεία για την ανάπτυξη και αξιολόγηση της κυβερνοασφάλειας IoMT συσκευών, ωστόσο εστιάζουν σε διαφορετικές πτυχές της διαδικασίας. Το FDA, σύμφωνα με τις επίσημες κατευθυντήριες οδηγίες του 2023 και 2018 [11], παρέχει λεπτομερείς τεχνικές και διαδικαστικές απαιτήσεις για τον τρόπο με τον οποίο οι κατασκευαστές πρέπει να τεκμηριώνουν την ασφάλεια κατά την premarket υποβολή και να συνεχίζουν να διαχειρίζονται τις ευπάθειες μετά την κυκλοφορία. Αντίθετα, τα NISTIR 8259 και 8259A αποτελούν γενικές τεχνικές προδιαγραφές που προσδιορίζουν τις ελάχιστες ικανότητες ασφάλειας που πρέπει να ενσωματώνει μια συσκευή IoT/IoMT [25], [25a].

Σύμφωνα με τη μελέτη Stern et al. [23], το FDA απαιτεί από τους κατασκευαστές να παρουσιάζουν συγκεκριμένους μηχανισμούς ασφάλειας — όπως authentication, logging, secure boot και ασφαλείς ενημερώσεις λογισμικού — οι οποίοι αξιολογούνται μέσα στις premarket διαδικασίες. Αυτές οι απαιτήσεις αντιστοιχούν άμεσα σε βασικά στοιχεία του IoT Device Cybersecurity Capability Core Baseline του NISTIR 8259A, το οποίο περιλαμβάνει device identification, secure configuration, data protection, logical access control, secure update capabilities και cybersecurity state awareness [25a].

Το NISTIR 8259, από την άλλη πλευρά, καθορίζει οργανωτικές δραστηριότητες για τους κατασκευαστές, όπως τον προσδιορισμό απαιτήσεων ασφάλειας, την ασφαλή ανάπτυξη λογισμικού και τη συνεχή διαχείριση ευπαθειών [25]. Αυτά τα στοιχεία είναι ευθυγραμμισμένα με τα premarket στοιχεία του FDA, όπου απαιτείται τεκμηριωμένο secure product development process, αξιολόγηση κινδύνων και διαδικασίες vulnerability handling [11]. Οι Ostermann et al. [27] επισημαίνουν ότι η καθοδήγηση του FDA έχει ισχυρότερο τεχνικό χαρακτήρα σε σχέση με ευρωπαϊκά πλαίσια, κάτι που το φέρνει πιο κοντά στο πνεύμα του NISTIR 8259A, το οποίο εστιάζει σε συγκεκριμένες συσκευασίες ασφάλειας.

Ενώ οι οδηγίες του FDA είναι νομικά δεσμευτικές για την αγορά των ΗΠΑ, τα NISTIR 8259/8259A δεν αποτελούν κανονιστικό πλαίσιο αλλά χρησιμοποιούνται ευρέως ως αναφορά για σχεδιασμό συστημάτων IoT/IoMT. Ωστόσο, η χαρτογράφηση των απαιτήσεων δείχνει ότι οι δύο προσεγγίσεις συγκλίνουν ουσιαστικά στα εξής σημεία:

- ανάγκη για ασφαλή αρχιτεκτονική συσκευής,
- ασφαλείς ενημερώσεις (secure updates),
- μηχανισμούς προστασίας δεδομένων,
- έλεγχο πρόσβασης,
- καταγραφή γεγονότων (logging),
- συνεχή διαχείριση ευπαθειών.

Έτσι, το NISTIR 8259A παρέχει ένα τεχνικό baseline συμβατό με τις απαιτήσεις του FDA, ενώ το NISTIR 8259 προσφέρει ένα πλαίσιο οργανωτικών δραστηριοτήτων που ευθυγραμμίζεται με τις διαδικασιακές απαιτήσεις του FDA για premarket και postmarket cybersecurity διαχείριση.

4.6.4 Σύγκριση ISO 14971 – NISTIR 8259 / 8259A

Το πρότυπο ISO 14971 και τα έγγραφα NISTIR 8259 / 8259A καλύπτουν διαφορετικές, αλλά αλληλοσυμπληρούμενες, πτυχές της ασφάλειας ιατρικών και IoT/IoMT συσκευών. Το ISO 14971 επικεντρώνεται στη διαχείριση κινδύνου σε όλο τον κύκλο ζωής της ιατρικής συσκευής, ενώ τα NISTIR 8259 και 8259A επικεντρώνονται στις τεχνικές ικανότητες ασφάλειας της συσκευής και στις δραστηριότητες του κατασκευαστή για την υλοποίησή τους.

Σύμφωνα με τους Yang [21] και Flood et al. [22], το ISO 14971 ορίζει μια δομημένη διαδικασία αναγνώρισης, ανάλυσης, αξιολόγησης και ελέγχου κινδύνων, καθώς και αξιολόγησης του υπολειπόμενου κινδύνου. Η διαδικασία αυτή είναι επαναληπτική και επεκτείνεται σε μετα-παραγωγικές δραστηριότητες, όπου συλλέγονται δεδομένα από την πραγματική χρήση της συσκευής. Όπως επισημαίνεται και στο white paper του BSI [24], το ISO 14971 δεν προσδιορίζει συγκεκριμένα τεχνικά μέτρα κυβερνοασφάλειας, αλλά απαιτεί κάθε μέτρο ελέγχου να τεκμηριώνεται και να συνδέεται με συγκεκριμένους κινδύνους που έχουν εντοπιστεί.

Αντίστοιχα, το NISTIR 8259A ορίζει ένα core baseline ικανοτήτων κυβερνοασφάλειας για IoT συσκευές, συμπεριλαμβανομένων της ταυτοποίησης συσκευής, της ασφαλούς διαμόρφωσης, της προστασίας δεδομένων, του ελέγχου πρόσβασης, των ασφαλών ενημερώσεων λογισμικού και της επίγνωσης κατάστασης ασφάλειας [25a]. Το NISTIR 8259 συμπληρώνει αυτό το baseline με ένα σύνολο θεμελιωδών δραστηριοτήτων για τους κατασκευαστές, όπως ο προσδιορισμός απαιτήσεων ασφάλειας, η ασφαλής ανάπτυξη και η συνεχιζόμενη διαχείριση ευπαθειών [25].

Σε αυτό το πλαίσιο, το ISO 14971 μπορεί να θεωρηθεί ως το μεθοδολογικό πλαίσιο διαχείρισης κινδύνου, ενώ τα NISTIR 8259/8259A προσφέρουν ένα σύνολο συγκεκριμένων τεχνικών ικανοτήτων και οργανωτικών δραστηριοτήτων που μπορούν να χρησιμοποιηθούν για την υλοποίηση των μέτρων ελέγχου που προκύπτουν από την ανάλυση κινδύνου. Για παράδειγμα, αν η ανάλυση κινδύνου βάσει ISO 14971 αναγνωρίσει κίνδυνο μη εξουσιοδοτημένης πρόσβασης ή τροποποίησης δεδομένων, τότε οι κατηγορίες “logical access control” και “data protection” του NISTIR 8259A προσδιορίζουν τις ελάχιστες λειτουργίες που πρέπει να υποστηρίζει η συσκευή για να αντιμετωπιστεί ο κίνδυνος [25a].

Τέλος, τόσο το ISO 14971 όσο και τα NISTIR 8259/8259A δίνουν έμφαση στη συνεχή διαχείριση κινδύνων και ευπαθειών μετά την κυκλοφορία της συσκευής, με το ISO 14971 να το εντάσσει στο πλαίσιο μετα-παραγωγικής παρακολούθησης [21], [22], [24] και το NISTIR 8259 να περιγράφει συγκεκριμένες δραστηριότητες για τη διαχείριση ευπαθειών και ενημερώσεων σε βάθος χρόνου [25]. Έτσι, τα δύο πλαίσια δεν έρχονται σε αντίθεση, αλλά μπορούν να συνδυαστούν, με το ISO 14971 να καθοδηγεί το “τι” σε επίπεδο κινδύνων και τα NISTIR να εξειδικεύουν το “πώς” σε επίπεδο τεχνικών ικανοτήτων και διαδικασιών.

4.6.5 Σύνοψη Συγκριτικής Ανάλυσης Προτύπων και Ρυθμιστικών Πλαισίων

Η συγκριτική μελέτη των MDR, ISO 14971, FDA Premarket/Postmarket Guidelines και NISTIR 8259/8259A αποδεικνύει ότι τα πλαίσια αυτά είναι συμπληρωματικά αλλά ακολουθούν διαφορετική φιλοσοφία. Ο MDR (ΕΕ 2017/745), όπως περιγράφεται από τον Greser [20], αποτελεί το ρυθμιστικό θεμέλιο για την ασφάλεια ιατρικών συσκευών στην Ευρώπη και απαιτεί ολοκληρωμένη τεκμηρίωση διαχείρισης κινδύνου σε όλο τον κύκλο ζωής της συσκευής. Το ISO 14971, σύμφωνα με τους Yang [21] και Flood et al. [22], παρέχει τη μεθοδολογία για την υλοποίηση αυτής της διαχείρισης κινδύνου.

Οι οδηγίες του FDA, βάσει των [11] και [23], εστιάζουν σε πολύ συγκεκριμένα τεχνικά μέτρα ασφάλειας, όπως authentication, secure updates, logging και προστασία firmware, και αποτελούν ένα από τα πιο λεπτομερή πλαίσια διεθνώς. Σε αντίθεση, τα NISTIR 8259 και 8259A [25], [25a] ορίζουν ένα baseline ικανοτήτων IoT/IoMT ασφάλειας και οργανωτικών δραστηριοτήτων για τους κατασκευαστές, το οποίο λειτουργεί σε υψηλό βαθμό συμπληρωματικά με τις απαιτήσεις του FDA.

Όπως επισημαίνουν οι Ostermann et al. [27], το FDA έχει μία περισσότερο τεχνοκεντρική προσέγγιση, ο MDR είναι διαδικασιοκεντρικός και το ISO 14971 μεθοδολογικό, ενώ τα NISTIR παρέχουν τεχνικές προδιαγραφές και ένα γενικό πλαίσιο λειτουργικών ικανοτήτων. Η συνέργεια των τεσσάρων πλαισίων επιτρέπει μια ολοκληρωμένη κάλυψη από την αναγνώριση κινδύνων έως την υλοποίηση τεχνικών και οργανωτικών μέτρων ασφάλειας.

Ο ακόλουθος πίνακας συνοψίζει τις κύριες διαφορές και τις περιοχές επικάλυψης.

Πίνακας 5.1 : Συγκριτική Ανάλυση MDR – ISO 14971 – FDA – NISTIR 8259/8259A

Πλαίσιο / Πρότυπο	Χαρακτήρας	Κύρια Εστίαση	Πηγές
MDR (ΕΕ 2017/745)	Ρυθμιστικό, νομικά δεσμευτικό	Διαδικασιοκεντρική διαχείριση κινδύνου, τεκμηρίωση, ασφάλεια λογισμικού & συνδεσιμότητας	[20], [27]
ISO 14971	Διεθνές τεχνικό πρότυπο	Μεθοδολογική ανάλυση κινδύνου, risk control, post-market παρακολούθηση	[21], [22], [24]
FDA Premarket / Postmarket	Ρυθμιστικό (ΗΠΑ)	Τεχνικά controls: authentication, secure updates, logging, firmware integrity, SBOM	[11], [23], [27]
NISTIR 8259A	Τεχνικό baseline	Ικανότητες IoT/IoMT συσκευής: data protection, access control, secure configuration, secure updates	[25a]
NISTIR 8259	Οργανωτικό πλαίσιο	Δραστηριότητες κατασκευαστή: secure development, vulnerability management, requirement setting	[25]

4.7 Εναρμόνιση Προτύπων και Ρυθμιστικών Πλαισίων (Harmonization)

4.7.1 Εναρμόνιση MDR – ISO 14971 – FDA – NISTIR 8259/8259A

Η εναρμόνιση των ρυθμιστικών πλαισίων MDR, ISO 14971, FDA και NISTIR 8259/8259A αναδεικνύει ένα σύνολο κοινών αρχών που διέπουν την ασφάλεια των IoMT συσκευών, παρά τις

διαφορές στο χαρακτήρα και τις απαιτήσεις των πλαισίων. Ο MDR (ΕΕ 2017/745), όπως παρουσιάζεται από τον Greser [20], θέτει ως υποχρεωτική προϋπόθεση τη συστηματική διαχείριση κινδύνου και την τεκμηριωμένη συμμόρφωση σε θέματα ασφάλειας λογισμικού και συνδεσιμότητας. Το ISO 14971, σύμφωνα με τους Yang [21] και Flood et al. [22], προσφέρει τη μεθοδολογική βάση για τη διαδικασία αυτή, ορίζοντας συγκεκριμένα βήματα αναγνώρισης, αξιολόγησης και ελέγχου κινδύνων σε όλο τον κύκλο ζωής της συσκευής.

Παράλληλα, οι οδηγίες του FDA για premarket και postmarket ασφάλεια [11] και τα ευρήματα της μελέτης Stern et al. [23] δείχνουν ότι η αμερικανική προσέγγιση εστιάζει στην τεχνική τεκμηρίωση των cybersecurity controls, όπως secure updates, authentication, logging και προστασία firmware. Αυτή η τεχνική προσέγγιση συμπληρώνεται από τα NISTIR 8259 και 8259A, τα οποία θέτουν ένα baseline τεχνικών ικανοτήτων (secure configuration, device identification, data protection, secure update mechanisms) και οργανωτικών δραστηριοτήτων για τους κατασκευαστές [25], [25a].

Όπως σημειώνουν οι Ostermann et al. [27], τα τέσσερα πλαίσια δεν λειτουργούν ανταγωνιστικά αλλά ευθυγραμμίζονται μέσα από κοινές αρχές, όπως:

- χρήση συστηματικής διαχείρισης κινδύνου,
- απαίτηση για τεχνικά μέτρα προστασίας της συσκευής,
- ανάγκη συνεχούς παρακολούθησης ευπαθειών,
- διασφάλιση της ποιότητας και της ασφάλειας σε όλο το lifecycle.

Έτσι, ο MDR απαιτεί τη χρήση μεθοδολογιών όπως το ISO 14971, το FDA παρέχει τεχνική καθοδήγηση σε alignment με τα NISTIR, ενώ τα NISTIR προσφέρουν το baseline που υποστηρίζει την τεχνική υλοποίηση των μέτρων. Το αποτέλεσμα είναι ένα συνεκτικό πλαίσιο που καλύπτει τόσο τη διαδικαστική/μεθοδολογική όσο και την τεχνική πλευρά της ασφάλειας IoMT συσκευών.

4.7.2 Κύκλος Ζωής IoMT Συσκευών και Εναρμόνιση Προτύπων

Η εναρμόνιση των MDR, ISO 14971, FDA και NISTIR 8259/8259A μπορεί να γίνει με βάση τις φάσεις του κύκλου ζωής μιας IoMT συσκευής. Οι φάσεις αυτές καλύπτουν το στάδιο σχεδιασμού, την ανάλυση κινδύνων, την premarket αξιολόγηση, τη λειτουργική υποστήριξη και τη μετα-κυκλοφοριακή επιτήρηση. Παρότι κάθε πλαίσιο έχει διαφορετικό ρόλο, οι πηγές μας αποδεικνύουν ότι υπάρχει σαφής αντιστοίχιση και συνέργεια.

1. Φάση 1: Σχεδιασμός και Ανάπτυξη (Design & Development)

Το στάδιο αυτό καλύπτεται από όλα τα βασικά πλαίσια, αλλά με διαφορετική έμφαση. Το ISO 14971, όπως περιγράφεται από Yang [21] και Flood et al. [22], αποτελεί τη βασική μεθοδολογία για την αναγνώριση και αξιολόγηση κινδύνων κατά τον σχεδιασμό μιας ιατρικής συσκευής. Το MDR, σύμφωνα με τον Greser [20], απαιτεί από τους κατασκευαστές την ενσωμάτωση διαδικασιών risk management και security-by-design ήδη από το στάδιο ανάπτυξης. Τα NISTIR 8259 και 8259A συμπληρώνουν αυτή τη διαδικασία προσδιορίζοντας συγκεκριμένες δραστηριότητες για τον κατασκευαστή, όπως την ανάλυση απαιτήσεων ασφάλειας, την ασφαλή ανάπτυξη και τη διασφάλιση της εφοδιαστικής αλυσίδας [25], καθώς και τεχνικές ικανότητες που πρέπει να ενσωματώνει η συσκευή, όπως secure configuration και device identification [25a]. Τέλος, το FDA απαιτεί τεκμηριωμένο Secure Product Development Framework (SPDF), που περιλαμβάνει code review, static και dynamic analysis και διαδικασίες ασφαλούς ανάπτυξης [11].

2. Φάση 2: Ανάλυση και Διαχείριση Κινδύνων

Η φάση αυτή αποτελεί τον πυρήνα των MDR και ISO 14971. Ο MDR θέτει τη διαχείριση κινδύνου ως νομικά δεσμευτική διαδικασία, που καλύπτει όλους τους κινδύνους που συνδέονται με το λογισμικό και τη συνδεσιμότητα της συσκευής [20]. Το ISO 14971 προσφέρει τη συστηματική μεθοδολογία για την υλοποίηση αυτών των απαιτήσεων μέσω risk assessment, risk control και αξιολόγησης υπολειπόμενου κινδύνου [21], [22]. Παράλληλα, το FDA απαιτεί κατά την premarket

διαδικασία την εφαρμογή threat modeling, attack surface analysis και ανάλυσης κινδύνου με τεχνικούς όρους [11]. Το NISTIR 8259A συνδέεται με αυτή τη φάση προσδιορίζοντας τεχνικές ικανότητες όπως access control και data protection, οι οποίες αποτελούν μέτρα αντιμετώπισης κινδύνων που αναγνωρίζονται από ISO και MDR [25a].

3. Φάση 3: Premarket Αξιολόγηση και Έγκριση

Η premarket αξιολόγηση αποτελεί το πεδίο όπου το FDA έχει το πιο αναλυτικό πλαίσιο. Σύμφωνα με τις οδηγίες του FDA [11], ο κατασκευαστής οφείλει να παρουσιάσει πλήρη τεχνική τεκμηρίωση, όπως μηχανισμούς αυθεντικοποίησης, προστασία ακεραιότητας firmware, καταγραφή συμβάντων και δυνατότητα ασφαλών ενημερώσεων. Η μελέτη Stern et al. [23] καταδεικνύει ότι αυτά τα στοιχεία αποτυπώνονται στα FDA product summaries. Το MDR λειτουργεί συμπληρωματικά ως ευρωπαϊκό ρυθμιστικό πλαίσιο, απαιτώντας την ύπαρξη ολοκληρωμένου τεχνικού φακέλου και risk management documentation [20]. Η συμβολή του ISO 14971 στο στάδιο αυτό είναι η παροχή της μεθοδολογικής βάσης για την αξιολόγηση κινδύνων, ενώ το NISTIR 8259A μπορεί να χρησιμοποιηθεί ως τεκμηρίωση ότι η συσκευή ενσωματώνει ελάχιστες τεχνικές ικανότητες ασφάλειας [25a].

4. Φάση 4: Λειτουργική Ασφάλεια και Υποστήριξη (Operational Security)

Κατά τη φάση της λειτουργικής χρήσης, οι απαιτήσεις επικεντρώνονται στην προστασία των δεδομένων, την ασφαλή διαμόρφωση της συσκευής και την παρακολούθηση της κατάστασης ασφάλειας. Το NISTIR 8259A περιγράφει λειτουργίες όπως cybersecurity state awareness και secure updates [25a], οι οποίες αποτελούν βασικές απαιτήσεις για συνεχή προστασία. Το FDA Postmarket Guidance [11] απαιτεί συνεχή παρακολούθηση ευπαθειών, μηχανισμούς αναφοράς συμβάντων και ταχεία διόρθωση προβλημάτων. Το ISO 14971 και το MDR υποστηρίζουν αυτή τη φάση μέσω της ανάγκης συλλογής πραγματικών δεδομένων χρήσης και επιτήρησης κινδύνων [20], [22].

5. Φάση 5: Post-Market Surveillance και Continuous Monitoring

Το MDR απαιτεί από τον κατασκευαστή ένα πλήρως τεκμηριωμένο σύστημα post-market surveillance, vigilance reporting και αξιολόγηση ασφάλειας σε πραγματικές συνθήκες, καθ’ όλη τη διάρκεια ζωής της συσκευής [20]. Το FDA επιβάλλει την ύπαρξη διαδικασιών continuous vulnerability monitoring και root cause analysis για συμβάντα κυβερνοασφάλειας [11]. Το NISTIR 8259 περιγράφει ανάλογες οργανωτικές δραστηριότητες, όπως systematic remediation και vulnerability handling [25]. Το ISO 14971 συμπληρώνει αυτή τη φάση με τη διαδικασία αναθεώρησης κινδύνων βάσει νέων πληροφοριών [22].

6. Φάση 6: Απόσυρση / Τέλος Ζωής

Αν και τα εξεταζόμενα πλαίσια δεν παρέχουν λεπτομερή τεχνική καθοδήγηση για τη φάση απόσυρσης, η αντιμετώπιση της περίοδου τέλους ζωής μπορεί να τεκμηριωθεί μέσω των πηγών μας. Το ISO 14971 καλύπτει όλον τον κύκλο ζωής της συσκευής, συμπεριλαμβανομένων των σταδίων παύσης χρήσης [21], [22], [24]. Το NISTIR 8259A επισημαίνει ότι οι τεχνικές ικανότητες ασφαλείας ισχύουν όσο η συσκευή υποστηρίζεται από τον κατασκευαστή [25a], ενώ το NISTIR 8259 περιλαμβάνει δραστηριότητες continuous vulnerability management μέχρι την παύση υποστήριξης [25]. Το FDA και ο MDR δεν περιγράφουν διαδικασίες απόσυρσης, αλλά απαιτούν συνεχή ασφάλεια για όσο η συσκευή βρίσκεται σε κυκλοφορία [11], [20]. Συνεπώς, το τέλος ζωής αποτελεί το σημείο όπου ολοκληρώνονται οι υποχρεώσεις ασφαλείας, χωρίς όμως να παρέχεται εξειδικευμένη διαδικασία.

4.7.3 Πίνακας Εναρμόνισης

Πίνακας 5.2 : Εναρμόνιση των MDR, ISO 14971, FDA και NISTIR 8259/8259A στον κύκλο ζωής των IoMT συσκευών.

Φάση Κύκλου Ζωής	***MDR (ΕΕ 2017/745)***	***ISO 14971***	***FDA Premarket / Postmarket***	***NISTIR 8259 / 8259A***
1. Σχεδιασμός & Ανάπτυξη	*Απαιτεί security-by-design, risk management από το στάδιο ανάπτυξης [20]*	*Structured risk management από το design stage [21], [22]*	*Secure Product Development Framework (SPDF), secure design, code review [11]*	*Foundational activities: requirement setting, secure development [25] & security capabilities όπως device ID, secure configuration [25a]*
2. Ανάλυση & Διαχείριση Κινδύνων	*Υποχρεωτική, πλήρης τεκμηρίωση κινδύνων (συμπεριλαμβανομένων cyber-risks) [20]*	*Βάση μεθοδολογίας risk assessment & residual risk evaluation [21], [22], [24]*	*Threat modeling, attack surface analysis, risk documentation [11]*	*Capabilities όπως data protection, access control ως μέτρα risk mitigation [25a]*
3. Premarket Αξιολόγηση	*Τεχνικός φάκελος συμμόρφωσης & risk documentation [20]*	*Απόδειξη ορθής ανάλυσης κινδύνου [22]*	*Authentication, encryption, logging, firmware integrity, secure updates (τεχνικά controls) [11], [23]*	*Χρησιμοποιείται για τεκμηρίωση ότι η συσκευή διαθέτει minimum capabilities [25a]*
4. Λειτουργική Ασφάλεια	*Απαιτεί λειτουργική ασφάλεια και συνεχή συμμόρφωση [20]*	*Επανεκτίμηση κινδύνων βάσει πραγματικής χρήσης [22], [24]*	*Postmarket monitoring, vulnerability handling, rapid patching [11]*	*Cybersecurity state awareness, secure updates [25a]*
5. Post-Market Surveillance	*Υποχρεωτικό σύστημα PMS & vigilance [20]*	*Παρακολούθηση κινδύνων και αναθεώρηση ανάλυσης [22]*	*Incident reporting, vulnerability monitoring, RCA [11]*	*Οργανωτικές δραστηριότητες για vulnerability management [25]*
6. Απόσυρση / Τέλος Ζωής	*Υποχρεώσεις ισχύουν όσο η συσκευή κυκλοφορεί & υποστηρίζεται [20]*	*Risk management καλύπτει όλο το lifecycle, περιλαμβάνει την παύση χρήσης [21], [22], [24]*	*Υποχρεώσεις ασφάλειας μέχρι το τέλος υποστήριξης [11]*	*Απαιτήσεις ασφάλειας ισχύουν όσο η συσκευή υποστηρίζεται [25], [25a]*

4.8 Συμπεράσματα

Η συνδυαστική ανάλυση των MDR, ISO 14971, FDA Premarket/Postmarket Guidelines και NISTIR 8259/8259A δείχνει ότι τα εξεταζόμενα πλαίσια, παρά τις ουσιαστικές διαφορές στη δομή και τη φιλοσοφία τους, συγκλίνουν προς έναν κοινό στόχο: τη διασφάλιση της ασφάλειας των IoMT συσκευών

σε όλο τον κύκλο ζωής τους. Ο MDR λειτουργεί ως το κεντρικό ρυθμιστικό πλαίσιο της Ευρωπαϊκής Ένωσης, επιβάλλοντας υποχρεωτική τεκμηρίωση κινδύνων και ολοκληρωμένο σύστημα ασφάλειας από το στάδιο σχεδιασμού έως και τη μετα-κυκλοφοριακή επιτήρηση [20]. Το ISO 14971, σύμφωνα με τους Yang [21] και Flood et al. [22], παρέχει τη μεθοδολογική βάση για την εφαρμογή αυτής της προσέγγισης, προσφέροντας μια πλήρως δομημένη διαδικασία αναγνώρισης, αξιολόγησης και ελέγχου κινδύνων.

Οι οδηγίες του FDA, όπως παρουσιάζονται στα premarket και postmarket έγγραφα [11] και στη μελέτη Stern et al. [23], έχουν περισσότερο τεχνικό προσανατολισμό και παρέχουν λεπτομερείς απαιτήσεις που αφορούν μηχανισμούς αυθεντικοποίησης, ασφαλείς ενημερώσεις, καταγραφή συμβάντων και προστασία firmware. Τα NISTIR 8259 και 8259A συμπληρώνουν αυτή την προσέγγιση προσδιορίζοντας το απαιτούμενο baseline τεχνικών ικανοτήτων και δραστηριοτήτων ασφάλειας για συσκευές IoT/IoMT [25], [25a].

Η εναρμόνιση των παραπάνω πλαισίων δείχνει ότι η ασφάλεια IoMT συσκευών δεν βασίζεται σε ένα μόνο πρότυπο, αλλά στην αλληλοσυμπλήρωση πολλών πηγών που καλύπτουν τόσο τα ρυθμιστικά όσο και τα τεχνικά και μεθοδολογικά επίπεδα. Η χαρτογράφηση στον κύκλο ζωής της συσκευής αποδεικνύει ότι κάθε πλαίσιο καλύπτει διαφορετική φάση, ενώ η αλληλεπικάλυψη των απαιτήσεων δημιουργεί ένα συνεκτικό, πολυεπίπεδο σύστημα προστασίας. Έτσι, το συνδυασμένο πλαίσιο MDR–ISO–FDA–NISTIR παρέχει μια πλήρη και αξιόπιστη βάση για την ανάπτυξη, αξιολόγηση και λειτουργική ασφάλεια των IoMT συστημάτων, διαμορφώνοντας τα θεμέλια για το επόμενο κεφάλαιο που αφορά τη λειτουργική αξιολόγηση και τις επιπτώσεις των ευπαθειών στην πράξη.

