



ΠΑΝΕΠΙΣΤΗΜΙΟ  
ΑΙΓΑΙΟΥ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ  
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ  
ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

---

# ΠΡΟΣΤΑΣΙΑ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΣΕ ΠΕΡΙΒΑΛΛΟΝΤΑ ΒΙΟΜΗΧΑΝΙΚΟΥ ΔΙΑΔΙΚΤΥΟΥ ΤΩΝ ΠΡΑΓΜΑΤΩΝ (INDUSTRIAL INTERNET OF THINGS – IIOT)

---

Διπλωματική εργασία των φοιτητών: Ιωάννα Γεωργίου (Α.Μ.  
321/2009018) & Παναγιώτη Κονταρίνη (Α.Μ. 321/2007053)  
Επιβλέπουσα καθηγήτρια: κα Διαμαντοπούλου Βασιλική



ΈΤΟΣ 2024

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

Τμήμα Μηχανικών Πληροφοριακών & Επικοινωνιακών Συστημάτων

## ΕΥΧΑΡΙΣΤΙΕΣ

Με την παρούσα Διπλωματική εργασία εμείς, η Ιωάννα Γεωργίου και ο Παναγιώτης Κονταρίνης, ολοκληρώνουμε τον κύκλο σπουδών μας στο Πανεπιστήμιο Αιγαίου, στο τμήμα των Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων,

Θα θέλαμε να ευχαριστήσουμε, εκ βάθης καρδίας, όσους στάθηκαν δίπλα μας κατά την εκπόνηση της εργασίας αυτής για την πολύτιμη στήριξή τους.

Τέλος, ευχαριστούμε θερμά την επιβλέπουσα καθηγήτριά μας, κυρία Βασιλική Διαμαντοπούλου, για τη συνεχή καθοδήγηση και συμβουλές που μας παρείχε καθ' όλη τη διάρκεια της πορείας μας καθώς και για τους νέους ορίζοντες που μας άνοιξε στο συγκεκριμένο επιστημονικό πεδίο.

## ΠΕΡΙΛΗΨΗ

Η ταχεία υιοθέτηση του Βιομηχανικού Διαδικτύου των Πραγμάτων (IIoT) σε βιομηχανικά περιβάλλοντα σηματοδοτεί μια νέα εποχή στη διαχείριση της παραγωγής και των λειτουργιών, αυξάνοντας την αποδοτικότητα και επιτρέποντας τον αυτοματισμό σε διάφορους τομείς. Αυτή η εργασία διερευνά τις προκλήσεις και τις πιθανές λύσεις για τη διασφάλιση της ιδιωτικότητας και της ασφάλειας δεδομένων στα συστήματα IIoT, ιδιαίτερα στο πλαίσιο της Βιομηχανίας 4.0. Με την αυξανόμενη σύνδεση συσκευών και τη δημιουργία τεράστιου όγκου δεδομένων, η ασφάλεια αυτών των δικτύων έχει καταστεί πρωταρχικής σημασίας. Η μελέτη παρέχει μια συνολική ανάλυση των περιβαλλόντων IIoT, διευκρινίζοντας θεμελιώδεις έννοιες και καθορίζοντας τα μοναδικά χαρακτηριστικά που διαφοροποιούν το IIoT από το παραδοσιακό IoT. Περιγράφει την εξέλιξη του IIoT, από τη Βιομηχανική Επανάσταση έως τον σημερινό ψηφιακό μετασχηματισμό, και τις επιπτώσεις από την ενσωμάτωση των τεχνολογιών IoT σε βιομηχανικά περιβάλλοντα. Εστιάζοντας σε δύο διαφορετικά σενάρια ασφαλείας, η ανάλυση εξετάζει στατικά και δυναμικά περιβάλλοντα δεδομένων, αναδεικνύοντας τις ξεχωριστές ανάγκες ασφαλείας και προσεγγίσεις για κάθε περίπτωση. Χρησιμοποιούνται τεχνικές, όπως οι μεθοδολογίες STRIDE και DREAD, για τον εντοπισμό απειλών και ευπαθειών, ενώ προτείνονται διάφορες στρατηγικές ασφαλείας για την αντιμετώπιση των πιθανών κινδύνων. Επιπλέον, προσφέρονται πρακτικές κατευθύνσεις και μια σειρά ερωτήσεων σε μορφή checklist για αναλυτές και μηχανικούς ασφαλείας, με έμφαση στον έλεγχο πρόσβασης με βάση ρόλους (RBAC), την κρυπτογράφηση δεδομένων και τη συμμόρφωση με κανονισμούς, όπως ο GDPR και το HIPAA. Η έρευνα στοχεύει να εξοπλίσει τους επαγγελματίες του κλάδου με τα απαραίτητα εργαλεία για την εφαρμογή ισχυρών μέτρων ασφαλείας σε περιβάλλοντα IIoT, διασφαλίζοντας την προστασία των δεδομένων και τη συμμόρφωση με τους κανονισμούς. Τα ευρήματα υπογραμμίζουν τη σημασία της συνεχούς παρακολούθησης, της τακτικής αξιολόγησης απειλών και της εκπαίδευσης των εργαζομένων για τη διατήρηση ενός ασφαλούς οικοσυστήματος IIoT. Καθώς οι βιομηχανίες βασίζονται όλο και περισσότερο στη λήψη αποφάσεων με βάση τα δεδομένα, η μελέτη αναδεικνύει την ανάγκη για μια ισορροπημένη προσέγγιση στην ασφάλεια, η οποία προάγει την καινοτομία, διασφαλίζοντας ταυτόχρονα την προστασία κρίσιμων και ευαίσθητων πληροφοριών.

## ABSTRACT

The rapid adoption of the Industrial Internet of Things (IIoT) in industrial environments marks a new era in production and operational management, driving efficiency and enabling automation across various sectors. This thesis explores the challenges and solutions for ensuring data privacy and security within IIoT systems, particularly in the context of Industry 4.0. With an increasing number of interconnected devices and vast amounts of data being generated, the security of these networks has become paramount. The study provides a comprehensive analysis of IIoT environments by clarifying fundamental concepts and defining the unique characteristics that differentiate IIoT from traditional IoT. It outlines the evolution of IIoT, from the Industrial Revolution to the current digital transformation, and the implications of integrating IoT technologies within industrial settings. Focusing on two different security scenarios, the analysis delves into static and dynamic data environments, showcasing distinct security needs and approaches for each case. Techniques such as STRIDE and DREAD methodologies are employed to identify threats and vulnerabilities, while various security strategies are proposed to mitigate potential risks. Moreover, practical guidelines and a set of checklist questions are offered for security analysts and engineers, emphasizing on role-based access control (RBAC), data encryption, and regulatory compliance with standards like GDPR and HIPAA. The research aims to equip industry professionals with the necessary tools to implement robust security measures in IIoT settings, ensuring data protection and regulatory adherence. The findings highlight the importance of continuous monitoring, regular threat assessment, and employee training in maintaining a secure IIoT ecosystem. As industries increasingly rely on data-driven decision-making, the study underscores the need for a balanced approach to security that fosters innovation while safeguarding critical and sensitive information.

## **ΠΕΡΙΕΧΟΜΕΝΑ**

|                                                                                                         |           |
|---------------------------------------------------------------------------------------------------------|-----------|
| <b>ΕΥΧΑΡΙΣΤΙΕΣ.....</b>                                                                                 | <b>1</b>  |
| <b>ΠΕΡΙΛΗΨΗ .....</b>                                                                                   | <b>2</b>  |
| <b>ABSTRACT .....</b>                                                                                   | <b>3</b>  |
| <b>ΠΕΡΙΕΧΟΜΕΝΑ .....</b>                                                                                | <b>4</b>  |
| <b>ΚΕΦΑΛΑΙΟ 1: ΕΙΣΑΓΩΓΗ.....</b>                                                                        | <b>11</b> |
| 1.1    Εξέλιξη του IIoT: Από τη Βιομηχανία στην Υψηλή Τεχνολογία.....                                   | 11        |
| 1.2    Επέκταση στο Industry 4.0 .....                                                                  | 13        |
| 1.3    Industry 4.0 και IIoT .....                                                                      | 16        |
| 1.4    Συμπεράσματα και Εφαρμογές της Γνώσης από την Ανάλυση του IIoT<br>και του Industry 4.0.....      | 16        |
| <b>ΚΕΦΑΛΑΙΟ 2: ΤΟ ΒΙΟΜΗΧΑΝΙΚΟ ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ (IIOT)<br/>.....</b>                              | <b>19</b> |
| 2.1    Ορισμός .....                                                                                    | 19        |
| 2.2    Εφαρμογές IIoT.....                                                                              | 20        |
| 2.3    Προκλήσεις που αντιμετωπίζει το IIoT .....                                                       | 22        |
| 2.4    Οι Τεχνολογίες που συνθέτουν το IIoT .....                                                       | 23        |
| <b>ΚΕΦΑΛΑΙΟ 3: ΙΔΙΑΙΤΕΡΟΤΗΤΕΣ IIOT ΣΕ ΣΥΓΚΡΙΣΗ ΜΕ ΠΑΡΑΔΟΣΙΑΚΑ<br/>ΠΕΡΙΒΑΛΛΟΝΤΑ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ .....</b> | <b>34</b> |
| 3.1    Από τα κυβερνοφυσικά συστήματα στο Βιομηχανικό Διαδίκτυο των<br>Πραγμάτων .....                  | 34        |
| 3.2    Διαφορές μεταξύ IoT και IIoT .....                                                               | 35        |

|                                                                                                |                                                                      |           |
|------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|-----------|
| 3.3                                                                                            | Απαιτήσεις του IIoT .....                                            | 37        |
| <b>ΚΕΦΑΛΑΙΟ 4: ΑΣΦΑΛΕΙΑ ΚΑΙ ΙΔΙΩΤΙΚΟΤΗΤΑ .....</b>                                             |                                                                      | <b>43</b> |
| 4.1                                                                                            | Ιδιωτικότητα .....                                                   | 43        |
| 4.2                                                                                            | Ασφάλεια .....                                                       | 44        |
| 4.3                                                                                            | Κανονιστική συμμόρφωση .....                                         | 46        |
| 4.4                                                                                            | Πραγματικές περιπτώσεις παραβιάσεων ιδιωτικότητας .....              | 46        |
| <b>ΚΕΦΑΛΑΙΟ 5: ΕΝΤΟΠΙΣΜΟΣ ΑΠΑΙΤΗΣΕΩΝ ΠΡΟΣΤΑΣΙΑΣ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΣΕ ΠΕΡΙΒΑΛΛΟΝ IIOT .....</b> |                                                                      | <b>48</b> |
| 5.1                                                                                            | Υποθετικό σενάριο διαχείρισης δεδομένων σε ένα περιβάλλον IIoT ..... | 48        |
| 5.1.1                                                                                          | Περιγραφή σεναρίου Α .....                                           | 48        |
| 5.1.2                                                                                          | Οντότητες σεναρίου Α.....                                            | 49        |
| 5.1.3                                                                                          | Περιγραφή δομής δεδομένων σεναρίου Α .....                           | 49        |
| 5.1.4                                                                                          | Περιγραφή περιπτώσεων και απειλών.....                               | 52        |
| 5.1.5                                                                                          | Εκμείευση απαιτήσεων.....                                            | 54        |
| 5.2.6                                                                                          | Αντιμετώπιση απαιτήσεων.....                                         | 57        |
| 5.2                                                                                            | Υποθετικό σενάριο διαχείρισης δεδομένων σε ένα περιβάλλον IIoT ..... | 57        |
| 5.2.1                                                                                          | Περιγραφή σεναρίου .....                                             | 58        |
| 5.2.2                                                                                          | Οντότητες σεναρίου .....                                             | 59        |
| 5.2.3                                                                                          | Δυναμικές σχέσεις μεταξύ οντοτήτων .....                             | 60        |
| 5.2.4                                                                                          | Σχεδίαση Σεναρίου .....                                              | 67        |
| 5.2.5                                                                                          | Μοντελοποίηση Σεναρίου .....                                         | 69        |

|                                      |                                                       |           |
|--------------------------------------|-------------------------------------------------------|-----------|
| 5.2.6                                | Καλές πρακτικές προστασίας προσωπικών δεδομένων ..... | 75        |
| 5.3                                  | Ασφάλεια και Ιδιωτικότητα στο IIoT.....               | 76        |
| <b>ΚΕΦΑΛΑΙΟ 6: ΣΥΜΠΕΡΑΣΜΑΤΑ.....</b> |                                                       | <b>80</b> |
| 6.1                                  | Οδηγίες για την δημιουργία ασφαλών συστημάτων .....   | 80        |
| 6.2                                  | Συζήτηση και μελλοντική εργασία .....                 | 82        |
| <b>ΒΙΒΛΙΟΓΡΑΦΙΑ.....</b>             |                                                       | <b>85</b> |
| <b>ΠΑΡΑΡΤΗΜΑ Α .....</b>             |                                                       | <b>89</b> |

## List of abbreviations

|                                                                   |        |
|-------------------------------------------------------------------|--------|
| Artificial Intelligence AI .....                                  | 44     |
| Bluetooth Low Energy (BLE) .....                                  | 26     |
| Data Flow Diagram (DFD) .....                                     | 52, 55 |
| EMAS – Eco-Management and Audit Scheme .....                      | 41     |
| Emissions Trading System – ETS .....                              | 41     |
| Entity Relation Diagrams (ERDs) .....                             | 68     |
| GDPR General Data Protection Regulation .....                     | 46     |
| HIPAA – Health Insurance Portability and Accountability Act ..... | 82     |
| Identity and Access Management (IAM) .....                        | 80     |
| IIoT Industrial Internet of Things .....                          | 19     |
| IIRA Industrial Internet Reference Architecture .....             | 19     |
| Intrusion Detection Systems (IDS) .....                           | 73     |
| IoT Internet of Things .....                                      | 11     |
| local area network (LAN) .....                                    | 25     |
| long term evolution (LTE) .....                                   | 26     |
| Low-Power Wide-Area Network (LPWAN) .....                         | 28     |
| LTE Cat M1 (LTE-M) .....                                          | 27     |
| multi-factor authentication (MFA) .....                           | 65     |
| Narrowband IoT (NB-IoT) .....                                     | 27     |
| National Security Agency (NSA) .....                              | 46     |
| Power Line Communication (PLC) .....                              | 25     |



|                                                   |    |
|---------------------------------------------------|----|
| RAMI Reference Architectural Model Industry ..... | 19 |
| role-based access control – RBAC.....             | 76 |
| Security Development Lifecycle (SDL) .....        | 71 |
| SSL (Secure Socket Layer) .....                   | 28 |
| Time-Sensitive Networking (TSN) .....             | 25 |
| TLS (Transport Layer Security) .....              | 28 |
| VPN (Virtual private network) .....               | 28 |
| μηχανή με μηχανή (M2M).....                       | 16 |

## LIST OF FIGURES

|                                                                                             |    |
|---------------------------------------------------------------------------------------------|----|
| Figure 1 Το Οικοσύστημα του Industry 4.0 (supplychain, 2024) .....                          | 14 |
| Figure 2 Υποδομή του IIoT (Gillis, n.d.) .....                                              | 20 |
| Figure 3 Ωκεανός των Πραγμάτων .....                                                        | 22 |
| Figure 4 Διάγραμμα λογικής αρχιτεκτονικής για το edge computing<br>(Consortium, 2018) ..... | 31 |
| Figure 5 Διάγραμμα ροής δεδομένων ενός συστήματος έξυπνης κλινικής ....                     | 51 |
| Figure 6 Διάγραμμα αλληλουχίας, περίπτωση προσποίησης ταυτότητας.....                       | 53 |
| Figure 7 SQL injection στη κεντρική βάση του συστήματος της έξυπνης<br>κλινικής .....       | 53 |
| Figure 8 Επίθεση άρνησης υπηρεσιών στο σύστημα της έξυπνης κλινικής....                     | 54 |
| Figure 9 ERD διάγραμμα ενός IIoT εργοστασίου .....                                          | 69 |
| Figure 10 Μοντελοποίηση απειλών ενός IIoT εργοστασίου .....                                 | 71 |
| Figure 11 Συμβολισμοί Οντοτήτων-Σχέσεων .....                                               | 89 |
| Figure 12 Συμβολισμοί καρδιναλιότητας στις οντολογικές σχέσεις .....                        | 89 |

## LIST OF TABLES

|                                                                                                       |    |
|-------------------------------------------------------------------------------------------------------|----|
| Table 1 Περιληπτική περιγραφή των διαφόρων τύπων αισθητήρων όπως παρατίθενται στο (Suman, 2021) ..... | 24 |
| Table 2 Βασικές διαφορές μεταξύ IoT και IIoT .....                                                    | 37 |
| Table 3 Πίνακας δεδομένων σεναρίου .....                                                              | 51 |
| Table 4 Συνοπτικός πίνακας με τα αποτελέσματα της μεθοδολογίας STRIDE .....                           | 76 |
| Table 5 Πίνακας δεδομένων σεναρίου .....                                                              | 78 |

## ΚΕΦΑΛΑΙΟ 1: ΕΙΣΑΓΩΓΗ

Το Industry 4.0 στοχεύει στην πλήρη ενσωμάτωση των παραδοσιακών βιομηχανικών πλατφορμών με την πιο πρόσφατη ευφυή τεχνολογία, π.χ. μεγάλα δεδομένα και τεχνητή νοημοσύνη. Λόγω της ψηφιοποίησης της μεταποίησης, ο τρόπος παραγωγής βρίσκεται εν μέσω ενός σημαντικού μετασχηματισμού (Cai, 2020). Οι παγκόσμιες βιομηχανίες διερευνούν συνεχώς νέους τρόπους για να ξεπεράσουν τα σημεία συμφόρησης της έξυπνης παραγωγής. Κυρίως εστιάζουν στην ανάπτυξη μεγάλης κλίμακας συστημάτων και στην πρακτική εφαρμογή τους με σκοπό την επικοινωνία από μηχανή σε μηχανή για την παροχή αυξημένου αυτοματισμού, συμπεριλαμβανομένης της προσαρμοστικής παρακολούθησης, της ανάλυσης δεδομένων και της εξόρυξης, της διάγνωσης βλαβών και της αντιμετώπισης έκτακτης ανάγκης (Yu W. D., 2020).