Κεφάλαιο 5ο: Αξιολόγηση Ευπαθειών και Επιπτώσεων σε IoMT Συσκευές

5.1 Εισαγωγή

Η κυβερνοασφάλεια των IoMT συσκευών αποτελεί έναν από τους πιο κρίσιμους τομείς για την ασφαλή λειτουργία των σύγχρονων συστημάτων υγειονομικής περίθαλψης. Οι IoMT συσκευές, όπως οι φορητές συσκευές παρακολούθησης υγείας, οι ιατρικοί αισθητήρες και τα ιατρικά συστήματα, είναι εκτεθειμένες σε πολλές ευπάθειες, οι οποίες ενδέχεται να οδηγήσουν σε σοβαρές συνέπειες για την ασφάλεια των ασθενών και τη λειτουργία των νοσοκομείων. Οι ευπάθειες αυτές προέρχονται από την ασφάλεια του hardware και software των συσκευών, καθώς και από την ασφάλεια των πληροφοριών που διακινούνται μέσω αυτών των συσκευών [20][21].

Η σκιαγράφηση αυτής της μελέτης είναι να αναλύσει τις βασικές ευπάθειες των IoMT συσκευών, καθώς και τις επιπτώσεις από επιθέσεις στην λειτουργία τους και στην εμπιστευτικότητα των ιατρικών δεδομένων [22]. Εξετάζοντας τις στρατηγικές και λύσεις που μπορούν να μειώσουν ή να εξαλείψουν αυτούς τους κινδύνους, η ανάπτυξη κατάλληλων στρατηγικών ασφαλείας θα πρέπει να στηρίζεται στις κατευθυντήριες γραμμές των κανονιστικών πλαισίων, όπως το MDR, το ISO 14971 και το FDA [25].

5.2 Κατηγορίες Ευπαθειών σε IoMT Συσκευές

Οι βασικές κατηγορίες ευπαθειών εντοπίζονται στο hardware, το λογισμικό, την ασφάλεια δεδομένων και την εφοδιαστική αλυσίδα. Οι συσκευές IoMT είναι ιδιαίτερα ευάλωτες σε επιθέσεις όπως malware, phishing και ransomware, αλλά και σε τεχνικές που στοχεύουν στην διαρροή δεδομένων και στην εκμετάλλευση ευπαθειών του hardware και software τους [22], [25].

5.2.1 Ευπάθειες σε Firmware και Hardware

Σύμφωνα με τη μελέτη του Stern et al. [23], οι ευπάθειες σε firmware και hardware είναι από τις πιο κρίσιμες στην ασφάλεια των IoMT συσκευών. Αυτές οι συσκευές συχνά ενσωματώνουν default passwords, αδύναμος μηχανισμός authentication ή ακόμα και ανοιχτούς ports, που μπορούν να εκμεταλλευτούν κακόβουλοι επιτιθέμενοι. Επιπλέον, οι ευπάθειες στο firmware και η ανεπάρκεια προστασίας των συνηθισμένων λογισμικών επιτρέπουν στους επιτιθέμενους να τροποποιούν ή να εισάγουν κακόβουλο κώδικα, ενισχύοντας τις επιθέσεις ransomware και άλλες επιθέσεις διακοπής υπηρεσιών [23], [26].

5.2.2 Ευπάθειες στο Λογισμικό και στη Συνδεσιμότητα

Οι IoMT συσκευές συνδέονται σε δίκτυα, γεγονός που τις καθιστά ευάλωτες σε επιθέσεις στο λογισμικό και τις συνδεδεμένες υποδομές. Σύμφωνα με την ENISA [12], οι απειλές αυτές περιλαμβάνουν επιθέσεις μέσω κρυπτογραφημένων καναλιών επικοινωνίας και τη χρήση ασθενών μηχανισμών authentication. Η ασφάλεια δικτύου, η έλλειψη ισχυρών ελέγχων πρόσβασης και η αστοχία στις διαδικασίες αυθεντικοποίησης χρηστών και συσκευών αποτελούν βασικές ευπάθειες που μπορεί να οδηγήσουν σε παραβίαση των δεδομένων υγείας των ασθενών ή σε τροποποίηση των ιατρικών αποτελεσμάτων [12]..

5.2.3 Ευπάθειες στην Ασφάλεια Δεδομένων

Η ασφάλεια δεδομένων αποτελεί κεντρικό θέμα για την προστασία των IoMT συσκευών. Σύμφωνα με τον Rasool et al. [7], οι IoMT συσκευές συνήθως μεταφέρουν ευαίσθητα ιατρικά δεδομένα (π.χ. ιστορικό ασθενών, καρδιογράφημα, δεδομένα από αισθητήρες). Οι ευπάθειες σε αυτόν τον τομέα περιλαμβάνουν data leakage, μη προστατευμένα δεδομένα κατά τη μεταφορά και μη επαρκή μέτρα

προστασίας ακρίβειας. Οποιεσδήποτε από αυτές τις ευπάθειες μπορεί να οδηγήσουν σε σοβαρή παραβίαση απορρήτου και εμπιστευτικότητας, κάτι που είναι εξαιρετικά επικίνδυνο στον τομέα της υγειονομικής περίθαλψης [7].

5.2.4 Ευπάθειες στην Ασφάλεια Εφοδιαστικής Αλυσίδας (Supply Chain)

Στην περίπτωση των IoMT συσκευών, οι επιθέσεις μπορούν να προκύψουν και από την εφοδιαστική αλυσίδα, δηλαδή από τις τρίτες εταιρείες που παρέχουν εξαρτήματα ή λογισμικό. Το FDA [11] αναφέρει ότι οι επιθέσεις supply chain είναι ιδιαίτερα επικίνδυνες επειδή η συσκευή μπορεί να παραβιαστεί κατά τη διάρκεια της παραγωγής ή της αναβάθμισης λογισμικού χωρίς να το γνωρίζει ο τελικός χρήστης. Οι επιθέσεις μέσω εφοδιαστικής αλυσίδας χρησιμοποιούν αδύναμα σημεία στις διαδικασίες ανάπτυξης και ενημέρωσης του λογισμικού για να επηρεάσουν τις IoMT συσκευές [11].

5.3 Επιπτώσεις Επιθέσεων σε IoMT Περιβάλλοντα

Η κυβερνοασφάλεια των IoMT συσκευών δεν περιορίζεται μόνο στη διασφάλιση της ακεραιότητας και της προστασίας των δεδομένων, αλλά επεκτείνεται και στην επίδραση που μπορεί να έχει η παραβίαση αυτών των συσκευών στην υγειονομική περιθαλψή και την ασφάλεια των ασθενών. Οι επιθέσεις σε IoMT συσκευές μπορούν να οδηγήσουν σε σοβαρές συνέπειες που επηρεάζουν τόσο τη λειτουργία των ιατρικών συστημάτων όσο και την υγεία των ασθενών. Ανάλογα με το είδος της επίθεσης, οι συνέπειες διαφέρουν, αλλά συνήθως περιλαμβάνουν διαταραχή της διαθεσιμότητας υπηρεσιών, παραβίαση της εμπιστευτικότητας των ιατρικών δεδομένων και εκτροπή των ιατρικών συσκευών από τους προκαθορισμένους τους ρόλους.

Η ENISA [12] υπογραμμίζει ότι οι επιθέσεις data leakage και ransomware είναι οι πιο συχνές επιθέσεις που επηρεάζουν τα IoMT περιβάλλοντα, καθώς παραβιάζουν την ασφάλεια των δεδομένων και την ασφάλεια επικοινωνίας. Επίσης, η ενημέρωση λογισμικού και η κακή διαχείριση των ενημερώσεων λογισμικού είναι κύρια σημεία ευπάθειας για τις IoMT συσκευές, κάτι που αναφέρουν και οι Rasool et al. [7] και Flood et al. [25], που αναλύουν τον κίνδυνο από κακόβουλο λογισμικό που έχει σαν στόχο να παραβιάσει την ασφάλεια των συσκευών.

Οι Tariq et al. [3] και Greser [20] αναφέρουν ότι οι επιθέσεις ransomware μπορούν να επηρεάσουν όχι μόνο την προστασία των δεδομένων αλλά και την λειτουργία των συσκευών σε επίπεδο διασύνδεσης και ιατρικών υπηρεσιών, γεγονός που θέτει σε κίνδυνο την υγειονομική περίθαλψη των ασθενών.

5.3.1 Κλινικές Επιπτώσεις (Patient Safety)

Η ασφάλεια των ασθενών είναι το πιο κρίσιμο ζήτημα όταν συζητάμε για τις συνέπειες των επιθέσεων στις IoMT συσκευές. Όπως αναφέρεται στη μελέτη του Rasool et al. [7], η παραβίαση ή η κακή διαχείριση των δεδομένων που συλλέγονται από αυτές τις συσκευές μπορεί να οδηγήσει σε λάθος διάγνωση ή ανακριβείς θεραπείες. Ειδικότερα:

- Λάθος δεδομένα που αποστέλλονται στον ιατρό μπορούν να οδηγήσουν σε λάθος θεραπεία ή διάγνωση. Για παράδειγμα, αν τα δεδομένα από έναν αισθητήρα καρδιογράφημα (ECG) παραποιηθούν, μπορεί να προκαλέσουν σοβαρά σφάλματα στις αποφάσεις του γιατρού.
- Αλλοίωση δεδομένων σχετικά με ζωτικά σημεία, όπως καρδιολογικά δεδομένα, μπορεί να οδηγήσει σε επικίνδυνες κλινικές αποφάσεις. Η μελέτη Stern et al. [23] υπογραμμίζει ότι η παραβίαση της ακεραιότητας των δεδομένων από IoMT συσκευές μπορεί να έχει άμεσο αντίκτυπο στην υγεία του ασθενούς.

Αυτές οι παραβιάσεις θέτουν σε κίνδυνο όχι μόνο την εμπιστοσύνη του ασθενή στο ιατρικό σύστημα, αλλά και την ασφάλεια της διαδικασίας θεραπείας.

5.3.2 Επιπτώσεις σε Διαθεσιμότητα Υπηρεσιών

Οι επιθέσεις ransomware και DDoS είναι από τις πιο συχνές επιθέσεις που επηρεάζουν την διαθεσιμότητα των IoMT συσκευών και, κατά συνέπεια, την διαθεσιμότητα των υπηρεσιών υγειονομικής περίθαλψης. Όπως σημειώνεται στην αναφορά της ENISA [12], οι επιθέσεις αυτές είναι σε μεγάλο βαθμό υπεύθυνες για την διακοπή της παροχής υπηρεσιών σε νοσοκομεία και ιατρικές μονάδες, ειδικά όταν οι επιτιθέμενοι στοχεύουν σε κρίσιμα ιατρικά συστήματα που σχετίζονται με τις IoMT συσκευές.

Οι ransomware επιθέσεις μπορούν να προκαλέσουν πλήρη διακοπή των IoMT συσκευών, κρυπτογραφώντας τα δεδομένα και αδρανοποιώντας τη λειτουργία τους, με συνέπεια την αναστολή της παρακολούθησης ασθενών και την αδυναμία προσβασιμότητας των δεδομένων τους για τους ιατρούς. Αυτού του είδους οι επιθέσεις καθιστούν τις υπηρεσίες μη διαθέσιμες για ώρες ή και μέρες, γεγονός που θέτει σε κίνδυνο τις ζωές των ασθενών [12].

Επιπλέον, οι DDoS επιθέσεις μπορεί να αποσκοπούν στην υπερφόρτωση των διακομιστών που διαχειρίζονται τις IoMT συσκευές ή το σύστημα του νοσοκομείου, προκαλώντας διάρρηξη της σύνδεσης και αποκοπή από τα δεδομένα ή τις ιατρικές συσκευές.

5.3.3 Επιπτώσεις στην Εμπιστευτικότητα και Ακεραιότητα Δεδομένων

Η παραβίαση της εμπιστευτικότητας των ιατρικών δεδομένων είναι μία από τις μεγαλύτερες ανησυχίες σε IoMT συσκευές. Όπως αναφέρεται από τη μελέτη Williams & Woodward [26], οι επιθέσεις αυτές ενδέχεται να οδηγήσουν σε data breaches, που θέτουν σε κίνδυνο την εμπιστευτικότητα των προσωπικών και ιατρικών δεδομένων. Η κλοπή ή η παραποίηση προσωπικών δεδομένων μπορεί να οδηγήσει σε παραβίαση απορρήτου, με συνέπειες τόσο για τους ασθενείς όσο και για το ιατρικό προσωπικό που χειρίζεται τα δεδομένα τους. Παράλληλα, η απώλεια της ακεραιότητας των δεδομένων μπορεί να αποδομήσει την αξία των ιατρικών εγγράφων και να αλλοιώσει τη θεραπευτική διαδικασία.

5.3.4 Επιπτώσεις σε Κανονιστική Συμμόρφωση (Regulatory Compliance)

Η παραβίαση των κανονιστικών απαιτήσεων, όπως το MDR και το FDA, είναι επίσης κρίσιμη συνέπεια της παραβίασης IoMT συσκευών. Οι ευπάθειες στις συσκευές που οδηγούν σε παραβίαση της προστασίας δεδομένων ή άλλων στοιχείων της ασφάλειας ενδέχεται να προκαλέσουν νομικές συνέπειες για τον κατασκευαστή και τον φορέα παροχής υπηρεσιών υγειονομικής περίθαλψης. Όπως αναφέρει ο Greser [20], οι κατασκευαστές ιατρικών συσκευών οφείλουν να συμμορφώνονται με τους κανονισμούς ασφαλείας των ΗΠΑ και της ΕΕ, όπως το HIPAA και το GDPR, οι οποίοι επιβάλλουν αυστηρές ποινές σε περίπτωση παραβίασης των δεδομένων των ασθενών.

5.4 Σύνδεση Ευρημάτων με Πρότυπα

Η παρούσα υποενότητα στοχεύει στη σύνδεση των ευρημάτων που παρουσιάστηκαν στα προηγούμενα τμήματα με τα υφιστάμενα ρυθμιστικά πλαίσια και πρότυπα κυβερνοασφάλειας, αναδεικνύοντας τη σημασία τους για την πρακτική εφαρμογή της ασφάλειας στις IoMT συσκευές.

5.4.1 Σύνδεση με το MDR (EU 2017/745)

Το MDR απαιτεί από τους κατασκευαστές να εφαρμόζουν διαδικασίες διαχείρισης κινδύνου καθ’ όλη τη διάρκεια ζωής των συσκευών, όπως περιγράφεται στο άρθρο 10 του κανονισμού [20]. Οι ευπάθειες που εντοπίστηκαν από την ENISA [12] και τους Stern et al. [23], όπως η ανεπαρκής προστασία δεδομένων ή οι αδύναμοι μηχανισμοί αυθεντικοποίησης, ευθυγραμμίζονται με τις απαιτήσεις του MDR για συνεχή διαχείριση κινδύνων και ασφάλεια λογισμικού.

Συγκεκριμένα, η παραβίαση της εμπιστευτικότητας δεδομένων (π.χ. παραβιάσεις του IoMT) αντιτίθεται στην απαίτηση του MDR για τη διασφάλιση της προστασίας δεδομένων των ασθενών και την προστασία από μη εξουσιοδοτημένη πρόσβαση.

5.4.2 Σύνδεση με το ISO 14971

Το πρότυπο ISO 14971 παρέχει μια συστηματική μεθοδολογία για την ανάλυση και τη διαχείριση κινδύνων σε ιατροτεχνολογικά προϊόντα, καλύπτοντας τα ζητήματα ασφάλειας των συσκευών IoMT σε όλα τα στάδια του κύκλου ζωής τους. Τα τεχνικά ευρήματα που έχουν καταγραφεί στη βιβλιογραφία σχετικά με ευπάθειες και απειλές στο IoMT, όπως αυτά που παρουσιάζονται από τους Rasool et al. [7], μπορούν να ενταχθούν στο πλαίσιο του ISO 14971 μέσω διαδικασιών αναγνώρισης, αξιολόγησης και μετριασμού κινδύνων, όπως περιγράφεται στις μελέτες των Yang [21] και Flood et al. [22].

Επιπλέον, το ISO 14971 δίνει έμφαση στη συνεχή αναθεώρηση των κινδύνων και στη μεταγενέστερη παρακολούθηση (postmarket surveillance), διαδικασίες που θεωρούνται κρίσιμες για την έγκαιρη ανίχνευση νέων ευπαθειών μετά την κυκλοφορία των συσκευών, όπως καταδεικνύεται και από την ανάλυση των Stern et al. [23].

5.4.3 Σύνδεση με τις Οδηγίες του FDA

Οι οδηγίες του FDA για την ασφάλεια των ιατρικών συσκευών, τόσο κατά την προαξιολόγηση (premarket) όσο και μετά την κυκλοφορία (postmarket), απαιτούν τη διαχείριση ευπαθειών και τη συνεχιζόμενη επιτήρηση των IoMT συσκευών για την πρόληψη επιθέσεων. Οι ευπάθειες που περιγράφονται στην αναφορά της ENISA [12] και τις Stern et al. [23], όπως η ανεπαρκής ασφάλεια στον έλεγχο πρόσβασης και η κακή διαχείριση λογισμικού, συνάδουν με τις κατευθυντήριες οδηγίες του FDA για την ασφάλεια λογισμικού και την παρακολούθηση ευπαθειών στο postmarket [11].

Το FDA υπογραμμίζει τη σημασία της γρήγορης διόρθωσης (rapid patching) και της ασφαλούς ενημέρωσης συσκευών για την αποτροπή επιθέσεων, κάτι που αναφέρεται επίσης στην έρευνα των Stern et al. [23].

5.4.4 Σύνδεση με το NISTIR 8259/8259A

Τα έγγραφα NISTIR 8259 και NISTIR 8259A περιγράφουν ένα σύνολο πρακτικών και τεχνικών ικανοτήτων που πρέπει να ενσωματώνουν οι IoMT συσκευές για να ανταποκριθούν στις απαιτήσεις ασφάλειας. Σύμφωνα με την μελέτη του NIST [25], οι IoMT συσκευές πρέπει να διαθέτουν χαρακτηριστικά ασφάλειας όπως η ταυτοποίηση συσκευής, η ασφαλής διαμόρφωση και η διαχείριση ευπαθειών για να παραμείνουν ασφαλείς καθ' όλη τη διάρκεια ζωής τους.

Οι ευπάθειες που εντοπίστηκαν, όπως η ανεπαρκής προστασία του firmware και η ανάγκη για ασφαλείς ενημερώσεις λογισμικού, σχετίζονται άμεσα με τις ικανότητες που απαιτούνται από τα NISTIR 8259A για την ασφαλή διαμόρφωση και ασφαλείς ενημερώσεις [25a].

Η συσχέτιση των ευρημάτων από τις πηγές μας με τα πρότυπα MDR, ISO 14971, FDA και NISTIR 8259/8259A υπογραμμίζει ότι, παρόλο που τα πλαίσια αυτά επικεντρώνονται σε διαφορετικά επίπεδα (ρυθμιστικό, μεθοδολογικό, τεχνικό), όλα επισημαίνουν τη σημασία της συνεχούς διαχείρισης κινδύνων και ευπαθειών κατά τον κύκλο ζωής της συσκευής. Ο συνδυασμός των απαιτήσεων αυτών προσφέρει μια ισχυρή βάση για την ανάπτυξη, λειτουργία και υποστήριξη ασφαλών IoMT συσκευών.

5.5 Συμπεράσματα Κεφαλαίου

Η εξέταση των ευπαθειών και των επιπτώσεων των IoMT συσκευών αναδεικνύει τις σημαντικές προκλήσεις που αντιμετωπίζουν οι κατασκευαστές και οι φορείς υγειονομικής περίθαλψης. Οι

επιθέσεις σε αυτές τις συσκευές, όπως οι επιθέσεις ransomware, data breaches και διακοπές υπηρεσιών, ενδέχεται να έχουν σοβαρές συνέπειες για τη διασφάλιση των δεδομένων των ασθενών και τη λειτουργία των ιατρικών συστημάτων. Οι ευπάθειες που εντοπίστηκαν, όπως οι αδύναμοι μηχανισμοί αυθεντικοποίησης, η ανεπαρκής προστασία δεδομένων και η έλλειψη ασφαλών ενημερώσεων λογισμικού, απαιτούν άμεσες στρατηγικές για την αντιμετώπιση και τη μείωση των κινδύνων.

Η σύνδεση των ευρημάτων με τα ρυθμιστικά πρότυπα (MDR, ISO 14971, FDA, NISTIR) καταδεικνύει ότι οι υποχρεώσεις ασφαλείας για τις IoMT συσκευές επεκτείνονται σε όλο τον κύκλο ζωής τους, από το σχεδιασμό μέχρι την παρακολούθηση μετά την κυκλοφορία. Η εναρμόνιση των απαιτήσεων αυτών προσφέρει ένα συνεκτικό και πολυεπίπεδο πλαίσιο για την ασφάλεια των συσκευών IoMT, που βασίζεται σε τεχνικά μέτρα, διαδικασίες διαχείρισης κινδύνων και συνεχή παρακολούθηση ευπαθειών.

Η αναγνώριση αυτών των ευπαθειών και επιπτώσεων και η ενσωμάτωσή τους στο συνολικό πλαίσιο ασφάλειας προσφέρει τη δυνατότητα για βελτίωση των πρακτικών ασφάλειας και τη μείωση των κινδύνων στην ιατρική τεχνολογία. Η επόμενη ενότητα θα επικεντρωθεί στην πρακτική εφαρμογή αυτών των θεωρητικών ευρημάτων, με τη χρήση του Simul8 για την προσομοίωση επιθέσεων και την αξιολόγηση της ασφάλειας των IoMT συσκευών.

Κεφάλαιο 6ο: Μελέτη Περίπτωσης και Προσομοίωση Συστήματος Ανίχνευσης Εισβολών (IDS) στο IoMT

6.1 Εισαγωγή

Το παρόν κεφάλαιο αποτελεί το εφαρμοσμένο μέρος της διπλωματικής εργασίας και αποσκοπεί στη σύνδεση της θεωρητικής ανάλυσης των προηγούμενων κεφαλαίων με την πρακτική αξιολόγηση της κυβερνοασφάλειας σε συστήματα Internet of Medical Things (IoMT). Αρχικά παρουσιάζεται βιβλιογραφική μελέτη περίπτωσης, στην οποία αναλύονται χαρακτηριστικές ευπάθειες και μηχανισμοί αντιμετώπισης που έχουν εντοπιστεί σε φορετές και ψηφιακές ιατρικές συσκευές. Στη συνέχεια, τα θεωρητικά ευρήματα διερευνώνται πρακτικά μέσω προσομοίωσης σε ελεγχόμενο περιβάλλον, με στόχο την κατανόηση της συμπεριφοράς του συστήματος υπό συνθήκες κανονικής λειτουργίας και κακόβουλης αλλοίωσης δεδομένων. Η προσομοίωση δεν στοχεύει στην αναπαράσταση συγκεκριμένης φυσικής IoMT συσκευής, αλλά στην αποτύπωση της λειτουργικής και πληροφοριακής ροής ενός τυπικού συστήματος IoMT, επιτρέποντας την ανάλυση επιθέσεων και μηχανισμών ανίχνευσης σε επίπεδο συστήματος.

6.2 Πρότυπα Συμμόρφωσης και Εφαρμογή Ασφάλειας στο IoMT

Στο τρίτο κεφάλαιο παρουσιάστηκαν τα βασικά διεθνή πρότυπα και τεχνολογίες ασφάλειας που πλαισιώνουν την κυβερνοασφάλεια στο οικοσύστημα του Internet of Medical Things (IoMT). Το παρόν κεφάλαιο εστιάζει στη διάσταση της συμμόρφωσης (compliance) και στη μετάφραση των προτύπων σε πρακτικές απαιτήσεις για φορετές και δικτυωμένες ιατρικές συσκευές. Ειδικότερα, εξετάζονται το κανονιστικό πλαίσιο της Ευρωπαϊκής Ένωσης για ιατρικές συσκευές (Regulation (EU) 2017/745 – MDR), το πρότυπο ISO 14971 για τη διαχείριση κινδύνου, οι κατευθυντήριες οδηγίες της FDA για την κυβερνοασφάλεια και το πλαίσιο NISTIR 8259/8259A για τις δυνατότητες ασφάλειας των IoT/IoMT συσκευών [20]–[23], [25].

Στόχος της παρούσας ενότητας είναι να αναδείξει πώς οι ρυθμιστικές απαιτήσεις και τα πρότυπα καθορίζουν συγκεκριμένες υποχρεώσεις για τους κατασκευαστές, τους παρόχους υπηρεσιών υγείας και τους φορείς που διαχειρίζονται IoMT υποδομές. Παράλληλα, αναλύεται το πώς τα πλαίσια αυτά συνδέονται με τις κατηγορίες απειλών και την πολυπλοκότητα που παρουσιάστηκαν στα Κεφάλαια 2 και 3, καθώς και το πώς μπορούν να αξιοποιηθούν για την οργάνωση μιας συστηματικής προσέγγισης κυβερνοασφάλειας σε φορετές ιατρικές συσκευές.

6.3 Πρότυπα Συμμόρφωσης για Ιατρικές Συσκευές και IoMT

6.3.1 Κανονιστικό Πλαίσιο Regulation (EU) 2017/745 (MDR)

Ο Κανονισμός (ΕΕ) 2017/745 για τα ιατροτεχνολογικά προϊόντα (Medical Device Regulation – MDR) αποτελεί το βασικό κανονιστικό πλαίσιο της Ευρωπαϊκής Ένωσης για την κυκλοφορία και χρήση ιατρικών συσκευών στην ενιαία αγορά. Σε αντίθεση με την προηγούμενη οδηγία, ο MDR εισάγει αυστηρότερες απαιτήσεις όσον αφορά την ασφάλεια, την απόδοση και την εποπτεία καθ’ όλη τη διάρκεια ζωής των συσκευών, συμπεριλαμβανομένων και των πτυχών που σχετίζονται με την κυβερνοασφάλεια και τη διασύνδεση σε δίκτυα [20].

Όπως αναλύει ο Greser [20], ο MDR εντάσσει την κυβερνοασφάλεια στο πλαίσιο της συνολικής διαχείρισης κινδύνων, όχι ως ξεχωριστό τεχνικό ζήτημα, αλλά ως αναπόσπαστο μέρος της συνολικής ασφάλειας και απόδοσης του ιατροτεχνολογικού προϊόντος. Στο Παράρτημα I (Annex I – General Safety and Performance Requirements) τίθενται απαιτήσεις που σχετίζονται με τη διαχείριση

κινδύνου, την προστασία από μη εξουσιοδοτημένη πρόσβαση, την εξασφάλιση της ακεραιότητας των δεδομένων και την πρόληψη βλαβών που μπορεί να προκύψουν από σφάλματα λογισμικού ή κακόβουλες παρεμβολές. Ο κατασκευαστής οφείλει να αποδείξει ότι έχει εφαρμόσει μια συστηματική διαδικασία αξιολόγησης και ελέγχου κινδύνων, ευθυγραμμισμένη με πρότυπα όπως το ISO 14971 [21], [22].

Ιδιαίτερη σημασία δίνεται στις συσκευές που περιλαμβάνουν λογισμικό ή βασίζονται σε συνδεσιμότητα (π.χ. ασύρματη επικοινωνία, cloud υπηρεσίες, διασύνδεση με άλλα πληροφοριακά συστήματα). Ο MDR απαιτεί από τους κατασκευαστές να λαμβάνουν υπόψη τις πιθανές απειλές κυβερνοασφάλειας κατά τον σχεδιασμό (security by design) και να τεκμηριώνουν τα μέτρα προστασίας, όπως μηχανισμούς ταυτοποίησης, κρυπτογράφησης και ελέγχου πρόσβασης [20]. Αυτό είναι ιδιαίτερα κρίσιμο για το IoMT, όπου οι φορετές ή εμφυτεύσιμες συσκευές επικοινωνούν συνεχώς με φορητές συσκευές, πύλες (gateways) και νοσοκομειακά δίκτυα.

Επιπλέον, ο MDR δίνει έμφαση στη διάρκεια ζωής της συσκευής (lifecycle approach). Ο κατασκευαστής δεν αξιολογείται μόνο στο στάδιο της αρχικής σχεδίασης, αλλά οφείλει να διασφαλίζει ότι η συσκευή παραμένει ασφαλής και ενημερωμένη καθ' όλη τη διάρκεια χρήσης της. Αυτό περιλαμβάνει διαδικασίες για παροχή ενημερώσεων λογισμικού, αντιμετώπιση ευπαθειών, διορθωτικές ενέργειες πεδίου (field safety corrective actions) και συνεχή παρακολούθηση συμβάντων (post-market surveillance) [20]. Η απαίτηση αυτή συνδέεται άμεσα με την ανάγκη για δομημένη διαχείριση κινδύνου σύμφωνα με το ISO 14971, καθώς και με πρακτικές που συναντώνται στα πλαίσια ISO και NIST [21], [22], [25].

Τέλος, το κανονιστικό πλαίσιο του MDR επηρεάζει άμεσα τους κατασκευαστές IoMT συσκευών, καθώς τους υποχρεώνει να αποδεικνύουν ότι οι λύσεις που προσφέρουν ενσωματώνουν "state of the art" μέτρα ασφάλειας, λαμβάνοντας υπόψη την εξέλιξη των απειλών και τις τρέχουσες βέλτιστες πρακτικές. Αυτό σημαίνει ότι η συμμόρφωση με τον MDR δεν είναι στατική, αλλά προϋποθέτει συνεχή αναθεώρηση και προσαρμογή των μηχανισμών κυβερνοασφάλειας, σε συνδυασμό με τις τεχνικές προδιαγραφές που ορίζονται από πρότυπα όπως το ISO 14971 και κατευθυντήριες όπως αυτές της FDA και του NIST [20]–[23], [25].

6.3.2 Διαχείριση Κινδύνου σύμφωνα με το ISO 14971

Το πρότυπο ISO 14971 αποτελεί το βασικό διεθνές πλαίσιο για τη διαχείριση κινδύνου σε ιατροτεχνολογικά προϊόντα, συμπεριλαμβανομένων των φορετών και δικτυωμένων συσκευών που εντάσσονται στο οικοσύστημα IoMT.

Σε αντίθεση με άλλα πρότυπα ασφάλειας, το ISO 14971 δεν περιορίζεται σε τεχνικά μέτρα προστασίας· περιγράφει μια συστηματική, κυκλική και τεκμηριωμένη διαδικασία που εφαρμόζεται καθ' όλη τη διάρκεια ζωής της συσκευής, από τον σχεδιασμό έως την απόσυρσή της.

Σύμφωνα με τον Yang [21], το ISO 14971 αποτελεί τη "ραχοκοκαλιά" των κανονιστικών απαιτήσεων, καθώς συνδέεται άμεσα με τον MDR και τη διαδικασία συμμόρφωσης.

A. Διαδικασία Διαχείρισης Κινδύνου (Risk Management Process)

Το ISO 14971 ορίζει ένα ολοκληρωμένο μοντέλο Risk Management Lifecycle, το οποίο περιλαμβάνει:

1. Ανάλυση κινδύνου (Risk Analysis)
   - Αναγνώριση κινδύνων (hazard identification)
   - Εκτίμηση πιθανότητας και σοβαρότητας
   - Καταγραφή σε risk tables και hazard logs
   - Εξέταση failure modes (ιδιαίτερα σημαντικό για IoMT λόγω συνδεσιμότητας)

2. Αξιολόγηση κινδύνου (Risk Evaluation)
   - Καθορισμός αποδεκτών επιπέδων κινδύνου
   - Απόφαση για το αν απαιτείται risk control
3. Έλεγχος κινδύνου (Risk Control)
   - Εφαρμογή μέτρων προστασίας
   - Επαλήθευση αποτελεσματικότητας
   - Ανάλυση υπολειπόμενου κινδύνου (residual risk)
   - Τεκμηρίωση διαδικασιών και αποτελεσμάτων
4. Παρακολούθηση μετά την κυκλοφορία (Post-Market Surveillance)
   - Συλλογή δεδομένων πραγματικής χρήσης
   - Αναθεώρηση εκτίμησης κινδύνου
   - Αντιμετώπιση συμβάντων ή ευπαθειών

Η διαδικασία αυτή, όπως σημειώνει ο Yang [21], είναι κυκλική και επαναλαμβανόμενη. Κάθε αλλαγή στο λογισμικό, στο firmware ή στη συνδεσιμότητα μιας IoMT συσκευής πρέπει να συνοδεύεται από νέα εκτίμηση κινδύνου.

B. Εφαρμογή του ISO 14971 σε ιατρικό λογισμικό και συνδεδεμένες συσκευές

Η εφαρμογή του προτύπου σε συσκευές που εντάσσονται στο IoMT παρουσιάζει πρόσθετες προκλήσεις. Οι Flood et al. [22] υπογραμμίζουν ότι ο παραδοσιακός κίνδυνος που αφορά μηχανικές ή ηλεκτρικές βλάβες δεν είναι πλέον επαρκής. Αντιθέτως, απαιτείται η αξιολόγηση κινδύνων που προκύπτουν από:

- κυβερνοεπιθέσεις,
- διαρροή δεδομένων,
- σφάλματα λογισμικού,
- αστοχία επικοινωνίας,
- παρεμβολές στη σύνδεση ή αλλοίωση δεδομένων.

Για παράδειγμα, μια φορετή συσκευή που παρακολουθεί καρδιακούς παλμούς πρέπει να αξιολογηθεί όχι μόνο ως hardware, αλλά ως σύστημα λογισμικού-επικοινωνίας, όπου ένας κυβερνοκίνδυνος μπορεί να επηρεάσει άμεσα την ασφάλεια του ασθενούς.

Σύμφωνα με Flood et al. [22], η ένταξη λογισμικού στο risk management απαιτεί:

- αξιολόγηση failure modes του software,
- ανάλυση επικοινωνιακών πρωτοκόλλων,
- καταγραφή cybersecurity threats ως hazards,
- τεκμηρίωση μηχανισμών προστασίας (authentication, encryption, secure update).

Το ISO 14971 είναι πλήρως ευθυγραμμισμένο με τις απαιτήσεις του MDR [20], το οποίο επιβάλλει τεκμηριωμένη ανάλυση κινδύνου σε όλο τον κύκλο ζωής της συσκευής.

C. Risk Controls και Κυβερνοασφάλεια στο IoMT

Για συσκευές IoMT, οι έλεγχοι κινδύνων (risk controls) πρέπει να περιλαμβάνουν ειδικές λειτουργίες κυβερνοασφάλειας, όπως:

- μηχανισμούς ασφαλούς ταυτοποίησης και εξουσιοδότησης,
- κρυπτογράφηση δεδομένων σε ανάπαυση και μεταφορά,
- προστασία από μη εξουσιοδοτημένες αλλαγές (tamper protection),
- ασφαλείς μηχανισμούς ενημερώσεων (secure firmware update),
- παρακολούθηση ανωμαλιών και καταγραφή συμβάντων.

Όπως επισημαίνει ο Yang [21], η αποτελεσματικότητα των μέτρων πρέπει να τεκμηριώνεται και να ελέγχεται μέσω verification activities, ενώ κάθε υπολειπόμενος κίνδυνος πρέπει να αξιολογείται ως αποδεκτός ή μη αποδεκτός σύμφωνα με τις κατευθυντήριες της εταιρείας και τις απαιτήσεις της νομοθεσίας.

D. Συμπερασματικά

Το ISO 14971 αποτελεί απαραίτητο εργαλείο για τη συμμόρφωση των IoMT συσκευών με τα ευρωπαϊκά και διεθνή πρότυπα. Η εφαρμογή του διασφαλίζει ότι:

- οι κίνδυνοι αναγνωρίζονται και ελέγχονται,
- το λογισμικό αντιμετωπίζεται ως κρίσιμος παράγοντας ασφάλειας,
- ο κύκλος ζωής της συσκευής παρακολουθείται συνεχώς,
- η συμμόρφωση με τον MDR, την FDA και το NIST επιτυγχάνεται τεκμηριωμένα.

Το πλαίσιο αυτό δημιουργεί τη βάση πάνω στην οποία μπορεί να αναπτυχθεί μια ολοκληρωμένη στρατηγική ασφάλειας για κάθε σύγχρονη IoMT συσκευή.

6.3.3 Κατευθυντήριες Οδηγίες της FDA για την Κυβερνοασφάλεια Ιατρικών Συσκευών

Η Υπηρεσία Τροφίμων και Φαρμάκων των ΗΠΑ (Food and Drug Administration – FDA) αποτελεί έναν από τους σημαντικότερους διεθνείς ρυθμιστικούς φορείς που καθορίζουν τις απαιτήσεις ασφάλειας για ιατρικές συσκευές, συμπεριλαμβανομένων εκείνων που συνδέονται σε δίκτυα ή επικοινωνούν με άλλα πληροφοριακά συστήματα. Σε αντίθεση με το ευρωπαϊκό πλαίσιο MDR, οι κατευθυντήριες της FDA εστιάζουν ιδιαίτερα στη διαχείριση κυβερνοκινδύνων τόσο πριν όσο και μετά την κυκλοφορία του προϊόντος στην αγορά, καλύπτοντας το πλήρες φάσμα του κύκλου ζωής των συσκευών.

Σύμφωνα με την ανάλυση των Stern et al. [23], η FDA αναδεικνύει την κυβερνοασφάλεια ως κρίσιμο παράγοντα ασφάλειας και αποτελεσματικότητας των ιατροτεχνολογικών συσκευών, ο οποίος οφείλει να ενσωματώνεται στην αρχιτεκτονική και στον σχεδιασμό κάθε συσκευής (security by design). Οι κατασκευαστές οφείλουν να τεκμηριώνουν τις λειτουργίες κυβερνοασφάλειας που ενσωματώνονται στη συσκευή, συμπεριλαμβανομένων μηχανισμών προστασίας δεδομένων, ταυτοποίησης χρηστών, ασφαλούς επικοινωνίας και αποτροπής μη εξουσιοδοτημένων αλλαγών στη διαμόρφωση ή στο λογισμικό.

A. Premarket Απαιτήσεις: Τεκμηρίωση Ασφάλειας πριν την Έγκριση

Η FDA απαιτεί από τους κατασκευαστές να παρέχουν λεπτομερή τεκμηρίωση κυβερνοασφάλειας κατά το στάδιο της premarket submission, η οποία περιλαμβάνει τουλάχιστον:

- Threat Modeling: αξιολόγηση πιθανών επιθέσεων και επιπτώσεων
- Διαχείριση ευπαθειών: μεθοδολογία ανάλυσης και αντιμετώπισης
- SBOM (Software Bill of Materials): πλήρης καταγραφή βιβλιοθηκών, modules και λογισμικών τρίτων
- Risk Control Measures: τεκμηρίωση μηχανισμών ελέγχου κινδύνου
- Cybersecurity Testing: penetration testing, code review, static/dynamic analysis
- Secure Update Mechanisms: διαδικασίες ασφαλούς ενημέρωσης firmware/software

Σύμφωνα με τους Stern et al. [23], οι περισσότερες συσκευές που αξιολογήθηκαν παρουσίαζαν σημαντικές αδυναμίες τεκμηρίωσης στα παραπάνω σημεία, γεγονός που υποδεικνύει ότι η συμμόρφωση αποτελεί ακόμη πρόκληση για τους κατασκευαστές.

B. Postmarket Απαιτήσεις: Ασφάλεια κατά τη Διάρκεια Χρήσης της Συσκευής

Η FDA επιβάλλει επίσης ένα ολοκληρωμένο πλαίσιο postmarket παρακολούθησης, το οποίο περιλαμβάνει:

- Παρακολούθηση συμβάντων κυβερνοασφάλειας
- Ανάλυση root cause για ευπάθειες που εντοπίζονται μετά την κυκλοφορία

- Διορθωτικές ενέργειες πεδίου (Field Safety Corrective Actions)
- Συνεχή ενημέρωση λογισμικού και firmware
- Διαδικασίες coordinated vulnerability disclosure

Η ανάγκη για συνεχή παρακολούθηση και ενημέρωση γίνεται ακόμη πιο κρίσιμη για τις IoMT συσκευές, οι οποίες συνδέονται σε δίκτυα και επικοινωνούν με νοσοκομειακά συστήματα, εκθέτοντας έτσι νέες επιφάνειες επίθεσης.

C. Συμπεράσματα από την Ανάλυση της FDA – Πραγματικά Εμπόδια και Προκλήσεις

Η μελέτη των Stern et al. [23] καταδεικνύει ότι, παρά τις προσπάθειες των κατασκευαστών, υπάρχουν σημαντικά κενά:

- ανεπαρκής τεκμηρίωση μέτρων ασφαλείας,
- ανεπαρκείς μηχανισμοί ενημέρωσης λογισμικού,
- ελλιπής αξιολόγηση κινδύνων κυβερνοασφάλειας,
- περιορισμένη υιοθέτηση δομημένων πρακτικών threat modeling,
- απουσία πλήρους SBOM σε πολλές συσκευές.

Οι ελλείψεις αυτές αυξάνουν την πολυπλοκότητα και καθιστούν την συμμόρφωση ένα δυναμικό και απαιτητικό έργο.

D. Σημασία για το IoMT και σύνδεση με τα υπόλοιπα πρότυπα

Για τις IoMT συσκευές, οι κατευθυντήριες της FDA λειτουργούν συμπληρωματικά με το MDR, το ISO 14971 και τα πλαίσια του NIST, καθώς καλύπτουν:

- την πρακτική εφαρμογή των μέτρων που ορίζει το ISO 14971,
- την αξιολόγηση πραγματικών παραμέτρων ασφάλειας σε δικτυωμένες συσκευές,
- την παροχή ενός πλαισίου συνεχούς ενημέρωσης και επιτήρησης,
- την ενσωμάτωση του secure-by-design και lifecycle security στον σχεδιασμό.

Στο περιβάλλον του IoMT, όπου οι συσκευές λειτουργούν ως κόμβοι συλλογής ευαίσθητων δεδομένων, η προσέγγιση της FDA αποτελεί κρίσιμο σημείο αναφοράς για την ανάλυση κινδύνων, τη συμμόρφωση και τη διασφάλιση της αξιοπιστίας των συσκευών.

6.3.4 Πλαίσιο NISTIR 8259 και NISTIR 8259A για την Ασφάλεια IoT/IoMT Συσκευών

Τα έγγραφα NISTIR 8259 και NISTIR 8259A, που εκδόθηκαν από το National Institute of Standards and Technology (NIST), αποτελούν το βασικό πλαίσιο των Ηνωμένων Πολιτειών για την ενίσχυση της κυβερνοασφάλειας στις συσκευές Internet of Things (IoT). Η σημασία τους είναι ιδιαίτερα μεγάλη για το IoMT, καθώς οι φορετές ιατρικές συσκευές μοιράζονται τα ίδια χαρακτηριστικά συνδεσιμότητας, δικτυακής λειτουργίας και έκθεσης σε κυβερνοαπειλές. Το NISTIR 8259 καθορίζει τις “θεμελιώδεις δραστηριότητες ασφάλειας” που οφείλουν να εφαρμόζουν οι κατασκευαστές, ενώ το NISTIR 8259A ορίζει τις “βασικές δυνατότητες κυβερνοασφάλειας συσκευών”, δημιουργώντας ένα ενιαίο πλαίσιο για secure-by-design ανάπτυξη συσκευών [25].

A. NISTIR 8259 – Foundational Cybersecurity Activities

Το NISTIR 8259 εστιάζει στις δραστηριότητες που οφείλουν να εκτελούν οι κατασκευαστές IoT συσκευών, με στόχο να ενσωματώσουν την κυβερνοασφάλεια στο lifecycle της συσκευής. Οι τέσσερις βασικές δραστηριότητες που ορίζει το έγγραφο [25] είναι:

1. Προσδιορισμός βασικών λειτουργιών ασφάλειας (Identify IoT Security Capabilities)

Ο κατασκευαστής πρέπει να αποφασίσει ποιες δυνατότητες ασφάλειας είναι απαραίτητες για τη συσκευή (π.χ. authentication, encryption, logging).

2. Διασφάλιση της ασφαλούς κατασκευής και προετοιμασίας της συσκευής (Ensure Device Security)
   Περιλαμβάνει secure coding, hardening, ενημέρωση βιβλιοθηκών και έλεγχο ευπαθειών.

3. Ασφαλής παροχή και υποστήριξη ενημερώσεων (Provide Secure Updates)
   Η συσκευή πρέπει να υποστηρίζει μηχανισμούς ασφαλών ενημερώσεων (cryptographically signed firmware, rollback protection).

4. Παροχή τεκμηρίωσης ασφάλειας (Provide Transparency)
   Ο κατασκευαστής έχει την ευθύνη να παρέχει SBOM, οδηγίες ρύθμισης, περιγραφή δυνατοτήτων και περιορισμών ασφάλειας.

Οι δραστηριότητες αυτές εναρμονίζονται με τις απαιτήσεις της FDA για premarket τεκμηρίωση, καθώς και με τον MDR σε θέματα lifecycle management, αποτελώντας έναν κορμό ελάχιστων απαιτήσεων για IoT/IoMT συσκευές [23].

B. NISTIR 8259A – IoT Device Cybersecurity Capability Core Baseline

Το NISTIR 8259A αναπτύσσει και τυποποιεί τις συγκεκριμένες κυβερνοασφαλείς δυνατότητες που πρέπει να ενσωματώνει κάθε IoT συσκευή. Οι έξι βασικές δυνατότητες που καθορίζονται στο έγγραφο [25a] είναι:

Κεφάλαιο 1ο: Device Identification
Η συσκευή πρέπει να έχει μοναδικό αναγνωριστικό (unique ID), το οποίο δεν πρέπει να μπορεί να τροποποιηθεί από μη εξουσιοδοτημένο χρήστη.

Κεφάλαιο 2ο: Device Configuration
Η συσκευή πρέπει να υποστηρίζει ασφαλή διαμόρφωση και να αποτρέπει μη εξουσιοδοτημένες αλλαγές.

Κεφάλαιο 3ο: Data Protection
Κρυπτογράφηση δεδομένων σε ανάπαυση και μεταφορά, προστασία ακεραιότητας και έλεγχος πρόσβασης.

Κεφάλαιο 4ο: Logical Access to Interfaces
Περιορισμός πρόσβασης σε θύρες, πρωτόκολλα και services μέσω authentication/authorization.

Κεφάλαιο 5ο: Software Update
Ασφαλείς ενημερώσεις firmware, επαλήθευση ψηφιακών υπογραφών, διαχείριση ευπαθειών.

Κεφάλαιο 6ο: Cybersecurity State Awareness
Καταγραφή, παρακολούθηση και αναφορά σημαντικών συμβάντων (logging, event monitoring).

Οι δυνατότητες αυτές αποτελούν “baseline” για όλες τις IoT συσκευές, αλλά για τις IoMT συσκευές είναι ακόμη πιο κρίσιμες, αφού η παραβίασή τους μπορεί να επηρεάσει άμεσα την υγεία του ασθενούς.

C. Σύνδεση του NISTIR 8259/8259A με IoMT και τα διεθνή πρότυπα

Το NISTIR πλαίσιο λειτουργεί συμπληρωματικά με:

- τον MDR (Annex I – General Safety and Performance Requirements) [20],
- το ISO 14971 για διαχείριση κινδύνου [21], [22],

- τις κατευθυντήριες της FDA για premarket και postmarket ασφάλεια [23].

Στο IoMT, το NISTIR προσφέρει:

- συγκεκριμένες τεχνικές δυνατότητες για secure-by-design ανάπτυξη,
- δομημένα βήματα για ασφάλεια συσκευών που βασίζονται σε λογισμικό,
- κατευθύνσεις για secure updates, data protection και identity management,
- τεχνικά standards που οι κατασκευαστές μπορούν να εφαρμόσουν πέρα από τις νομικές απαιτήσεις του MDR/FDA.

Σε επίπεδο συμμόρφωσης, το NISTIR 8259A παρέχει ένα τεχνικό baseline, το οποίο μπορεί να χρησιμοποιηθεί από κατασκευαστές IoMT συσκευών προκειμένου να αποδείξουν ότι οι λύσεις τους βασίζονται σε σύγχρονες και τεκμηριωμένες πρακτικές ασφάλειας.

D. Συμπερασματικά

Τα NISTIR 8259 και 8259A αποτελούν δύο από τα σημαντικότερα διεθνή τεχνικά πλαίσια για την ασφάλεια IoT συσκευών.

Ο συνδυασμός τους εξασφαλίζει ότι οι IoMT συσκευές:

- ενσωματώνουν βασικές λειτουργίες ασφάλειας,
- υποστηρίζουν ασφαλείς ενημερώσεις,
- διαθέτουν τεκμηρίωση και δυνατότητες monitoring,
- παραμένουν ασφαλείς καθ’ όλη τη διάρκεια ζωής τους.

Αποτελούν κρίσιμη αναφορά για τον σχεδιασμό, την ανάπτυξη και τη συμμόρφωση φορετών και εμφυτεύσιμων ιατρικών συσκευών.

6.4 Πρακτικές Εφαρμογές Ασφάλειας σε IoMT Συστήματα

Η εφαρμογή της κυβερνοασφάλειας στο IoMT απαιτεί συνδυασμένη προσέγγιση που περιλαμβάνει τεχνικά μέτρα, διαδικασίες διαχείρισης κινδύνων και συνεχή παρακολούθηση καθ’ όλη τη διάρκεια ζωής της συσκευής. Σε αυτό το πλαίσιο, οι απαιτήσεις του MDR [20], οι διαδικασίες του ISO 14971 [21], [22], οι οδηγίες της FDA [23] και οι τεχνικές κατευθύνσεις των NISTIR 8259/8259A [25] μεταφράζονται σε συγκεκριμένες πρακτικές εφαρμογής, οι οποίες διασφαλίζουν την ασφάλεια των δικτυωμένων ιατρικών συστημάτων.

6.4.1 Secure-by-Design Αρχιτεκτονική

Η αρχιτεκτονική των IoMT συσκευών οφείλει να βασίζεται σε αρχές ασφαλούς σχεδιασμού, όπως ορίζεται από το MDR και τις premaket οδηγίες της FDA. Αυτό περιλαμβάνει:

- Ελαχιστοποίηση της επιφάνειας επίθεσης (attack surface reduction)
- Secure coding και χρήση ενημερωμένων βιβλιοθηκών
- Ασφαλή πρωτόκολλα επικοινωνίας (TLS 1.2+, DTLS, WPA3 όπου εφαρμόζεται)
- Hardware security controls (TPM modules, secure elements)

Τα παραπάνω ευθυγραμμίζονται με τις δραστηριότητες του NISTIR 8259 που επιβάλλουν την ενσωμάτωση βασικών μηχανισμών ασφαλείας ήδη από το στάδιο του σχεδιασμού [25].

6.4.2 Ασφαλής Ταυτοποίηση και Έλεγχος Πρόσβασης

Οι IoMT συσκευές οφείλουν να υλοποιούν ισχυρούς μηχανισμούς ταυτοποίησης και ελέγχου πρόσβασης, οι οποίοι περιλαμβάνουν:

- Unique device identity [25a]
- Μηχανισμούς πολυπαραγοντικής ταυτοποίησης για επαγγελματίες υγείας
- RBAC (Role-Based Access Control) για πρόσβαση σε δεδομένα ασθενών
- Πολυεπίπεδη εξουσιοδότηση σε mobile apps, gateways και cloud services

Σύμφωνα με το ISO 14971, τα μέτρα αυτά εντάσσονται στα risk controls που πρέπει να τεκμηριωθούν και να αξιολογηθούν για την αποτελεσματικότητά τους [21], [22].

6.4.3 Προστασία Δεδομένων και Κρυπτογράφηση

Η προστασία της ακεραιότητας και εμπιστευτικότητας των δεδομένων αποτελεί κεντρικό άξονα του MDR και του FDA. Πρακτικές εφαρμογές περιλαμβάνουν:

- Κρυπτογράφηση δεδομένων σε μεταφορά και ανάπαυση
- Integrity verification μέσω hash και message authentication codes
- Secure storage σε dedicated hardware modules
- Ανίχνευση αλλοίωσης δεδομένων (data tampering detection)

Το NISTIR 8259A ορίζει ρητά την ικανότητα προστασίας δεδομένων (Data Protection Capability), ενώ οι οδηγίες του FDA απαιτούν την τεκμηρίωση της χρήσης κρυπτογραφικών μηχανισμών στα premarket submissions [23].

6.4.4 Ασφαλείς Ενημερώσεις Λογισμικού (Secure Update Mechanisms)

Σύμφωνα με την FDA και το NISTIR 8259, οι κατασκευαστές οφείλουν να παρέχουν ασφαλή κανάλια ενημέρωσης firmware και λογισμικού, τα οποία περιλαμβάνουν:

- Firmware signing με κρυπτογραφικές υπογραφές
- Verification mechanisms πριν από την εγκατάσταση
- Rollback protection
- Coordinated vulnerability disclosure
- Αυτόματα ή manual update policies

Το ISO 14971 απαιτεί κάθε firmware update να συνοδεύεται από νέα risk assessment για να αξιολογηθεί ο νέος residual risk [21].

6.4.5 Καταγραφή Συμβάντων, Logging και Monitoring

Η καταγραφή συμβάντων αποτελεί βασική λειτουργική απαίτηση για:

- ανίχνευση επιθέσεων,
- διαγνωστική παρακολούθηση,
- έλεγχο συμμόρφωσης με MDR/FDA,
- εφαρμογή postmarket surveillance.

Το NISTIR 8259A ορίζει ξεκάθαρα την απαίτηση για Cybersecurity State Awareness, δηλαδή την ικανότητα της συσκευής να παρακολουθεί την κατάστασή της και να αναφέρει ασυνήθιστη δραστηριότητα [25a].

6.4.6 Δικτυακή Άμυνα σε Περιβάλλον IoMT

Στην πράξη, οι συσκευές IoMT λειτουργούν σε πολύπλοκα νοσοκομειακά δίκτυα. Οι πρακτικές άμυνας που συστήνονται από ENISA και παγκόσμιους οργανισμούς περιλαμβάνουν [12], [17]:

- Network segmentation (διαχωρισμός IoMT συσκευών από IT δίκτυο)
- Zero Trust Network Access (ZTNA)
- Firewall κανόνες για IoMT gateways
- Intrusion Detection/Prevention Systems (IDS/IPS)

- Περιορισμός μη απαραίτητων θυρών και πρωτοκόλλων

Οι πρακτικές αυτές μειώνουν σημαντικά την επιφάνεια επίθεσης και περιορίζουν την εξάπλωση επιθέσεων ransomware ή lateral movement επιτιθέμενων [12], [17].

6.4.7 Post-Market Παρακολούθηση και Διαχείριση Ευπαθειών

Το MDR, η FDA και το ISO 14971 απαιτούν συνεχή επιτήρηση των συσκευών μετά την κυκλοφορία τους [20], [21], [23]. Πρακτικά αυτό σημαίνει:

- Συνεχή συλλογή telemetry data
- Ανάλυση πραγματικών περιστατικών (incident analysis – root cause)
- Περιοδικά penetration tests
- Risk re-evaluation όταν εντοπίζονται νέες ευπάθειες
- Field Safety Corrective Actions (FSCA)

Αυτή η προσέγγιση εξασφαλίζει ότι οι συσκευές παραμένουν ασφαλείς σε έναν διαρκώς μεταβαλλόμενο χώρο απειλών, όπως αναδεικνύει και η FDA [23].

6.4.8 Συμπερασματικά

Οι πρακτικές εφαρμογές ασφάλειας στο IoMT αποτελούν την ουσιαστική “μετάφραση” των απαιτήσεων που θέτουν τα πρότυπα MDR, ISO 14971, FDA και NISTIR σε λειτουργικά και τεχνικά μέτρα. Ο συνδυασμός αυτών των πλαισίων οδηγεί στη διαμόρφωση ενός ολοκληρωμένου οικοσυστήματος ασφάλειας, το οποίο ενσωματώνει τον ασφαλή σχεδιασμό, τη συστηματική διαχείριση κινδύνων, τις τεχνικές λειτουργίες προστασίας και τη συνεχή παρακολούθηση καθ’ όλη τη διάρκεια ζωής των IoMT συσκευών.

6.5 Μελέτη Περίπτωσης: Ευπάθειες και Αντιμετώπιση σε IoMT Συστήματα

6.5.1 Στόχος και Μεθοδολογία της Μελέτης Περίπτωσης

Στο παρόν κεφάλαιο, η μελέτη περίπτωσης στοχεύει να αναδείξει πώς οι θεωρητικές αρχές ασφάλειας και τα κανονιστικά πλαίσια που παρουσιάστηκαν στα προηγούμενα κεφάλαια εφαρμόζονται σε ένα πραγματικό, σύνθετο περιβάλλον IoMT. Βασίζεται σε παραδείγματα και περιστατικά ευπαθειών που έχουν αναλυθεί στη διεθνή βιβλιογραφία, με έμφαση στις εργασίες των Williams και Woodward [26], καθώς και στη διασύνδεση των ευρημάτων με τις απαιτήσεις των MDR, ISO 14971, FDA και NISTIR [20]–[23], [25].