Η χρήση προηγμένων τεχνολογιών, όπως η τεχνητή νοημοσύνη, το διαδίκτυο των πραγμάτων (IoT) και τα μεγάλα δεδομένα, βελτιώνει την αποτελεσματικότητα και της ευελιξία της παραγωγής. Με την αυτοματοποίηση πολλών διαδικασιών, οι εργαζόμενοι μπορούν να απελευθερωθούν από τις επαναλαμβανόμενες, χειρωνακτικές εργασίες και να επικεντρωθούν σε πιο σύνθετες και δημιουργικές δραστηριότητες. Ωστόσο, ένα από τα βασικά ζητήματα που προκύπτουν είναι η ασφάλεια των δεδομένων κατά τη διάρκεια της παραγωγής (Zheng X. &, 2020). Για παράδειγμα, μια εταιρεία μπορεί να συγκεντρώσει ακατέργαστα δεδομένα από τις συσκευές, τους αισθητήρες, ακόμη και τα περιουσιακά της στοιχεία. Τα ακατέργαστα δεδομένα επιτρέπουν στην εταιρεία να παρέχει επεκτάσιμες και αξιόπιστες εφαρμογές γρηγορότερα για να καλύψει τις μεταβλητές απαιτήσεις του πελάτη. Ωστόσο, ενδέχεται να υπάρχουν ιδιωτικές πληροφορίες σε πρωτογενή δεδομένα, όπως χαρακτηριστικά συμπεριφοράς πελατών, προγραμματισμός λεπτομερειών παραγωγής και κατάσταση λειτουργίας της συσκευής (Huo, 2020).

Οι ιδιωτικές πληροφορίες μπορεί να εξορύσσονται παράνομα από ακατέργαστα δεδομένα, να χρησιμοποιούνται για άγνωστους εμπορικούς σκοπούς ή ακόμη και να πωλούνται δημόσια στο διαδίκτυο. Επομένως, το ποιος μπορεί να έχει πρόσβαση, να χρησιμοποιεί με ασφάλεια και να δημοσιεύει νόμιμα ακατέργαστα δεδομένα αποτελεί εμπόδιο στην ανάπτυξη του Βιομηχανικού IoT (Hui, 2020). Η κατάλληλη προστασία απορρήτου δεδομένων όχι μόνο επιτρέπει σε μια εταιρεία να χρησιμοποιεί αποτελεσματικά τα δεδομένα διασφαλίζοντας ταυτόχρονα την ασφάλεια των δεδομένων, αλλά έχει επίσης σημασία για το βιώσιμο και υγιές οικοσύστημα του βιομηχανικού IoT.

### 1.1 Εξέλιξη του IIoT: Από τη Βιομηχανία στην Υψηλή Τεχνολογία

Το Βιομηχανικό διαδίκτυο των πραγμάτων δεν εφευρέθηκε ξαφνικά τον 21<sup>ο</sup> αιώνα. Στην πραγματικότητα πρόκειται για μία σειρά τεχνολογικών εξελίξεων και επιτευγμάτων των τελευταίων χρόνων που ενσωματώθηκαν στο χώρο της Βιομηχανίας. Η μία τεχνολογική

ανακάλυψη διαδέχθηκε την άλλη, ώσπου αυτές ωρίμασαν και έγινε εφικτό να αξιοποιηθούν από το χώρο της Βιομηχανίας, προκειμένου να αυτοματοποιηθούν οι βιομηχανικές διαδικασίες, να αυξηθούν οι ρυθμοί παραγωγής, να υπάρχει καλύτερη επίβλεψη της παραγωγικής διαδικασίας και μεγαλύτερη ευελιξία. Η ιστορία του IIoT ξεκινάει στα τέλη του 18<sup>ου</sup> αιώνα με την 1<sup>η</sup> Βιομηχανική Επανάσταση και συνεχίζει με τις επόμενες βιομηχανικές επιτεύξεις, φτάνοντας στο σήμερα και στην ψηφιοποίηση και τον αυτοματισμό του Industry 4.0.

**Πρώτη Βιομηχανική Επανάσταση:** Στη Βρετανία στα τέλη του 18<sup>ου</sup> αιώνα γεννιέται η ιδέα της χρήσης της τεχνολογίας στη μαζική παραγωγή. Μέχρι τότε η παραγωγική διαδικασία βασιζόταν αποκλειστικά και μόνο στα χέρια ανθρώπων και τη δύναμη των ζώων (IBM, 2024). Εκείνη την εποχή, η βιομηχανία αρχίζει να καταλαβαίνει ότι η ενσωμάτωση της ατμομηχανής στη παραγωγική διαδικασία μπορεί να αυξήσει σημαντικά την αποδοτικότητα. Έτσι γεννήθηκε η ιδέα της χρήσης της τεχνολογίας στη Βιομηχανία, η οποία παραμένει μέχρι και σήμερα.

**Δεύτερη Βιομηχανική Επανάσταση:** Ξεκίνησε τον 19<sup>ο</sup> αιώνα με την ανακάλυψη του ηλεκτρισμού. Η λογική της αναμετάδοσης (Relay Logic) και η ηλεκτροδότηση επιτάχυναν ραγδαία την βιομηχανική αυτοματοποίηση. Η επεκτεινόμενη χρήση των κεντρικών ηλεκτρικών σταθμών σε συνδυασμό με τη λειτουργία νέων υψηλής πίεσης λεβήτων και ατμοστροβίλων οδήγησε σε αυξημένη ζήτηση για όργανα και ελέγχους. Οι βιομηχανικές μονάδες άρχισαν να μεταβαίνουν σε ηλεκτρικούς κινητήρες και όλο και λιγότερες εγκαταστάσεις συνέχισαν να χρησιμοποιούν ιμάντες κίνησης με ατμομηχανές. Οι ηλεκτρικοί κινητήρες αύξησαν την παραγωγή κατά 30% λόγω της μεγαλύτερης αποδοτικότητας σε σύγκριση με τις ατμομηχανές, είχαν λιγότερες τριβές και χαμηλότερες απαιτήσεις συντήρησης (Bong, 2022). Αξίζει να σημειωθεί και η συμβολή του Henry Ford, ο οποίος εφάρμοσε για πρώτη φορά την ιδέα της γραμμής παραγωγής στη βιομηχανία. Ο Henry Ford άντλησε τις ιδέες του για τη μαζική παραγωγή από ένα σφαγείο στο Σικάγο, στο οποίο γουρούνια κρεμόντουσαν από ταινίες μεταφοράς και κάθε σφαγέας εκτελούσε μόνο ένα μέρος της διαδικασίας του σφαγίου του ζώου. Μετέφερε αυτές τις αρχές στη παραγωγή των αυτοκινήτων, επιφέροντας δραστικές αλλαγές στη διαδικασία. Ενώ προηγουμένως μία στάση συναρμολογούσε ολόκληρο το αυτοκίνητο, τώρα τα οχήματα παρήχθησαν σε επιμέρους βήματα πάνω στην κινούμενη ταινία - πολύ πιο γρήγορα και με χαμηλότερο κόστος (desouttertools, 2024).

**Τρίτη Βιομηχανική Επανάσταση:** Τα ρελεϊκά συστήματα ελέγχου ήταν σχετικά μεγάλα, περίπλοκα και δυσκίνητα. Η λύση δόθηκε από τον Dick Morley, γνωστός και ως ο "πατέρα" του Programmable Logic Controller (PLC). Το 1968 κατασκεύασε το πρώτο PLC, Modicon 084. Παράλληλα, ο Θεόδωρος Παρασκευάκος συνειδητοποίησε πρώτος τις δυνατότητες της επικοινωνιακής τεχνολογίας και πως αυτές μπορούν να συνεργαστούν με υπολογιστικές διαδικασίες μέσα από ηλεκτρονικές συσκευές (Desjardins, 2018). Η τρίτη βιομηχανική επανάσταση, που ξεκίνησε στα μέσα του 20<sup>ου</sup> αιώνα, πρόσθεσε υπολογιστές, προηγμένες τηλεπικοινωνίες και ανάλυση δεδομένων στις κατασκευαστικές διαδικασίες. Η ψηφιοποίηση

των εργοστασίων άρχισε με την ενσωμάτωση προγραμματιζόμενων λογικών ελεγκτών (PLCs) στα μηχανήματα για να βοηθήσουν στην αυτοματοποίηση κάποιων διαδικασιών και στη συλλογή και ανταλλαγή δεδομένων (IBM, 2024).

**Τέταρτη Βιομηχανική Επανάσταση:** Σταθμός ορόσημο στην ιστορία της τεχνολογίας αποτελεί η εφεύρεση του Παγκόσμιου Ιστού από τον Tim Berners-Lee (1989). Τα συστήματα παραγωγής που ήδη διαθέτουν τεχνολογία υπολογιστών επεκτείνονται με δικτυακή σύνδεση. Αυτά επιτρέπουν την επικοινωνία με άλλες εγκαταστάσεις και την εκπομπή πληροφοριών για τον εαυτό τους. Αυτό είναι το επόμενο βήμα στην αυτοματοποίηση της παραγωγής. Η δικτύωση όλων των συστημάτων οδηγεί σε "κυβερνοφυσικά συστήματα παραγωγής" και, επομένως, σε έξυπνα εργοστάσια, όπου τα συστήματα παραγωγής, τα εξαρτήματα και οι άνθρωποι επικοινωνούν μέσω δικτύου και η παραγωγή είναι σχεδόν αυτόνομη. Τώρα πια οι μηχανές είναι ικανές να προβλέψουν βλάβες και να ενεργοποιήσουν αυτόνομα τις διαδικασίες συντήρησης ή αυτοοργανωμένες λογιστικές που αντιδρούν σε απρόσμενες αλλαγές στην παραγωγή. Η ψηφιοποίηση του κατασκευαστικού περιβάλλοντος επιτρέπει πιο ευέλικτους τρόπους παροχής των σωστών πληροφοριών στο σωστό άτομο την κατάλληλη στιγμή. Η αυξανόμενη χρήση ψηφιακών συσκευών μέσα στα εργοστάσια σημαίνει ότι η συντήρηση, η επισκευή και η απασφαλμάτωση μπορούν να παρέχονται αποτελεσματικότερα αφού υπάρχει καταγεγραμμένο ιστορικό με ακρίβεια (desouttertools, 2024).

## 1.2 Επέκταση στο Industry 4.0

Η μεταμόρφωση της Βιομηχανίας σε επίπεδο 4 έχει αυξήσει τις δυνατότητες της παραγωγικής διαδικασίας. Οι νέες τεχνολογίες ενσωματώνονται αποτελεσματικά στα εργοστάσια και η γραμμή παραγωγής αλλά και ο τρόπος λειτουργίας της βιομηχανίας αλλάζει συνεχώς. Η τελευταία επανάσταση του διαδικτύου οδηγεί συνεχώς σε καινούργιες τεχνολογίες και επιτεύξεις, με αποτέλεσμα η ψηφιοποίηση της βιομηχανίας ολοένα και αυξάνεται.

**Το Οικοσύστημα του Industry 4.0:** Οι ψηφιακές τεχνολογίες του Industry 4.0 δεν χρησιμοποιούνται από μεμονωμένες επιχειρήσεις αλλά από ολόκληρη την εφοδιαστική αλυσίδα δημιουργώντας ένα ολόκληρο οικοσύστημα. Αυτή η διασύνδεση εκτείνεται από τους προμηθευτές μέσω των κατασκευαστών στους πελάτες, και ακόμη παραπέρα, στους τελικούς χρήστες και άλλους ενδιαφερόμενους φορείς του οικοσυστήματος. Στην εφοδιαστική αλυσίδα η πλήρης ορατότητα σε ολόκληρο το δίκτυο είναι απαραίτητη για αποτελεσματικές λειτουργίες. Επιπρόσθετα, η μετάφραση αυτής της ορατότητας και του συντριπτικού όγκου ψηφιακών δεδομένων σε αναλυτικά στοιχεία και πληροφορίες μπορούν να χρησιμοποιηθούν για τη διαχείριση κάθε σταδίου της βιομηχανίας σε πραγματικό χρόνο. Στην παρακάτω εικόνα φαίνεται το οικοσύστημα του Industry 4.0.

## Industry 4.0 ecosystem

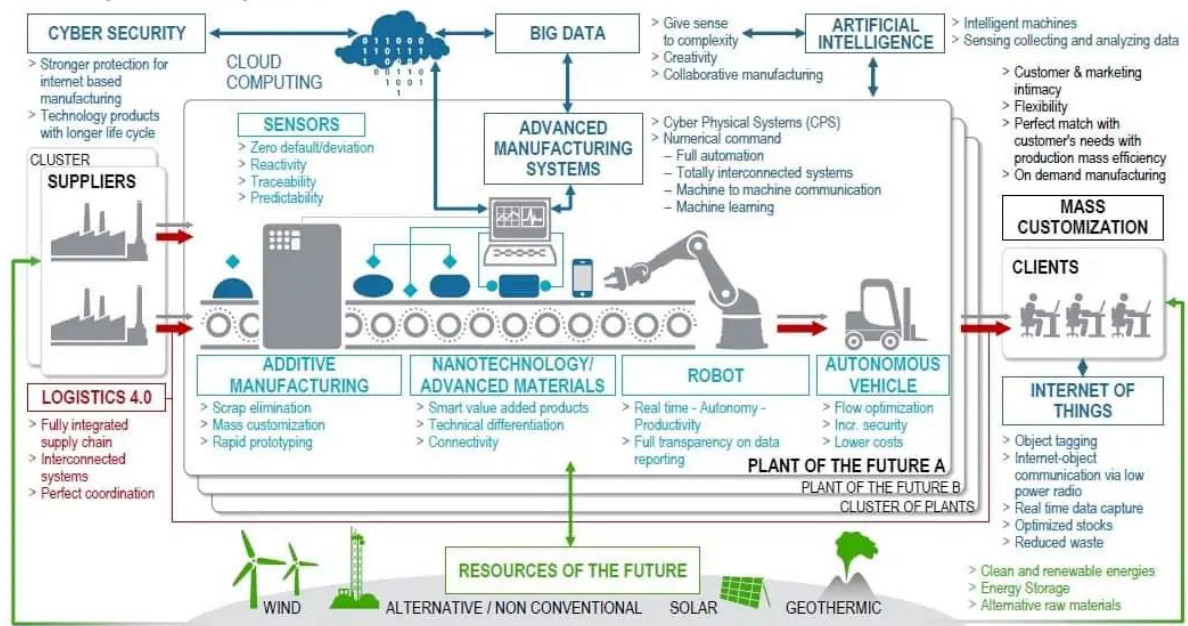


Figure 1 Το Οικοσύστημα του Industry 4.0 (supplychain, 2024)

Συγκεκριμένα απεικονίζεται η διασυνδεδεμένη και πολύπλευρη φύση του Industry 4.0, δείχνοντας πως διάφορες τεχνολογικές εξελίξεις και έννοιες συνδυάζονται για να δημιουργήσουν ένα σύγχρονο βιομηχανικό σύστημα. Η επιχείρηση που έχει αναλάβει την γραμμή παραγωγής χρησιμοποιεί διάφορες προηγμένες συσκευές, οι οποίες ελέγχουν την γραμμή και τα στάδια παραγωγής. Ο όγκος των πληροφοριών αποθηκεύεται και επεξεργάζεται στο cloud από μία άλλη επιχείρηση. Οι δύο αυτές επιχειρήσεις ανήκουν στο ίδιο οικοσύστημα αφού συνεργάζονται και μετέχουν στην ίδια βιομηχανική διαδικασία. Μάλιστα, ενσωματώνοντας αισθητήρες και έξυπνες συσκευές σε εξοπλισμό και προϊόντα παραγωγής, τα δεδομένα μπορούν να συλλέγονται συνεχώς και να μοιράζονται σε πραγματικό χρόνο με όλους τους ενδιαφερόμενους. Για παράδειγμα, ένας προμηθευτής μπορεί να λάβει αυτόματα δεδομένα σχετικά με τα επίπεδα αποθέματος ενός κατασκευαστή και μπορεί να προετοιμάσει τις αποστολές ανάλογα για τη βελτιστοποίηση της αλυσίδας εφοδιασμού.

**Η τεχνολογία του ψηφιακού δίδυμου (digital twin):** Η τεχνολογία αυτή χρησιμεύει ως εικονικό μοντέλο μιας διαδικασίας, προϊόντος ή υπηρεσίας που συνδυάζει το φυσικό και εικονικό κόσμο. Με άλλα λόγια, ένα ψηφιακό δίδυμο είναι ένα εικονικό αντίγραφο ενός φυσικού αντικειμένου, ατόμου ή διαδικασίας που μπορεί να χρησιμοποιηθεί για την προσομοίωση της συμπεριφοράς του για την καλύτερη δυνατή κατανόηση της λειτουργίας του στην πραγματική ζωή. Τα ψηφιακά δίδυμα συνδέονται με πραγματικές πηγές δεδομένων από το περιβάλλον, πράγμα που σημαίνει ότι το δίδυμο ενημερώνεται σε πραγματικό χρόνο για να αντικατοπτρίζει την αρχική έκδοση. Τα ψηφιακά δίδυμα περιλαμβάνουν επίσης ένα στρώμα συμπεριφορικών γνώσεων και οπτικοποιήσεων που προέρχονται από δεδομένα. Όταν διασυνδέονται σε ένα

σύστημα, τα ψηφιακά δίδυμα μπορούν να σχηματίσουν αυτό που είναι γνωστό ως «μετασύνδεση της επιχείρησης»: ένα ψηφιακό περιβάλλον που αναπαράγει και συνδέει κάθε πτυχή ενός οργανισμού για τη, βοηθώντας στη βελτιστοποίηση των προσομοιώσεων, του σχεδιασμού σεναρίων και της λήψης αποφάσεων (mckinsey, 2023). Αυτή η δομή δύο επιπέδων επιτρέπει στις εταιρείες να προβλέπουν και να επιλύουν προβλήματα μέσα από την προσομοίωση διαφορετικών σεναρίων ή την πρόβλεψη των αποτελεσμάτων των πιθανών αλλαγών. Οι εταιρείες μπορούν να προβλέψουν προβλήματα πριν προκύψουν ή να βελτιστοποιήσουν τις λειτουργίες για καλύτερα αποτελέσματα. Ακόμα, ο σχεδιασμός και η λειτουργικότητα μπορούν να δοκιμαστούν και να τροποποιηθούν στο εικονικό περιβάλλον πριν από την πραγματική εφαρμογή, εξοικονομώντας κόστος και χρόνο στην ανάπτυξη πρωτοτύπων.