Η μελέτη ακολουθεί μία ποιοτική προσέγγιση:

a) περιγραφή του περιβάλλοντος και των εμπλεκόμενων συσκευών,
b) αναγνώριση των βασικών κατηγοριών ευπαθειών και επιθέσεων,
c) ανάλυση των συνεπειών για την ασφάλεια των ασθενών και των δεδομένων,
d) αποτύπωση των μέτρων αντιμετώπισης και χαρτογράφησή τους στα πρότυπα συμμόρφωσης.

Στόχος δεν είναι η πλήρης τεχνική αναπαραγωγή ενός συγκεκριμένου penetration test, αλλά η συστηματική αποτύπωση των προβλημάτων ασφαλείας σε IoMT συστήματα και η σύνδεσή τους με πρακτικές άμυνας και κανονιστικές απαιτήσεις.

6.5.2 Περιγραφή Περιβάλλοντος και Τύπων Συσκευών

Η μελέτη περίπτωσης επικεντρώνεται σε ένα τυπικό νοσοκομειακό περιβάλλον, στο οποίο χρησιμοποιούνται διάφορες κατηγορίες ψηφιακών ιατρικών συσκευών που συνδέονται σε δίκτυο ή σε πλατφόρμες τηλεϊατρικής. Ενδεικτικά, περιλαμβάνονται [26]:

- φορετές συσκευές παρακολούθησης ζωτικών σημείων (π.χ. καρδιακός ρυθμός, οξυγόνωση),

- αντλίες έγχυσης (infusion pumps) και αντλίες ινσουλίνης,
- εμφυτεύσιμες συσκευές, όπως βηματοδότες και απινιδωτές,
- σταθμοί εργασίας και τερματικά επαγγελματιών υγείας που αλληλεπιδρούν με τις συσκευές,
- κεντρικά πληροφοριακά συστήματα και πλατφόρμες αποθήκευσης/ανάλυσης δεδομένων.

Όπως επισημαίνουν οι Williams και Woodward [26], το περιβάλλον αυτό χαρακτηρίζεται από υψηλή πολυπλοκότητα: πολλαπλοί προμηθευτές, ετερογενείς πλατφόρμες λογισμικού, διαφορετικά πρωτόκολλα επικοινωνίας, συνδυασμός παλαιότερου εξοπλισμού (legacy systems) με σύγχρονες IoT/IoMT λύσεις. Αυτή η πολυπλοκότητα μεγαλώνει την επιφάνεια επίθεσης και δυσκολεύει την εφαρμογή ομοιόμορφων πολιτικών ασφάλειας σε όλα τα επίπεδα του συστήματος.

Στο συγκεκριμένο πλαίσιο, οι ερευνητές αναδεικνύουν ότι οι συσκευές δεν λειτουργούν απομονωμένα, αλλά ως κόμβοι ενός ευρύτερου οικοσυστήματος: τα δεδομένα μεταφέρονται από τις φορετές ή εμφυτεύσιμες συσκευές σε κινητές συσκευές (π.χ. smartphones, tablets), από εκεί σε νοσοκομειακούς servers ή cloud πλατφόρμες, και τελικά σε κλινικές εφαρμογές που υποστηρίζουν τη λήψη αποφάσεων [26]. Το γεγονός αυτό καθιστά αναγκαία την ολιστική αξιολόγηση της ασφάλειας, λαμβάνοντας υπόψη όλες τις διαδρομές δεδομένων και όλα τα σημεία διασύνδεσης.

6.5.3 Αναγνωρισμένες Ευπάθειες και Κατηγορίες Απειλών στο IoMT

Οι Williams και Woodward [26] αναδεικνύουν ότι το οικοσύστημα των ιατρικών συσκευών που συνδέονται σε δίκτυα εμφανίζει ένα ιδιαίτερα σύνθετο και πολυεπίπεδο προφίλ ευπαθειών. Η ανάλυση των περιστατικών που εξετάζουν καταδεικνύει ότι οι ευπάθειες αυτές δεν περιορίζονται σε ένα σημείο του συστήματος, αλλά κατανέμονται σε όλες τις βαθμίδες της τεχνολογικής αλυσίδας: στο hardware της συσκευής, στο λογισμικό της, στα πρωτόκολλα επικοινωνίας, στα κλινικά συστήματα που την υποστηρίζουν, αλλά και στα ίδια τα νοσοκομειακά δίκτυα.

Οι πιο σημαντικές κατηγορίες ευπαθειών που εντοπίζονται στη βιβλιογραφία [26] περιλαμβάνουν:

a) Ευπάθειες λογισμικού και firmware

Παλαιωμένες βιβλιοθήκες, μη υπογεγραμμένες ενημερώσεις, ελλιπείς μηχανισμοί επαλήθευσης firmware, καθώς και bugs που μπορούν να αξιοποιηθούν μέσω remote code execution.

b) Αδύναμα ή ανεπαρκώς προστατευμένα πρωτόκολλα επικοινωνίας

Πολλές συσκευές εξακολουθούν να βασίζονται σε μη κρυπτογραφημένη ασύρματη επικοινωνία (π.χ. Bluetooth LE χωρίς ενισχυμένα security layers), επιτρέποντας επιθέσεις τύπου sniffing, spoofing ή man-in-the-middle.

c) Ανεπαρκείς μηχανισμοί ταυτοποίησης και εξουσιοδότησης

Σε αρκετά περιστατικά, η πρόσβαση στη συσκευή ή στο backend σύστημα μπορούσε να πραγματοποιηθεί με default ή σκληροκωδικοποιημένα credentials, παραβιάζοντας βασικές αρχές ασφαλείας.

d) Ανασφαλείς φυσικές θύρες και διασυνδέσεις

Η φυσική πρόσβαση, όπως μέσω USB ή service ports, επέτρεψε σε επιτιθέμενους να τροποποιήσουν κρίσιμες παραμέτρους λειτουργίας σε αντλίες έγχυσης και άλλες κλινικές συσκευές.

e) Ευπάθειες σε συστήματα αποθήκευσης και cloud πλατφόρμες

Τα δεδομένα ασθενών που συλλέγονται από φορετές συσκευές αποστέλλονται συχνά σε συστήματα που δεν διαθέτουν επαρκή έλεγχο πρόσβασης ή ισχυρή προστασία της ακεραιότητας των δεδομένων.

f) Προβλήματα ενσωμάτωσης με legacy συστήματα

Η συνύπαρξη σύγχρονων IoMT συσκευών με παλαιά πληροφοριακά συστήματα δημιουργεί ασυμβατότητες και κενά ασφαλείας, τα οποία οι Williams και Woodward εντοπίζουν ως έναν από τους σημαντικότερους παράγοντες κινδύνου [26].

Οι επιθέσεις που προκύπτουν από τις προηγούμενες κατηγορίες ευπαθειών περιλαμβάνουν αλλοίωση εντολών σε αντλίες ινσουλίνης, μη εξουσιοδοτημένη πρόσβαση σε εμφυτεύσιμους βηματοδότες, προβολή ευαίσθητων δεδομένων ασθενών χωρίς έγκριση, καθώς και περιπτώσεις όπου ransomware σε νοσοκομειακά δίκτυα επηρέασε τη λειτουργία συνδεδεμένων ιατρικών συσκευών.

Όπως τονίζουν οι Williams και Woodward [26], αυτές οι ευπάθειες δεν αποτελούν απλώς τεχνικά προβλήματα· μεταφράζονται άμεσα σε κινδύνους για την ασφάλεια των ασθενών, αφού η κακόβουλη αλλοίωση δεδομένων ή εντολών μπορεί να οδηγήσει σε λανθασμένη διάγνωση, λανθασμένη θεραπευτική δόση ή ακόμη και σε διακοπή ζωτικών λειτουργιών συσκευών. Επομένως, η διαχείριση των ευπαθειών και η ορθή εφαρμογή των προτύπων ασφαλείας αποτελεί κρίσιμο παράγοντα για την ασφάλεια και αξιοπιστία των IoMT συστημάτων.

6.5.4 Μέτρα Αντιμετώπισης και Συσχέτιση με MDR – ISO 14971 – FDA – NISTIR

Οι ευπάθειες που παρουσιάστηκαν στην προηγούμενη ενότητα αναδεικνύουν την ανάγκη για ολοκληρωμένη και πολυεπίπεδη προσέγγιση ασφάλειας. Η διεθνής βιβλιογραφία, καθώς και τα πρότυπα MDR [20], ISO 14971 [21], [22], FDA [23] και NISTIR 8259/8259A [25], προτείνουν ένα πλαίσιο με συγκεκριμένα τεχνικά και διαδικαστικά μέτρα που μπορούν να μειώσουν ουσιαστικά τους κινδύνους στις IoMT συσκευές. Το πλαίσιο αυτό περιλαμβάνει πρακτικές που καλύπτουν όλους τους κρίσιμους άξονες: τον σχεδιασμό της συσκευής, τη διαχείριση λογισμικού, την προστασία δεδομένων, την ασφάλεια επικοινωνιών, και την παρακολούθηση του συστήματος μετά την κυκλοφορία του.

A. Ενσωμάτωση Risk Controls (ISO 14971) στον Κύκλο Ζωής της Συσκευής

Η αντιμετώπιση των ευπαθειών ξεκινά από τον ίδιο τον σχεδιασμό της συσκευής. Το ISO 14971 ορίζει ότι οι κατασκευαστές οφείλουν να:

- αναγνωρίζουν όλους τους κινδύνους σε hardware, software και επικοινωνίες,
- εφαρμόζουν τεκμηριωμένα μέτρα risk control,
- επαληθεύουν την αποτελεσματικότητά τους με testing,
- και επαναξιολογούν τους κινδύνους μετά από κάθε αλλαγή στον κώδικα ή το firmware [21], [22].

Για παράδειγμα, η ύπαρξη μοναδικών αναγνωριστικών συσκευών, η χρήση κρυπτογράφησης και οι ασφαλείς μηχανισμοί update αποτελούν άμεσα risk controls που μειώνουν συγκεκριμένες ευπάθειες που εντοπίστηκαν από τους Williams & Woodward [26].

B. Ασφαλής Ενημέρωση Λογισμικού (Secure Updates) – Απαίτηση FDA & NISTIR

Η FDA απαιτεί από τους κατασκευαστές να προσφέρουν:

- ασφαλείς ψηφιακές υπογραφές firmware,
- διαδικασίες επαλήθευσης ακεραιότητας πριν την εγκατάσταση,
- rollback protection,
- και οργανωμένη διαδικασία γνωστοποίησης ευπαθειών [23].

Το NISTIR 8259A ενισχύει αυτήν την απαίτηση ορίζοντας τη “Software Update Capability”, δηλαδή ότι κάθε IoT/IoMT συσκευή πρέπει να μπορεί να λαμβάνει ενημερώσεις με ασφαλή τρόπο, χωρίς να εκθέτει το σύστημα σε μη εξουσιοδοτημένες αλλαγές [25].

Αυτές οι απαιτήσεις αντιμετωπίζουν ευπάθειες firmware που οι Williams & Woodward [26] εντόπισαν ως κρίσιμες.

C. Ασφάλεια Επικοινωνιών και Προστασία Δεδομένων (MDR – NISTIR)

Η προστασία των δεδομένων ασθενών και της επικοινωνίας της συσκευής αποτελεί κοινή απαίτηση όλων των πλαισίων. Τα μέτρα περιλαμβάνουν:

- κρυπτογράφηση TLS/DTLS,

- προστασία ακεραιότητας μέσω MAC/hashing,
- προστασία σε ασύρματα πρωτόκολλα (Bluetooth LE security mode 1/level 4),
- αποφυγή plaintext επικοινωνίας.

Το MDR, στο Annex I, προϋποθέτει ότι οι συσκευές πρέπει να προστατεύονται από μη εξουσιοδοτημένη πρόσβαση και αλλοίωση δεδομένων [20].Τα μέτρα αυτά απαντούν άμεσα στις επιθέσεις sniffing και man-in-the-middle που περιγράφονται στο case study [26].

D. Έλεγχος Πρόσβασης και Ταυτοποίηση (FDA – NISTIR 8259A)

Οι απαιτήσεις των FDA και NISTIR απαιτούν:

- μοναδικά αναγνωριστικά συσκευής,
- ασφαλείς μηχανισμούς ταυτοποίησης χρηστών,
- έλεγχο πρόσβασης RBAC,
- περιορισμό απενεργοποιημένων θύρων και πρωτοκόλλων,
- αποφυγή σκληροκωδικοποιημένων credentials [23], [25].

Τα μέτρα αυτά μειώνουν άμεσα κινδύνους όπως μη εξουσιοδοτημένη πρόσβαση σε ιατρικούς βηματοδότες ή αντλίες έγχυσης, που έχουν καταγραφεί στη βιβλιογραφία [26].

E. Δικτυακή Θωράκιση (ENISA – MDR – FDA)

Οι IoMT συσκευές πρέπει να λειτουργούν μέσα σε δομημένο και διαχωρισμένο δίκτυο:

- network segmentation (διαχώριση IoMT υποσυστημάτων),
- firewall policies ειδικά για IoMT traffic,
- intrusion detection (IDS/IPS),
- zero-trust αρχιτεκτονική,
- απομόνωση legacy συστημάτων.

Αυτές οι πρακτικές αντιμετωπίζουν την "πολυπλοκότητα του οικοσυστήματος" που οι Williams & Woodward [26] θεωρούν βασική ρίζα προβλημάτων.

F. Post-Market Surveillance & Incident Response (MDR – FDA – ISO)

Απαιτήσεις:

- συνεχής παρακολούθηση συσκευών μετά την κυκλοφορία (postmarket surveillance),
- συλλογή αναφορών περιστατικών,
- root cause analysis για κάθε κυβερνοσυμβάν,
- κοστολογημένες διορθωτικές ενέργειες (FSCA),
- επανεκτίμηση κινδύνων σύμφωνα με ISO 14971 (risk re-evaluation).

Με αυτόν τον τρόπο, τα πρότυπα συνδέονται με πραγματικές απειλές όπως ransomware σε νοσοκομειακά δίκτυα.

6.5.5 Χαρτογράφηση Ευπαθειών – Αντιμέτρων – Προτύπων Συμμόρφωσης

Η μελέτη περίπτωσης που παρουσιάστηκε ανέδειξε ένα σύνολο κρίσιμων ευπαθειών σε IoMT συστήματα, οι οποίες προκύπτουν τόσο από τεχνικούς περιορισμούς όσο και από την πολυπλοκότητα του οικοσυστήματος. Για να διασφαλιστεί η συμμόρφωση και να μειωθεί ουσιαστικά ο κίνδυνος για τους ασθενείς, είναι απαραίτητο να αντιστοιχίσουμε τις ευπάθειες αυτές στα υπάρχοντα πρότυπα και κανονιστικά πλαίσια. Η διαδικασία αυτή της «χαρτογράφησης» (mapping) συνδέει τις πραγματικές απειλές της βιβλιογραφίας [26] με τις απαιτήσεις των MDR [20], ISO 14971 [21], [22], FDA [23] και NISTIR 8259/8259A [25].

Η παρακάτω ανάλυση αποτελεί μια ενιαία δομημένη αποτύπωση της σχέσης ανάμεσα σε:

a) τις κύριες κατηγορίες ευπαθειών στο IoMT,
b) τα αντίστοιχα τεχνικά ή οργανωτικά μέτρα αντιμετώπισης,
c) και το πρότυπο ή κανονιστικό πλαίσιο στο οποίο βασίζονται.

A. Ευπάθειες Λογισμικού & Firmware → Ανάγκη για Secure Updates

Ευπάθεια (Case Study): Παλαιωμένο firmware, έλλειψη ψηφιακά υπογεγραμμένων ενημερώσεων, ευπάθειες βιβλιοθηκών τρίτων [26].

Μέτρο Αντιμετώπισης:

- Secure software/firmware updates
- Ψηφιακές υπογραφές, integrity checking
- Rollback protection

Πρότυπο / Πλαίσιο:

- FDA premarket/postmarket απαιτεί secure update mechanisms [23]
- NISTIR 8259A: “Software Update Capability” [25]
- ISO 14971: υποχρεωτική αναθεώρηση risk assessment μετά από κάθε update [21], [22]

B. Ανασφαλείς Επικοινωνίες → Ανάγκη για Κρυπτογράφηση & Integrity Protection

Ευπάθεια (Case Study): Plaintext Bluetooth/ασύρματη επικοινωνία χωρίς κρυπτογράφηση, δυνατότητα MITM και sniffing [26].

Μέτρο Αντιμετώπισης:

- Κρυπτογράφηση TLS/DTLS
- Secure pairing & bonding
- Integrity verification

Πρότυπο / Πλαίσιο:

- MDR Annex I: απαίτηση προστασίας από μη εξουσιοδοτημένη πρόσβαση και αλλοίωση δεδομένων [20]
- NISTIR 8259A: “Data Protection Capability” [25]
- FDA: απαιτεί secure communication pathways [23]

C. Ανεπαρκής Έλεγχος Πρόσβασης → Ανάγκη για Identity & Access Management

Ευπάθεια (Case Study): Χρήση default passwords, shared credentials, μη εξουσιοδοτημένη πρόσβαση σε εμφυτεύσιμες συσκευές [26].

Μέτρο Αντιμετώπισης:

- Unique device identity
- RBAC / Access control
- MFA σε κλινικά συστήματα
- Απενεργοποίηση μη χρησιμοποιούμενων θυρών

Πρότυπο / Πλαίσιο:

- NISTIR 8259A: “Device Identification” & “Logical Access to Interfaces” [25]
- FDA: απαιτεί διαχείριση credentials και περιορισμό ανεξουσιοδότητων αλλαγών [23]

D. Ευπάθειες Δικτύου → Ανάγκη για Δικτυακή Θωράκιση (Segmentation / IDS)

Ευπάθεια (Case Study): Οι IoMT συσκευές βρίσκονται στο ίδιο επίπεδο δικτύου με legacy συστήματα και γενική IT υποδομή [26].

Μέτρο Αντιμετώπισης:

- Network segmentation
- Zero-trust architecture
- Firewalls & IDS/IPS
- Απομόνωση παλαιότερου εξοπλισμού

Πρότυπο / Πλαίσιο:

- ENISA & MDR: network security as part of risk controls [20]
- FDA: συστήνει network hardening & monitoring [23]

Ε. Έλλειψη Monitoring → Ανάγκη για Logging & Cybersecurity State Awareness
Ευπάθεια (Case Study): Αδυναμία ανίχνευσης επιθέσεων, έλλειψη logs, έλλειψη real-time alerting [26].

Μέτρο Αντιμετώπισης:

- Logging
- Event monitoring
- Anomaly detection
- Post-market surveillance

Πρότυπο / Πλαίσιο:

- NISTIR 8259A: “Cybersecurity State Awareness” [25]
- ISO 14971: monitoring της συσκευής μετά την κυκλοφορία [21], [22]
- FDA Postmarket Guidance: απαιτεί continuous monitoring [23]

Πίνακας 6.5.5: Χαρτογράφηση ευπαθειών, αντιμέτρων και προτύπων συμμόρφωσης στο IoMT.

Ευπάθεια	**Μέτρο Αντιμετώπισης**	**Πλαίσιο / Πρότυπο**
Ευπάθειες firmware & βιβλιοθηκών	Secure updates, ψηφιακές υπογραφές, integrity checking	FDA [23], NISTIR 8259A [25], ISO 14971 [21], [22]
Ασφαλείς επικοινωνίες	Κρυπτογράφηση TLS/DTLS, secure pairing, integrity	MDR [20], NISTIR [25], FDA [23]
Access control weaknesses	Unique device ID, RBAC, MFA, secure interfaces	NISTIR 8259A [25], FDA [23]
Network exposure	Segmentation, IDS/IPS, firewalls, zero-trust	ENISA [12], MDR [20], FDA [23]
Ανεπαρκές monitoring	Logging, anomaly detection, post-market surveillance	NISTIR 8259A [25], ISO 14971 [21], FDA [23]

6.5.6 Συμπεράσματα βιβλιογραφικής Μελέτης Περίπτωσης

Η μελέτη περίπτωσης ανέδειξε ότι η κυβερνοασφάλεια των IoMT συστημάτων επηρεάζεται από ένα σύνολο διασυνδεδεμένων παραγόντων: την πολυπλοκότητα της αρχιτεκτονικής τους, την

αλληλεπίδραση πολλών διαφορετικών φορέων (κατασκευαστών, παρόχων λογισμικού, νοσοκομείων), καθώς και την απουσία ενοποιημένων προτύπων ασφαλείας. Οι ευπάθειες που εντοπίστηκαν –από firmware και ασύρματα πρωτόκολλα έως ασθενή ελέγχους πρόσβασης και έλλειψη monitoring– συνάδουν με τα ευρήματα της διεθνούς βιβλιογραφίας [20], [23], [26], επιβεβαιώνοντας ότι το IoMT αποτελεί έναν από τους πιο ευάλωτους τομείς της σύγχρονης ψηφιακής υγείας.

Η ανάλυση έδειξε επίσης ότι κάθε κατηγορία ευπάθειας μπορεί να μειωθεί σημαντικά με την υιοθέτηση των κατάλληλων μέτρων αντιστάθμισης (risk controls) που προτείνονται από τα βασικά πρότυπα MDR, ISO 14971, FDA και NISTIR. Για παράδειγμα, τα μέτρα secure updates και integrity checking που προτείνονται από το FDA και το NISTIR [23], [25] αντιμετωπίζουν άμεσα τις αδυναμίες του firmware, ενώ η κρυπτογράφηση και η ασφαλής διαχείριση επικοινωνιών που απαιτείται από το MDR [20] περιορίζει ουσιαστικά επιθέσεις τύπου MITM και sniffing. Παράλληλα, μηχανισμοί ταυτοποίησης, RBAC και ισχυρός έλεγχος πρόσβασης μειώνουν τον κίνδυνο από μη εξουσιοδοτημένες παρεμβάσεις σε ιατρικές συσκευές, ενώ η δικτυακή θωράκιση και ο διαχωρισμός δικτύων (segmentation) αντιμετωπίζουν την έκθεση των IoMT συσκευών σε ευρύτερα νοσοκομειακά δίκτυα [23], [26].

Ένα κρίσιμο εύρημα είναι ότι η αποτελεσματική ασφάλεια στα IoMT δεν επιτυγχάνεται με μεμονωμένα μέτρα, αλλά απαιτεί ολιστική και πολυεπίπεδη προσέγγιση, όπου τα πρότυπα λειτουργούν συμπληρωματικά: το MDR καθορίζει τις νομικές και λειτουργικές απαιτήσεις ασφαλείας, το ISO 14971 παρέχει το πλαίσιο για τη διαχείριση κινδύνου, η FDA προσδιορίζει τεχνικά μέτρα για ασφαλή σχεδίαση και ενημέρωση συσκευών, ενώ το NISTIR 8259A προσφέρει πρακτικές “baseline” δυνατότητες ασφάλειας για IoT και IoMT συσκευές.

Η συνολική χαρτογράφηση ευπαθειών, αντιμέτρων και προτύπων δείχνει ότι οι υφιστάμενες οδηγίες μπορούν να μειώσουν σημαντικά τους κινδύνους, υπό την προϋπόθεση ότι εφαρμόζονται συστηματικά από όλους τους εμπλεκόμενους φορείς. Η μελέτη καταλήγει ότι η ενίσχυση της ασφάλειας των IoMT συστημάτων προϋποθέτει: συνεχή παρακολούθηση μετά την κυκλοφορία (post-market surveillance), διαρκή ενημέρωση λογισμικού, ενσωμάτωση security-by-design, υιοθέτηση τεχνικών ελέγχου πρόσβασης και πλήρη εναρμόνιση με τα διεθνή πρότυπα.

Τα συμπεράσματα αυτά αξιοποιούνται στο επόμενο κεφάλαιο για την υλοποίηση και αξιολόγηση ενός προσομοιωμένου συστήματος ανίχνευσης εισβολών (Intrusion Detection System – IDS), με στόχο τη μελέτη της επίδρασης επιθέσεων αλλοίωσης δεδομένων σε περιβάλλον IoMT.

6.6 Περιβάλλον Προσομοίωσης Simul8

Στο σημείο αυτό ολοκληρώνεται το θεωρητικό σκέλος του παρόντος κεφαλαίου, στο οποίο παρουσιάστηκε το ρυθμιστικό και τεχνολογικό πλαίσιο ασφάλειας για το IoMT, καθώς και η αντιστοίχιση απαιτήσεων των προτύπων MDR, ISO 14971, FDA και NISTIR με πρακτικές τεχνικές αντιμετώπισης. Για την αξιολόγηση των επιπτώσεων επιθέσεων αλλοίωσης δεδομένων σε περιβάλλον IoMT, το επόμενο υποκεφάλαιο επικεντρώνεται στην ανάπτυξη σεναρίων προσομοίωσης μέσω του εργαλείου Simul8.

Η ενότητα που ακολουθεί, αν και βασίζεται στη θεωρία που έχει αναλυθεί, μεταβαίνει στο εφαρμοσμένο σκέλος της διπλωματικής εργασίας, παρουσιάζοντας τη δομή, τις παραδοχές και τη μεθοδολογία της προσομοίωσης, καθώς και τα σενάρια και τα αναμενόμενα αποτελέσματα.

6.6.1 Σκοπός και αντικείμενο της προσομοίωσης

Η παρούσα ενότητα επικεντρώνεται στην προσομοίωση ενός Συστήματος Ανίχνευσης Εισβολών (Intrusion Detection System – IDS), το οποίο εφαρμόζεται σε περιβάλλον συλλογής ιατρικών δεδομένων από φορητές συσκευές (wearables). Η προσομοίωση υλοποιείται με σκοπό τη μελέτη της συμπεριφοράς του συστήματος σε συνθήκες κανονικής λειτουργίας, απώλειας δεδομένων και

αλλοιωμένων μετρήσεων, οι οποίες δύνανται να προκύψουν είτε λόγω τεχνικών σφαλμάτων είτε ως αποτέλεσμα κακόβουλων επιθέσεων.

Στο πλαίσιο της παρούσας διπλωματικής εργασίας, το IDS σχεδιάστηκε βάσει κανόνων (rule-based approach), επιτρέποντας την ανίχνευση ανωμαλιών μέσω προκαθορισμένων ορίων στις τιμές ζωτικών παραμέτρων των ασθενών, όπως ο καρδιακός ρυθμός, ο κορεσμός οξυγόνου και η αρτηριακή πίεση. Η επιλογή της συγκεκριμένης προσέγγισης αποσκοπεί στη διασφάλιση πλήρους ερμηνευσιμότητας των αποφάσεων του συστήματος, καθώς και στη σαφή αντιστοίχιση κάθε ανίχνευσης με συγκεκριμένο τύπο επίθεσης ή ανωμαλίας.

Η χρήση προσομοίωσης κρίνεται ιδιαίτερα σημαντική, καθώς επιτρέπει την αξιολόγηση της λειτουργικότητας και της αποτελεσματικότητας του IDS χωρίς την ανάγκη ανάπτυξης ή χρήσης πραγματικών ιατρικών συσκευών και πραγματικών ασθενών. Παράλληλα, παρέχεται η δυνατότητα ελέγχου διαφορετικών σεναρίων αλλοίωσης δεδομένων με επαναλήψιμο και ελεγχόμενο τρόπο, ενισχύοντας την αξιοπιστία των αποτελεσμάτων.

Στόχος της προσομοίωσης δεν είναι μόνο η ανίχνευση της παρουσίας ανωμαλιών, αλλά και η κατηγοριοποίησή τους σε διαφορετικούς τύπους επιθέσεων, καθώς και η εκτίμηση της σοβαρότητάς τους. Με τον τρόπο αυτό, το προτεινόμενο σύστημα προσομοιώνει τη λειτουργία ενός IDS που θα μπορούσε να χρησιμοποιηθεί ως βασικό επίπεδο άμυνας σε υποδομές ηλεκτρονικής υγείας, αποτελώντας τη βάση για μελλοντική ενσωμάτωση πιο εξελιγμένων τεχνικών, όπως αλγορίθμων τεχνητής νοημοσύνης και μηχανικής μάθησης, για την περαιτέρω ενίσχυση της ακρίβειας ανίχνευσης.

6.2.2 Επιλογή Περιβάλλοντος

Η ανάπτυξη και εκτέλεση της προσομοίωσης πραγματοποιήθηκε με χρήση του λογισμικού SIMUL8 2024 (Student Edition), το οποίο παραχωρείται από την εταιρεία SIMUL8 Corporation για ακαδημαϊκή χρήση. Η συγκεκριμένη άδεια επιτρέπει τη χρήση του λογισμικού αποκλειστικά για εκπαιδευτικούς και ερευνητικούς σκοπούς, γεγονός που καθιστά τη χρήση του συμβατή με το αντικείμενο και τους στόχους της παρούσας διπλωματικής εργασίας.