**Έξυπνα εργοστάσια:** Αντιπροσωπεύουν τον ακρογωνιαίο λίθο του Industry 4.0, μιας ιδέας που ενσωματώνει προηγμένες τεχνικές κατασκευής με το Διαδίκτυο των Πραγμάτων (IoT) για να δημιουργήσει εξαιρετικά αυτοματοποιημένα, διασυνδεδεμένα και αποδοτικά περιβάλλοντα παραγωγής. Τα εργοστάσια αυτά χαρακτηρίζονται για την προσαρμοστικότητα, αποδοτικότητα πόρων, εργονομία και ενσωμάτωση πελατών και επιχειρηματικών εταίρων σε επιχειρηματικές διαδικασίες και διαδικασίες αξίας. Οι τεχνολογίες που επιτρέπουν αυτές τις δυνατότητες περιλαμβάνουν το Βιομηχανικό Διαδίκτυο των Πραγμάτων (IIoT), τα κυβερνοφυσικά συστήματα και την ανάλυση δεδομένων σε πραγματικό χρόνο. Στα έξυπνα εργοστάσια, οι συσκευές IIoT μπορούν να κυμαίνονται από αισθητήρες σε μηχανήματα που παρακολουθούν την κατάσταση λειτουργίας έως ενεργοποιητές που προσαρμόζουν αυτόματα τις διαδικασίες σε πραγματικό χρόνο. Αυτές οι συσκευές συλλέγουν τεράστιες ποσότητες δεδομένων από το εργοστάσιο, το οποίο χρησιμοποιείται για την παρακολούθηση, την ανάλυση και τη βελτιστοποίηση των λειτουργιών. Αυτή η γνώση που βασίζεται σε δεδομένα βοηθά στην προγνωστική συντήρηση, στη μείωση του χρόνου διακοπής λειτουργίας και στην αύξηση της συνολικής αποτελεσματικότητας της διαδικασίας παραγωγής. Τα κυβερνοφυσικά συστήματα (CPS) στα έξυπνα εργοστάσια επιφέρουν μια απρόσκοπτη ενοποίηση των φυσικών μηχανημάτων του εργοστασίου με συστήματα παρακολούθησης και ελέγχου που βασίζονται σε λογισμικό. Αυτή η ενοποίηση επιτρέπει την αυτόνομη και αυτοβελτιστοποιημένη απόδοση σύνθετων διαδικασιών παραγωγής. Για παράδειγμα, ένα CPS μπορεί να προσαρμόζει δυναμικά τις λειτουργίες σε απόκριση σε αλλαγές στην ποιότητα των υλικών ή στις περιβαλλοντικές συνθήκες. Τέλος, η χρήση αναλύσεων δεδομένων σε πραγματικό χρόνο σε έξυπνα εργοστάσια επιτρέπει την άμεση ανάλυση πληροφοριών από το IIoT και το CPS, επιτρέποντας στο εργοστάσιο να προσαρμόζεται δυναμικά στις νέες συνθήκες, να βελτιστοποιεί τις διαδικασίες και να αποτρέπει πιθανά προβλήματα πριν προκύψουν. Στο πλαίσιο ενός έξυπνου εργοστασίου αλγόριθμοι μηχανικής μάθησης, τεχνητής νοημοσύνης, καθώς και αναλύσεις μεγάλων δεδομένων, οι οποίες επεξεργάζονται τα δεδομένα που συλλέγονται από το IIoT και το CPS συνθέτουν και ερμηνεύουν νέα αναλυτικά στοιχεία που δύναται να χρησιμοποιηθούν ανά περίπτωση. Για παράδειγμα, εάν ένας αισθητήρας εντοπίσει



μια απόκλιση από την κανονική συμπεριφορά του μηχανήματος, τα αναλυτικά στοιχεία σε πραγματικό χρόνο μπορούν να αναλύσουν γρήγορα εάν αυτό αντιπροσωπεύει ένα πιθανό σφάλμα και να εκκινήσει διαδικασίες συντήρησης.

### 1.3 Industry 4.0 και IIoT

Είναι φανερό ότι τα έξυπνα εργοστάσια και το οικοσύστημα του Industry 4.0 χρησιμοποιούν συσκευές και αισθητήρες που συλλέγουν και επεξεργάζονται πληροφορίες και όλα αυτά συμβαίνουν και συνδέονται μέσα από ένα ευρύτερο δίκτυο. Πολλές φορές, ο όρος Industry 4.0 και IIoT συγχέονται, ωστόσο περιέχουν άλλη εννοιολογική σημασία. Το Industry 4.0 αναφέρεται σε ολόκληρο το οικοσύστημα και ότι μέσα αυτό χρησιμοποιεί, ενώ το IIoT περιλαμβάνει το κύριο κορμό που συνδέει τα μέσα αυτά. Το Industry 4.0 είναι μία ευρύτερη κατηγορία λοιπόν και IIoT αναφέρεται στην επέκταση και χρήση IoT σε βιομηχανικούς τομείς και εφαρμογές με μεγάλη εστίαση στην επικοινωνία από μηχανή με μηχανή (M2M), μεγάλα δεδομένα και μηχανική μάθηση.

**Ομοιότητες:** Τόσο το IIoT όσο και το Industry 4.0 προορίζονται να εξορθολογήσουν τις διαδικασίες παραγωγής και να διατηρήσουν την παραγωγή βιώσιμη και κερδοφόρα. Και τα δύο βασίζονται στη σημερινή υψηλή ταχύτητα, ασύρματη και ενσωματωμένη συνδεσιμότητα στο Διαδίκτυο. Τέλος, ο αυτοματισμός, που εφαρμόζεται τόσο στο IIoT όσο και στο Industry 4.0, μπορεί μόνο να κάνει τις υπάρχουσες διαδικασίες ταχύτερες και πιο αποτελεσματικές. Άτομα που γνωρίζουν πώς να ερμηνεύουν και να εφαρμόζουν δεδομένα και ενέργειες που παρέχονται από αυτήν την τεχνολογία είναι το κλειδί για την απόδοση της βιομηχανίας.

**Διαφορές:** Σε ότι αφορά το πεδίο εφαρμογής, το IIoT θα αναφέρεται σχεδόν πάντα αποκλειστικά στον εξοπλισμό μιας εγκατάστασης (και σε τυχόν πιθανές τοποθεσίες διακομιστή εκτός τοποθεσίας). Το Industry 4.0, από την άλλη πλευρά, περιλαμβάνει το IIoT και το τοποθετεί σε ένα πολύ μεγαλύτερο πλαίσιο ανάλυσης, δράσης και μακροπρόθεσμης βιωσιμότητας για τον βιομηχανικό τομέα. Επιπλέον, το IIoT είναι μια εφαρμογή τεχνολογίας — είτε αναφέρεται σε νέες, συνδεδεμένες συσκευές. ή εκ των υστέρων τοποθετημένων αισθητήρων, πομπών δεδομένων, ασύρματου εξοπλισμού κ.λπ. Το Industry 4.0 είναι περισσότερο μια φιλοσοφία που βασίζεται σε τεχνολογία όπως το IIoT, αλλά διατηρεί ένα ευρύτερο πεδίο εφαρμογής και ένα όραμα μεγαλύτερης εικόνας. Το IIoT μπορεί να εκδηλωθεί σε επενδύσεις σε εξοπλισμό, αλλά το Industry 4.0 εκδηλώνεται με συμμετοχή μεταξύ της διοίκησης και της ηγεσίας ( Industrial Technology, 2024).

### 1.4 Συμπεράσματα και Εφαρμογές της Γνώσης από την Ανάλυση του IIoT και του Industry 4.0

Η ενότητα αυτή προσφέρει μια εκτενή εισαγωγή και ανάλυση γύρω από το Βιομηχανικό Διαδίκτυο των Πραγμάτων (IIoT) και τη σύνδεσή του με την εξέλιξη της βιομηχανίας, ειδικά στο πλαίσιο του Industry 4.0. Ανακεφαλαιώνοντας, η εξέλιξη του IIoT πηγάζει από την ιστορική ανάπτυξη των βιομηχανικών επαναστάσεων και την εποχή της μηχανικής παραγωγής με

ατμομηχανές φτάνοντας μέχρι την ψηφιακή εποχή του Industry 4.0. Το IIoT αποτελεί τη φυσική συνέχεια αυτών των τεχνολογικών αλλαγών, με στόχο την αυτοματοποίηση των βιομηχανικών διαδικασιών και την ενίσχυση της αποδοτικότητας μέσω τεχνολογιών όπως οι αισθητήρες, τα μεγάλα δεδομένα και οι συνδεδεμένες συσκευές. Το Industry 4.0 φέρνει την πλήρη ενσωμάτωση των ευφυών τεχνολογιών στις βιομηχανικές διαδικασίες, επιτρέποντας την επικοινωνία μεταξύ συστημάτων, ανθρώπων και μηχανών. Αυτή η επέκταση επιτρέπει τη δημιουργία ενός δικτύου διασυνδεδεμένων εργοστασίων, όπου η παραγωγή μπορεί να γίνει πιο ευέλικτη, αποδοτική και προσαρμοστική. Οι τεχνολογίες, όπως τα ψηφιακά δίδυμα, επιτρέπουν την προσομοίωση και τη βελτιστοποίηση των διαδικασιών, οδηγώντας σε ταχύτερες και πιο οικονομικές παραγωγές. Το Industry 4.0 και το IIoT συνδέονται στενά, με το πρώτο να περιλαμβάνει μια ευρύτερη φιλοσοφία, ενώ το IIoT εστιάζει στην πρακτική εφαρμογή τεχνολογιών, όπως η επικοινωνία μεταξύ μηχανών (M2M) και η συλλογή και ανάλυση δεδομένων σε πραγματικό χρόνο. Η σημαντική διαφορά έγκειται στο ότι το IIoT αφορά κυρίως τις εφαρμογές σε βιομηχανικούς τομείς, ενώ το Industry 4.0 ενσωματώνει αυτές τις τεχνολογίες σε μια μεγαλύτερη στρατηγική μετασχηματισμού των διαδικασιών παραγωγής.

Η γνώση που αποκομίζει ο αναγνώστης από αυτή την ενότητα αποτελεί μία εξαιρετική βάση για την κατανόηση του Βιομηχανικού Διαδικτύου των Πραγμάτων (IIoT) και το Industry 4.0. Με απλό τρόπο, εξηγείται η σημασία αυτών των τεχνολογιών και πώς επηρεάζουν τη βιομηχανία. Ο μέσος αναγνώστης μπορεί να ξεκαθαρίσει σημαντικές έννοιες, όπως τη σχέση μεταξύ του IIoT και του Industry 4.0, και να κατανοήσει την εξέλιξη των τεχνολογιών από την παραδοσιακή βιομηχανία μέχρι την ψηφιοποιημένη παραγωγή. Η σαφή εικόνα για την δυνατότητα εφαρμογής των τεχνολογιών στη βιομηχανία μπορεί να φανεί χρήσιμη για μελλοντικές εργασίες. Παράλληλα αποτελεί μία σύντομη πηγή γνώσης για όσους θέλουν να κατανοήσουν τις έννοιες που αναλύονται και έχει σκοπό να εμπνεύσει για περαιτέρω ενασχόληση με το IIoT και τις δυνατότητες που προσφέρει στον τομέα της τεχνολογίας και της παραγωγής. Η ανησυχία που αναδεικνύεται για την ασφάλεια των χρησιμοποιούμενων συστημάτων και τεχνολογιών, μπορεί να οδηγήσει στην ανάπτυξη νέων μοντέλων και διαδικασιών λειτουργίας των οικοσυστημάτων του Industry 4.0. Είναι σημαντικό να προβάλλονται τόσο τα οφέλη των νέων τεχνολογιών, με σκοπό την γρηγορότερη τους ενσωμάτωση και αξιοποίηση τους από τις επιχειρήσεις, όσο και μειονεκτήματα τους σε ότι αφορά την ασφάλεια και ιδιωτικότητα που προσφέρουν ώστε να γίνουν έγκαιρα οι απαραίτητες διορθώσεις χωρίς να υποβαθμιστεί η αξία του των προσωπικών δεδομένων στο βωμό του γρήγορου κέρδους.

Επιπρόσθετα, όσο γρηγορότερα γίνει αντιληπτή η σημασία των τεχνολογιών του IIoT τόσο αποδοτικότερες και επικερδείς θα γίνουν οι επιχειρήσεις, αφού θα μειωθούν τα κόστη παραγωγής και θα βελτιωθεί η ποιότητα των προϊόντων τους. Πιο συγκεκριμένα, η αυτοματοποίηση μέσω του IIoT μπορεί να μειώσει την ανάγκη για ανθρώπινη παρέμβαση σε καθημερινές διαδικασίες, επιτρέποντας στους εργαζομένους να εστιάσουν σε πιο στρατηγικές εργασίες. Τα έξυπνα εργοστάσια μπορούν να προσαρμόζονται δυναμικά στις συνθήκες της αγοράς, μειώνοντας τους χρόνους διακοπής λειτουργίας και αυξάνοντας την παραγωγικότητα.

Ακόμη, οι αναλύσεις δεδομένων σε πραγματικό χρόνο που παρέχονται από τα συστήματα IIoT μπορούν να αποτρέψουν βλάβες στον εξοπλισμό πριν αυτές εμφανιστούν, μειώνοντας τα κόστη συντήρησης. Επίσης, η πρόβλεψη μέσω ψηφιακών διδύμων μπορεί να βελτιστοποιήσει τα στάδια της παραγωγής, επιτυγχάνοντας καλύτερα αποτελέσματα με χαμηλότερο κόστος. Καθώς οι τεχνολογίες αυτές επεκτείνονται, τα θέματα ασφάλειας των δεδομένων είναι ζωτικής σημασίας. Η προστασία των δεδομένων και η ασφαλής διαχείριση των πληροφοριών θα ενισχύσουν την εμπιστοσύνη των καταναλωτών και των επιχειρηματικών εταίρων.

Συνοψίζοντας, η γνώση που αποκομίζεται από την κατανόηση του IIoT και του Industry 4.0 είναι εξαιρετικά χρήσιμη για τη μελλοντική βιωσιμότητα των βιομηχανιών, καθώς οι τεχνολογίες αυτές αποτελούν τη βάση για την καινοτομία και την αποδοτικότητα.

## ΚΕΦΑΛΑΙΟ 2: ΤΟ ΒΙΟΜΗΧΑΝΙΚΟ ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ (IIOT)

### 2.1 Ορισμός

Το Βιομηχανικό Διαδίκτυο των Πραγμάτων- Industrial Internet of Things (IIoT) είναι ένας σχετικά νέος τομέας έρευνας και ανάπτυξης, όπου εξακολουθούν να λείπουν καθιερωμένες τεχνολογίες και λύσεις. Η σύγκλιση της Πληροφορικής (IT) και της Επιχειρησιακής Τεχνολογίας (Operational Technology OT) είναι ένα σημαντικό ζήτημα για τις βιομηχανίες και πρέπει να παρουσιαστούν κοινές προσεγγίσεις για την ανάπτυξη προϊόντων και υπηρεσιών για την επιτυχή εκμετάλλευση των τεχνολογιών IIoT. Η υλοποίηση εφαρμογών IIoT είναι ένα πρόβλημα μηχανικής συστημάτων και απαιτείται μια διεπιστημονική και ολιστική προσέγγιση για την ανάπτυξη λύσεων για πολύπλοκα προβλήματα που περιλαμβάνουν υλικό, λογισμικό, δεδομένα, μηχανήματα και προσωπικό (E. Sisinni, 2018).

Ο σχεδιασμός των εφαρμογών IIoT απαιτεί την αντιμετώπιση νέων απαιτήσεων, συμπεριλαμβανομένων εκείνων που σχετίζονται με υπολογιστές ακμών και ομίχλης, αποτελεσματικές αρχιτεκτονικές επικοινωνίας, ασφάλεια στον κυβερνοχώρο, ιδιωτικότητα, επεκτασιμότητα, υποστήριξη πρωτοκόλλου και γνωστικούς υπολογιστές. Η υιοθέτηση ανοιχτών προτύπων, προδιαγραφών και αρχιτεκτονικών IIoT θα βοηθήσει επίσης το IIoT να κυριαρχήσει στον κλάδο. Τα τελευταία χρόνια οι παρακάτω δύο οργανισμοί προωθούν το IIoT (Drosatos, 2020):

- Βιομηχανική Κοινοπραξία Διαδικτύου<sup>1</sup>, η οποία ακολουθεί μια προσέγγιση μεταξύ τομέων για να επιταχύνει την ανάπτυξη, την υιοθέτηση και την ευρεία διάδοση του IIoT.
- Plattform Industrie 4.0<sup>2</sup>, που εστιάζει στις έννοιες της αποδοτικής κατασκευής και το εργοστάσιο smart (στη Γερμανία).

Και οι δύο ομάδες έχουν αναπτύξει αρχιτεκτονικές αναφοράς, την Industrial Internet Reference Architecture (IIRA) και την Reference Architectural Model Industry 4.0 (RAMI 4.0), αντίστοιχα, για να βοηθήσουν στον εξορθολογισμό της τυποποίησης και της υιοθέτησης της τεχνολογίας IIoT.

Στην εικόνα Figure 2, απεικονίζεται η υποδομή του IIoT. Αισθητήρες συλλέγουν δεδομένα από το περιβάλλον όπως η θερμοκρασία και η υγρασία, ενεργοποιητές δύναται να ελέγξουν μηχανικά και ηλεκτρονικά την κατάσταση ενός συστήματος και περιφερειακοί κόμβοι επεξεργάζονται τα δεδομένα που συλλέγονται από τους αισθητήρες σε τοπικό επίπεδο. Πύλες λειτουργούν ως ενδιάμεσοι κόμβοι επιτρέποντας την ασφαλή μετάδοση δεδομένων. Στη συνέχεια τα δεδομένα φτάνουν στην πλατφόρμα IoT για ανάλυση ή σε διακομιστές. Στο πάνω

---

<sup>1</sup> IIC – <https://www.iiconsortium.org>

<sup>2</sup> <https://www.plattform-i40.de>

μέρος της εικόνας βρίσκονται οι λειτουργίες που υποστηρίζονται από τη συγκεκριμένη υποδομή όπως είναι η επεξεργασία και ανάλυση δεδομένων, ενσωμάτωση επιχειρησιακών εφαρμογών και βάσεις αυτοματοποιημένων διεργασιών.

## IloT infrastructure

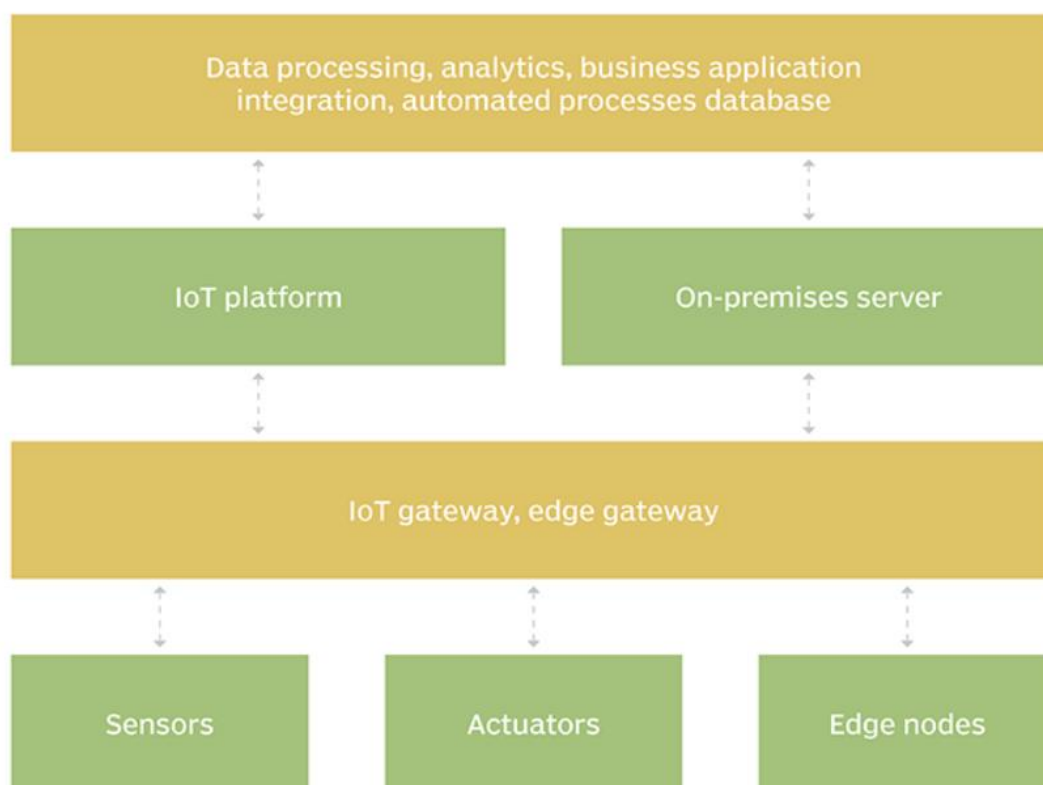


Figure 2 Υποδομή του IloT (Gillis, n.d.)

### 2.2 Εφαρμογές IloT

Η αναβαθμισμένη απόδοση, οι παρατηρήσεις και η τροποποίηση του χώρου εργασίας περιλαμβάνονται στο Industrial Internet of Things (IIoT). Μέχρι το τέλος του 2030, πιστεύεται ότι το παγκόσμιο ΑΕΠ θα αυξηθεί στα 15 τρισεκατομμύρια δολάρια όταν το IIoT θα είναι εγκατεστημένο παγκοσμίως. Μερικές από τις εφαρμογές του IIoT είναι οι παρακάτω (Jaidka, 2020):

- **Κατασκευή:** Πολλές πόρτες είναι ανοιχτές, για τη δημιουργία ολοκαίνουργιων επιχειρήσεων και καλών στιγμών στην αγορά από αυτόν τον εξαιρετικά ενοποιημένο κυβερνοφυσικό χώρο. Το IIoT ενισχύει την επιχειρηματική αξία και θα οδηγήσει στο Industry 4.0. Κατά την κατασκευή, οι προσεγγίσεις IIoT δίνουν προτεραιότητα στα δεδομένα πελατών και τη συλλογή τους από πολλαπλές πηγές για την ανάπτυξη

πρακτικών πληροφοριών. Αυτό οδηγεί σε βελτιωμένες λύσεις που επιτρέπουν στους κατασκευαστές να ανταποκρίνονται πιο γρήγορα στους πελάτες τους. Επίσης, το IIoT μειώνει τους χρόνους απόκρισης.

- **Γεωργία:** Το IoT έχει μεγάλη ποικιλία εφαρμογών στη γεωργία, όπως συλλογή δεδομένων βροχοπτώσεων, υγρασίας, ταχύτητας ανέμου, περιεκτικότητας εδάφους, θερμοκρασίας και προσβολής από παράσιτα. Αυτά τα δεδομένα είναι πολύ χρήσιμα για τη βελτίωση των γεωργικών τεχνικών, μειώνουν τα απόβλητα και ελαχιστοποιούν τις προσπάθειες που απαιτούνται για τη διαχείριση των καλλιεργειών και για την αναβάθμιση της ποσότητας και της ποιότητας των καλλιεργειών και της εργασίας.
- **Στρατιωτικές εφαρμογές:** Στον στρατιωτικό τομέα, η εφαρμογή των τεχνολογιών IoT χρησιμοποιείται κυρίως για σκοπούς έρευνας, επιθεώρησης και σε οποιουσδήποτε άλλους σκοπούς που σχετίζονται με τη μάχη και σε αυτό η χρήση αισθητήρων, ρομπότ, βιομετρικών στοιχείων, οχημάτων και άλλης έξυπνης τεχνολογίας θα βοηθήσει περαιτέρω.
- **Internet of Battlefield Things:** Το Εργαστήριο Έρευνας Στρατού των ΗΠΑ (ARL) ξεκίνησε ένα έργο Internet of Battlefield Things (IoBT) του οποίου η προτεραιότητα είναι να αυξήσει τις δυνατότητες των στελεχών του στρατού με τη βοήθεια του IoT. Το ARL σχημάτισε μια συμμαχία με ερευνητές πανεπιστημίου, βιομηχανίας και στρατού το 2017, στόχος των οποίων είναι να ενισχύσει τον εννοιολογικό θεσμό των τεχνολογιών IoT και τις χρήσεις τους στη λειτουργία του Στρατού. Το όνομα αυτής της πρωτοβουλίας που ξεκίνησε από την ARL είναι επίσης γνωστό ως Internet of Battlefield Things.
- **Ocean of Things:** Η Υπηρεσία Προηγμένων Ερευνητικών Προγραμμάτων Άμυνας (DARPA) των ΗΠΑ εγκαινίασε τον Ωκεανό των Πραγμάτων<sup>3</sup>. Το κίνητρο του έργου Ocean 2.0 ή Ocean of Things (OoT) είναι η έναρξη ή η διάδοση του Διαδικτύου των Πραγμάτων (IoT) που καλύπτει τις μεγάλες ωκεάνιες περιοχές με κίνητρο τη συλλογή, παρατήρηση, συγκέντρωση και επιθεώρηση περιβαλλοντικών δεδομένων και δεδομένων δράσης πλοίων. Διάφοροι αισθητήρες που επιπλέουν στους Ωκεανούς συλλέγουν και στέλνουν δεδομένα σε ένα δίκτυο υπολογιστών. Εκεί τα δεδομένα επεξεργάζονται και συνθέτουν μία εικόνα σχετικά με τη θερμοκρασία των Ωκεανών, το θόρυβο της υποθαλάσσιας περιοχής και άλλες ενδιαφέρουσες εικόνες με σκοπό την προστασία του περιβάλλοντος.

---

<sup>3</sup> <https://oceanofthings.darpa.mil/>



**Figure 3 Ωκεανός των Πραγμάτων**

### 2.3 Προκλήσεις που αντιμετωπίζει το IIoT

Ο φυσικός κόσμος μετατρέπεται αργά σε ψηφιακό κόσμο από τον συνηθισμένο κόσμο λόγω της έξυπνης τεχνολογίας και συσκευών που επιτρέπουν στους χρήστες και τις συσκευές να βρίσκονται σε συνεχή επικοινωνία μεταξύ τους. Πλέον είναι πιο αποτελεσματικό λόγω της τεχνητής νοημοσύνης, της μηχανικής μάθησης κ.λπ. Όταν η επικοινωνία μηχανής με μηχανή συνδυάζεται με ανάλυση μεγάλων δεδομένων σε έναν κλάδο, τότε αυξάνονται άμεσα τα επίπεδα παραγωγικότητας, αποδοτικότητας και απόδοσης στα συστήματα IIoT. Τώρα, οι περισσότερες επιχειρηματικές εταιρείες θέλουν να συνεργαστούν με εταιρείες ανάπτυξης IoT για να εμπλέξουν την πιο πρόσφατη τεχνολογία στην επιχείρησή τους. Αυτό δημιουργεί νέες προκλήσεις και ευκαιρίες για τους ηγέτες των επιχειρήσεων. Αναλύεται ότι στο μέλλον, το 72% αυτών των εταιρειών μπορεί να χάσουν μερίδιο αγοράς εάν δεν καταφέρουν να συμβαδίσουν με τα νέα δεδομένα.

Μερικές από τις πιο σημαντικές προκλήσεις που εντοπίζονται για το IIoT είναι οι παρακάτω (Jaidka, 2020):

- **Ασφάλεια:** Καθώς απολαμβάνουμε πολλές ανέσεις από το IoT, πρέπει επίσης να φροντίζουμε για την ασφάλεια και το απόρρητο στις έξυπνες συσκευές. Πρέπει να δώσουμε κύρια προτεραιότητα στην ασφάλεια κατά το σχεδιασμό των συσκευών IoT. Το απόρρητο των προσωπικών μας δεδομένων και το απόρρητο της σωματικής μας ευεξίας περιλαμβάνονται σε αυτό. Η ασφάλεια είναι η μεγαλύτερη πρόκληση για την ομάδα τεχνολογίας IIoT, καθώς μια μικρή ή τακτική απειλή θα μπορούσε να διαλύσει ολόκληρη την επιχείρηση. Αν μια εταιρεία λύσει αυτό το ζήτημα με το IIoT ή εάν παρέχονται νέα εργαλεία ασφαλείας στο δίκτυο, κάτι τέτοιο απαιτεί αυξημένο κόστος και συντήρηση. Έτσι, οι επιχειρήσεις συχνά αποφεύγουν την ιδέα του IIoT μέχρι να εξοπλιστούν με ένα σταθερό σχέδιο ασφαλείας.
- **Αποθήκευση δεδομένων:** Η αποθήκευση δεδομένων είναι μια άλλη σημαντική πρόκληση για κάθε εταιρεία ή επιχείρηση. Τα δεδομένα που είχαν αποθηκευτεί στο παρελθόν

χρησιμοποιούνται για όλες τις προβλεπόμενες δραστηριότητες. Σήμερα, καμία από τις επιχειρήσεις δεν χρησιμοποιεί μια παλιά συμβατική μέθοδο για την αντιμετώπιση δεδομένων που θα ήταν κυρίως η ανάλυση δεδομένων υψηλής συχνότητας, η παρατήρησή τους και η έγκαιρη απόρριψή τους. Είναι υποχρεωτικό για κάθε εταιρεία να υιοθετήσει το κατάλληλο σχέδιο για την ασφαλή αποθήκευση δεδομένων πριν από την εκτέλεση του IIoT σε πλήρη λειτουργία.

- **Προκλήσεις Analytics:** Είναι απαραίτητο για τους συνεργάτες του Data Analytics να συμπεριλάβουν την επεξεργασία, τον καθαρισμό και την αναπαράσταση δεδομένων κατά την εκτέλεση της αρχιτεκτονικής του IIoT. Υπάρχει σίγουρα αρκετός χώρος για παράγοντα λειτουργικότητας και αυτός ο παράγοντας προσθέτει αναλυτικά στοιχεία σε πραγματικό χρόνο ή προγνωστικά σε μια λύση IIoT απλά.

## 2.4 Οι Τεχνολογίες που συνθέτουν το IIoT

**Αισθητήρες και Ενεργοποιητές:** Οι αισθητήρες και οι ενεργοποιητές αποτελούν τους ακρογωνιαίους λίθους του βιομηχανικού αυτοματισμού. Αυτές οι εξελιγμένες συσκευές δεν είναι απλώς εξαρτήματα, αποτελούν το ίδιο το θεμέλιο πάνω στο οποίο οικοδομήθηκε η τέταρτη βιομηχανική επανάσταση, μετατρέποντας τα παραδοσιακά εργοστάσια σε έξυπνα, προσαρμοστικά και εξαιρετικά αποδοτικά συστήματα. Αρχικά, οι αισθητήρες είναι τα μάτια και τα αυτιά του βιομηχανικού περιβάλλοντος, που συγκεντρώνουν κρίσιμα σημεία δεδομένων όπως η θερμοκρασία, η πίεση και οι ρυθμοί ροής. Αυτός ο πλούτος πληροφοριών επιτρέπει στις μηχανές να λαμβάνουν τεκμηριωμένες αποφάσεις, ενισχύοντας την αυτοματοποίηση και ανοίγοντας το δρόμο για πιο έξυπνες διαδικασίες παραγωγής. Οι ενεργοποιητές, από την άλλη πλευρά, λειτουργούν όπως οι μύες στο ανθρώπινο σώμα, αντιδρώντας σε εντολές που βασίζονται σε δεδομένα, προσαρμόζοντας τους φυσικούς μηχανισμούς σε πραγματικό χρόνο και διασφαλίζοντας ότι οι διαδικασίες παραγωγής προσαρμόζονται απρόσκοπτα στις μεταβαλλόμενες συνθήκες. Δεύτερον, ένα από τα κύρια πλεονεκτήματα αυτών των τεχνολογιών είναι η προγνωστική συντήρηση. Οι αισθητήρες παρακολουθούν συνεχώς την κατάσταση του εξοπλισμού και προβλέπουν πιθανές βλάβες πριν συμβούν, μειώνοντας σημαντικά το χρόνο διακοπής λειτουργίας και το κόστος συντήρησης. Οι ενεργοποιητές ανταποκρίνονται κάνοντας τις απαραίτητες ρυθμίσεις για την αποφυγή ζημιών, βελτιστοποιώντας περαιτέρω τις λειτουργίες και διατηρώντας συνεχείς ροές παραγωγής. Τόσο οι αισθητήρες όσο και οι ενεργοποιητές βελτιστοποιούν τη χρήση ενέργειας και γενικότερα τη διαχείριση των πόρων. Παρέχοντας λεπτομερείς πληροφορίες για τη διαδικασία παραγωγής, συμβάλλουν στην ελαχιστοποίηση των απορριμμάτων και στη μεγιστοποίηση της αποτελεσματικότητας. Αυτό όχι μόνο μειώνει το λειτουργικό κόστος, αλλά μειώνει επίσης τις περιβαλλοντικές επιπτώσεις της Βιομηχανίας. Οι αισθητήρες ανάλογα με το ερέθισμα στο οποίο αντιδρούν μπορούν να κατηγοριοποιηθούν στις ακόλουθες κατηγορίες όπως φαίνονται στον παρακάτω πίνακα.



**Table 1** Περιληπτική περιγραφή των διαφόρων τύπων αισθητήρων όπως παρατίθενται στο (Suman, 2021)

| α/α | Είδη Αισθητήρων         | Περιγραφή                                                                                                                                             |
|-----|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1   | Αισθητήρας πίεσης       | Μετρά την πίεση αερίων ή υγρών, παρέχοντας σήματα στις συσκευές ελέγχου και απεικόνισης.                                                              |
| 2   | Αισθητήρας θερμοκρασίας | Ανιχνεύει θερμικές παραμέτρους, μετατρέπει τα δεδομένα σε ηλεκτρονικά σήματα για την παρακολούθηση ή σηματοδότηση αλλαγών θερμοκρασίας.               |
| 3   | Αισθητήρας εγγύτητας    | Εντοπίζει την παρουσία κοντινών αντικειμένων χωρίς φυσική επαφή, χρησιμοποιώντας ηλεκτρομαγνητικά πεδία.                                              |
| 4   | Αισθητήρας υγρασίας     | Μετρά τους υδρατμούς στο περιβάλλον, μετατρέποντας αυτές τις μετρήσεις σε σήματα εισόδου.                                                             |
| 5   | Αισθητήρας δύναμης      | Μεταφράζει τις μηχανικές δυνάμεις σε ψηφιακά σήματα που αντικατοπτρίζουν το μέγεθος της ασκούμενης δύναμης.                                           |
| 6   | Αισθητήρας ροής         | Μετρά τον ρυθμό ροής ενός ρευστού και δίνει σήματα εξόδου στον ελεγκτή.                                                                               |
| 7   | Αισθητήρας αερίου       | Εντοπίζει την παρουσία και τις ιδιότητες των αερίων, παρέχοντας σήματα εξόδου στον ελεγκτή.                                                           |
| 8   | Αισθητήρας ελαττωμάτων  | Προσδιορίζει ελαττώματα σε υλικά χρησιμοποιώντας υπερήχους, ακουστικά ή άλλα μέσα, ζωτικής σημασίας για τον ποιοτικό έλεγχο.                          |
| 9   | Αισθητήρας χρώματος     | Ανιχνεύει το χρώμα επιφανειών ή υγρών χρησιμοποιώντας φως που εκπέμπεται και ανακλάται πίσω σε έναν δέκτη.                                            |
| 10  | Αισθητήρας φωτός        | Μετατρέπει τη φωτεινή ενέργεια σε ηλεκτρική ενέργεια, που χρησιμοποιείται σε διάφορες βιομηχανίες για την ανίχνευση και τη μέτρηση της έντασης φωτός. |

**Τεχνολογίες Συνδεσιμότητας:** Οι τεχνολογίες συνδεσιμότητας είναι θεμελιώδεις για το Βιομηχανικό Διαδίκτυο των Πραγμάτων (IIoT), επιτρέποντας την απρόσκοπτη επικοινωνία μεταξύ συσκευών, μηχανημάτων και συστημάτων σε βιομηχανικά περιβάλλοντα. Αυτές οι τεχνολογίες κυμαίνονται από παραδοσιακές ενσύρματες συνδέσεις έως προηγμένες ασύρματες λύσεις, η καθεμία από τις οποίες εξυπηρετεί διαφορετικές ανάγκες και εφαρμογές.