Το SIMUL8 αποτελεί ένα ευρέως χρησιμοποιούμενο εργαλείο διακριτής προσομοίωσης γεγονότων (Discrete Event Simulation – DES), το οποίο επιτρέπει τη μοντελοποίηση και ανάλυση σύνθετων ροών διαδικασιών με τη χρήση γραφικών αντικειμένων και κανόνων λογικής απόφασης.

Η επιλογή του συγκεκριμένου περιβάλλοντος προσομοίωσης βασίστηκε στη δυνατότητά του να αναπαριστά συστήματα που παράγουν, επεξεργάζονται και δρομολογούν δεδομένα σε πραγματικό χρόνο, χαρακτηριστικό που προσομοιάζει τη λειτουργία κυβερνο-φυσικών συστημάτων και υποδομών ηλεκτρονικής υγείας. Μέσω της έννοιας των work items, το SIMUL8 επιτρέπει την αναπαράσταση μεμονωμένων οντοτήτων, όπως είναι οι μετρήσεις ασθενών από φορητές συσκευές, ενώ παράλληλα παρέχει μηχανισμούς ελέγχου ροής, χρονισμού και αποθήκευσης ενδιάμεσων αποτελεσμάτων.

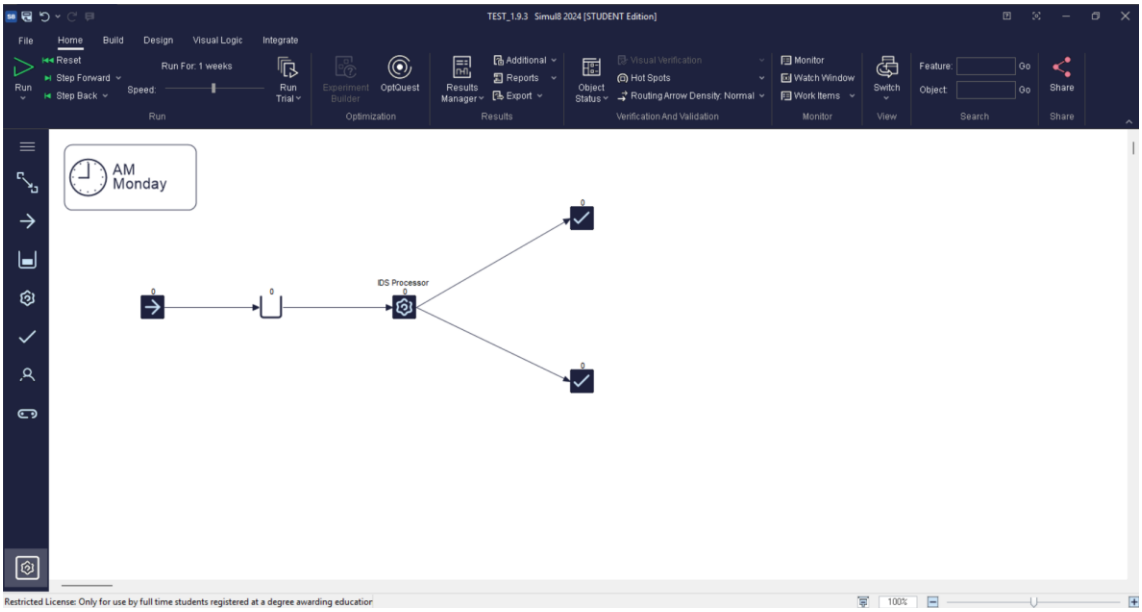
Ιδιαίτερη σημασία για την παρούσα εργασία έχει η υποστήριξη της Visual Logic, ενός ενσωματωμένου μηχανισμού κανόνων, μέσω του οποίου είναι δυνατή η υλοποίηση λογικής ανίχνευσης ανωμαλιών με βάση προκαθορισμένες συνθήκες. Η λειτουργικότητα αυτή επιτρέπει την ανάπτυξη ενός rule-based συστήματος ανίχνευσης εισβολών, στο οποίο κάθε απόφαση μπορεί να ερμηνευθεί άμεσα, στοιχείο ιδιαίτερα σημαντικό για εφαρμογές IDS σε περιβάλλοντα ηλεκτρονικής υγείας.

Επιπλέον, το περιβάλλον SIMUL8 παρέχει δυνατότητα διασύνδεσης με εξωτερικά υπολογιστικά φύλλα, επιτρέποντας την εισαγωγή πραγματικών ή συνθετικών δεδομένων αισθητήρων από αρχεία Excel. Η δυνατότητα αυτή αξιοποιήθηκε για την τροφοδότηση της προσομοίωσης με δεδομένα ασθενών, τα οποία περιλαμβάνουν τόσο φυσιολογικές τιμές όσο και περιπτώσεις ελλιπών ή

αλλοιωμένων μετρήσεων, διευκολύνοντας την αξιολόγηση της συμπεριφοράς του IDS υπό διαφορετικά σενάρια.

Αν και η έκδοση Student Edition του SIMUL8 δεν υποστηρίζει την ενσωμάτωση αλγορίθμων τεχνητής νοημοσύνης ή μηχανικής μάθησης, προσφέρει επαρκή λειτουργικότητα για την υλοποίηση και ανάλυση ενός συστήματος ανίχνευσης εισβολών βασισμένου σε κανόνες. Η επιλογή αυτή θεωρείται κατάλληλη για τους σκοπούς της παρούσας διπλωματικής, καθώς επιτρέπει τη σαφή κατανόηση και τεκμηρίωση της λογικής αποφάσεων του συστήματος, ενώ παράλληλα θέτει τις βάσεις για μελλοντική επέκταση σε πιο εξελιγμένες μεθόδους ανίχνευσης.

Στο Σχήμα 6.1 παρουσιάζεται το περιβάλλον ανάπτυξης της προσομοίωσης στο SIMUL8 2024 (Student Edition).

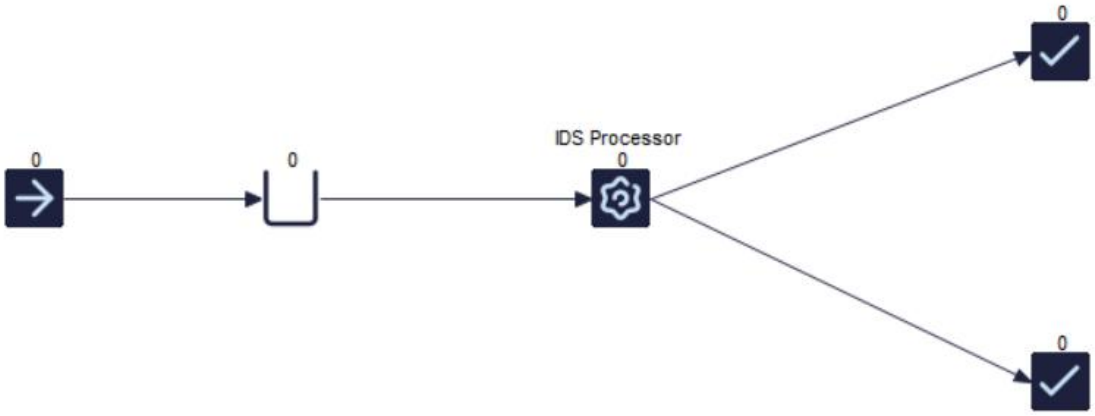


Σχήμα 6.1: Περιβάλλον ανάπτυξης προσομοίωσης στο SIMUL8 2024 (Student Edition)

6.7 Γενική Αρχιτεκτονική και Ροή της Προσομοίωσης

Η γενική αρχιτεκτονική της προσομοίωσης σχεδιάστηκε με στόχο την αναπαράσταση της ροής δεδομένων από φορητές ιατρικές συσκευές προς ένα Σύστημα Ανίχνευσης Εισβολών (Intrusion Detection System – IDS), το οποίο αξιολογεί τις μετρήσεις και αποφασίζει για την κανονική τους επεξεργασία ή την ενεργοποίηση μηχανισμών ειδοποίησης ασφάλειας. Η προσέγγιση που ακολουθήθηκε βασίζεται στη διακριτή προσομοίωση γεγονότων, όπου κάθε σύνολο μετρήσεων αντιμετωπίζεται ως ανεξάρτητη οντότητα (work item), επιτρέποντας την αναλυτική παρακολούθηση της πορείας των δεδομένων μέσα στο σύστημα.

Η ροή της προσομοίωσης αποτελείται από τέσσερα βασικά δομικά στοιχεία: το σημείο εκκίνησης (Start Point), την ουρά αναμονής (Queue), τον επεξεργαστή ανίχνευσης εισβολών (IDS Processor) και τα τελικά σημεία εξόδου (End Points). Κάθε ένα από τα στοιχεία αυτά επιτελεί διακριτό ρόλο και συμβάλλει στη σαφή οργάνωση των σταδίων εισαγωγής, επεξεργασίας και εξόδου των δεδομένων. Η συνολική αρχιτεκτονική και η μεταξύ τους διασύνδεση παρουσιάζονται στο Σχήμα 6.2.



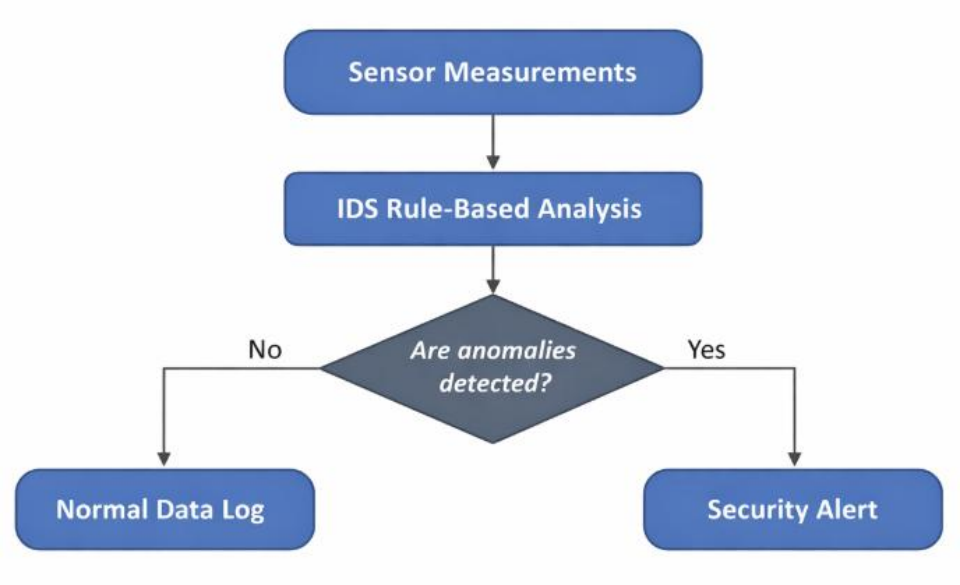
Σχήμα 6.2: Γενική αρχιτεκτονική και ροή της προσομοίωσης στο περιβάλλον Simul8

Στο πρώτο στάδιο, τα δεδομένα εισέρχονται στο σύστημα μέσω του σημείου εκκίνησης (Start Point), το οποίο αναπαριστά την παραγωγή μετρήσεων από IoMT συσκευές. Τα δεδομένα αυτά προωθούνται στη συνέχεια σε ενδιάμεσο στάδιο προσωρινής αποθήκευσης (Queque), το οποίο επιτρέπει την ομαλή διαχείριση της ροής και τη διαδοχική επεξεργασία των εισερχόμενων οντοτήτων. Η ύπαρξη ενδιάμεσου σταδίου καθιστά το μοντέλο πιο ρεαλιστικό, καθώς αντικατοπτρίζει συνθήκες όπου τα δεδομένα δεν επεξεργάζονται πάντοτε άμεσα, αλλά ενδέχεται να εμφανίζουν χρονικές καθυστερήσεις.

Στη συνέχεια, τα δεδομένα προωθούνται στον επεξεργαστή ανίχνευσης εισβολών (IDS Processor), ο οποίος αποτελεί τον πυρήνα της προσομοίωσης. Στο σημείο αυτό εφαρμόζεται η λογική ανίχνευσης ανωμαλιών, μέσω της οποίας αξιολογείται η κατάσταση των δεδομένων και λαμβάνεται απόφαση σχετικά με την παρουσία ή μη ύποπτης συμπεριφοράς. Η λειτουργία του IDS βασίζεται σε προκαθορισμένους κανόνες, επιτρέποντας τη σαφή διάκριση μεταξύ κανονικών και προβληματικών περιπτώσεων και τη διαφανή ερμηνεία των αποφάσεων του συστήματος.

Μετά την ολοκλήρωση της επεξεργασίας από το IDS, η ροή των δεδομένων διακλαδώνεται προς τα τελικά σημεία εξόδου. Τα δεδομένα που χαρακτηρίζονται ως κανονικά δρομολογούνται προς σημείο καταγραφής φυσιολογικών μετρήσεων (Normal Data Log), ενώ εκείνα που ανιχνεύονται ως ύποπτα ή αλλοιωμένα οδηγούνται προς σημείο ειδοποίησης ασφάλειας (Security Alert). Ο διαχωρισμός αυτός επιτρέπει την ανεξάρτητη ανάλυση των κανονικών και των προβληματικών περιπτώσεων και διευκολύνει την αξιολόγηση της αποτελεσματικότητας του συστήματος ανίχνευσης εισβολών.

Η λογική απόφασης του IDS, όπως εφαρμόζεται στο πλαίσιο της προσομοίωσης, μπορεί να αποτυπωθεί σχηματικά ως μια διαδικασία αξιολόγησης των δεδομένων αισθητήρων και διακλάδωσης της ροής ανάλογα με την ανίχνευση ανωμαλιών. Η εν λόγω λογική παρουσιάζεται στο Σχήμα 7.3.



Σχήμα 6.3: Λογική απόφασης του IDS κατά την επεξεργασία δεδομένων αισθητήρων

Η συνολική αρχιτεκτονική της προσομοίωσης διασφαλίζει σαφή διάκριση μεταξύ των σταδίων εισαγωγής, προσωρινής αποθήκευσης, επεξεργασίας και εξόδου των δεδομένων. Η δομή αυτή καθιστά το μοντέλο κατανοητό, επεκτάσιμο και κατάλληλο για πειραματισμό με διαφορετικά σενάρια αλλοίωσης δεδομένων, θέτοντας τις βάσεις για την αναλυτική περιγραφή των επιμέρους αντικειμένων της προσομοίωσης που ακολουθεί στις επόμενες υποενότητες.

6.7.1 Start Point – Αναλυτική Περιγραφή, Ρυθμίσεις και Λογική Εισόδου

Το Start Point αποτελεί το σημείο εισόδου των δεδομένων στην προσομοίωση και αναπαριστά τη συνεχή παραγωγή μετρήσεων από φορητές ιατρικές συσκευές (IoMT wearables). Κάθε οντότητα που δημιουργείται στο σημείο αυτό μοντελοποιεί ένα σύνολο ιατρικών μετρήσεων ασθενούς σε συγκεκριμένη χρονική στιγμή και εισάγεται στο σύστημα ως ανεξάρτητο work item.

Η λειτουργία του Start Point είναι κρίσιμη, καθώς καθορίζει:

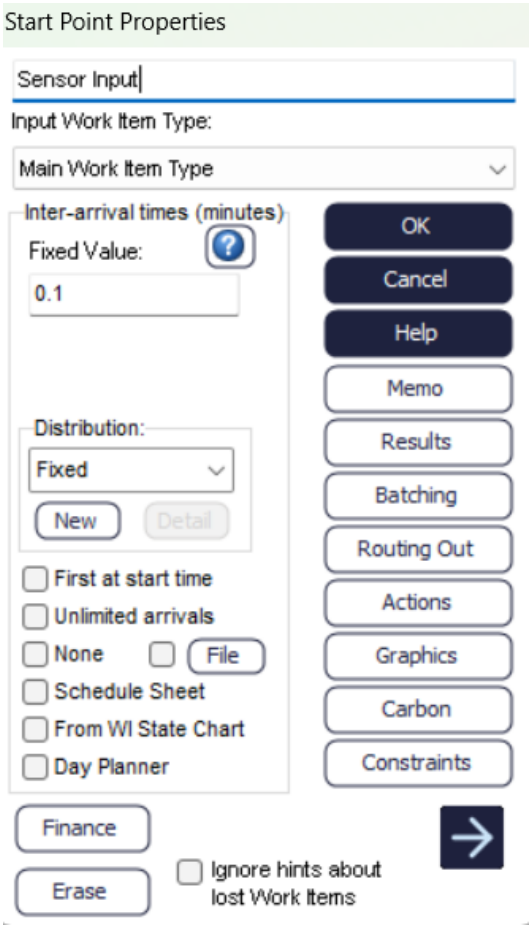
- τον ρυθμό εισαγωγής των δεδομένων,
- τα όρια και τους περιορισμούς της προσομοίωσης,
- καθώς και την αρχική κατάσταση κάθε work item πριν από την ανάλυσή του από το σύστημα ανίχνευσης εισβολών (IDS).

6.7.1.1 Ρυθμίσεις Ρυθμού Άφιξης Δεδομένων (Inter-arrival Time)

Η εισαγωγή των δεδομένων στο Start Point πραγματοποιείται με σταθερό ρυθμό άφιξης (Fixed Value) ίσο με 0.1 λεπτά, ο οποίος επιλέχθηκε ώστε να προσομοιώνει τη συνεχή και υψηλής συχνότητας παραγωγή δεδομένων από αισθητήρες IoMT. Η χρήση σταθερού ρυθμού, αντί στοχαστικής κατανομής, επιτρέπει τον πλήρη έλεγχο των πειραματικών συνθηκών και τη συγκρισιμότητα των αποτελεσμάτων μεταξύ διαφορετικών σεναρίων.

Η συγκεκριμένη ρύθμιση διευκολύνει:

- την επαναληψιμότητα της προσομοίωσης,
- τη μελέτη της συμπεριφοράς του IDS υπό αυξημένο φόρτο δεδομένων,
- την αποφυγή τυχαίων διακυμάνσεων που θα δυσχέραιναν την ερμηνεία των αποτελεσμάτων.

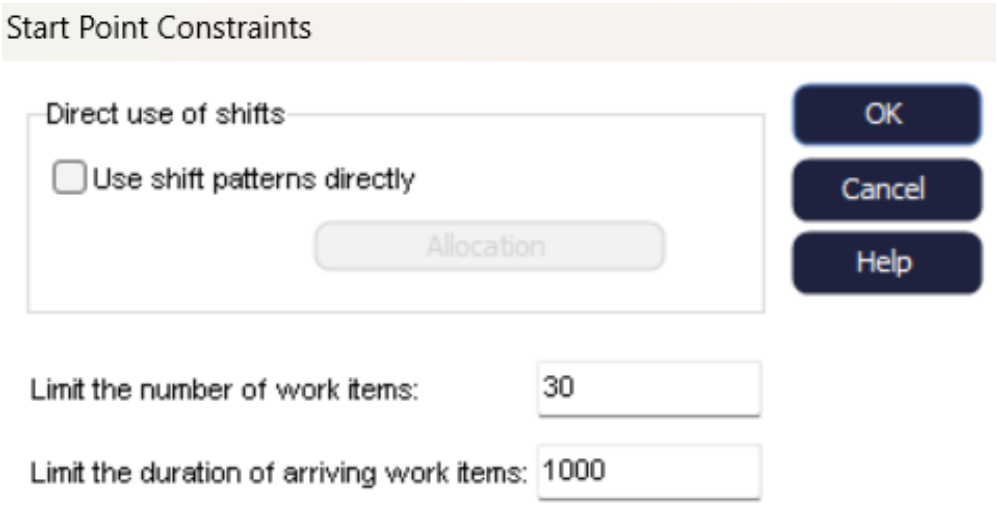


Σχήμα 6.4: Ρυθμίσεις ρυθμού άφιξης δεδομένων στο Start Point

6.7.1.2 Περιορισμοί και Έλεγχος Εκτέλεσης (Constraints)

Για τον έλεγχο της διάρκειας και της κλίμακας της προσομοίωσης εφαρμόστηκαν συγκεκριμένοι περιορισμοί στο Start Point. Συγκεκριμένα, ορίστηκε μέγιστος αριθμός work items ίσος με 30, τιμή που αντιστοιχεί στον αριθμό των γραμμών δεδομένων που διαβάζονται από το αρχείο εισόδου (spreadsheet). Με τον τρόπο αυτό διασφαλίζεται ότι κάθε γραμμή δεδομένων επεξεργάζεται ακριβώς μία φορά.

Παράλληλα, τέθηκε όριο διάρκειας άφιξης work items ίσο με 1000 μονάδες χρόνου, ώστε να αποφεύγεται η ανεξέλεγκτη ή άπειρη εκτέλεση της προσομοίωσης. Οι περιορισμοί αυτοί συμβάλλουν στη σταθερότητα του μοντέλου και στη σαφή οριοθέτηση των πειραματικών συνθηκών.



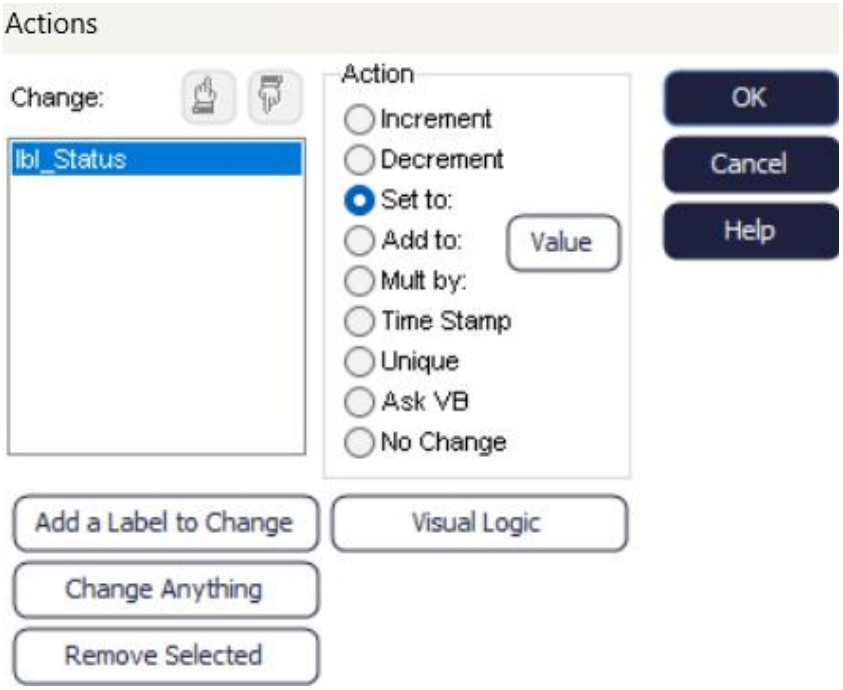
Σχήμα 6.5: Περιορισμοί πλήθους και χρονικού ορίου άφιξης work items στο Start Point

6.7.1.3 Αρχικοποίηση Κατάστασης μέσω Actions

Πριν την προώθηση των δεδομένων στο επόμενο στάδιο της προσομοίωσης, κάθε work item αρχικοποιείται μέσω της λειτουργίας Actions του Start Point. Συγκεκριμένα, χρησιμοποιείται το label lbl_Status, το οποίο λαμβάνει αρχική τιμή που δηλώνει ότι το εισερχόμενο σύνολο δεδομένων βρίσκεται σε κανονική κατάσταση.

Η αρχικοποίηση αυτή:

- εξασφαλίζει κοινό σημείο εκκίνησης για όλα τα δεδομένα,
- διευκολύνει τη μεταγενέστερη λογική δρομολόγησης,
- επιτρέπει τη σαφή διάκριση μεταξύ φυσιολογικών και ανώμαλων περιπτώσεων κατά την επεξεργασία από το IDS.



Σχήμα 6.6: Αρχικοποίηση κατάστασης work item μέσω Actions στο Start Point

6.7.1.4 Λογική Εισόδου και Ανάγνωση Δεδομένων (Visual Logic)

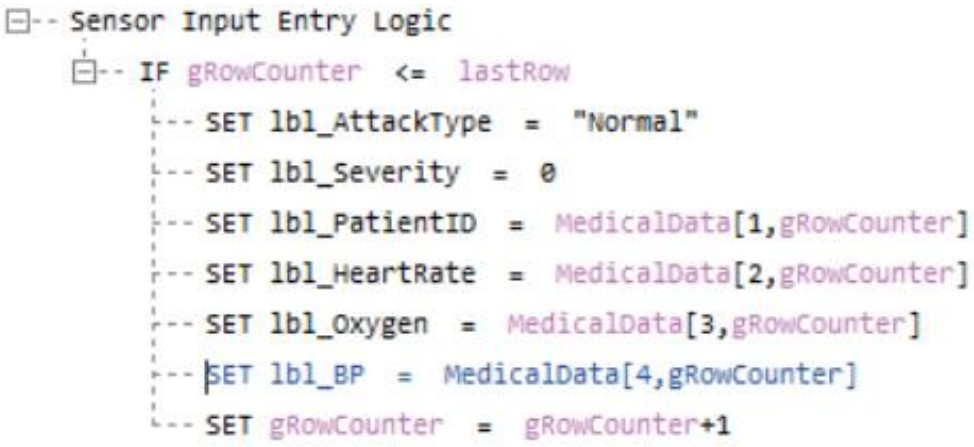
Η ανάγνωση των δεδομένων αισθητήρων από το αρχείο εισόδου (spreadsheet) υλοποιείται μέσω Visual Logic στο Start Point. Κάθε γραμμή του αρχείου αντιστοιχεί σε ένα σύνολο μετρήσεων ασθενούς και μεταφέρεται σε labels του work item, όπως το αναγνωριστικό ασθενούς, ο καρδιακός ρυθμός, ο κορεσμός οξυγόνου και η αρτηριακή πίεση.

Για τη διαχείριση της αλληλουχίας ανάγνωσης χρησιμοποιούνται global μεταβλητές, όπως ο μετρητής γραμμών και το όριο των διαθέσιμων δεδομένων, οι οποίες ορίζονται κεντρικά στο μοντέλο και αναλύονται στην επόμενη ενότητα. Επιπλέον, κατά την είσοδο κάθε work item:

- ο τύπος επίθεσης αρχικοποιείται ως Normal,
- η σοβαρότητα ορίζεται σε μηδενική τιμή,

επιτρέποντας στο IDS να αξιολογήσει στη συνέχεια αν προκύπτει απόκλιση από τη φυσιολογική λειτουργία.

Η χρήση του Visual Logic στο στάδιο εισόδου διασφαλίζει ότι τα δεδομένα εισέρχονται στο σύστημα με δομημένο και ελεγχόμενο τρόπο, προσομοιώνοντας ρεαλιστικά τη ροή μετρήσεων από IoMT συσκευές προς ένα σύστημα κυβερνοασφάλειας.



Σχήμα 6.7: Visual Logic του Start Point για ανάγνωση και αρχικοποίηση δεδομένων αισθητήρων

Οι global μεταβλητές και τα labels που χρησιμοποιούνται στη λογική εισόδου ορίζονται κεντρικά στο μοντέλο προσομοίωσης και παρουσιάζονται αναλυτικά στην επόμενη υποενότητα.

6.7.2 Global Data Items και Labels της Προσομοίωσης

Η προσομοίωση βασίζεται στη χρήση Global Data Items και Labels, τα οποία επιτρέπουν την κεντρική διαχείριση κατάστασης, τη συνεπή ανταλλαγή πληροφοριών μεταξύ των αντικειμένων της προσομοίωσης και την υλοποίηση της λογικής ανίχνευσης ανωμαλιών. Ο διαχωρισμός μεταξύ global μεταβλητών και labels είναι κρίσιμος: οι πρώτες διατηρούν συνολική κατάσταση σε επίπεδο μοντέλου, ενώ τα labels αφορούν ιδιότητες κάθε μεμονωμένου work item.

6.7.2.1 Global Data Items – Κεντρικές Μεταβλητές Προσομοίωσης

Τα Global Data Items χρησιμοποιούνται για τον έλεγχο της ροής, την καταμέτρηση συμβάντων και τη διαχείριση της ανάγνωσης δεδομένων από το αρχείο εισόδου. Οι μεταβλητές αυτές είναι προσβάσιμες από όλα τα αντικείμενα της προσομοίωσης και διασφαλίζουν συνεκτική συμπεριφορά.