#### Ενσύρματες συνδέσεις

Αρχικά, οι ενσύρματες συνδέσεις προσφέρουν αξιοπιστία, ασφάλεια και δυνατότητα χειρισμού υψηλών ρυθμών δεδομένων. Ως εκ τούτου, αποτελούν την κατάλληλη επιλογή για τη σύνδεση σταθερών συσκευών IIoT που βρίσκονται σε κοντινή απόσταση μεταξύ τους. Ωστόσο, το υψηλότερο κόστος που σχετίζεται με την εφαρμογή καλωδίων, μαζί με την έλλειψη ευελιξίας

και επεκτασιμότητας, καθιστούν τις ενσύρματες συνδέσεις λιγότερο ελκυστικές για ορισμένες εφαρμογές IoT. Το Ethernet και το Power Line Communication (PLC) είναι οι κύριες τεχνολογίες που χρησιμοποιούνται για τις ενσύρματες συνδέσεις συσκευών (Dian, 2020). Πρώτα, το **Ethernet** είναι μια ευρέως χρησιμοποιούμενη τεχνολογία τοπικού δικτύου local area network (LAN), ιδανική για τη σύνδεση συσκευών IoT μέσω ενός μεταγωγέα Ethernet, παρέχοντας συνδεσιμότητα IP. Είναι καλύτερο για σταθερές συσκευές IoT, καθώς απαιτεί μικρές αποστάσεις μεταξύ των συσκευών και του μεταγωγέα λόγω περιορισμών στο μήκος καλωδίου και των επιπλέον κοστών που σχετίζονται με αυτό. Σήμερα οι ταχύτητες ξεπερνούν τα 100 Gbps με πρότυπα έως 400 Gbps που έχουν ήδη εγκριθεί και οι μελλοντικές ταχύτητες αναμένεται να φτάσουν έως και 1,6 Tbps. Ωστόσο, τέτοιες υψηλές ταχύτητες είναι γενικά περιττές για τις περισσότερες εφαρμογές IoT, οι οποίες συχνά μεταδίδουν μικρές ποσότητες δεδομένων. Αν και το παραδοσιακό Ethernet δεν υποστηρίζει διαφορετικά επίπεδα ποιότητας υπηρεσίας, έχουν αναπτυχθεί προσαρμογές όπως το δίκτυο με χρονική ευαισθησία Time-Sensitive Networking (TSN) για να καλύπτουν τις ανάγκες των εφαρμογών που απαιτούν επικοινωνία σε πραγματικό χρόνο. Το TSN ενισχύει το Ethernet για να υποστηρίξει κίνηση τόσο ευαίσθητη στον χρόνο όσο και μη ευαίσθητη στον χρόνο στην ίδια υποδομή δικτύου, διασφαλίζοντας την έγκαιρη παράδοση πακέτων μέσω συγχρονισμένου εξοπλισμού δικτύου και προγραμματισμένης διαχείρισης κίνησης. Περιλαμβάνει χαρακτηριστικά όπως το δικαίωμα προτίμησης (Preemption) για τη μείωση του λανθάνοντος χρόνου μετάδοσης. Αυτό το χαρακτηριστικό επιτρέπει στα πακέτα υψηλής προτεραιότητας να διακόπτουν τα πακέτα χαμηλότερης προτεραιότητας και να παίρνουν τη θέση του στη μεταφορά των δεδομένων, βελτιώνοντας έτσι την αποτελεσματικότητα και την απόδοση του δικτύου. Οικονομικές λύσεις ενσύρματης συνδεσιμότητας χωρίς εκτεταμένη υποδομή δύναται να προσφέρει η τεχνολογία **PLC**. Αυτή μπορεί να χωριστεί σε κατηγορίες στενής ζώνης και ευρυζωνικότητας.

Το PLC στενής ζώνης λειτουργεί μεταξύ 3 KHz και 500 kHz, υποστηρίζοντας ταχύτητες δεδομένων έως και αρκετές εκατοντάδες kbps και μπορεί να καλύψει αποστάσεις έως και αρκετά χιλιόμετρα χωρίς να χρειάζεται επαναλήπτες. Συχνά χρησιμοποιεί τεχνικές διαμόρφωσης όπως η ορθογώνια πολυπλεξία διαίρεσης συχνότητας (OFDM), η δυαδική μετατόπιση φάσης (BPSK) και η πληκτρολόγηση μετατόπισης συχνότητας (FSK), με τα πρότυπα να ποικίλλουν μεταξύ των παγκόσμιων φορέων τυποποίησης όπως CENELEC, ARIB, EPRI και FCC. Το ευρυζωνικό PLC, από την άλλη πλευρά, λειτουργεί σε υψηλότερες συχνότητες (1,8 MHz έως 250 MHz) και μπορεί να επιτύχει υψηλότερους ρυθμούς δεδομένων έως και αρκετές εκατοντάδες Mbps, αλλά σε μικρότερες αποστάσεις. Τεχνολογίες όπως το HomePlug έχουν εξελιχθεί σε αυτήν την κατηγορία, υποστηρίζοντας υψηλότερες ταχύτητες δεδομένων και ενεργειακή απόδοση, και είναι ιδιαίτερα χρήσιμες σε αστικά περιβάλλοντα όπου η εξασθένηση του ασύρματου σήματος είναι υψηλή, όπως σε εφαρμογές έξυπνων μετρητών. Η τεχνολογία **Fieldbus** αποτελεί μία παλαιότερη τεχνολογία μεταφοράς δεδομένων σε πραγματικό χρόνο. Με την εξέλιξη του Ethernet και τα χαρακτηριστικά που προστέθηκαν, η σύγχρονη Βιομηχανία δεν επενδύει αρκετά σε αυτή. Ωστόσο το Fieldbus περιλαμβάνει διάφορα

πρωτόκολλα σχεδιασμένα για κατανεμημένο έλεγχο σε πραγματικό χρόνο και αποτελεί βασικό στοιχείο στα βιομηχανικά περιβάλλοντα εδώ και δεκαετίες. Αυτά τα συστήματα είναι γνωστά για την αξιοπιστία τους και είναι βαθιά ενσωματωμένα σε πολλές υπάρχουσες λειτουργίες. Παρά τα σαφή πλεονεκτήματα του Ethernet, η πλήρης μετατόπιση του Fieldbus δεν είναι άμεση ή καθολικά εφαρμόσιμη. Πολλές βιομηχανίες συνεχίζουν να χρησιμοποιούν το Fieldbus λόγω της υπάρχουσας υποδομής, του κόστους που σχετίζεται με τη μετάβαση στο Ethernet και της εκπαίδευσης που απαιτείται για την εφαρμογή νέων τεχνολογιών. Τα συστήματα Fieldbus εξακολουθούν να είναι λειτουργικά και επαρκή για πολλές εφαρμογές, ιδιαίτερα όπου δεν απαιτούνται οι πλήρεις δυνατότητες του Ethernet. Η μετάβαση στο Ethernet είναι πιθανό να είναι σταδιακή, με τα δύο συστήματα να συνυπάρχουν για κάποιο χρονικό διάστημα, ειδικά σε περιβάλλοντα όπου το κόστος ή η διακοπή μιας πλήρους μετάβασης στο Ethernet θα ήταν απαγορευτική.

### Ασύρματες συνδέσεις

Τα ασύρματα δίκτυα κατοικοεδρεύουν στο χώρο του IoT/IIoT αφού παρουσιάζουν αρκετά πλεονεκτήματα σε σχέση με τα ενσύρματα δίκτυα, κυρίως λόγω της ικανότητάς τους να υποστηρίζουν κινητούς κόμβους και της επεκτασιμότητάς τους. Οι ασύρματες τεχνολογίες όπως το Bluetooth Low Energy (BLE), το Zigbee και το WiFi είναι κρίσιμες για τη συνδεσιμότητα IoT συσκευών λόγω της ευελιξίας και της οικονομικής τους αποδοτικότητας (Dian, 2020). Το **BLE** παρουσιάστηκε το 2010 ως μέρος του Bluetooth 4.0 και πρόκειται για μια ενεργειακά αποδοτική έκδοση του Bluetooth, ιδανική για εφαρμογές που λειτουργούν με μπαταρία και απαιτούν ελάχιστη κατανάλωση ενέργειας. Υποστηρίζει συνδεσιμότητα μικρής εμβέλειας μέσω διαφόρων τρόπων λειτουργίας, όπως διαφήμιση, σάρωση και εκκίνηση, επιτρέποντας στις συσκευές να ανακαλύπτουν και να συνδέονται αποτελεσματικά μεταξύ τους. Το **Zigbee** λειτουργεί με το πρότυπο IEEE 802.15.4 και χρησιμοποιείται κυρίως σε εφαρμογές που απαιτούν χαμηλούς ρυθμούς δεδομένων και υψηλή χωρητικότητα δικτύου, υποστηρίζοντας έως και 64K συσκευές. Χρησιμοποιεί μια τοπολογία δικτύου που βελτιώνει την αξιοπιστία και την εμβέλεια της σύνδεσης, καθιστώντας το κατάλληλο για έξυπνα οικιακά συστήματα και άλλες εφαρμογές IoT. Το WiFi από την έναρξή του το 1997, έχει εξελιχθεί σημαντικά, υποστηρίζοντας υψηλούς ρυθμούς δεδομένων και εκτεταμένη κάλυψη. Λειτουργεί κάτω από διάφορα πρότυπα, με το πιο πρόσφατο, WiFi 6, προσφέροντας ταχύτητες έως και 9,6 Gbps. Η τεχνολογία WiFi προσαρμόζεται τόσο στις ζώνες των 2,4 GHz όσο και στα 5 GHz και οι νεότερες εκδόσεις όπως το WiFi 6E επεκτείνονται στο φάσμα των 6 GHz, παρέχοντας βελτιωμένη απόδοση και μειωμένη καθυστέρηση. Ο ρόλος του WiFi στο IIoT περιλαμβάνει τη σύνδεση μιας μεγάλης σειράς συσκευών ρυθμισμένες για βιομηχανική χρήση όπου η ευέλικτη ανάπτυξη και οι οικονομικές λύσεις είναι ζωτικής σημασίας. Αυτές οι συσκευές μπορούν να κυμαίνονται από αισθητήρες και ενεργοποιητές έως μεγαλύτερα, πιο σύνθετα ρομποτικά συστήματα που απαιτούν αξιόπιστη επικοινωνία για επεξεργασία και έλεγχο δεδομένων σε πραγματικό χρόνο. Τα δίκτυα κινητής τηλεφωνίας, ειδικά οι εξελίξεις στο long term evolution (LTE) και η εισαγωγή του 5G, καθίστανται ζωτικής σημασίας για το IIoT. Αυτές οι τεχνολογίες παρέχουν την

απαραίτητη υποδομή για το IIoT, προσφέροντας αξιόπιστη, υψηλής ταχύτητας και ευρέως προσβάσιμη συνδεσιμότητα που υποστηρίζει ένα ευρύ φάσμα βιομηχανικών εφαρμογών. Αρχικά, η τεχνολογία **LTE** επεκτείνεται συνεχώς και χαρακτηρίζεται ως το ταχύτερα αναπτυσσόμενο πρότυπο κινητής τηλεφωνίας, επηρεάζοντας σημαντικά το IIoT. Ευνοεί ιδιαίτερα βιομηχανικά περιβάλλοντα λόγω της ικανότητάς του να παρέχει αξιόπιστη συνδεσιμότητα χαμηλής καθυστέρησης σε ευρείες περιοχές, υποστηρίζοντας μια πληθώρα συσκευών. Αυτό καθιστά το LTE ιδανικό για εφαρμογές κρίσιμες για την αποστολή, όπως έξυπνα συστήματα μεταφοράς, διανομή ηλεκτρικής ενέργειας και εγκαταστάσεις επεξεργασίας νερού, όπου η αδιάλειπτη συνδεσιμότητα και οι υψηλές ταχύτητες δεδομένων είναι ζωτικής σημασίας. Επιπλέον, η αρχιτεκτονική όλα- IP (all-IP) του LTE προσφέρει ευελιξία και επεκτασιμότητα, κάτι που είναι κρίσιμο για τις μελλοντικές εφαρμογές IIoT και το προστατεύουν από την απαρχαίωση και από δαπανηρές αναβαθμίσεις. Η υιοθέτηση της τεχνολογίας επιταχύνεται περαιτέρω με την ανάπτυξη ολοκληρωμένων κυκλωμάτων και μονάδων ειδικά για LTE, μειώνοντας το κόστος και ενισχύοντας την ενσωμάτωση προηγμένων χαρακτηριστικών, ενθαρρύνοντας την ευρεία χρήση σε διάφορους κλάδους (μοχα, 2016). Η τεχνολογία **5G** προωθεί τις δυνατότητες των κυψελοειδών δικτύων, προσφέροντας ακόμη μεγαλύτερη ταχύτητα και δυνατότητα σύνδεσης περισσότερων συσκευών ανά τετραγωνικό χιλιόμετρο σε σχέση τις προηγούμενες τεχνολογίες. Τα υψηλής ταχύτητας δίκτυα 5G επιτρέπουν στους κατασκευαστές να παρακολουθούν τα μηχανήματα και τον εξοπλισμό τους σε πραγματικό χρόνο. Αυτό σημαίνει ότι τα πιθανά ζητήματα μπορούν να εντοπιστούν και να επιλυθούν προτού γίνουν σοβαρά, μειώνοντας τον χρόνο διακοπής λειτουργίας και βελτιώνοντας τη συνολική παραγωγικότητα. Με δεδομένα και πληροφορίες σε πραγματικό χρόνο, οι κατασκευαστές μπορούν να βελτιστοποιήσουν τις διαδικασίες τους και να εντοπίσουν ευκαιρίες για βελτίωση. Κατ' επέκταση, βελτιστοποιώντας τις διαδικασίες τους, οι βιομηχανίες μπορούν να μειώσουν την κατανάλωση ενέργειας (IoTNoW, n.d.). Τέλος, συνδεσιμότητα μεταξύ των διαφόρων συσκευών μπορεί να επιτευχθεί μέσω των χαμηλής κατανάλωσης ευρείας περιοχής δικτύων Low-Power Wide-Area Network (LPWAN). Το **LPWAN** είναι ένας τύπος ασύρματου δικτύου τηλεπικοινωνιών που έχει σχεδιαστεί για να επιτρέπει επικοινωνίες μεγάλης εμβέλειας με χαμηλό ρυθμό μετάδοσης bit μεταξύ των διασυνδεδεμένων αντικειμένων, όπως αισθητήρες που λειτουργούν σε μια ευρεία περιοχή. Τα LPWAN είναι βελτιστοποιημένα για χαμηλή κατανάλωση ενέργειας, γεγονός που επεκτείνει τη διάρκεια ζωής της μπαταρίας των συνδεδεμένων συσκευών και επιτρέπει λειτουργίες σε μεγάλη γεωγραφική περιοχή, συχνά με χαμηλότερο κόστος από τα δίκτυα κινητής τηλεφωνίας. Το LPWAN μπορεί να κατηγοριοποιηθεί σε τεχνολογίες ζώνης με άδεια και χωρίς άδεια, καθεμία από τις οποίες εξυπηρετεί συγκεκριμένες ανάγκες βάσει κανονιστικών και λειτουργικών απαιτήσεων (Dian, 2020). Στην πρώτη κατηγορία οι κυψελοειδείς τεχνολογίες όπως είναι η LTE Cat M1 (LTE-M) and Narrowband IoT (NB-IoT). Επειδή αυτές λειτουργούν σε ζώνες συχνοτήτων που ρυθμίζονται από κυβερνητικούς φορείς, απαιτούν άδεια χρήσης. Στην ουσία πρόκειται για παραλλαγές του LTE που αναπτύχθηκαν για να καλύψουν τις ανάγκες της αναπτυσσόμενης αγοράς IoT,

συμπεριλαμβανομένων ορισμένων χαρακτηριστικών παρόμοιων με το LPWAN, όπως η βελτιωμένη απόδοση ισχύος και καλύτερη κάλυψη σε δύσκολα περιβάλλοντα. Μπορούν να κατηγοριοποιηθούν ως μέρος των τεχνολογιών LPWAN όταν σχεδιάζονται ειδικά για επικοινωνίες τύπου μηχανής με απαιτήσεις χαμηλού ρυθμού δεδομένων και μεγάλη διάρκεια ζωής της μπαταρίας. Στην δεύτερη κατηγορία, αυτή των ζωνών χωρίς άδεια, βρίσκονται τεχνολογίες όπως το LoRaWAN και το Sigfox. Αυτές λειτουργούν σε ζώνες συχνοτήτων που δεν απαιτούν άδεια, καθιστώντας τις πιο ευέλικτες και οικονομικά αποδοτικές για ιδιωτικές αναπτύξεις. Το LoRaWAN είναι αξιοσημείωτο για τη χρήση μιας τεχνικής ευρέος φάσματος που εξασφαλίζει επικοινωνία σε μεγάλες αποστάσεις με ελάχιστη ισχύ. Υποστηρίζει προσαρμοστικούς ρυθμούς δεδομένων και το διαχειρίζεται η LoRa Alliance<sup>4</sup>. Η Sigfox προσφέρει μια μοναδική προσέγγιση παρέχοντας ένα παγκόσμιο δίκτυο αφιερωμένο στο IoT, χρησιμοποιώντας εξαιρετικά στενό εύρος ζώνης που του επιτρέπει να διατηρεί χαμηλή κατανάλωση ενέργειας και να καλύπτει τεράστιες περιοχές. Ακόμα για την ασφαλή επικοινωνία των ασύρματων επικοινωνιών δύναται να χρησιμοποιηθούν πρωτόκολλα όπως το **TLS/SSL** και **VPN**. Τα πρωτόκολλα TLS (Transport Layer Security) και SSL (Secure Socket Layer) χρησιμοποιούνται για την ασφαλή μεταφορά των μηνυμάτων με τη χρήση της κρυπτογραφίας. Το SSL δημιουργεί μία κρυπτογραφημένη σύνδεση μεταξύ δύο διακομιστών καθιστώντας τα δεδομένα που ανταλλάσσουν οι δύο διακομιστές ιδιωτικά. Αυτή η ασφαλής σύνδεση ενισχύεται περαιτέρω με την προσθήκη ενός πιστοποιητικού SSL, διασφαλίζοντας το απόρρητο και την ακεραιότητα της μεταφοράς των δεδομένων. Το πρωτόκολλο TLS είναι μία πιο ενημερωμένη και ασφαλής έκδοση του SSL. Διαφέρει αρκετά ως προς τις τεχνικές που χρησιμοποιεί, ωστόσο στόχος του είναι επίσης η παροχή ιδιωτικότητας και ακεραιότητας μεταξύ της ανταλλαγής μηνυμάτων (S., 2024). Ένα εικονικό ιδιωτικό δίκτυο VPN (Virtual Private Network) είναι μία κρυπτογραφημένη σύνδεση μέσω διαδικτύου από μία συσκευή σε ένα δίκτυο. Αυτή η σύνδεση βοηθάει στην ασφαλή μετάδοση δεδομένων αποτρέποντας μη εξουσιοδοτημένα άτομα να παρακολουθούν την κυκλοφορία. Ένα εικονικό ιδιωτικό δίκτυο είναι ένας τρόπος επέκτασης ενός ιδιωτικού δικτύου χρησιμοποιώντας ένα δημόσιο δίκτυο όπως το Διαδίκτυο. Το όνομα υποδηλώνει ότι ο χρήστης μπορεί να είναι μέρος ενός τοπικού δικτύου που βρίσκεται σε απομακρυσμένη τοποθεσία (geeksforgeeks, 2024).