A. Μεταβλητές Ελέγχου Ροής και Ανάγνωσης Δεδομένων
- gRowCounter: Μετρητής γραμμών του spreadsheet. Χρησιμοποιείται για τη σειριακή ανάγνωση των δεδομένων αισθητήρων και αυξάνεται κατά μία μονάδα με την εισαγωγή κάθε νέου work item.
- lastRow: Καθορίζει το ανώτατο όριο διαθέσιμων γραμμών στο αρχείο δεδομένων. Χρησιμοποιείται για την αποφυγή ανάγνωσης εκτός ορίων.

Οι δύο αυτές μεταβλητές εξασφαλίζουν ότι κάθε σύνολο δεδομένων εισάγεται ακριβώς μία φορά και ότι η προσομοίωση παραμένει ευθυγραμμισμένη με το περιεχόμενο του αρχείου εισόδου.

B. Μεταβλητές Καταμέτρησης και Κατάστασης
- countAlert: Καταγράφει το πλήθος των περιπτώσεων που ταξινομούνται ως ανωμαλίες/επιθέσεις από το IDS.
- countNormal: Καταγράφει το πλήθος των κανονικών περιπτώσεων.
- gAnomCount: Συνολικός μετρητής ανωμαλιών, χρήσιμος για στατιστική ανάλυση.
- Count_Attacks_Detected: Συγκεντρωτικός δείκτης ανιχνευμένων επιθέσεων.
- Flag_Tampered: Λογική μεταβλητή που υποδηλώνει αν έχει εντοπιστεί αλλοίωση δεδομένων.

Οι μεταβλητές αυτές επιτρέπουν την ποσοτική αξιολόγηση της απόδοσης του IDS και τη σύγκριση μεταξύ διαφορετικών σεναρίων προσομοίωσης.

Όπως φαίνεται στο Σχήμα 6.8, στη στήλη On Reset απεικονίζονται οι αρχικές τιμές των global μεταβλητών, οι οποίες επαναφέρονται αυτόματα κάθε φορά που ξεκινά ή επανεκκινείται η προσομοίωση. Η λειτουργία αυτή διασφαλίζει ότι κάθε εκτέλεση ξεκινά από κοινή και ελεγχόμενη αρχική κατάσταση, επιτρέποντας τη συγκρισιμότητα των αποτελεσμάτων μεταξύ διαφορετικών σεναρίων.

Information Store

Global Data Item	On Reset	Current Value
Recent		
Numbers		
Count_Attacks_Detected	0	0
Day Duration		480
Flag_Tampered	0	0
Graph Sync Interval		5
Overhead Cost		0
Overhead Revenue		0
Results Collection Period		2399,4999
Simulation Time		0
Warm Up Period		0
countAlert	0	0
countNormal	0	0
gAnomCount	0	0
gRowCounter	2	2
lastRow	31	31

Σχήμα 6.8: Global Data Items της προσομοίωσης στο SIMUL8 (Information Store)

6.7.2.2 Spreadsheet / Arrays – Δομή Δεδομένων Εισόδου

Τα δεδομένα αισθητήρων IoMT αποθηκεύονται σε πίνακα τύπου Spreadsheet/Array με όνομα MedicalData. Κάθε γραμμή αντιστοιχεί σε ένα χρονικό στιγμιότυπο μετρήσεων ασθενούς και περιλαμβάνει:

- Αναγνωριστικό ασθενούς,
- Καρδιακό ρυθμό,
- Κορεσμό οξυγόνου,
- Αρτηριακή πίεση.

Η δομή αυτή επιτρέπει την εύκολη παραμετροποίηση της προσομοίωσης και την επανάληψη πειραμάτων με διαφορετικά σύνολα δεδομένων.

Για λόγους σαφήνειας παρουσιάζεται στο Σχήμα 6.9 ενδεικτικό απόσπασμα του πίνακα δεδομένων. Το πλήρες σύνολο δεδομένων βρίσκεται στο Παράρτημα Α.

	A	B	C	D
1	**ID Patient**	**HeartRate**	**Oxygen**	**BloodPressure**
2	1	76	99	129
3	2	89	98	125
4	3	84	98	129
5	4	80	98	121
6	5	77	99	117
7	6	89	98	121
8	7	82	98	125
9	8	88	98	124
10	9	80	99	116

Σχήμα 6.9: Ενδεικτικό απόσπασμα του πίνακα MedicalData με μετρήσεις IoMT δεδομένων

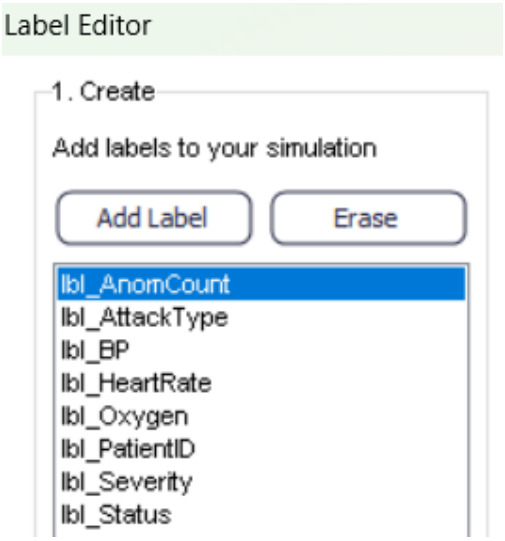
6.7.2.3 Labels – Ιδιότητες Work Items

Τα Labels χρησιμοποιούνται για την αποθήκευση ιδιοτήτων που συνοδεύουν κάθε work item καθ' όλη τη διάρκεια της επεξεργασίας του από το IDS.

A. Labels Ιατρικών Μετρήσεων
- lbl_PatientID
- lbl_HeartRate
- lbl_Oxygen
- lbl_BP

Τα labels αυτά τροφοδοτούν άμεσα τη λογική ανίχνευσης ανωμαλιών, καθώς συγκρίνονται με προκαθορισμένα όρια φυσιολογικών τιμών.

B. Labels Ασφάλειας και Κατάστασης
- lbl_AttackType: Υποδηλώνει τον τύπο επίθεσης ή Normal σε περίπτωση κανονικής λειτουργίας.
- lbl_Severity: Εκφράζει τη σοβαρότητα της ανιχνευθείσας ανωμαλίας.
- lbl_Status: Καθορίζει τη συνολική κατάσταση του work item (κανονικό ή ανώμαλο) και χρησιμοποιείται για τη δρομολόγηση της ροής προς τα τελικά σημεία εξόδου.



Σχήμα 6.10: Ορισμός labels για τα work items στο SIMUL8

6.7.2.4 Σχέση Global Data Items και Labels με τη Λογική IDS

Ο συνδυασμός global μεταβλητών και labels επιτρέπει:

- τον διαχωρισμό μεταξύ συνολικής κατάστασης συστήματος και μεμονωμένων περιστατικών,
- την επεξεργασία κάθε work item ως ανεξάρτητου συμβάντος,
- τη συλλογή στατιστικών αποτελεσμάτων χωρίς απώλεια πληροφορίας.

Η αρχιτεκτονική αυτή καθιστά το μοντέλο επεκτάσιμο, επιτρέποντας μελλοντική ενσωμάτωση πιο σύνθετων τεχνικών ανίχνευσης, όπως αλγορίθμων μηχανικής μάθησης ή τεχνητής νοημοσύνης.

Στις επόμενες υποενότητες παρουσιάζεται η επεξεργασία των work items από τα επιμέρους αντικείμενα της προσομοίωσης, ξεκινώντας από την ουρά αναμονής (Queue) και καταλήγοντας στον μηχανισμό ανίχνευσης εισβολών (IDS Processor).

6.7.3 Queue – Ρόλος και Ρυθμίσεις

Η ουρά αναμονής (Queue) παρεμβάλλεται μεταξύ του σημείου εισόδου (Start Point) και του μηχανισμού ανίχνευσης εισβολών (IDS Processor) και χρησιμοποιείται ως ενδιάμεσο στάδιο προσωρινής αποθήκευσης των εισερχόμενων work items. Ο ρόλος της δεν σχετίζεται με την ανάλυση ασφάλειας, αλλά με τη ρεαλιστική μοντελοποίηση της ροής δεδομένων σε συστήματα IoMT, όπου η επεξεργασία δεν πραγματοποιείται πάντα άμεσα με την άφιξη των μετρήσεων.

Η ύπαρξη της ουράς επιτρέπει:

- την απορρόφηση αιχμών εισερχόμενων δεδομένων,
- την ομαλή διαχείριση της ροής όταν ο ρυθμός άφιξης υπερβαίνει στιγμιαία τον ρυθμό επεξεργασίας,
- τη διατήρηση της σταθερότητας της προσομοίωσης χωρίς απώλεια δεδομένων.

Στο πλαίσιο της παρούσας εργασίας, η Queue χρησιμοποιείται κυρίως για λόγους αρχιτεκτονικής πληρότητας, ώστε το μοντέλο να προσεγγίζει τη λειτουργία πραγματικών συστημάτων ηλεκτρονικής υγείας, στα οποία παρεμβάλλονται μηχανισμοί προσωρινής αποθήκευσης (buffers, message queues). Δεν εφαρμόζονται ειδικοί κανόνες προτεραιότητας ή περιορισμοί χωρητικότητας, καθώς η ανάλυση δεν εστιάζει στη συμφόρηση αλλά στη λογική ανίχνευσης ανωμαλιών.

Η παρουσία της ουράς καθιστά το μοντέλο επεκτάσιμο, επιτρέποντας μελλοντικά τη μελέτη σεναρίων αυξημένου φόρτου, καθυστερήσεων ή επιθέσεων άρνησης υπηρεσίας (Denial of Service – DoS), χωρίς να απαιτείται ανασχεδιασμός της βασικής ροής της προσομοίωσης.

6.8 Μηχανισμός Ανίχνευσης Ανωμαλιών IDS και Κατηγοριοποίηση Επιθέσεων

Στην παρούσα ενότητα περιγράφεται αναλυτικά ο μηχανισμός ανίχνευσης ανωμαλιών που υλοποιήθηκε στο περιβάλλον προσομοίωσης SIMUL8 2024 (Student Edition), καθώς και η λογική κατηγοριοποίησης των ανιχνευόμενων περιστατικών σε διαφορετικούς τύπους επιθέσεων. Σε αντίθεση με τις προηγούμενες ενότητες, οι οποίες επικεντρώθηκαν στη δομή και τη ροή της προσομοίωσης, εδώ δίνεται έμφαση στη λογική απόφασης του συστήματος ανίχνευσης εισβολών (IDS).

Ο μηχανισμός λειτουργεί ως ένα κανόνα-βασισμένο Σύστημα Ανίχνευσης Εισβολών (Rule-Based IDS), το οποίο επεξεργάζεται σε πραγματικό χρόνο τα δεδομένα που λαμβάνονται από αισθητήρες φορητών ιατρικών συσκευών. Τα δεδομένα αυτά αφορούν κρίσιμες φυσιολογικές παραμέτρους, όπως ο καρδιακός ρυθμός (Heart Rate), ο κορεσμός οξυγόνου στο αίμα (Oxygen Saturation) και η αρτηριακή πίεση (Blood Pressure), οι οποίες αποτελούν βασικούς δείκτες τόσο της κλινικής κατάστασης του ασθενούς όσο και της ακεραιότητας των δεδομένων.

Η επιλογή κανόνα-βασισμένης προσέγγισης επιτρέπει τη σαφή ερμηνεία κάθε απόφασης του IDS, καθώς κάθε ανίχνευση ανωμαλίας μπορεί να συσχετιστεί άμεσα με συγκεκριμένη παραβίαση προκαθορισμένων κανόνων.

6.8.1 Κριτήρια Ανίχνευσης Ανωμαλιών

Για κάθε work item που εισέρχεται στον κόμβο IDS Processor, πραγματοποιείται έλεγχος βάσει συγκεκριμένων κριτηρίων ανίχνευσης, τα οποία έχουν σχεδιαστεί ώστε να εντοπίζουν τόσο τεχνικές ανωμαλίες όσο και πιθανές επιθέσεις αλλοίωσης δεδομένων.

Α. Μη διαθέσιμα ή ελλιπή δεδομένα (Missing Data)

Όταν όλες οι μετρούμενες παράμετροι (Heart Rate, Oxygen, Blood Pressure) λαμβάνουν μηδενική τιμή, το σύστημα θεωρεί ότι τα δεδομένα απουσιάζουν ή δεν έχουν ληφθεί ορθά. Η περίπτωση αυτή αντιμετωπίζεται ως ανωμαλία τύπου Missing Data, καθώς ενδέχεται να οφείλεται σε αστοχία αισθητήρων, διακοπή επικοινωνίας ή σκόπιμη αλλοίωση δεδομένων.

Β. Ακραίες ή μη φυσιολογικές τιμές

Επιπλέον, το IDS ελέγχει αν οι μετρούμενες τιμές υπερβαίνουν προκαθορισμένα φυσιολογικά όρια, τα οποία λειτουργούν ως κανόνες ανίχνευσης (detection rules). Ενδεικτικά, ανιχνεύονται ανωμαλίες όταν ισχύει κάποια από τις ακόλουθες συνθήκες:

- Heart Rate < 40 ή Heart Rate > 180
- Oxygen Saturation < 85 ή Oxygen Saturation > 100
- Blood Pressure < 60 ή Blood Pressure > 180

Τα όρια αυτά βασίζονται σε ενδεικτικές φυσιολογικές τιμές που χρησιμοποιούνται στην κλινική πρακτική και επιτρέπουν την ανίχνευση αποκλίσεων που δεν είναι συμβατές με φυσιολογική λειτουργία.

Κάθε παραβίαση των παραπάνω κανόνων καταγράφεται ως ανωμαλία και οδηγεί σε αύξηση του μετρητή lbl_AnomCount, ο οποίος χρησιμοποιείται για τη συνολική αποτίμηση της συμπεριφοράς του συστήματος ανίχνευσης.

Στις επόμενες υποενότητες παρουσιάζεται η διαδικασία κατηγοριοποίησης των ανιχνευόμενων ανωμαλιών σε τύπους επιθέσεων, καθώς και η αντιστοίχισή τους με επίπεδα σοβαρότητας και μηχανισμούς δρομολόγησης της ροής

6.8.2 Υλοποίηση Κανόνων Ανίχνευσης και Λογική Απόφασης στο IDS Processor

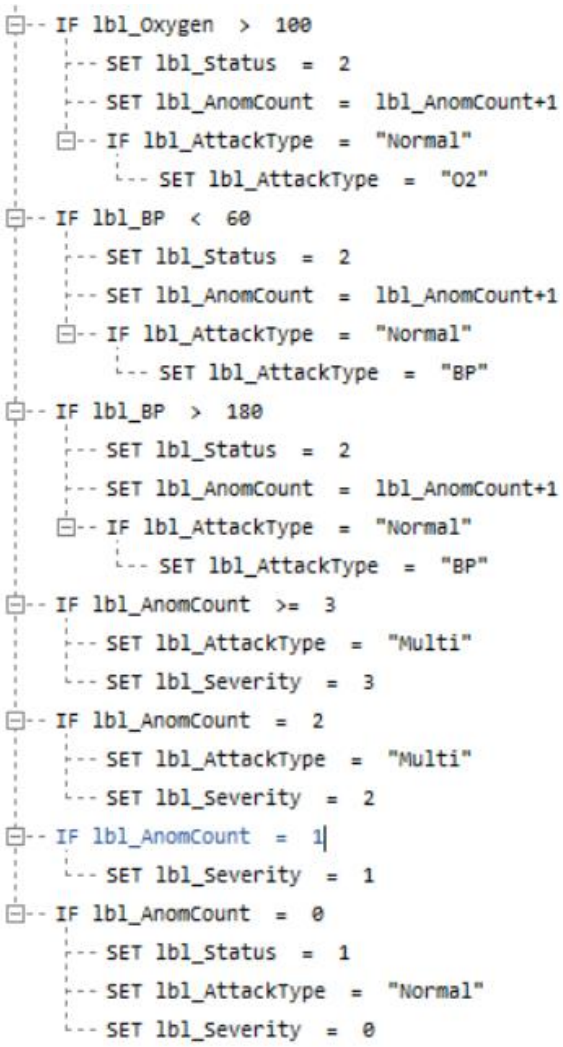
Η υλοποίηση των κανόνων ανίχνευσης ανωμαλιών πραγματοποιείται στον κόμβο IDS Processor, ο οποίος αποτελεί τον πυρήνα της λογικής απόφασης του συστήματος ανίχνευσης εισβολών. Η επεξεργασία των δεδομένων υλοποιείται μέσω Visual Logic, το οποίο εκτελείται κατά την είσοδο κάθε work item στον κόμβο, στο στάδιο Routing In – After Loading Work. Με τον τρόπο αυτό, οι κανόνες ανίχνευσης εφαρμόζονται άμεσα μετά τη φόρτωση των δεδομένων, πριν από οποιαδήποτε περαιτέρω δρομολόγηση της ροής.

Στο σημείο αυτό, το σύστημα εφαρμόζει τους κανόνες ανίχνευσης που περιγράφηκαν στην προηγούμενη υποενότητα. Συγκεκριμένα, για κάθε work item:

- ελέγχεται η ύπαρξη ελλιπών ή μη διαθέσιμων δεδομένων (Missing Data),
- αξιολογούνται οι τιμές των φυσιολογικών παραμέτρων σε σχέση με τα προκαθορισμένα όρια,
- σε περίπτωση παραβίασης οποιουδήποτε κανόνα, το περιστατικό χαρακτηρίζεται ως ανωμαλία.

Κατά την εκτέλεση της λογικής ανίχνευσης ενημερώνονται τα αντίστοιχα labels του work item, όπως ο τύπος επίθεσης (lbl_AttackType), το επίπεδο σοβαρότητας (lbl_Severity) και η συνολική κατάσταση (lbl_Status). Τα labels αυτά καθορίζουν τη μετέπειτα δρομολόγηση της ροής και την τελική κατηγοριοποίηση του περιστατικού.

```
IDS Processor Route In After Logic
    SET lbl_Status = 1
    SET lbl_AnomCount = 0
    SET lbl_AttackType = "Normal"
    SET lbl_Severity = 0
    IF lbl_HeartRate = 0
        IF lbl_Oxygen = 0
            IF lbl_BP = 0
                SET lbl_Status = 2
                SET lbl_AttackType = "Missing"
                SET lbl_Severity = 3
                SET lbl_AnomCount = 3
    IF lbl_AttackType <> "Missing"
        IF lbl_HeartRate < 40
            SET lbl_Status = 2
            SET lbl_AnomCount = lbl_AnomCount+1
            IF lbl_AttackType = "Normal"
                SET lbl_AttackType = "HR"
        IF lbl_HeartRate > 180
            SET lbl_Status = 2
            SET lbl_AnomCount = lbl_AnomCount+1
            IF lbl_AttackType = "Normal"
                SET lbl_AttackType = "HR"
        IF lbl_Oxygen < 85
            SET lbl_Status = 2
            SET lbl_AnomCount = lbl_AnomCount+1
            IF lbl_AttackType = "Normal"
                SET lbl_AttackType = "O2"
```



Σχήμα 6.11: Visual Logic του IDS Processor για την εφαρμογή κανόνων ανίχνευσης ανωμαλιών.

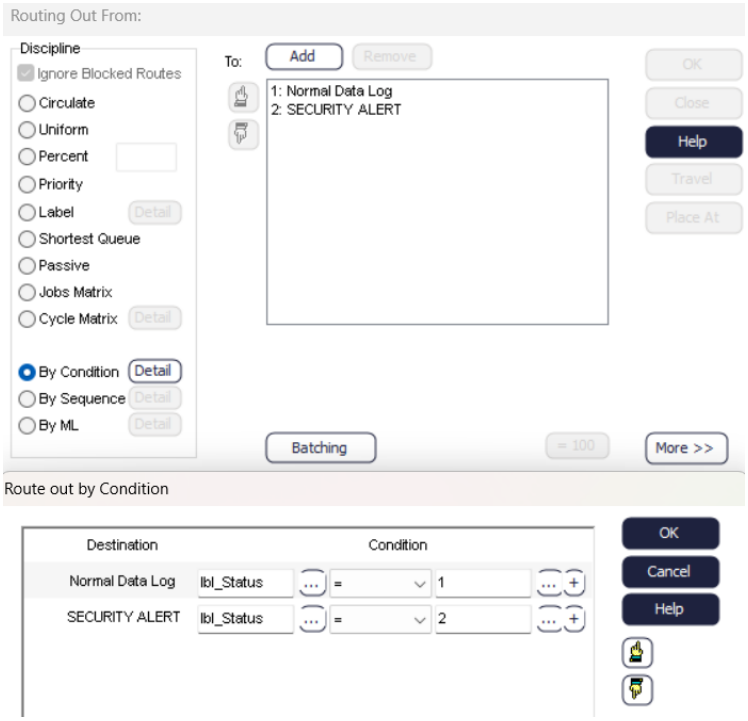
(*Ο κώδικας παρουσιάζεται σε δύο τμήματα λόγω έκτασης, για καλυτερη αναγνωσιμότητα.)*

Μετά την ολοκλήρωση της ανάλυσης από τον IDS Processor, η ροή των δεδομένων διαχωρίζεται μέσω μηχανισμού Routing Out by Condition, ο οποίος βασίζεται στην τιμή του label lbl_Status.

Συγκεκριμένα:

- work items με lbl_Status = 1 θεωρούνται κανονικά και δρομολογούνται προς το τελικό σημείο εξόδου Normal Data Log, όπου καταγράφονται ως φυσιολογικές μετρήσεις,
- work items με lbl_Status = 2 χαρακτηρίζονται ως ανώμαλα και δρομολογούνται προς το τελικό σημείο Security Alert, ενεργοποιώντας μηχανισμό ειδοποίησης ασφάλειας.

Ο διαχωρισμός αυτός επιτρέπει τη σαφή διάκριση μεταξύ φυσιολογικών και προβληματικών περιστατικών και διευκολύνει την ανεξάρτητη ανάλυση των δύο κατηγοριών.



Σχήμα 6.12: Routing Out by Condition με βάση το label κατάστασης (lbl_Status)

6.8.3 Εκτίμηση Σοβαρότητας (Severity Level)

Η σοβαρότητα κάθε περιστατικού προσδιορίζεται με βάση τον συνολικό αριθμό ανωμαλιών (lbl_AnomCount):

- Severity = 0 → Κανονική λειτουργία (Normal)
- Severity = 1 → Μία ανωμαλία (χαμηλής επικινδυνότητας)
- Severity = 2 → Δύο ανωμαλίες (μέτριας επικινδυνότητας)
- Severity = 3 → Τρεις ή περισσότερες ανωμαλίες (υψηλής επικινδυνότητας)

Η κλιμάκωση αυτή επιτρέπει την ποσοτικοποίηση της επικινδυνότητας και μπορεί να αξιοποιηθεί σε μελλοντικές επεκτάσεις του συστήματος για αυτοματοποιημένες αντιδράσεις ή ειδοποιήσεις.

Η αντιστοίχιση αριθμού ανωμαλιών, τύπου επίθεσης και επιπέδου σοβαρότητας συνοψίζεται στον παρακάτω πίνακα.

Πίνακας 6.8.3: Αντιστοίχιση ανωμαλιών, τύπων επίθεσης και επιπέδων σοβαρότητας

Πλήθος ανωμαλιών (lbl_AnomCount)	**Συνθήκη δεδομένων**	**Attack Type**	**Severity**
0	Όλες οι τιμές εντός ορίων	Normal	0
1	Μια ανωμαλία (HR ή O2 ή BP)	HP/O2/BP	1
2	Δύο ταυτόχρονες ανωμαλίες	Multi	2
≥3	Πολλαπλές ανωμαλίες	Multi	3
Όλες οι τιμές = 0	Έλλειψη Δεδομένων	Missing	3

6.8.4 Παραγωγή Αποτελεσμάτων και Καταγραφή

Τα αποτελέσματα της ανάλυσης καταγράφονται σε αρχείο αποτελεσμάτων (Flow File), το οποίο περιλαμβάνει για κάθε ασθενή:

- Αναγνωριστικό ασθενούς
- Τιμές αισθητήρων
- Τύπο επίθεσης
- Επίπεδο σοβαρότητας
- Συνολικό αριθμό ανωμαλιών

Η δομημένη αυτή καταγραφή διασφαλίζει τη δυνατότητα επαναληψιμότητας των πειραμάτων και τη σύγκριση εναλλακτικών σεναρίων αλλοίωσης δεδομένων. Η καταγραφή σε δομημένη μορφή επιτρέπει τη μεταγενέστερη στατιστική ανάλυση, τη σύγκριση σεναρίων και την αξιολόγηση της απόδοσης του IDS.

6.9 Αποτελέσματα Προσομοίωσης και Ανάλυση

6.9.1 Συλλογή και μορφή αποτελεσμάτων

Μετά την ολοκλήρωση της προσομοίωσης, τα αποτελέσματα καταγράφονται σε εξωτερικό αρχείο μορφής CSV μέσω του μηχανισμού εξαγωγής του SIMUL8.

Για κάθε Work Item (ασθενή) καταγράφονται τα εξής πεδία:

- Χρόνος διέλευσης (Time)
- Κατάσταση συστήματος (lbl_Status)
- Αναγνωριστικό ασθενούς (lbl_PatientID)
- Τιμές ζωτικών ενδείξεων (HeartRate, Oxygen, BloodPressure)
- Τύπος επίθεσης (lbl_AttackType)
- Επίπεδο σοβαρότητας (lbl_Severity)
- Πλήθος ανωμαλιών (lbl_AnomCount)

Η δομή αυτή επιτρέπει την πλήρη ιχνηλασιμότητα κάθε Work Item, από τις αρχικές μετρήσεις αισθητήρων έως την τελική απόφαση του συστήματος IDS.

Η καταγραφή των αποτελεσμάτων πραγματοποιείται μέσω των τελικών σημείων εξόδου της προσομοίωσης, όπου τα κανονικά περιστατικά δρομολογούνται στο Normal Data Log, ενώ τα ανιχνευμένα ανώμαλα περιστατικά καταλήγουν στο Security Alert. Τα δεδομένα από αμφότερα τα endpoints εξάγονται σε ενιαίο αρχείο CSV, επιτρέποντας τη συγκριτική ανάλυση φυσιολογικών και προβληματικών περιπτώσεων.

6.9.2 Κατηγοριοποίηση περιστατικών

Με βάση τα δεδομένα εισόδου και τη λογική κανόνων που υλοποιήθηκε στον IDS Processor, οι περιπτώσεις ταξινομούνται στις ακόλουθες κατηγορίες:

- Normal: Όλες οι μετρήσεις εντός προκαθορισμένων ορίων
- Missing: Απουσία τιμών (HeartRate = 0, Oxygen = 0, BP = 0)
- HR: Ανωμαλία καρδιακού ρυθμού
- O2: Ανωμαλία κορεσμού οξυγόνου
- BP: Ανωμαλία αρτηριακής πίεσης
- Multi: Ταυτόχρονη εμφάνιση δύο ή περισσότερων ανωμαλιών

Η κατηγοριοποίηση αυτή επιτρέπει τη συστηματική αναπαράσταση διαφορετικών σεναρίων ανωμαλιών, τόσο λόγω κυβερνοεπιθέσεων όσο και λόγω σφαλμάτων αισθητήρων, διευκολύνοντας την ανάλυση της συμπεριφοράς του IDS.

6.9.3 Ανάλυση επιπέδων σοβαρότητας (Severity Analysis)

Σε αντίθεση με την ενότητα 6.8.3, όπου ορίστηκε η λογική υπολογισμού του severity, στην παρούσα ενότητα αναλύεται η κατανομή των επιπέδων σοβαρότητας στα πειραματικά σενάρια. Η ανάλυση των επιπέδων σοβαρότητας επιτρέπει την αποτίμηση της έντασης και της επικινδυνότητας των ανιχνευμένων περιστατικών στο σύνολο των σεναρίων προσομοίωσης, με βάση τη συσσώρευση ανωμαλιών που καταγράφονται από το IDS. Μέσω της τιμής lbl_Severity, κάθε περιστατικό ταξινομείται δυναμικά, επιτρέποντας τη διάκριση μεταξύ απλών αποκλίσεων και κρίσιμων καταστάσεων.