### **Βιομηχανικό IoT με υπολογιστικό νέφος**

Ως τυπική συγκεντρωτική μέθοδος υπολογισμού, το cloud computing μπορεί να έχει πρόσβαση σε ένα κέντρο πόρων ανά πάσα στιγμή και οπουδήποτε μέσω του Διαδικτύου (Yu L. S., 2017). Βασισμένο σε ισχυρές λειτουργίες υπολογιστών και αποθήκευσης κεντρικών διακομιστών, μπορεί να ικανοποιήσει τις απαιτήσεις επεξεργασίας και ανάλυσης για μεγάλο αριθμό

---

<sup>4</sup> LoRa Alliance: ανοικτή, μη κερδοσκοπική ένωση που αποτελείται από πολλές εταιρείες, <https://loralliance.org/>

ετερογενών δεδομένων που παράγονται από το βιομηχανικό IoT. Παρόμοια με την παραδοσιακή αρχιτεκτονική του υπολογιστικού νέφους, το βιομηχανικό IoT που βασίζεται στο cloud μπορεί να χωριστεί σε τρία επίπεδα, συμπεριλαμβανομένου ενός επιπέδου υποδομής, ενός επιπέδου πλατφόρμας και ενός επιπέδου υπηρεσίας λογισμικού για διαφορετικές εφαρμογές (Huo, 2020).

Τεράστιες βιομηχανικές συσκευές IoT με αισθητήρες σε επίπεδο υποδομής βρίσκονται στο κάτω μέρος του συστήματος, το οποίο μπορεί να συλλέγει ακατέργαστα δεδομένα από βιομηχανικές συσκευές. Αυτά τα ακατέργαστα δεδομένα στη συνέχεια μεταδίδονται σε διακομιστές cloud μέσω ενός επιπέδου πλατφόρμας. Το επίπεδο πλατφόρμας είναι η ραχοκοκαλιά ολόκληρου του βιομηχανικού IoT που βασίζεται στο cloud. Με τις ισχυρές δυνατότητες υπολογισμού και ανάλυσης δεδομένων, ένας κεντρικός διακομιστής cloud μπορεί να επεξεργάζεται, να αναλύει και να αποθηκεύει αυτά τα ανεπεξέργαστα δεδομένα εύκολα. Στη συνέχεια, τα αποτελέσματα επεξεργασίας δεδομένων επιστρέφονται τελικά στο επίπεδο υπηρεσίας. Αυτό το επίπεδο αντιστοιχεί σε διάφορα σενάρια εφαρμογής. Εξάγοντας αυτά τα αποτελέσματα από το cloud computing, μπορούμε εύκολα να επιτύχουμε προγραμματισμό και διαχείριση παραγωγής, παρακολούθηση και έλεγχο εξοπλισμού, κατανομή πόρων και βελτιστοποίηση σε βιομηχανικά σενάρια (Mao J., 2017). Σε αυτή την περίπτωση, μπορεί να πραγματοποιήσει μια έξυπνη βιομηχανία με βαθιά μάθηση γνώσης.

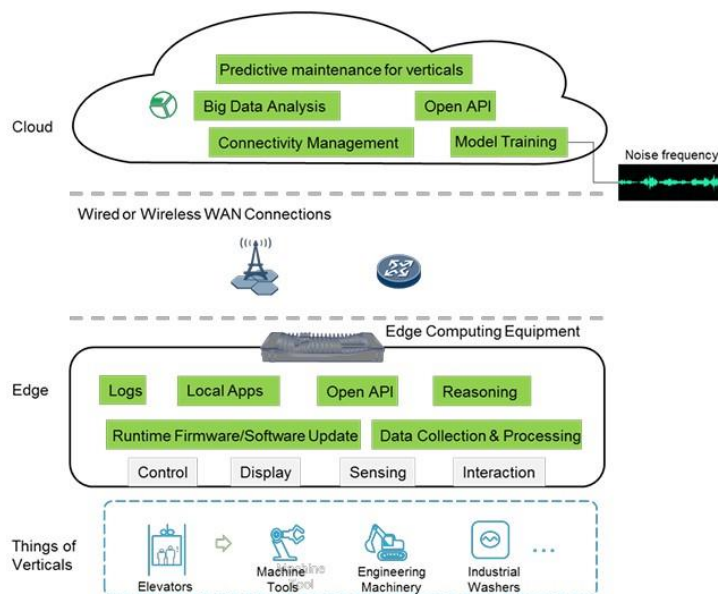
### **Βιομηχανικό IoT με edge computing**

Παρόλο που ένας διακομιστής cloud με ισχυρές δυνατότητες υπολογισμού και αποθήκευσης μπορεί να εκτελέσει εξαιρετικά περίπλοκους υπολογισμούς, απαιτεί υψηλές απαιτήσεις εύρους ζώνης και υπάρχει σημαντική χρονική καθυστέρηση. Αυτό είναι ιδιαίτερα σοβαρό ζήτημα σε ένα βιομηχανικό σύστημα IoT με πρόσβαση σε μεγάλο αριθμό έξυπνων συσκευών (Gong C., 2020). Τα τεράστια δεδομένα που παράγονται από αυτές τις έξυπνες συσκευές καταλαμβάνουν εξαιρετικά μεγάλο και πλάτος για να μεταδοθούν στους διακομιστές cloud. Επίσης, η ουρά των εργασιών όχι μόνο προκαλεί καθυστέρηση στην ποιότητα των υπηρεσιών, αλλά και αυξάνει την επιβάρυνση των κεντρικών διακομιστών. Αντίστοιχα, εκτεταμένες έρευνες ενσωματώνουν το edge computing στο βιομηχανικό IoT. Διαφορετικό από το cloud computing, ένα βιομηχανικό σύστημα IoT με edge computing αποκεντρώνει τις λειτουργίες cloud στην άκρη ενός δικτύου, δηλαδή σε πηγές δεδομένων και τερματικά. Είναι ένα κατακεντρωμένο σύστημα για την ενοποίηση διαφόρων λειτουργιών δικτύωσης, υπολογιστών, αποθήκευσης και εφαρμογών. Μπορεί να ικανοποιήσει βασικές απαιτήσεις ψηφιοποίησης για ένα βιομηχανικό σύστημα IoT σε ευέλικτη σύνδεση, υπηρεσίες σε πραγματικό χρόνο, βελτιστοποίηση δεδομένων και έξυπνες εφαρμογές. Σε ένα τυπικό βιομηχανικό μοντέλο IoT με edge computing, οι βιομηχανικές συσκευές IoT εκμεταλλεύονται αισθητήρες για να συλλέξουν πληροφορίες παραγωγής, καταστάσεις συσκευών και δεδομένα υλικού και στη συνέχεια ανεβάζουν αυτά τα δεδομένα σε τοπικούς διακομιστές αντί για διακομιστές cloud. Οι τοπικοί διακομιστές θα φιλτράρουν και θα αναλύουν δεδομένα, θα διαχωρίζουν εργασίες και θα προγραμματίζουν πόρους για να

ανατροφοδοτήσουν τον βιομηχανικό έλεγχο και να αυξήσουν την παραγωγικότητα και να εξοικονομήσουν κόστος παραγωγής (Huo, 2020).

Ουσιαστικά, αυτοί οι τοπικοί διακομιστές σε ένα επίπεδο υπολογιστικού επιπέδου είναι μια αποτελεσματική λύση για τη βελτίωση των δυνατοτήτων του υπολογιστικού νέφους. Για μια απλή εργασία, μπορούμε να υπολογίσουμε απευθείας σε έναν ανεξάρτητο κόμβο και να επιστρέψουμε το αντίστοιχο αποτέλεσμα. Για μια πολύπλοκη εργασία, η χρήση υπολογιστών αιχμής είναι να δοθεί έμφαση στον κατανεμημένο συνεργατικό υπολογισμό, δηλαδή στη χρήση πολλαπλών κόμβων για την επίτευξη υπηρεσιών crowdsourcing. Χρησιμοποιώντας edge computing σε ένα βιομηχανικό IoT, τεράστια ακατέργαστα δεδομένα μπορούν να αναλυθούν και να υποβληθούν σε επεξεργασία σε τοπικούς διακομιστές χωρίς να χρειάζεται να φορτωθούν στο cloud. Αυτό μπορεί να προστατεύσει τα ευαίσθητα δεδομένα χρήστη και να μειώσει τον κίνδυνο αποκάλυψης πρωτογενών δεδομένων τερματικών συσκευών.

Με βάση την κατανεμημένη αρχιτεκτονική, ένα βιομηχανικό IoT που βασίζεται σε edge computing έχει τα ακόλουθα πλεονεκτήματα. Πρώτον, σε ένα σενάριο βιομηχανικής κατασκευής, πρέπει να παρακολουθούμε και να ελέγχουμε τις συσκευές σε πραγματικό χρόνο. Εάν συνεχίσουμε να ανεβάζουμε τα συγκεντρωμένα δεδομένα σε διακομιστές cloud, το κόστος χρόνου είναι σχετικά μεγάλο και προκαλεί ακόμη και μεγάλα ατυχήματα. Έτσι, οι εργασίες θα πρέπει να γίνονται στο τοπικό ενός βιομηχανικού συστήματος για να επιτευχθεί απόκριση σε πραγματικό χρόνο. Δεύτερον, είναι δύσκολο για το εύρος ζώνης του δικτύου να ικανοποιήσει τους ρυθμούς μετάδοσης που βασίζονται στο σύννεφο λόγω της εκθετικής αύξησης του όγκου δεδομένων. Το Edge computing μπορεί να επεξεργάζεται δεδομένα στην άκρη του βιομηχανικού IoT, εξοικονομώντας σημαντικά εύρος ζώνης μετάδοσης, μειώνοντας το κόστος δικτύου και βελτιώνοντας την αποδοτικότητα της παραγωγής. Τρίτον, είναι πιο αποτελεσματικό για ένα βιομηχανικό σενάριο IoT με τερματικά περιορισμένης ενέργειας με τη μεταφόρτωση εργασιών υπολογιστών σε έναν διακομιστή αιχμής αντί για τη μεταφόρτωση σε έναν διακομιστή cloud (Shi W., 2016). Τέλος, η ανάλυση και η επεξεργασία δεδομένων σε έναν διακομιστή αιχμής μπορεί να προστατεύσει τα ανεπεξέργαστα δεδομένα από την υποκλοπή ή την εξόρυξη από ανταγωνιστές. Επιπλέον, μπορούμε να χρησιμοποιήσουμε γενικές διεπαφές στο edge computing για να αντιμετωπίσουμε ζητήματα συνύπαρξης συσκευών και να επιτύχουμε βελτίωση της ασφάλειας για διαφορετικούς τύπους συσκευών χωρίς να διαχειριζόμαστε πολύπλοκους διακομιστές cloud μεγάλης κλίμακας (Huo, 2020).



**Figure 4** Διάγραμμα λογικής αρχιτεκτονικής για το edge computing (Consortium, 2018)

### Βιομηχανικά πρωτόκολλα

Τα βιομηχανικά πρωτόκολλα είναι τυποποιημένες μέθοδοι επικοινωνίας που επιτρέπουν την αξιόπιστη και ασφαλή ανταλλαγή δεδομένων μεταξύ διαφόρων συσκευών και συστημάτων σε ένα βιομηχανικό. Αυτά τα πρωτόκολλα έχουν καθοριστικό ρόλο για την ενοποίηση ετερογενών συστημάτων και συσκευών, που δύναται να χρησιμοποιούνται σε ένα βιομηχανικό περιβάλλον. Καθιερώνοντας τυπικά κανάλια επικοινωνίας, διασφαλίζουν τη διαλειτουργικότητα και διευκολύνουν την εφαρμογή προηγμένων συστημάτων αυτοματισμού και ελέγχου. Ένα βιομηχανικό πρωτόκολλο που χρησιμοποιείται ευρέως σε βιομηχανικά περιβάλλοντα είναι το **Modbus**. Το Modbus επιτρέπει την ανταλλαγή δεδομένων μεταξύ συσκευών συνδεδεμένων μέσω σειριακού δικτύου ή δικτύου Ethernet, καθιστώντας το μια προτιμώμενη επιλογή για μια σειρά βιομηχανικών εφαρμογών. Το πρωτόκολλο Modbus, αναπτύχθηκε αρχικά από τη Modicon το 1979, κυρίως για τον έλεγχο οργάνων, τη λήψη δεδομένων και τη διασύνδεση με μονάδες μικροελεγκτών (MCU) ή συστήματα συλλογής δεδομένων. Χρησιμοποιείται ευρέως σε προγραμματιζόμενους λογικούς ελεγκτές (PLC) για βιομηχανικούς αυτοματισμούς. Το 2004, το Modbus γίνεται ένα de facto πρότυπο στη βιομηχανική επικοινωνία, εξελισσόμενο σε μια ποικιλία πρωτοκόλλων όπως το Modbus TCP/IP και το Modbus RTU, που διατίθενται δωρεάν χωρίς τέλη άδειας χρήσης. Στο πλαίσιο του IIoT, το Modbus διαδραματίζει κρίσιμο ρόλο. Διευκολύνει τη σύνδεση στο Διαδίκτυο στις βιομηχανίες αυτοματισμού και ελέγχου, που χρησιμοποιείται συχνά για τη σύνδεση Εποπτικού Ελέγχου και Απόκτησης Δεδομένων (SCADA<sup>5</sup>) ή Συστημάτων Διαχείρισης Κτιρίων (BMS<sup>6</sup>). Το Modbus επιτρέπει στις συσκευές IIoT,

<sup>5</sup> Supervisory Control and Data Acquisition (SCADA)

<sup>6</sup> Building Management Systems (BMS)



που αναφέρονται ως Modbus 'Things', να συνδέονται μέσω μιας πύλης IIoT και να διαχειρίζονται πολυάριθμες συσκευές μέσω μιας ασφαλούς, αμφίδρομης σύνδεσης στο Διαδίκτυο χωρίς την ανάγκη περίπλοκων λύσεων δικτύωσης όπως VPN (Virtual private network) ή τείχη προστασίας. Η υιοθέτηση του Modbus στο IIoT έχει βελτιώσει σημαντικά την απόδοση, τις δυνατότητες και τη συνδεσιμότητα, ενώ μειώνει το κόστος. Η αρχιτεκτονική master-slave του υποστηρίζει έως και 247 συσκευές που ανταποκρίνονται σε έναν master, ενισχύοντας την αποτελεσματική επικοινωνία σε διάφορες βιομηχανικές ρυθμίσεις (wemakeiot, n.d.). Το **OPC** Unified Architecture (UA), είναι μια άλλη αρχιτεκτονική που παρουσιάστηκε το 2008 και ενσωματώνει όλη τη λειτουργικότητα των προδιαγραφών OPC Classic σε ένα ενιαίο, επεκτάσιμο πλαίσιο. Στο πλαίσιο του IIoT, η αρχιτεκτονική του OPC UA διευκολύνει την ισχυρή, ασφαλή και αποτελεσματική επικοινωνία μεταξύ συσκευών και συστημάτων, καθιστώντας την σημαντική για την αυτοματοποίηση και για κάθε είδους λειτουργία που βασίζεται σε δεδομένα σε βιομηχανίες. Η ικανότητά του να λειτουργεί σε διάφορες πλατφόρμες και οι ολοκληρωμένες δυνατότητες ασφάλειας και μοντελοποίησης καθιστούν το OPC UA βασικό στοιχείο για την εύρεση και ανάπτυξη λύσεων IIoT. Πιο αναλυτικά, αντιστοιχίζει όλες τις λειτουργίες των προδιαγραφών COM OPC Classic (προγενέστερες προδιαγραφές που είχαν αναπτυχθεί) στο πλαίσιο UA. Στα αξιοσημείωτα χαρακτηριστικά περιλαμβάνονται η ανακάλυψη διακομιστών, η ιεραρχική αναπαράσταση δεδομένων, η πρόσβαση σε δεδομένα κατ' απαίτηση, οι συνδρομές για παρακολούθηση αλλαγών δεδομένων, οι ειδοποιήσεις συμβάντων και οι εκτελέσεις μεθόδων στον διακομιστή. Το OPC UA έχει κατασκευαστεί για να φιλοξενεί μελλοντικές τεχνολογίες χωρίς να διακόπτει τις υπάρχουσες εφαρμογές. Αυτό περιλαμβάνει την ενσωμάτωση νέων πρωτοκόλλων μεταφοράς, αλγορίθμων ασφαλείας και προτύπων κωδικοποίησης και τη διατήρηση της συμβατότητας με τα υπάρχοντα προϊόντα OPC UA. Τέλος, το OPC UA υπερέχει στον ορισμό πολύπλοκων πληροφοριών μέσω ενός δομημένου, αντικειμενοστραφούς πλαισίου μοντελοποίησης που επιτρέπει τη δημιουργία και την επέκταση δομών δεδομένων πολλαπλών επιπέδων. Αυτή η ικανότητα είναι θεμελιώδης για την αρχιτεκτονική του, επιτρέποντας λεπτομερή διαχείριση δεδομένων και αλληλεπίδραση εντός των βιομηχανικών συστημάτων (opcfoundation, n.d.). Τέλος, το Message Queuing Telemetry Transport (MQTT) είναι ακόμη ένα πρωτόκολλο ιδανικό για σενάρια IIoT που περιλαμβάνουν απομακρυσμένη παρακολούθηση και έλεγχο όπου η απόδοση εύρους ζώνης και η χαμηλή κατανάλωση ενέργειας είναι απαραίτητα. Το MQTT χρησιμοποιεί το μοντέλο δημοσίευσης/εγγραφής (publish/subscribe), γεγονός που το καθιστά εξαιρετικά επεκτάσιμο και κατάλληλο για ανταλλαγή μηνυμάτων μεταξύ πολλών συσκευών. Ωστόσο, το MQTT δεν παρέχει εγγενώς ένα πρότυπο για τον ορισμό του χώρου ονομάτων ή του ωφέλιμου φορτίου (payload), το οποίο μπορεί να οδηγήσει σε ασυνέπειες και προκλήσεις ενοποίησης όταν εφαρμόζεται σε διάφορες συσκευές και συστήματα σε βιομηχανικές ρυθμίσεις. Για το λόγο αυτό, δημιουργήθηκε το Sparkplug (στα ελληνικά σημαίνει «μπουζί») όπου πρόκειται για μια προδιαγραφή που καθορίζει τον τρόπο χρήσης του MQTT με τρόπο βελτιστοποιημένο για βιομηχανικές εφαρμογές που απαιτούν εξαιρετικά αξιόπιστη μεταφορά δεδομένων. Τα κύρια

πλεονεκτήματα του είναι η συγκέντρωση διάφορων τύπων εργοστασιακών δεδομένων σε έναν ενοποιημένο χώρο ονομάτων, η εξασφάλιση απόκτησης δεδομένων σε πραγματικό χρόνο, η πλατυσιοποίηση των δεδομένων μέσω του Sparkplug, η κλιμακούμενη και αξιόπιστη επικοινωνία δεδομένων (scalable data flow) και η ισχυρή ασφάλεια μέσω κρυπτογράφησης (Subramanyan, 2024).

## **ΚΕΦΑΛΑΙΟ 3: ΙΔΙΑΙΤΕΡΟΤΗΤΕΣ ΙΙΟΤ ΣΕ ΣΥΓΚΡΙΣΗ ΜΕ ΠΑΡΑΔΟΣΙΑΚΑ ΠΕΡΙΒΑΛΛΟΝΤΑ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ**

Στο κεφάλαιο αυτό παρουσιάζεται μια λεπτομερή ανάλυση των ιδιαιτεροτήτων του Βιομηχανικού Διαδικτύου των Πραγμάτων (IIoT) σε σύγκριση με τα παραδοσιακά περιβάλλοντα του Διαδικτύου. Εξετάζεται η εξέλιξη από τα κυβερνοφυσικά συστήματα προς το IoT και την μετέπειτα εμφάνιση του Βιομηχανικού IoT (IIoT), αναδεικνύεται η σημασία της έξυπνης τεχνολογίας και των αντικειμένων εξοπλισμένων με ηλεκτρονικά που επιτρέπουν δυνατότητες όπως η αναγνώριση, ο γρήγορος υπολογισμός και η επικοινωνία μεταξύ των σύγχρονων τεχνολογιών. Παρέχεται επίσης μια συγκριτική ανάλυση μεταξύ IoT και IIoT, επισημαίνοντας τις διαφορές στις υπηρεσίες, τις συνδεδεμένες συσκευές, τις απαιτήσεις δικτύου και την κλίμακα των δεδομένων.

### **3.1 Από τα κυβερνοφυσικά συστήματα στο Βιομηχανικό Διαδίκτυο των Πραγμάτων**

Ένας αυξανόμενος αριθμός καθημερινών αντικειμένων είναι εξοπλισμένος με ηλεκτρονικά, τα οποία παρέχουν σε αυτά τα αντικείμενα δυνατότητες αναγνώρισης, υπολογισμού και επικοινωνίας. Παραδείγματα περιλαμβάνουν βασική τεχνολογία, όπως Αναγνώριση ραδιοσυχνοτήτων (RFID) για την αναγνώριση και παρακολούθηση προϊόντων, πακέτων και παλετών σε σενάρια εφοδιαστικής αλυσίδας, σε έξυπνες συσκευές, όπως έξυπνα τηλέφωνα και φορητές συσκευές (π.χ. έξυπνα ρολόγια) με σημαντικές υπολογιστικές δυνατότητες και συνδέσεις στο Διαδίκτυο. Αυτό το δίκτυο πανταχού παρών έξυπνων αντικειμένων είναι γνωστό ως Internet of Things (IoT) και επιτρέπει νέες εφαρμογές και υπηρεσίες, ιδιαίτερα στον βιομηχανικό τομέα (Sadeghi, 2015).

Οι εγκαταστάσεις παραγωγής αποτελούνται συνήθως από πολλά ανεξάρτητα λειτουργικά συστήματα παραγωγής χωρίς ή περιορισμένες μόνο δυνατότητες επικοινωνίας. Μια αναδυόμενη τάση είναι η ενσωμάτωση πιο εξελιγμένων ηλεκτρονικών σε συστήματα παραγωγής, διασύνδεσή τους και ενσωμάτωση σε συμβατικά επιχειρηματικά συστήματα πληροφορικής. Το βιομηχανικό IoT που προκύπτει αποτελεί τη βάση για ένα νέο επίπεδο οργάνωσης και διαχείρισης των βιομηχανικών αλυσίδων αξίας και επιτρέπει την εξαιρετικά ευέλικτη παραγωγή και εξοικονόμηση πόρων καθώς και την ενισχυμένη εξατομίκευση των προϊόντων με κόστος μαζικής παραγωγής.

Το θεμέλιο του Industrial IoT είναι τα cyberphysical συστήματα (CPS), τα οποία είναι υπολογιστικές πλατφόρμες που παρακολουθούν και ελέγχουν τις φυσικές διεργασίες (Kumar, 2014). Το CPS επιτρέπει την παρακολούθηση της κατάστασης, την παρακολούθηση της δομικής υγείας, την απομακρυσμένη διάγνωση και τον απομακρυσμένο έλεγχο των συστημάτων παραγωγής σε πραγματικό χρόνο. Επιπλέον, το CPS είναι η βάση έξυπνων εργοστασίων που οργανώνουν δυναμικά και βελτιστοποιούν τις διαδικασίες παραγωγής όσον

αφορά τη χρήση των πόρων (δηλαδή, κόστος, διαθεσιμότητα, υλικό και εργασία) με βάση δεδομένα που δημιουργούνται και συλλέγονται από το υποκείμενο CPS, ακόμη και πέρα από τα όρια της εταιρείας (Sadeghi, 2015).

Στα έξυπνα εργοστάσια, τα έξυπνα προϊόντα γνωρίζουν τη δική τους ταυτότητα, ιστορία, προδιαγραφές, τεκμηρίωση, ακόμη και ελέγχουν τη δική τους διαδικασία παραγωγής. Πέρα από την κατασκευή, τα έξυπνα προϊόντα αποτελούν τη βάση νέων υπηρεσιών που βασίζονται στη γνώση, που ονομάζονται έξυπνες υπηρεσίες. Συγκεκριμένα, τα έξυπνα προϊόντα δεν συλλέγουν δεδομένα μόνο κατά την παραγωγή τους αλλά και όταν αναπτύσσονται και χρησιμοποιούνται από πελάτες. Αυτό επιτρέπει τη βελτιστοποίησή τους σε σχέση με τον τρόπο που χρησιμοποιούνται στην πραγματικότητα. Τα έξυπνα προϊόντα είναι εξοπλισμένα με ψηφιακή ταυτότητα (π.χ. αποθηκευμένα σε γραμμικό κώδικα ή τσιπ RFID) και όλες οι πληροφορίες που σχετίζονται με το προϊόν αποθηκεύονται σε κάποια βάση δεδομένων υποστήριξης. Εναλλακτικά, το προϊόν είναι εξοπλισμένο με ηλεκτρονικά (π.χ. μνήμη και επεξεργαστή) και αποθηκεύει το ίδιο αυτά τα δεδομένα. Το βιομηχανικό IoT φέρνει πολλές νέες προκλήσεις σε σχέση με διάφορες πτυχές, όπως η ασφάλεια, η ιδιωτικότητα, η τυποποίηση, οι νομικές και κοινωνικές πτυχές. Ειδικότερα, η αυξημένη ποικιλομορφία και ο μεγάλος αριθμός συσκευών στα συστήματα IoT απαιτούν λύσεις υψηλής κλιμάκωσης για, π.χ., ονομασία και διεύθυνση, επικοινωνία δεδομένων, διαχείριση γνώσης και παροχή υπηρεσιών. Επιπλέον, οι περισσότερες συσκευές IoT έχουν περιορισμένους μόνο πόρους που απαιτούνται για αρχιτεκτονικές που υποστηρίζουν ενσωματωμένες συσκευές χαμηλής ισχύος, χαμηλού κόστους, πλήρως δικτυωμένες που είναι συμβατές με τυπικές τεχνικές επικοινωνίας (Sadeghi, 2015).

### **3.2 Διαφορές μεταξύ IoT και IIoT**

Το 1999, ο Kelvin Ashton επινόησε τον όρο «Διαδίκτυο των πραγμάτων», έδωσε το όνομα για να καταδείξει την ιδέα ότι χειροκίνητα αντικείμενα θα μπορούσαν να συνδεθούν στο δίκτυο. Στη συνέχεια, αργότερα, το Industrial Internet of Things οδήγησε σε καινοτομίες όπως το έξυπνο εργοστάσιο και η τεχνολογία υπολογιστών. Το IIoT δεν δημιουργεί μόνο μια σύνδεση μεταξύ μηχανών, αλλά διαθέτει επίσης μονάδα ανθρώπινης διασύνδεσης για άψογο σύστημα. Οι απλές και μονότονες εργασίες όπως ο ποιοτικός έλεγχος, η συναρμολόγηση, η διαχείριση και η διευθέτηση θα αντικατασταθούν από το IIoT με τεράστιες προσδοκίες.

Ένα βιομηχανικό σύστημα IoT αναφέρεται στη χρήση τεχνολογιών επικοινωνίας και υπολογιστών και έξυπνης ανάλυσης για τη σύνδεση συσκευών, τη συλλογή δεδομένων και την εξόρυξη πληροφοριών για την αύξηση της παραγωγικής απόδοσης, τη βελτίωση της ποιότητας των προϊόντων, το χαμηλότερο κόστος και την κατανάλωση πόρων και, τέλος, την υλοποίηση της αναβάθμισης των παραδοσιακών βιομηχανιών σε ευφυείς.

Αν και ένα γενικό σύστημα IoT και ένα βιομηχανικό σύστημα IoT έχουν πολλές κοινές τεχνολογίες, όπως πλατφόρμες cloud, συνδέσεις δικτύου και επικοινωνία μηχανής με μηχανή, εξακολουθούν να έχουν διαφορετικά χαρακτηριστικά. Συνοπτικά, οι διαφορές μπορούν να συμπεραθούν στις ακόλουθες τέσσερις πτυχές. Το πρώτο είναι διαφορετικοί τύποι υπηρεσιών. Το γενικό IoT είναι ένα ανθρωποκεντρικό σύστημα με την ικανότητα να αυξάνει την αντίληψη και την απόκριση στο περιβάλλον. Ένα βιομηχανικό σύστημα IoT εστιάζει κυρίως στην παρακολούθηση και τον έλεγχο του εξοπλισμού, του περιβάλλοντος και των υλικών στην κατασκευή και στη συνέχεια πραγματοποιεί τον στόχο της έξυπνης κατασκευής στα εργοστάσια. Το δεύτερο είναι διαφορετικές συνδεδεμένες συσκευές. Το γενικό IoT εστιάζει στον σχεδιασμό νέων προτύπων, στη σύνδεση νέων συσκευών με το οικοσύστημα του Διαδικτύου με ευέλικτο και φιλικό τρόπο, αλλά το βιομηχανικό IoT χρησιμοποιείται για την ενοποίηση και τη σύνδεση εργοστασίων και μηχανών για την παροχή πιο αποτελεσματικών υπηρεσιών παραγωγής. Τρίτον, οι απαιτήσεις δικτύου είναι διαφορετικές. Το πρώτο υποστηρίζει δομές δικτύου κινητής τηλεφωνίας που έχουν χαμηλές απαιτήσεις χρονισμού και αξιοπιστίας. Το τελευταίο είναι να επιτευχθεί μια επικοινωνία μηχανής με μηχανή, η οποία συνήθως χρησιμοποιεί μια σταθερή δομή δικτύου και πρέπει να ικανοποιεί την αυστηρή ζήτηση σε πραγματικό χρόνο και αξιόπιστη. Τέλος, η κλίμακα του όγκου δεδομένων αυτών των δύο σεναρίων είναι διαφορετική. Τα δεδομένα που παράγονται από ένα γενικό σύστημα IoT προέρχονται από τυπικές εφαρμογές. Ο όγκος δεδομένων του καθορίζεται από διαφορετικά σενάρια εφαρμογής. Ωστόσο, ένα βιομηχανικό σύστημα IoT συνήθως έχει τεράστιο όγκο δεδομένων που μεταδίδονται ή αποθηκεύονται σε δίκτυα λόγω της ταχείας ανάπτυξης των συνδεδεμένων τερματικών συσκευών. Σύμφωνα με τα χαρακτηριστικά ενός βιομηχανικού συστήματος IoT, πρώτα αφαιρούμε τυπικές αρχιτεκτονικές και στη συνέχεια αναλύουμε ζητήματα απορρήτου σε αυτές τις αρχιτεκτονικές (Huo, 2020).

Οι παραπάνω διαφορές μπορούν να συμπυκνωθούν σε ένα πίνακα, προκειμένου να διευκολυνθεί η ανάγνωση τους από τον αναγνώστη. Έτσι, στον πίνακα 2 συνοψίζονται οι βασικές διαφορές μεταξύ του IoT και IIoT με βάση το κριτήριο της εφαρμογής, το σκοπό χρήσης τους, τον προσανατολισμό τους, τη διαχείριση των δεδομένων και των δικτύων που χρησιμοποιούν, τις απαιτήσεις σε ασφάλεια και ιδιωτικότητα.

**Table 2 Βασικές διαφορές μεταξύ IoT και IIoT**

| Κριτήριο        | IoT                                                                | IIoT                                                                                                  |
|-----------------|--------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| Εφαρμογή        | Ποικιλία τομέων (οικιακά, φορητές συσκευές, υγεία, έξυπνες πόλεις) | Ειδικευμένο για τη βιομηχανία (παραγωγή, μεταφορές)                                                   |
| Σκοπός          | Βελτίωση της ποιότητας ζωής των ατόμων                             | Βελτίωση βιομηχανικής αποδοτικότητας, αξιοπιστίας και παραγωγικότητας                                 |
| Προσανατολισμός | Καταναλωτικά προσανατολισμένο                                      | Βιομηχανικά προσανατολισμένο                                                                          |
| Διαχείριση      | Διαχείριση δικτύων μεσαίας πολυπλοκότητας                          | Σύνθετη διαχείριση πολύπλοκων βιομηχανικών δικτύων με αυστηρές προδιαγραφές                           |
| Ασφάλεια        | Χαμηλές απαιτήσεις                                                 | Υψηλές και αυστηρές απαιτήσεις, λόγω της κρίσιμότητας των λειτουργιών                                 |
| Ιδιωτικότητα    | Προστασία προσωπικών δεδομένων σύμφωνα με τους κανονισμούς GDPR    | Προστασία τόσο προσωπικών δεδομένων όσο και βιομηχανικών υπό την απειλή της βιομηχανικής κατασκοπείας |

### 3.3 Απαιτήσεις του IIoT

Οι παραπάνω διαφορές που παρατέθηκαν, δείχνουν την πολυπλοκότητα του IIoT σε σύγκριση με τα παραδοσιακά περιβάλλοντα διαδικτύου. Ως εκ τούτου, το IIoT απαιτεί πολύ αυστηρότερες προδιαγραφές σε σχέση με ένα IoT λόγω του βιομηχανικού του χαρακτήρα. Οι εξειδικευμένες απαιτήσεις του IIoT περιγράφονται και αναλύονται παρακάτω.