Σε σενάρια πλήρους απουσίας δεδομένων ή ταυτόχρονης εμφάνισης πολλαπλών ανωμαλιών, παρατηρούνται υψηλότερα επίπεδα σοβαρότητας, γεγονός που επιβεβαιώνει τη ρεαλιστική λειτουργία του IDS σε συνθήκες αυξημένου κινδύνου. Η πληροφορία αυτή είναι ιδιαίτερα κρίσιμη για μελλοντική χρήση του συστήματος σε περιβάλλοντα υγείας, όπου η προτεραιοποίηση περιστατικών αποτελεί βασικό λειτουργικό ζητούμενο.

6.9.4 Πειραματική Αξιολόγηση με Σενάρια Αλλοίωσης Δεδομένων

Στην παρούσα δοκιμή, το σύστημα αξιολογήθηκε υπό συνθήκες μερικής και ολικής αλλοίωσης δεδομένων αισθητήρων, προκειμένου να εξεταστεί η ορθότητα της λογικής ανίχνευσης του συστήματος IDS.

Το σύνολο των δεδομένων περιλάμβανε:

- κανονικές μετρήσεις,
- περιπτώσεις πλήρους απουσίας δεδομένων (Missing),
- μεμονωμένες ανωμαλίες σε έναν αισθητήρα,
- καθώς και συνδυασμένες ανωμαλίες σε δύο ή περισσότερους αισθητήρες (Multi).

Όπως παρατηρείται στα αποτελέσματα, οι περιπτώσεις όπου όλες οι μετρήσεις είχαν μηδενικές τιμές (HeartRate = 0, Oxygen = 0, BloodPressure = 0) ταξινομήθηκαν ως επιθέσεις τύπου Missing, με μέγιστη σοβαρότητα (Severity = 3) και αριθμό ανωμαλιών ίσο με τρεις.

Οι μεμονωμένες αποκλίσεις από τα αποδεκτά όρια αναγνωρίστηκαν ως επιθέσεις τύπου HR, O2 ή BP αντίστοιχα, με χαμηλή σοβαρότητα (Severity = 1), ενώ οι ταυτόχρονες αποκλίσεις σε πολλαπλές παραμέτρους ταξινομήθηκαν ως επιθέσεις τύπου Multi, με αυξημένο επίπεδο σοβαρότητας.

Τα αποτελέσματα επιβεβαιώνουν ότι το σύστημα IDS λειτουργεί ορθά, διακρίνοντας τόσο το είδος όσο και την ένταση των επιθέσεων, ακόμα και σε περιπτώσεις συνδυασμένων αλλοιώσεων.

11	0	0	0
12	0	0	0
13	182	105	131
14	110	91	183
15	76	82	125
16	185	113	58
17	39	86	117
18	184	107	190
19	79	80	125

Σχήμα 6.13: Παράδειγμα αλλοιωμένων δεδομένων αισθητήρων

ID	Time	lbl_Status	lbl_PatientID	lbl_HeartRate	lbl_Oxygen	lbl_BP	lbl_AttackType	lbl_Severity	lbl_AnomCount
1	390642	2	11	0	0	0	Missing	3	3
2	398751	2	12	0	0	0	Missing	3	3
3	41302	2	13	182	105	131	Multi	2	2
4	421995	2	14	110	91	183	BP	1	1
5	433489	2	15	76	82	125	O2	1	1
6	440208	2	16	185	113	58	Multi	3	3
7	45002	2	17	39	86	117	HR	1	1
8	459539	2	18	184	107	190	Multi	3	3
9	467287	2	19	79	80	125	O2	1	1
10	475686	2	20	0	0	0	Missing	3	3

Σχήμα 6.14: Αποτελέσματα ταξινόμησης επιθέσεων από το IDS

Τα αποτελέσματα της δοκιμής συνοψίζονται στον Πίνακα 7.5, ο οποίος παρουσιάζει τόσο τις τιμές εισόδου όσο και την τελική απόφαση του IDS.

Πίνακας 6.9.4: Συνοπτική απεικόνιση φυσιολογικών και αλλοιωμένων μετρήσεων και της αντίστοιχης ταξινόμησης από το IDS

PatientID	**HR**	**O2**	**BP**	**AttackType**	**Severity**	**AnomCount**
3	84	98	129	Normal	0	0
11	0	0	0	Missing	3	3
13	182	105	131	Multi	2	2
14	110	91	183	BP	1	1
15	76	82	125	O2	1	1
17	39	86	117	HR	1	1
18	184	107	190	Multi	3	3

Όπως προκύπτει, το σύστημα αναγνωρίζει με συνέπεια τις διαφορετικές κατηγορίες αλλοίωσης, αποδίδοντας επίπεδα σοβαρότητας ανάλογα με το πλήθος και τον τύπο των ανωμαλιών.

Η παρούσα πειραματική αξιολόγηση επικεντρώνεται σε ένα αντιπροσωπευτικό σενάριο αλλοίωσης δεδομένων, το οποίο έχει σχεδιαστεί ώστε να καλύπτει όλες τις λογικές περιπτώσεις που προβλέπονται από το κανονοβασισμένο μοντέλο IDS.

Δεδομένου ότι το σύστημα βασίζεται σε στατικούς κανόνες και προκαθορισμένα όρια ανίχνευσης, η επανάληψη της προσομοίωσης με διαφορετικές κατανομές αλλοιωμένων δεδομένων δεν μεταβάλλει τη συμπεριφορά του συστήματος. Ως εκ τούτου, μία ολοκληρωμένη δοκιμή, η οποία περιλαμβάνει φυσιολογικές μετρήσεις, μεμονωμένες ανωμαλίες, πολλαπλές ταυτόχρονες αλλοιώσεις και πλήρη απουσία δεδομένων, κρίνεται επαρκής για την επαλήθευση της ορθότητας της λογικής ανίχνευσης.

6.9.5 Παρατηρήσεις από τα αποτελέσματα

Από την ανάλυση των αποτελεσμάτων της προσομοίωσης προκύπτουν τα ακόλουθα:

1. Το σύστημα ανίχνευσης εντοπίζει με επιτυχία όλες τις περιπτώσεις αλλοίωσης ή απουσίας δεδομένων, επιβεβαιώνοντας την ορθότητα της λογικής ανίχνευσης.
2. Οι περιπτώσεις Missing Data αντιμετωπίζονται ως κρίσιμα περιστατικά, γεγονός που αντανακλά τη σημασία της ακεραιότητας των δεδομένων σε ιατρικά συστήματα.
3. Οι συνδυαστικές ανωμαλίες οδηγούν σε αυξημένα επίπεδα σοβαρότητας, προσομοιώνοντας ρεαλιστικά σενάρια σύνθετων επιθέσεων ή πολλαπλών σφαλμάτων.
4. Η ροή της προσομοίωσης παραμένει σταθερή και προβλέψιμη, επιβεβαιώνοντας τη σωστή σχεδίαση των κανόνων ανίχνευσης και της αρχιτεκτονικής του συστήματος.

6.9.6 Περιορισμοί της προσομοιωσης

Η παρούσα προσομοίωση βασίζεται σε ένα σύστημα ανίχνευσης εισβολών (IDS) κανόνων (rule-based), το οποίο αξιοποιεί προκαθορισμένα όρια και λογικές συνθήκες για την αναγνώριση ανωμαλιών σε δεδομένα φορητών ιατρικών συσκευών. Η προσέγγιση αυτή προσφέρει διαφάνεια στη λήψη αποφάσεων και άμεση ερμηνευσιμότητα των αποτελεσμάτων, ωστόσο συνοδεύεται από συγκεκριμένους περιορισμούς.

Πρώτον, οι κανόνες ανίχνευσης έχουν στατικό χαρακτήρα: τα όρια για τις παραμέτρους HeartRate, Oxygen και BloodPressure ορίζονται εκ των προτέρων και δεν προσαρμόζονται κατά τη διάρκεια της εκτέλεσης. Ως αποτέλεσμα, δεν λαμβάνονται δυναμικά υπόψη διαφοροποιήσεις πληθυσμών, ατομικά χαρακτηριστικά ασθενών ή μακροχρόνιες τάσεις που ενδέχεται να επηρεάζουν τη “φυσιολογική” συμπεριφορά των μετρήσεων.

Δεύτερον, η υλοποίηση πραγματοποιήθηκε στο περιβάλλον SIMUL8 2024 (Student Edition), το οποίο είναι επαρκές για την προσομοίωση λογικών κανόνων και ροών διαδικασίας, αλλά δεν στοχεύει στην ενσωμάτωση ή εκπαίδευση μοντέλων μηχανικής μάθησης/τεχνητής νοημοσύνης στο πλαίσιο της συγκεκριμένης έκδοσης. Κατά συνέπεια, η ανίχνευση περιορίζεται σε ντετερμινιστικούς κανόνες και όχι σε προσεγγίσεις που θα μπορούσαν να εντοπίζουν άγνωστα πρότυπα επιθέσεων μέσω μάθησης από δεδομένα.

Τρίτον, το μοντέλο αποτελεί αφαιρετική αναπαράσταση πραγματικών υποδομών IoMT, εστιάζοντας σε επιλεγμένα σενάρια αλλοίωσης με στόχο τον έλεγχο και την αξιολόγηση της λογικής του IDS., χωρίς να αναπαριστά πλήρως όλες τις παραμέτρους ενός παραγωγικού περιβάλλοντος (π.χ. ετερογένεια συσκευών, θόρυβος αισθητήρων, μεταβαλλόμενα προφίλ ασθενών, σύνθετες αλληλεξαρτήσεις συστημάτων).

Συνολικά, οι παραπάνω περιορισμοί δεν αναιρούν τη χρησιμότητα της προσομοίωσης, αλλά αποσαφηνίζουν το πλαίσιο εγκυρότητας των αποτελεσμάτων: η παρούσα υλοποίηση τεκμηριώνει με σαφή τρόπο τη λειτουργία ενός κανονοκεντρικού IDS και τη συμπεριφορά του σε συγκεκριμένες κατηγορίες ανωμαλιών.

6.10 Σύνοψη

Στο παρόν κεφάλαιο παρουσιάστηκε η υλοποίηση και η αξιολόγηση ενός συστήματος ανίχνευσης εισβολών (Intrusion Detection System – IDS) για δεδομένα φορητών ιατρικών συσκευών, μέσω προσομοίωσης στο περιβάλλον SIMUL8 2024 (Student Edition). Αρχικά, περιγράφηκε το περιβάλλον προσομοίωσης και η αρχιτεκτονική της ροής, η οποία περιλαμβάνει την είσοδο δεδομένων αισθητήρων, τη λογική επεξεργασίας του IDS και τα τελικά σημεία καταγραφής φυσιολογικών και ύποπτων περιστατικών.

Στη συνέχεια, αναλύθηκε η λογική ανίχνευσης που βασίζεται σε προκαθορισμένους κανόνες και όρια για τις παραμέτρους HeartRate, Oxygen και BloodPressure, επιτρέποντας την ταξινόμηση των δεδομένων σε φυσιολογικά ή αλλοιωμένα. Το σύστημα είναι σε θέση να διακρίνει μεμονωμένες ανωμαλίες, πλήρη απουσία δεδομένων (Missing), καθώς και ταυτόχρονες αλλοιώσεις σε πολλαπλούς αισθητήρες (Multi), αποδίδοντας αντίστοιχα επίπεδα σοβαρότητας.

Η πειραματική αξιολόγηση πραγματοποιήθηκε μέσω αντιπροσωπευτικών σεναρίων αλλοίωσης δεδομένων, καλύπτοντας όλες τις λογικές περιπτώσεις που προβλέπει το μοντέλο. Τα αποτελέσματα επιβεβαίωσαν την ορθότητα και τη συνέπεια της λογικής ανίχνευσης, καθώς το IDS κατηγοριοποίησε επιτυχώς τόσο το είδος όσο και την ένταση των επιθέσεων, ακόμη και σε περιπτώσεις συνδυασμένων ανωμαλιών.

Συνολικά, το κεφάλαιο τεκμηριώνει ότι η προτεινόμενη προσομοιωτική προσέγγιση αποτελεί αξιόπιστη βάση για τη μελέτη της κυβερνοασφάλειας σε φορητές ιατρικές συσκευές IoMT,

προσφέροντας ένα ελεγχόμενο και επεκτάσιμο πλαίσιο αξιολόγησης, ικανό να υποστηρίξει περαιτέρω ερευνητική και τεχνολογική εξέλιξη.

Για λόγους πληρότητας και τεκμηρίωσης της προσομοιωτικής διαδικασίας, στο Παράρτημα Α παρατίθενται τα αρχικά δεδομένα εισόδου που χρησιμοποιήθηκαν στην προσομοίωση. Στο Παράρτημα Β παρουσιάζονται ενδεικτικές καταγραφές κανονικής λειτουργίας του συστήματος, οι οποίες λειτουργούν ως σημείο αναφοράς για τη σύγκριση με τα σενάρια αλλοίωσης δεδομένων. Τέλος, στο Παράρτημα Γ αποτυπώνονται χαρακτηριστικές καταγραφές ανιχνευμένων συμβάντων ασφαλείας, τεκμηριώνοντας τη συμπεριφορά του συστήματος ανίχνευσης εισβολών υπό συνθήκες αλλοίωσης δεδομένων.

Κεφάλαιο 7ο: Συμπεράσματα και Μελλοντικές Επεκτάσεις

7.1 Συνολικά Συμπεράσματα της Διπλωματικής Εργασίας

Η παρούσα διπλωματική εργασία επικεντρώθηκε στην κυβερνοασφάλεια του οικοσυστήματος Internet of Medical Things (IoMT), με έμφαση στις φορητές ιατρικές συσκευές και στους κινδύνους που απορρέουν από τη συνεχή διασύνδεσή τους με δίκτυα και πληροφοριακά συστήματα υγείας. Κεντρικός στόχος της εργασίας ήταν η συστηματική μελέτη των απειλών, των επιθέσεων και των μηχανισμών προστασίας που αφορούν τα IoMT συστήματα, καθώς και η πρακτική αποτύπωση των επιπτώσεων της κυβερνοασφάλειας μέσω προσομοίωσης.

Σε θεωρητικό επίπεδο, η εργασία ανέδειξε την πολυπλοκότητα των IoMT συστημάτων και την ανάγκη υιοθέτησης μιας ολιστικής προσέγγισης ασφάλειας, η οποία δεν περιορίζεται μόνο στα τεχνολογικά μέτρα, αλλά περιλαμβάνει τη διαχείριση κινδύνου, τη συμμόρφωση με κανονιστικά πλαίσια και την ασφάλεια καθ' όλο τον κύκλο ζωής των ιατρικών συσκευών. Μέσα από τη μελέτη διεθνών προτύπων και κανονισμών, όπως τα MDR, ISO 14971, ISO/IEC 27001, FDA και NIST, κατέστη σαφές ότι η αποτελεσματική κυβερνοασφάλεια στο IoMT απαιτεί συνδυασμό τεχνικών, οργανωτικών και κανονιστικών μέτρων.

Σε πρακτικό επίπεδο, η εργασία προχώρησε στην υλοποίηση και αξιολόγηση ενός Συστήματος Ανίχνευσης Εισβολών (Intrusion Detection System – IDS) βασισμένου σε κανόνες, μέσω προσομοίωσης στο περιβάλλον SIMUL8. Η προσομοίωση επέτρεψε την αναπαράσταση της ροής δεδομένων από φορητές ιατρικές συσκευές, την εφαρμογή λογικής ανίχνευσης ανωμαλιών και την κατηγοριοποίηση περιστατικών αλλοίωσης δεδομένων σε διαφορετικές κατηγορίες, όπως μεμονωμένες ανωμαλίες, πλήρης απουσία δεδομένων και ταυτόχρονες αλλοιώσεις σε πολλαπλούς αισθητήρες. Τα πειραματικά αποτελέσματα επιβεβαίωσαν την ορθότητα και τη συνέπεια της λογικής ανίχνευσης, καθώς το IDS κατόρθωσε να αναγνωρίσει τόσο το είδος όσο και την ένταση των επιθέσεων, αποδίδοντας αντίστοιχα επίπεδα σοβαρότητας.

Συνολικά, η διπλωματική εργασία πέτυχε τη σύνδεση της θεωρητικής ανάλυσης, των κανονιστικών απαιτήσεων και της πρακτικής αξιολόγησης σε ένα ενιαίο και συνεκτικό πλαίσιο μελέτης της κυβερνοασφάλειας στο IoMT. Παράλληλα, αναδείχθηκαν συγκεκριμένοι περιορισμοί της προσέγγισης, οι οποίοι αποτέλεσαν τη βάση για την πρόταση μελλοντικών επεκτάσεων και βελτιώσεων, οι οποίες αναλύονται στη συνέχεια του κεφαλαίου. Η προτεινόμενη προσομοιωτική προσέγγιση συνιστά μια αξιόπιστη και ερμηνεύσιμη βάση για την κατανόηση των κινδύνων και των μηχανισμών άμυνας σε φορητές ιατρικές συσκευές, υπογραμμίζοντας τη σημασία της έγκαιρης ανίχνευσης ανωμαλιών σε περιβάλλοντα υψηλής κρισιμότητας, όπως ο τομέας της υγείας.

7.2 Περιορισμοί και Διδάγματα της Προσέγγισης

Η παρούσα διπλωματική εργασία, αν και πέτυχε την επίτευξη των στόχων που τέθηκαν, ανέδειξε ορισμένους περιορισμούς που σχετίζονται τόσο με τη φύση της επιλεγμένης μεθοδολογίας όσο και με το χρησιμοποιούμενο προσομοιωτικό περιβάλλον. Η αναγνώριση των περιορισμών αυτών είναι κρίσιμη, καθώς συμβάλλει στην ορθότερη ερμηνεία των αποτελεσμάτων και στη διαμόρφωση ουσιαστικών διδαγμάτων για μελλοντική έρευνα.

Ένας βασικός περιορισμός αφορά τη χρήση κανονοβασισμένης (rule-based) λογικής ανίχνευσης ανωμαλιών στο σύστημα IDS. Η προσέγγιση αυτή βασίζεται σε προκαθορισμένα όρια και στατικούς κανόνες για τις παραμέτρους Heart Rate, Oxygen και Blood Pressure, γεγονός που καθιστά το σύστημα διαφανές και ερμηνεύσιμο. Ωστόσο, η στατική φύση των κανόνων περιορίζει την ικανότητα

του συστήματος να προσαρμόζεται σε δυναμικά μεταβαλλόμενα πρότυπα δεδομένων, διαφοροποιήσεις πληθυσμών ή νέες και άγνωστες μορφές επιθέσεων.

Επιπλέον, η προσομοίωση υλοποιήθηκε σε ελεγχόμενο περιβάλλον, με τη χρήση αντιπροσωπευτικών αλλά περιορισμένων σεναρίων αλλοίωσης δεδομένων. Αν και τα σενάρια αυτά καλύπτουν τις βασικές λογικές περιπτώσεις που προβλέπονται από το μοντέλο ανίχνευσης, δεν αποτυπώνουν πλήρως την πολυπλοκότητα και τη στοχαστικότητα πραγματικών οικοσυστημάτων IoMT, όπως θόρυβο αισθητήρων, ασύγχρονες ροές δεδομένων ή απρόβλεπτες αλληλεπιδράσεις μεταξύ συσκευών και δικτύων.

Παράλληλα, η χρήση του προσομοιωτικού περιβάλλοντος SIMUL8 (Student Edition) δεν υποστηρίζει την ενσωμάτωση και εκπαίδευση αλγορίθμων μηχανικής μάθησης. Ο περιορισμός αυτός επηρέασε συνειδητά τη μεθοδολογική επιλογή της εργασίας, δίνοντας έμφαση στη διαφάνεια και την επαναληψιμότητα της λογικής ανίχνευσης, εις βάρος της προσαρμοστικότητας και της αυτόματης μάθησης από δεδομένα.

Παρά τους παραπάνω περιορισμούς, η εργασία προσέφερε σημαντικά διδάγματα. Κατέδειξε ότι τα κανονοβασισμένα συστήματα ανίχνευσης ανωμαλιών μπορούν να αποτελέσουν αξιόπιστη αρχική γραμμή άμυνας σε περιβάλλοντα υψηλής κρισιμότητας, όπως ο τομέας της υγείας, όπου η ερμηνευσιμότητα και η συμμόρφωση με κανονιστικά πλαίσια είναι καθοριστικής σημασίας. Επιπλέον, ανέδειξε τη σημασία της πειραματικής αξιολόγησης μέσω προσομοίωσης ως εργαλείου κατανόησης της συμπεριφοράς συστημάτων ασφάλειας, πριν από την υλοποίησή τους σε πραγματικά περιβάλλοντα.

Συνολικά, οι περιορισμοί και τα διδάγματα που προκύπτουν από την παρούσα προσέγγιση δεν αναιρούν τη συνεισφορά της εργασίας, αλλά αντίθετα προσδιορίζουν με σαφήνεια τα όρια εφαρμογής της και ενισχύουν την ορθή ερμηνεία των αποτελεσμάτων, δημιουργώντας ένα δομημένο πλαίσιο κατανόησης της προτεινόμενης λύσης.

7.3 Μελλοντικές Επεκτάσεις της Διπλωματικής Εργασίας

7.3.1 Επισκόπηση σύγχρονων τεχνικών άμυνας με Τεχνητή Νοημοσύνη και Μηχανική Μάθηση

Στο πλαίσιο της παρούσας διπλωματικής εργασίας, το σύστημα ανίχνευσης εισβολών που υλοποιήθηκε βασίζεται σε κανόνες (rule-based IDS), προσφέροντας υψηλή ερμηνευσιμότητα, προβλέψιμη συμπεριφορά και σαφή αντιστοίχιση ανιχνευόμενων ανωμαλιών με συγκεκριμένες συνθήκες απόφασης. Ωστόσο, η σύγχρονη βιβλιογραφία αναδεικνύει ότι, σε πιο σύνθετα και δυναμικά περιβάλλοντα Internet of Medical Things (IoMT), εξετάζεται ολοένα και περισσότερο η αξιοποίηση τεχνικών Τεχνητής Νοημοσύνης (Artificial Intelligence – AI) και Μηχανικής Μάθησης (Machine Learning – ML) ως συμπληρωματική ή εναλλακτική προσέγγιση ανίχνευσης επιθέσεων.

Οι Sommer και Paxson [28] επισημαίνουν ότι, παρότι οι τεχνικές μηχανικής μάθησης παρουσιάζουν θεωρητικά πλεονεκτήματα στην ανίχνευση πολύπλοκων και άγνωστων επιθέσεων, η πρακτική τους εφαρμογή σε συστήματα ανίχνευσης εισβολών συνοδεύεται από σημαντικές προκλήσεις, όπως η έλλειψη επαρκώς επισημασμένων δεδομένων, η μεταβολή της κανονικής συμπεριφοράς με την πάροδο του χρόνου (concept drift) και η περιορισμένη ερμηνευσιμότητα των αποφάσεων. Για τον λόγο αυτό, τα rule-based και υβριδικά συστήματα IDS εξακολουθούν να θεωρούνται ιδιαίτερα κατάλληλα για κρίσιμα περιβάλλοντα, όπου η διαφάνεια και η προβλεψιμότητα των αποφάσεων αποτελούν βασικές απαιτήσεις.

Σε θεωρητικό επίπεδο, η ανίχνευση ανωμαλιών μέσω τεχνικών μηχανικής μάθησης έχει μελετηθεί εκτενώς, με προσεγγίσεις που περιλαμβάνουν στατιστικές μεθόδους, αλγορίθμους ομαδοποίησης (clustering), ταξινόμησης και απόστασης [29]. Οι μέθοδοι αυτές επιτρέπουν τον εντοπισμό

αποκλίσεων από την αναμενόμενη συμπεριφορά, χωρίς την ανάγκη ρητού ορισμού κανόνων, ωστόσο απαιτούν προσεκτική προσαρμογή στο εκάστοτε πεδίο εφαρμογής.

Πιο πρόσφατες μελέτες εστιάζουν στην εφαρμογή τεχνικών βαθιάς μάθησης (Deep Learning) σε περιβάλλοντα IoT και IoMT. Ενδεικτικά, η εργασία των Alimian et al. [30] παρουσιάζει ένα σύστημα ανίχνευσης εισβολών βασισμένο σε επαναλαμβανόμενα νευρωνικά δίκτυα (Deep Recurrent Neural Networks), το οποίο αξιολογείται μέσω προσομοίωσης και επιδεικνύει βελτιωμένη ικανότητα ανίχνευσης σύνθετων επιθέσεων. Παράλληλα, οι ίδιοι οι συγγραφείς αναγνωρίζουν περιορισμούς που σχετίζονται με το υπολογιστικό κόστος, την ανάγκη εκπαίδευσης σε αντιπροσωπευτικά δεδομένα και τη δυσκολία ερμηνείας των αποφάσεων του μοντέλου.

Στον τομέα της υγειονομικής περίθαλψης, η βιβλιογραφία αναδεικνύει ότι η ασφάλεια των IoMT συστημάτων δεν περιορίζεται μόνο στην ανίχνευση εισβολών, αλλά επεκτείνεται και σε ζητήματα προστασίας δεδομένων, ελέγχου πρόσβασης και ιδιωτικότητας. Η μελέτη των Yang et al. [31] παρουσιάζει ένα πλαίσιο ασφαλούς αποθήκευσης και προσαρμοστικού ελέγχου πρόσβασης σε έξυπνα συστήματα υγείας, υπογραμμίζοντας την ανάγκη πολυεπίπεδων μηχανισμών ασφάλειας σε περιβάλλοντα υψηλής κρισιμότητας.

Συνολικά, η βιβλιογραφία καταδεικνύει ότι οι τεχνικές Τεχνητής Νοημοσύνης και Μηχανικής Μάθησης αποτελούν μια ιδιαίτερα υποσχόμενη κατεύθυνση για την ενίσχυση των συστημάτων ανίχνευσης εισβολών σε IoMT περιβάλλοντα. Ωστόσο, η εφαρμογή τους απαιτεί προσεκτική αξιολόγηση, ειδικά σε κρίσιμα συστήματα υγείας, όπου η ερμηνευσιμότητα, η αξιοπιστία και η συμμόρφωση με κανονιστικά πλαίσια παραμένουν καθοριστικοί παράγοντες. Στο πλαίσιο αυτό, η παρούσα διπλωματική εργασία θέτει μια σταθερή και ερμηνεύσιμη βάση rule-based ανίχνευσης, η οποία μπορεί να λειτουργήσει ως σημείο αναφοράς ή συνδυασμού με πιο εξελιγμένες τεχνικές σε μελλοντική έρευνα.

7.3.2 Μηχανική Μάθηση για ανίχνευση ανωμαλιών σε δεδομένα φορητών ιατρικών συσκευών

Τα δεδομένα που παράγονται από φορητές ιατρικές συσκευές χαρακτηρίζονται από συνεχή ροή, χρονική εξάρτηση και υψηλό βαθμό ετερογένειας. Μετρήσεις όπως ο καρδιακός ρυθμός (Heart Rate), ο κορεσμός οξυγόνου στο αίμα (Oxygen Saturation) και η αρτηριακή πίεση (Blood Pressure) παρουσιάζουν φυσιολογικές διακυμάνσεις, οι οποίες διαφοροποιούνται σημαντικά μεταξύ διαφορετικών ασθενών, αλλά και για τον ίδιο ασθενή σε διαφορετικές χρονικές στιγμές. Η ιδιαιτερότητα αυτή καθιστά δύσκολη την αποκλειστική χρήση στατικών κανόνων ανίχνευσης και έχει οδηγήσει τη βιβλιογραφία στη διερεύνηση τεχνικών μηχανικής μάθησης για την ανίχνευση ανωμαλιών.

Σε αντίθεση με τα rule-based συστήματα, τα οποία βασίζονται σε προκαθορισμένα όρια και κανόνες, οι μέθοδοι μηχανικής μάθησης μπορούν θεωρητικά να προσαρμόζονται σε πολύπλοκα πρότυπα συμπεριφοράς και να εντοπίζουν αποκλίσεις που δεν έχουν οριστεί ρητά εκ των προτέρων [29]. Ωστόσο, όπως επισημαίνουν οι Sommer και Paxson [28], η εφαρμογή τέτοιων μεθόδων σε συστήματα ανίχνευσης εισβολών συνοδεύεται από σημαντικές προκλήσεις, κυρίως λόγω της έλλειψης αξιόπιστων και πλήρως επισημασμένων δεδομένων, καθώς και της περιορισμένης ερμηνευσιμότητας των αποφάσεων.

Στον χώρο του IoMT, η ανίχνευση ανωμαλιών μέσω μηχανικής μάθησης έχει μελετηθεί με τη χρήση τόσο παραδοσιακών όσο και βαθύτερων μοντέλων. Σύμφωνα με την επισκόπηση των Chandola et al. [29], μέθοδοι όπως τα Isolation Forests και οι Autoencoders έχουν χρησιμοποιηθεί για τον εντοπισμό ανωμαλιών σε πολυδιάστατα δεδομένα αισθητήρων, χωρίς την ανάγκη ρητής γνώσης όλων των τύπων επιθέσεων. Ωστόσο, η αξιοπιστία των αποτελεσμάτων εξαρτάται άμεσα από την ποιότητα και την αντιπροσωπευτικότητα των δεδομένων εκπαίδευσης.

Πιο πρόσφατα, προσεγγίσεις βαθιάς μάθησης έχουν αξιοποιηθεί για την ανάλυση χρονικών σειρών σε IoT και IoMT περιβάλλοντα. Η εργασία των Alimian et al. [30] παρουσιάζει ένα σύστημα ανίχνευσης εισβολών βασισμένο σε επαναλαμβανόμενα νευρωνικά δίκτυα, το οποίο εκμεταλλεύεται τη χρονική συσχέτιση των δεδομένων αισθητήρων για τη βελτίωση της ακρίβειας ανίχνευσης. Παρά τα θετικά αποτελέσματα, οι συγγραφείς τονίζουν ότι τα μοντέλα αυτά απαιτούν αυξημένο υπολογιστικό κόστος και είναι λιγότερο κατάλληλα για περιβάλλοντα με αυστηρούς περιορισμούς πόρων, όπως πολλές φορητές ιατρικές συσκευές.

Επιπλέον, σε περιβάλλοντα υγείας, η ανίχνευση ανωμαλιών δεν μπορεί να εξετάζεται απομονωμένα από ζητήματα ασφάλειας δεδομένων και ελέγχου πρόσβασης. Οι Yang et al. [31] αναδεικνύουν την ανάγκη συνδυασμού τεχνικών ανίχνευσης ανωμαλιών με μηχανισμούς προστασίας ιδιωτικότητας και προσαρμοστικού ελέγχου πρόσβασης, ώστε να διασφαλίζεται η ακεραιότητα και η εμπιστευτικότητα των ιατρικών δεδομένων.

Συνολικά, η μηχανική μάθηση προσφέρει σημαντικές δυνατότητες για την ανίχνευση σύνθετων και άγνωστων ανωμαλιών σε δεδομένα φορητών ιατρικών συσκευών. Ωστόσο, οι περιορισμοί που σχετίζονται με την ερμηνευσιμότητα, τις απαιτήσεις εκπαίδευσης και τους υπολογιστικούς πόρους καθιστούν αναγκαία την προσεκτική αξιολόγηση της καταλληλότητάς της σε κρίσιμα IoMT περιβάλλοντα. Στο πλαίσιο αυτό, η rule-based προσέγγιση που υιοθετείται στην παρούσα εργασία παρέχει ένα ελεγχόμενο και επαληθεύσιμο σημείο αναφοράς, πάνω στο οποίο μπορούν να ενσωματωθούν πιο εξελιγμένες τεχνικές σε μελλοντικές επεκτάσεις.

7.3.3 Υβριδικά Συστήματα Ανίχνευσης (Rule-based και Machine Learning)

Μία από τις πλέον υποσχόμενες κατευθύνσεις για τη μελλοντική εξέλιξη συστημάτων ανίχνευσης εισβολών στο οικοσύστημα IoMT αφορά την ανάπτυξη υβριδικών προσεγγίσεων, οι οποίες συνδυάζουν τα πλεονεκτήματα της κανονοβασισμένης (rule-based) λογικής με τη δυναμική προσαρμοστικότητα των τεχνικών μηχανικής μάθησης. Στην παρούσα διπλωματική εργασία υλοποιήθηκε κανονοκεντρικό IDS, ωστόσο η βιβλιογραφία αναδεικνύει ότι η υβριδική αρχιτεκτονική αποτελεί φυσική επέκταση τέτοιων συστημάτων όταν απαιτείται ανίχνευση πιο σύνθετων ή μη προβλεπόμενων προτύπων επιθέσεων.

Όπως επισημαίνουν οι Sommer και Paxson [28], τα μοντέλα μηχανικής μάθησης στη δικτυακή ανίχνευση μπορούν να εντοπίσουν ανωμαλίες που δεν περιγράφονται εύκολα με στατικούς κανόνες, αλλά η πρακτική τους αξιοποίηση απαιτεί προσοχή λόγω κινδύνων όπως η υπερπροσαρμογή, οι ψευδείς συναγερμοί και η δυσκολία ερμηνείας. Παράλληλα, η ανασκόπηση των Chandola et al. [29] συνοψίζει ότι οι μέθοδοι anomaly detection είναι αποτελεσματικές σε περιβάλλοντα με πολύπλοκη συμπεριφορά, αλλά η αξιοπιστία τους εξαρτάται ισχυρά από την ποιότητα των δεδομένων και τον ορθό ορισμό του “φυσιολογικού” προτύπου.

Στο IoMT, η ανάγκη για ερμηνευσιμότητα και για σαφή χαρτογράφηση αποφάσεων (π.χ. ώστε να τεκμηριώνονται συμβάντα ασφάλειας ή να υποστηρίζονται διαδικασίες αξιολόγησης κινδύνου) καθιστά ιδιαίτερα χρήσιμη τη διατήρηση ενός κανονοβασισμένου πυρήνα, στον οποίο μπορούν να ενσωματώνονται ML μηχανισμοί ως συμπληρωματικές μονάδες ανίχνευσης. Επιπλέον, λύσεις όπως privacy-preserving και self-adaptive μηχανισμοί αποθήκευσης/ελέγχου πρόσβασης σε smart IoT healthcare πλαίσια δείχνουν ότι η προσαρμοστικότητα και η ασφάλεια μπορούν να συνδυαστούν με κατάλληλες αρχιτεκτονικές επιλογές [31].

Συνεπώς, μία ρεαλιστική μελλοντική κατεύθυνση είναι η ανάπτυξη υβριδικού IDS, όπου: (α) οι κανόνες διατηρούνται για τις κρίσιμες και καλά ορισμένες περιπτώσεις (π.χ. όρια ζωτικών ενδείξεων ή συνθήκες “Missing”), ενώ (β) ML μοντέλα χρησιμοποιούνται επικουρικά για την αναγνώριση πιο σύνθετων προτύπων αποκλίσεων ή επιθέσεων που δεν αποτυπώνονται πλήρως με κανόνες. Η

προσέγγιση αυτή μπορεί να ενισχύσει την ανθεκτικότητα και την προσαρμοστικότητα του συστήματος, χωρίς να θυσιάζεται η απαιτούμενη διαφάνεια σε εφαρμογές υγείας.

7.3.4 Επέκταση της προσομοίωσης σε πραγματικά δεδομένα και real-time περιβάλλοντα

Μία ουσιαστική κατεύθυνση μελλοντικής επέκτασης της παρούσας διπλωματικής εργασίας αφορά τη μετάβαση από το προσομοιωμένο περιβάλλον σε ροές πραγματικών δεδομένων και σε real-time λειτουργία. Στην υφιστάμενη προσέγγιση, η προσομοίωση στο SIMUL8 αξιοποιεί προ-καταγεγραμμένες μετρήσεις (ή συνθετικά σενάρια αλλοίωσης) ώστε να ελεγχθεί η ορθότητα και η συνέπεια της κανονοβασισμένης λογικής του IDS. Σε πραγματικές συνθήκες, η συλλογή μετρήσεων από φορητές ιατρικές συσκευές πραγματοποιείται ως συνεχής ροή (stream), με χρονική συσχέτιση, μεταβαλλόμενη ποιότητα σήματος και δυναμικές αλλαγές στο προφίλ του χρήστη.

Για να υποστηριχθεί real-time αξιολόγηση, απαιτείται διασύνδεση με ενδιάμεσες υποδομές όπως gateways, message brokers ή cloud πλατφόρμες, ώστε τα δεδομένα να μεταφέρονται με ελεγχόμενο τρόπο προς τον μηχανισμό ανάλυσης. Παράλληλα, η real-time λειτουργία εισάγει πρόσθετες απαιτήσεις, όπως διαχείριση καθυστερήσεων (latency), χειρισμός ελλιπών/ασυνεχών μετρήσεων, και μηχανισμοί ελέγχου εγκυρότητας και ακεραιότητας σε επίπεδο ροής.

Επιπλέον, η αξιολόγηση με πραγματικά δεδομένα διευκολύνει τη μελέτη πιο σύνθετων και ρεαλιστικών παραγόντων, όπως ο θόρυβος αισθητήρων, οι διαφορές μεταξύ ασθενών, οι μεταβολές λόγω δραστηριότητας, καθώς και η συνύπαρξη πολλών συσκευών και υπηρεσιών στο ίδιο οικοσύστημα. Με αυτόν τον τρόπο, η προσομοίωση μπορεί να εξελιχθεί από "έλεγχο λογικής" σε πλαίσιο πειραματικής επικύρωσης (validation) για μηχανισμούς ανίχνευσης, καταγραφής συμβάντων και αντίδρασης σε περιστατικά ασφάλειας, σε συνθήκες που προσεγγίζουν περισσότερο την πραγματική λειτουργία IoMT συστημάτων.

Συνολικά, η επέκταση σε real-time και πραγματικά δεδομένα μπορεί να ενισχύσει τη γενικευσιμότητα των συμπερασμάτων της διπλωματικής και να μετατρέψει την υλοποίηση σε πιο άμεσο υπόβαθρο για πρακτικές εφαρμογές παρακολούθησης ασθενών και αξιολόγησης κυβερνοασφάλειας σε περιβάλλοντα υγείας.

7.3.5 Προοπτικές για μελλοντική έρευνα και πρακτική εφαρμογή

Οι μελλοντικές επεκτάσεις που παρουσιάστηκαν στις προηγούμενες υποενότητες αναδεικνύουν ότι η παρούσα εργασία μπορεί να λειτουργήσει ως σταθερή βάση για περαιτέρω ερευνητικό και πρακτικό έργο στον χώρο της κυβερνοασφάλειας σε IoMT περιβάλλοντα. Η μετάβαση προς υβριδικά συστήματα ανίχνευσης, η αξιοποίηση τεχνικών μηχανικής μάθησης και η επέκταση της προσομοίωσης σε real-time ροές δεδομένων αποτελούν κατευθύνσεις που μπορούν να αυξήσουν την προσαρμοστικότητα και την επιχειρησιακή αξία των μηχανισμών άμυνας.

Σε ερευνητικό επίπεδο, η ενσωμάτωση ML μπορεί να επιτρέψει την ανίχνευση πιο σύνθετων ή άγνωστων προτύπων επιθέσεων, υπό την προϋπόθεση ότι διατηρείται η απαιτούμενη ερμηνευσιμότητα και ότι αξιολογούνται με συνέπεια οι ψευδώς θετικοί/αρνητικοί συναγερμοί. Αντίστοιχα, η επέκταση σε πραγματικά δεδομένα και real-time λειτουργία επιτρέπει την αξιολόγηση της μεθοδολογίας σε ρεαλιστικές συνθήκες, όπου παράγοντες όπως θόρυβος, καθυστερήσεις και ετερογένεια συσκευών επηρεάζουν σημαντικά την απόδοση και την αξιοπιστία του συστήματος.

Σε πρακτικό επίπεδο, τα αποτελέσματα της παρούσας διπλωματικής μπορούν να αξιοποιηθούν ως πλαίσιο για την ανάπτυξη πρωτογενών πολιτικών ανίχνευσης και παρακολούθησης σε IoMT οικοσυστήματα, ιδιαίτερα σε περιβάλλοντα υψηλής κρισιμότητας όπως ο τομέας της υγείας. Η υλοποίηση ενός κανονοκεντρικού IDS παρέχει ένα διαφανές και τεκμηριώσιμο σημείο αναφοράς, το

οποίο μπορεί να υποστηρίξει διαδικασίες αξιολόγησης κινδύνου, συμμόρφωσης και επιχειρησιακής απόκρισης σε συμβάντα.

Συνολικά, η παρούσα διπλωματική εργασία καταδεικνύει ότι η προσομοίωση κανονοκεντρικών συστημάτων ανίχνευσης εισβολών μπορεί να αποτελέσει αξιόπιστη και ερμηνεύσιμη βάση για τη μελέτη της κυβερνοασφάλειας σε IoMT περιβάλλοντα, υποστηρίζοντας τόσο την κατανόηση των κινδύνων όσο και τον σχεδιασμό μελλοντικών μηχανισμών άμυνας.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] B. Alegría, L. Wong, and D. Bedriñiana, “Model for Implementing an IoMT Architecture with ISO/IEC 27001 Security Controls for Remote Patient Monitoring,” Proc. 32nd Conf. of Open Innovations Association (FRUCT), Tampere, Finland, 2022, pp. 38–48, doi: 10.23919/FRUCT56874.2022.9953893.

[2] F. Alsubaei, A. Abuhussein, and S. Shiva, “Security and Privacy in the Internet of Medical Things: Taxonomy and Risk Assessment,” Proc. IEEE 42nd Conf. on Local Computer Networks Workshops (LCN Workshops), Singapore, 2017, pp. 112–120, doi: 10.1109/LCN.Workshops.2017.72.

[3] U. Tariq, F. Jaafar, and Y. Malik, “Mitigating Ransomware Attacks in Internet of Medical Things Networks,” Proc. 5th Intelligent Cybersecurity Conf. (ICSC), Tampa, FL, USA, 2025, pp. 242–247, doi: 10.1109/ICSC65596.2025.11140094.

[4] P. S. T. Aitty, A. V. S. Hemanth Kumar, T. K. V. Krishna, V. R. Nadagoudar, N. Rajamohan Reddy, and A. V. Turukmane, “Cybersecurity in Healthcare: IoT Security for Medical Devices,” Proc. 15th Int. Conf. on Computing Communication and Networking Technologies (ICCCNT), Kamand, India, 2024, pp. 1–8, doi: 10.1109/ICCCNT61001.2024.10724329.

[5] M. Yasir and A. Iqbal, “Cybersecurity Standards for AI-Based Healthcare Networks,” in Artificial Intelligence-Based Smart Healthcare Systems, K. N. Qureshi, T. Newe, and G. Jeon, Eds., Academic Press, 2025, pp. 237–270, doi: 10.1016/B978-0-443-26476-4.00009-5.

[6] V. Malamas, F. Chantzis, T. K. Dasaklis, G. Stergiopoulos, P. Kotzanikolaou, and C. Douligeris, “Risk Assessment Methodologies for the Internet of Medical Things: A Survey and Comparative Appraisal,” IEEE Access, vol. 9, pp. 40049–40075, 2021, doi: 10.1109/ACCESS.2021.3064682.

[7] R. U. Rasool, M. U. Janjua, M. A. Shah, and H. U. Khan, “Security and Privacy of Internet of Medical Things,” Ad Hoc Networks, vol. 137, p. 103074, 2022, doi: 10.1016/j.adhoc.2022.103074.

[8] C. Huang, J. Wang, Y. Liu, and P. Li, “Internet of Medical Things: A Systematic Review,” Neurocomputing, vol. 547, pp. 127–142, 2023, doi: 10.1016/j.neucom.2023.126112.

[9] D. Koutras, N. Tsalis, P. Kotzanikolaou, and C. Douligeris, “Security in IoMT Communications: A Survey,” Sensors, vol. 20, no. 17, pp. 4828–4848, 2020, doi: 10.3390/s20174828.

[10] National Institute of Standards and Technology (NIST), NISTIR 8259: Foundational Cybersecurity for IoT Device Manufacturers, Gaithersburg, MD, USA, 2020. [Online]. Available: https://doi.org/10.6028/NIST.IR.8259

[11] U.S. Food and Drug Administration (FDA), Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions, Final Guidance, Sept. 2023; and Postmarket Management of Cybersecurity in Medical Devices, Guidance for Industry and FDA Staff, Dec. 2018. [Online].Available:https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity-medical-devices

[12] European Union Agency for Cybersecurity (ENISA), Health Sector Threat Landscape 2023–2024, Nov. 2023. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-health-sector-threat-landscape-2023-2024

[13] International Organization for Standardization, ISO/IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements, Geneva, Switzerland, 2022. [Online]. Available: https://www.iso.org/standard/82875.html

[14] National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, Gaithersburg, MD, USA, 2018; Cybersecurity Framework 2.0 (draft), 2023. [Online]. Available: https://www.nist.gov/cyberframework

[15] U.S. Department of Health & Human Services (HHS), Health Insurance Portability and Accountability Act (HIPAA) Security Rule, Washington, DC, USA, 1996 (Updated 2013). [Online]. Available: https://www.hhs.gov/hipaa/for-professionals/security/index.html

[16] European Union, General Data Protection Regulation (GDPR) – Regulation (EU) 2016/679, Official Journal of the European Union, Apr. 2016. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[17] European Union Agency for Cybersecurity (ENISA), Cybersecurity of Hospitals – Good Practices for Security of Health Services and Infrastructures, Heraklion, Greece, 2022. [Online]. Available: https://www.enisa.europa.eu/publications/cybersecurity-of-hospitals

[18] V. Hassija, V. Chamola, D. Gupta, A. Goyal, and M. Guizani, "Blockchain-based Security Solutions for Internet of Medical Things: A Review," Computer Communications, vol. 169, pp. 129-152, 2021, doi: 10.1016/j.comcom.2021.01.009.

[19] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli and M. Rehmani, "Applications of Blockchains in the Internet of Things: A Comprehensive Survey," IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1676–1717, 2019, doi: 10.1109/COMST.2018.2886932.

[20] J. Greser, "Cybersecurity of Medical Devices from the Perspective of Regulation No. 2017/745," Internetowy Kwartalnik Antymonopolowy i Regulacyjny, vol. 9, no. 2, pp. 78–91, 2020, doi: 10.7172/2299-5749.IKAR.2.9.6.

[21] K. Yang, "Risk Management in Medical Devices: An Application of ISO 14971," 2024 IEEE International Symposium on Product Compliance Engineering (ISPCE), Chicago, IL, USA, pp. 1–3, 2024, doi: 10.1109/ISPCE61193.2024.10541258.

[22] D. Flood, F. McCaffery, V. Casey, R. McKeever, and P. Rust, "A Roadmap to ISO 14971 Implementation," Journal of Software: Evolution and Process, vol. 27, pp. 319–336, 2015, doi: 10.1002/smr.1711.

[23] A. D. Stern, W. J. Gordon, A. B. Landman, et al., "Cybersecurity Features of Digital Medical Devices: An Analysis of FDA Product Summaries," BMJ Open, vol. 9, no. e025374, 2019, doi: 10.1136/bmjopen-2018-025374.

[24] J. van Vroonhoven, Risk Management for Medical Devices and the New BS EN ISO 14971, BSI White Paper Series, 2022.

[25] M. Fagan, K. N. Megas, K. Scarfone, and M. Smith, NISTIR 8259: Foundational Cybersecurity Activities for IoT Device Manufacturers, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2020, doi: 10.6028/NIST.IR.8259.

[25a] M. Fagan, K. N. Megas, K. Scarfone, and M. Smith, NISTIR 8259A: IoT Device Cybersecurity Capability Core Baseline, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2020, doi: 10.6028/NIST.IR.8259A.

[26] P. A. Williams and A. J. Woodward, "Cybersecurity Vulnerabilities in Medical Devices: A Complex Environment and Multifaceted Problem," Medical Devices: Evidence and Research, vol. 8, pp. 305–316, 2015, doi: 10.2147/MDER.S50048.

[27] M. Ostermann et al., "Cybersecurity Requirements for Medical Devices in the EU and US: A Comparison and Gap Analysis of the MDCG 2019-16 and FDA Premarket Cybersecurity Guidance,"

Computational and Structural Biotechnology Journal, vol. 28, pp. 259–266, 2025, doi: 10.1016/j.csbj.2025.01.019.

[28] R. Sommer and V. Paxson, "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection," *2010 IEEE Symposium on Security and Privacy*, Oakland, CA, USA, 2010, pp. 305-316, doi: 10.1109/SP.2010.25.

[29] Varun Chandola, Arindam Banerjee, and Vipin Kumar. 2009. Anomaly detection: A survey. ACM Comput. Surv. 41, 3, Article 15 (July 2009), 58 pages. https://doi.org/10.1145/1541880.1541882

[30] Muder Almiani, Alia AbuGhazleh, Amer Al-Rahayfeh, Saleh Atiewi, Abdul Razaque, Deep recurrent neural network for IoT intrusion detection system, Simulation Modelling Practice and Theory, Volume 101,2020,102031, ISSN 1569-190X, https://doi.org/10.1016/j.simpat.2019.102031.

[31] Yang Yang, Xianghan Zheng, Wenzhong Guo, Ximeng Liu, Victor Chang, Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system, Information Sciences, Volume 479, 2019, Pages 567-592, ISSN 0020-0255, https://doi.org/10.1016/j.ins.2018.02.005.

ΠΑΡΑΡΤΗΜΑ Α: Αρχικά δεδομένα προσομοίωσης

	A	B	C	D
1	ID Patient	HeartRate	Oxygen	BloodPressure
2	1	76	99	129
3	2	89	98	125
4	3	84	98	129
5	4	80	98	121
6	5	77	99	117
7	6	89	98	121
8	7	82	98	125
9	8	88	98	124
10	9	80	99	116
11	10	87	96	123
12	11	0	0	0
13	12	0	0	0
14	13	182	105	131
15	14	110	91	183
16	15	76	82	125
17	16	185	113	58
18	17	39	86	117
19	18	184	107	190
20	19	79	80	125
21	20	0	0	0
22	21	91	92	137
23	22	96	93	138
24	23	94	92	138
25	24	93	92	137
26	25	93	91	138
27	26	96	92	135
28	27	95	92	138
29	28	97	92	136
30	29	94	91	137
31	30	90	92	136

Το παρόν παράρτημα παρουσιάζει το αρχικό σύνολο δεδομένων εισόδου που χρησιμοποιήθηκε στην προσομοίωση του συστήματος IoMT. Τα δεδομένα αφορούν βασικές βιοϊατρικές μετρήσεις (καρδιακός ρυθμός, επίπεδα οξυγόνου και αρτηριακή πίεση) ανά ασθενή και αποτέλεσαν τη βάση για την αξιολόγηση της λειτουργίας του συστήματος ανίχνευσης εισβολών (IDS).

ΠΑΡΑΡΤΗΜΑ Β: Καταγραφές Κανονικής Λειτουργίας (Normal Data Logs)

	A	B	C	D	E	F	G	H	I	J
7	5,3.20235,1,5,77,99,117,Normal,0,0									
8	6,3.27318,1,6,89,98,121,Normal,0,0									
9	7,3.35565,1,7,82,98,125,Normal,0,0									
10	8,3.5163,1,8,88,98,124,Normal,0,0									
11	9,3.62913,1,9,80,99,116,Normal,0,0									
12	10,3.74219,1,10,87,96,123,Normal,0,0									
13	11,4.86328,1,21,91,92,137,Normal,0,0									
14	12,4.94486,1,22,96,93,138,Normal,0,0									
15	13,5.06175,1,23,94,92,138,Normal,0,0									
16	14,5.13805,1,24,93,92,137,Normal,0,0									
17	15,5.22941,1,25,93,91,138,Normal,0,0									
18	16,5.38362,1,26,96,92,135,Normal,0,0									
19	17,5.52162,1,27,95,92,138,Normal,0,0									
20	18,5.61191,1,28,97,92,136,Normal,0,0									
21	19,5.67693,1,29,94,91,137,Normal,0,0									
22	20,5.7497,1,30,90,92,136,Normal,0,0									
23										
24	ID	Time	lbl_Status	lbl_PatientID	lbl_HeartRate	lbl_Oxygen	lbl_BP	lbl_AttackType	lbl_Severity	lbl_AnomCount
25	1	26901	1	1	76	99	129	Normal	0	0
26	2	282911	1	2	89	98	125	Normal	0	0
27	3	297491	1	3	84	98	129	Normal	0	0
28	4	306499	1	4	80	98	121	Normal	0	0
29	5	320235	1	5	77	99	117	Normal	0	0
30	6	327318	1	6	89	98	121	Normal	0	0
31	7	335565	1	7	82	98	125	Normal	0	0
32	8	35163	1	8	88	98	124	Normal	0	0
33	9	362913	1	9	80	99	116	Normal	0	0
34	10	374219	1	10	87	96	123	Normal	0	0
35	11	486328	1	21	91	92	137	Normal	0	0
36	12	494486	1	22	96	93	138	Normal	0	0
37	13	506175	1	23	94	92	138	Normal	0	0
38	14	513805	1	24	93	92	137	Normal	0	0
39	15	522941	1	25	93	91	138	Normal	0	0
40	16	538362	1	26	96	92	135	Normal	0	0
41	17	552162	1	27	95	92	138	Normal	0	0
42	18	561191	1	28	97	92	136	Normal	0	0
43	19	567693	1	29	94	91	137	Normal	0	0
44	20	57497	1	30	90	92	136	Normal	0	0

Το παρόν παράρτημα παρουσιάζει ενδεικτικές καταγραφές κανονικής λειτουργίας του συστήματος, στις οποίες οι βιοϊατρικές μετρήσεις των ασθενών κυμαίνονται εντός των προκαθορισμένων αποδεκτών ορίων. Για τις καταγραφές αυτές το σύστημα IDS ταξινομεί τα δεδομένα ως «Normal», με μηδενικό πλήθος ανωμαλιών (AnomCount = 0) και επίπεδο σοβαρότητας ίσο με μηδέν (Severity = 0).

Όπως και στην περίπτωση των καταγραφών ασφαλείας, η άνω απεικόνιση παρουσιάζει τα δεδομένα στη μορφή που εξάγονται απευθείας από το περιβάλλον προσομοίωσης, ενώ ακολουθεί καθαρογραμμένη αναπαράσταση των ίδιων εγγραφών για λόγους αναγνωσιμότητας και τεκμηρίωσης της ορθής λειτουργίας του συστήματος.

ΠΑΡΑΡΤΗΜΑ Γ: Καταγραφές Ασφαλείας και Ανιχνευμένα Συμβάντα (Security Alerts)

	A	B	C	D	E	F	G	H	I	J
1	SIMUL8 Flow File Version 1.00									
2	ID,Time,lbl_Status,lbl_PatientID,lbl_HeartRate,lbl_Oxygen,lbl_BP,lbl_AttackType,lbl_Severity,lbl_AnomCount									
3	1,3.90642,2,11,0,0,0,Missing,3,3									
4	2,3.98751,2,12,0,0,0,Missing,3,3									
5	3,4.1302,2,13,182,105,131,Multi,2,2									
6	4,4.21995,2,14,110,91,183,BP,1,1									
7	5,4.33489,2,15,76,82,125,O2,1,1									
8	6,4.40208,2,16,185,113,58,Multi,3,3									
9	7,4.5002,2,17,39,86,117,HR,1,1									
10	8,4.59539,2,18,184,107,190,Multi,3,3									
11	9,4.67287,2,19,79,80,125,O2,1,1									
12	10,4.75686,2,20,0,0,0,Missing,3,3									
13										
14	ID	Time	lbl_Status	lbl_PatientID	lbl_HeartRate	lbl_Oxygen	lbl_BP	lbl_AttackType	lbl_Severity	lbl_AnomCount
15	1	390642	2	11	0	0	0	Missing	3	3
16	2	398751	2	12	0	0	0	Missing	3	3
17	3	41302	2	13	182	105	131	Multi	2	2
18	4	421995	2	14	110	91	183	BP	1	1
19	5	433489	2	15	76	82	125	O2	1	1
20	6	440208	2	16	185	113	58	Multi	3	3
21	7	45002	2	17	39	86	117	HR	1	1
22	8	459539	2	18	184	107	190	Multi	3	3
23	9	467287	2	19	79	80	125	O2	1	1
24	10	475686	2	20	0	0	0	Missing	3	3

Με βάση τους κανόνες ανίχνευσης του συστήματος IDS που παρουσιασα στην ενοτητα 6.8.2 , τα αλλοιωμένα δεδομένα εντοπίζονται ενδεικτικά σε ασθενείς με αναγνωριστικά ID 11, 12 και 20 (απούσες μετρήσεις – Missing), καθώς και σε ασθενείς με ID 13, 16 και 18, όπου παρατηρούνται συνδυασμένες ανωμαλίες (Multi). Επιπλέον, μεμονωμένες ανωμαλίες καταγράφονται σε ασθενείς με ID 14, 15, 17 και 19.