**Απαιτήσεις πραγματικού χρόνου:** Το βιομηχανικό IoT συχνά απαιτεί άμεση ανταπόκριση (real-time performance), καθώς τα συστήματα συνδέονται με βιομηχανικές διαδικασίες, όπως η αυτοματοποίηση εργοστασίων, που δεν μπορούν να ανεχθούν καθυστερήσεις. Η άμεση ανταπόκριση είναι κρίσιμη για την αποφυγή βλαβών και την αποτελεσματική λειτουργία των μηχανών. Το IoT μπορεί επίσης να απαιτεί ανταπόκριση σε πραγματικό χρόνο (πχ έξυπνα σπίτια και φορητές συσκευές υγείας), οι καθυστερήσεις όμως αυτών των εφαρμογών είναι συνήθως αποδεκτές. Ο χρόνος απόκρισης μπορεί να είναι πιο χαλαρός και τα δεδομένα να αναλύονται και να χρησιμοποιούνται σε δεύτερο χρόνο. Ο Μπένκε και οι άλλοι (Behnke, 2023) εξέτασαν διάφορα IIoT σενάρια και άντλησαν δικτυακές απαιτήσεις πραγματικού χρόνου για καθεμιά από αυτές. Σε ένα από αυτά, αυτόνομα μετακινούμενες μηχανές όπως μεταφορικά ρομπότ, περονοφόρα ανυψωτικά και ρομπότ αποθήκης, χρειάζονται να πλοηγηθούν σε δυναμικά περιβάλλοντα και να πάρουν αποφάσεις σε πραγματικό χρόνο για την εκτέλεση των

καθηκόντων τους, την αποφυγή συγκρούσεων και την βελτιστοποίηση των διαδρομών τους. Σε τέτοιες περιπτώσεις η υψηλή προβλεψιμότητα και η χαμηλή καθυστέρηση είναι κρίσιμοι παράμετροι, αφού οι μηχανές λειτουργούν σε κοντινή απόσταση με το ανθρώπινο δυναμικό και άλλες μηχανές. Ειδικότερα όταν η μεταφορά των δεδομένων έχει να κάνει με οπτικές αναπαραστάσεις από τους χώρους που επεξεργάζονται οι μηχανές και η μεταδιδόμενη πληροφορία βίντεο είναι υψηλού όγκου, οι απαιτήσεις για γρήγορες ταχύτητες δικτύου αυξάνονται. Σε ένα άλλο παράδειγμα όπου υπάρχουν αισθητήρες που παρακολουθούν την θερμοκρασία και την πίεση σε κρίσιμες μηχανές, η αντίδραση του συστήματος θα πρέπει να είναι άμεση ώστε να αποφευχθούν καταστροφές. Σε τέτοιες περιπτώσεις, υπάρχει ανάγκη για μείωση του αντίδρασης και η ανάπτυξη λύσεων όπως αυτή του υπολογισμού αιχμής (edge computing) μπορεί να είναι ιδιαίτερα χρήσιμη. Η επεξεργασία των δεδομένων γίνεται τοπικά, κοντά στους αισθητήρες, με αποτέλεσμα να μειώνεται η μεταφορά δεδομένων στο κεντρικό σύστημα. Ο σχεδιασμός των απαιτήσεων για αντιδράσεις πραγματικού χρόνου θα πρέπει να γίνεται σε βάθος και με την προοπτική της εξέλιξης και της κλιμάκωσης. Όσο η τεχνολογία προχωράει και το εργοστάσιο μεγαλώνει, μεγαλώνουν και οι απαιτήσεις του, όπως επίσης είναι δυνατό να μεγαλώσει και ο αριθμός των αισθητήρων που χρησιμοποιούνται. Είναι σημαντικό ένα περιβάλλον IIoT να μπορεί να διαχειριστεί μια αυξανόμενη ποσότητα συσκευών και δεδομένων χωρίς να επηρεάζεται η ταχύτητα και η απόδοση του. Η χρήση του υπολογιστικού νέφους, βοηθάει στην αποθήκευση και επεξεργασία μεγάλης κλίμακας δεδομένων ανάλογα με τις υπάρχουσες απαιτήσεις. Η τεχνολογία του “pay as you go” και “pay as you use” όπου οι χρεώσεις γίνονται κατά απαίτηση και η χρήση των πόρων αλλάζει δυναμικά ανάλογα τις απαιτήσεις αποτελεί μία βελτιστοποιημένη σχεδίαση για τη διαχείριση των υπηρεσιών ενός εργοστασίου. Τέλος, ένα περιβάλλον IIoT θα πρέπει να είναι σε θέση να αντιδράσει άμεσα σε κακόβουλες ενέργειες. Για αυτό το λόγο, η ασφάλεια του δικτύου και των δεδομένων πρέπει να είναι σε θέση να εντοπίζει και να αντιμετωπίζει επιθέσεις χωρίς καθυστέρηση, αφού αυτό μπορεί να έχει ολέθριες συνέπειες στην οικονομία της επιχείρησης. Απεναντίας, σε ένα περιβάλλον IoT, το κόστος μιας επίθεσης και το αντίκτυπο αυτής είναι πολύ μικρότερο, εάν αφορά ένα νοικοκυριό. Το IoT είναι λιγότερο ελκυστικό για επιθέσεις καθώς, δεν υπάρχουν ανταγωνιστές και η οικονομία του είναι μικρή κλίμακας και έχει νόημα μόνο εάν γίνει ταυτόχρονα σε πολλά διαφορετικά περιβάλλοντα.

**Απαιτήσεις ανθεκτικότητας και αξιοπιστίας:** Η φύση του IIoT δημιουργεί υψηλές απαιτήσεις όσον αφορά την ανθεκτικότητα και αξιοπιστία των λειτουργιών και διαδικασιών του, για την αποφυγή διακοπών που μπορεί να οδηγήσουν σε οικονομικές απώλειες. Σε μία βιομηχανία που χρησιμοποιεί ρομποτικούς βραχίονες, το σφάλμα ενός αισθητήρα μπορεί να οδηγήσει στη διακοπή ολόκληρης της γραμμής παραγωγής. Για την αποφυγή παρόμοιων καταστάσεων, είναι καλή πρακτική να υπάρχουν πλεονάζουσες συσκευές (redundant), ώστε οι λειτουργίες να μεταφέρονται αυτόματα σε αυτές (πχ τους πλεονάζων αισθητήρες) χωρίς να επηρεαστεί η παραγωγή. Εναλλακτικά, θα πρέπει η γραμμή παραγωγής να έχει ανοχή σε σφάλματα, με την έννοια ότι εάν ένας αισθητήρας βγάλει κάποιο προσωρινό σφάλμα, θα πρέπει να ληφθούν

δεδομένα και να υπάρχει προκαθορισμένη σχεδίαση για το πως θα αντιδράσει το σύστημα. Για παράδειγμα, εάν ένας αισθητήρας θερμοκρασίας αποτύχει να στείλει δεδομένα θερμοκρασίας, δεν θα πρέπει να σταματήσει η παραγωγή, αλλά να ληφθούν δεδομένα και από άλλου είδους αισθητήρες που να βεβαιώνουν ότι το μηχάνημα λειτουργεί σωστά, παρόλο που δεν υπάρχουν δεδομένα για τη θερμοκρασία του. Επιπρόσθετα, απαραίτητο κομμάτι της υψηλής αξιοπιστίας είναι η συντήρηση. Ένα σύστημα IIoT πρέπει να υποστηρίζει την τακτική συντήρηση και να ενσωματώνει τεχνικές για προληπτική συντήρηση, δηλαδή το σύστημα θα πρέπει να προειδοποιεί για προβλήματα προτού οδηγήσουν σε αποτυχίες, ώστε να λαμβάνονται τα κατάλληλα μέτρα έγκαιρα.

**Απαιτήσεις επεκτασιμότητας:** Όπως έχει ήδη αναφερθεί, η αυξανόμενη ποσότητα συσκευών μπορεί να οδηγήσει σε μη αποδεκτές καθυστερήσεις. Δεδομένου ότι τα τεχνολογικά περιβάλλοντα IIoT είναι δυναμικά και εξελίσσονται, θα πρέπει να σχεδιάζονται με τη δυνατότητα προσαρμογής στις αυξανόμενες ανάγκες χωρίς να υποβαθμίζεται η απόδοση και η αξιοπιστία τους. Εκτός από τις συσκευές που μπορεί να αυξηθούν, το ίδιο μπορεί να συμβεί και με τα δεδομένα. Τα δεδομένα που διαχειρίζεται ένα περιβάλλον IIoT μπορεί να αυξηθούν με εκθετικό ρυθμό για διάφορους λόγους, όπως η αύξηση των συσκευών που τα παράγουν, η νέα απαίτηση για την αποστολή πιο τακτικών δεδομένων από τους αισθητήρες, η συνεχόμενη συσσωρευμένη προσθήκη ιστορικού δεδομένων για την λήψη αποφάσεων κλπ., ωστόσο το σύστημα πρέπει να είναι ικανό να διαχειριστεί τον αυξανόμενο όγκο δεδομένων χωρίς την πρόκληση καθυστερήσεων ή την απώλεια δεδομένων. Η επεξεργαστική ισχύς του συστήματος πρέπει να επεκτείνεται δυναμικά για να διασφαλίζεται η έγκαιρη λήψη αποφάσεων. Το ίδιο ισχύει και για τις υποδομές δικτύου, όπου οι απαιτήσεις στη μεταφορά δεδομένων μπορεί να αυξηθούν ραγδαία. Η σταθερή σύνδεση και η ελάχιστη δυνατή καθυστέρηση είναι ζωτικής σημασίας για την ομαλή διεξαγωγή των λειτουργιών του εργοστασίου. Αντιθέτως, οικιακές εφαρμογές IoT, είναι πολύ δύσκολο να φτάσουν απαιτήσεις που δεν καλύπτονται από τα υπάρχοντα δίκτυα (πχ WiFi), κι εάν συμβεί κάτι τέτοιο το αντίκτυπο συνήθως είναι μικρό. Εκτός από την διατήρηση των χρόνων αντίδρασης, η επεκτασιμότητα των συστημάτων IIoT θα πρέπει να γίνεται και με γνώμονα μελλοντικής συμβατότητας συσκευών διαφόρων τύπων. Με άλλα λόγια, θα πρέπει να υποστηρίζεται η διασύνδεση διαφορετικών συσκευών και πρωτοκόλλων, αφού νέες συσκευές ή τεχνολογίες που χρησιμοποιούν διαφορετικά πρωτόκολλα επικοινωνίας πιθανόν να χρειαστεί να ενσωματωθούν στο υπάρχων σύστημα/υποδομή. Παλαιές και καινούριες μηχανές μπορεί να χρειαστεί να συνυπάρχουν κάτω από το ίδιο δίκτυο ή υποδομή, και θα πρέπει να υποστηρίζονται ταυτόχρονα.

**Απαιτήσεις ενεργειακής αποδοτικότητας:** Η ενεργειακή αποδοτικότητα σε ένα περιβάλλον IIoT είναι ιδιαίτερα σημαντική, διότι πολλά συστήματα και συσκευές λειτουργούν αδιάκοπα, σε απαιτητικές συνθήκες. Η διατήρηση χαμηλής κατανάλωσης ενέργειας, μπορεί να μειώσει τα λειτουργικά κόστη του εργοστασίου, αλλά και το βιομηχανικό αποτύπωμα της βιομηχανίας. Εφόσον το περιβάλλον είναι βιομηχανικού τύπου και διαθέτει επωνυμία, θα πρέπει αφενός να



συμμορφώνεται στους κανόνες που ισχύουν για την περιβαλλοντική ευθύνη των επιχειρήσεων και αφετέρου να διατήρηση την κοινωνική του υπόληψη υψηλά, αφού οι επιπτώσεις των βιομηχανιών στο περιβάλλον, είναι ένα ιδιαίτερα ευαίσθητο κοινωνικό θέμα. Αρχικά, η απαίτηση για χρήση ενεργειακά αποδοτικών συσκευών και αισθητήρων είναι σημαντική, αφού αυτές λειτουργούν αδιάκοπα και είναι αριθμητικά πολλές. Η χρήση συσκευών χαμηλών σε κατανάλωση ενέργειας μπορεί να έχει μεγάλο οικονομικό όφελος για ένα εργοστάσιο σε βάθος χρόνου. Για παράδειγμα, έστω ο μη αποδοτικός αισθητήρας θερμοκρασίας DHT22<sup>7</sup>, οποίος στα ηλεκτρικά του χαρακτηριστικά χρειάζεται 5Volt τάση και 1.5mA ρεύμα τροφοδοσίας. Αυτό ισοδυναμεί με  $\text{Ισχύς} = \text{Τάση} \times \text{Ρεύμα} = 5\text{V} \times 1.5\text{mA} = 7.5 \text{ mWatt}$  και ετήσια κατανάλωση ίση με  $0.0075 \text{ watts} \times 24 \text{ ώρες/ημερησίως} \times 365 \text{ ημέρες/έτος} = 65.7 \text{ βατώρες ετησίως}$ . Αντίστοιχα, για τον ενεργειακά αποδοτικό αισθητήρα θερμοκρασίας SHT31<sup>8</sup>, οι προδιαγραφές του δίνουν μέγιστη κατανάλωση ίση με 2.55 mWatt, οπότε αντίστοιχα έχει ετήσια κατανάλωση ίση με 22.338 βατώρες ετησίως. Αυτό σημαίνει ότι η κατανάλωση ρεύματος του αποδοτικού αισθητήρα είναι 66% λιγότερη σε σχέση με τον μη αποδοτικό. Σε ένα περιβάλλον IIoT μπορεί να χρησιμοποιούνται χιλιάδες αισθητήρες, οπότε οι επιβαρύνσεις από την κατανάλωση ρεύματος των συσκευών να είναι υψηλές. Επιπρόσθετα, η υλοποίηση του υπολογισμού αιχμής μπορεί να βοηθήσει στη μείωση της κατανάλωσης ενέργειας, καθώς τα δεδομένα επεξεργάζονται τοπικά στις συσκευές και μόνο τα σημαντικά δεδομένα μεταφέρονται στις βάσεις του σύννεφου. Επίσης, η χρήση ενεργειακά αποδοτικών πρωτοκόλλων επικοινωνίας όπως το Zigbee, το LoRaWAN, και το NB-IoT επιτρέπουν την αποδοτική μετάδοση δεδομένων με ελάχιστη ενεργειακή κατανάλωση, καθιστώντας κατάλληλα για βιομηχανικά περιβάλλοντα με μεγάλες αποστάσεις και περιορισμένες πηγές ενέργειας. Ακόμα, συσκευές που δεν χρησιμοποιούνται θα πρέπει να μπαίνουν σε κατάσταση αδράνειας για την ελαχιστοποίηση των ενεργειακών καταναλώσεων. Για παράδειγμα, αισθητήρες μπορούν να ενεργοποιούνται και να στέλνουν δεδομένα μόνο όταν ανιχνεύουν κρίσιμες αλλαγές στο περιβάλλον. Έτσι, όσο δεν στέλνουν δεδομένα, έχει προαποφασιστεί μία κατάσταση ηρεμίας, κατά την οποία θεωρείται ότι οι συνθήκες είναι ιδανικές και κατάλληλες και δεν χρειάζεται να ληφθούν μέτρα. Επιπλέον, ίσως είναι αναγκαίο να εξεταστούν εναλλακτικοί τρόποι πηγών ενέργειας, ιδιαίτερα για εγκαταστάσεις απομακρυσμένες ή για εγκαταστάσεις όπου το δίκτυο ηλεκτροδότησης είναι μη αξιόπιστο. Ηλιακά πάνελ και ανεμογεννήτριες δύναται να χρησιμοποιηθούν εάν είναι σκόπιμο. Τέλος, μειωμένη ενεργειακή κατανάλωση μπορεί να επιτευχθεί στα πράσινα κέντρα δεδομένων (green data centers) (Tasmiha Khan, 2024), που χρησιμοποιούν ενεργειακά αποδοτικές τεχνολογίες για να βελτιστοποιήσουν τη χρήση ενέργειας και να μειώσουν τις

---

<sup>7</sup> <https://www.sparkfun.com/datasheets/Sensors/Temperature/DHT22.pdf>

<sup>8</sup> [https://www.te.com/commerce/DocumentDelivery/DDEController?Action=showdoc&DocId=Data+Sheet%7FHTU31\\_RHT\\_SENSOR\\_IC%7F3%7Fpdf%7FEnglish%7FENG\\_DS\\_HTU31\\_RHT\\_SENSOR\\_IC\\_3.pdf%7F10142048-01](https://www.te.com/commerce/DocumentDelivery/DDEController?Action=showdoc&DocId=Data+Sheet%7FHTU31_RHT_SENSOR_IC%7F3%7Fpdf%7FEnglish%7FENG_DS_HTU31_RHT_SENSOR_IC_3.pdf%7F10142048-01)

περιβαλλοντικές επιπτώσεις. Τα IIoT συστήματα που επεξεργάζονται και αποθηκεύουν μεγάλα δεδομένα έχουν υψηλές ενεργειακές απαιτήσεις, τα πράσινα κέντρα δεδομένων δύναται να ανανεώνουν εξοπλισμό και να χρησιμοποιούν ανανεώσιμες πηγές ενέργειας όπως η αιολική και η ηλιακή, ελαχιστοποιώντας τις εκπομπές άνθρακα και μειώνοντας τις ενεργειακές δαπάνες. Ακόμη, χρησιμοποιούνται τεχνικές όπως αυτή της εικονοποίησης (virtualization), όπου πολλές εικονικές μηχανές λειτουργούν σε μία πραγματική μηχανή. Κατά αυτό τον τρόπο, γίνεται αποδοτικότερη κατανομή φορτίου στις μηχανές, υπάρχουν λιγότερες ανάγκες ψύξης λόγω των λιγότερων πραγματικών μηχανών που απαιτούνται και η χρήση των πόρων είναι ασφαλώς καλύτερη.

Η Ευρωπαϊκή Ένωση έχει θέσει ρυθμίσεις που αφορούν την ενεργειακή αποδοτικότητα και τη μείωση των περιβαλλοντικών επιπτώσεων των επιχειρήσεων. Οι ίδιες οδηγίες επηρεάζουν και τα περιβάλλοντα IIoT. Το σύστημα εμπορίας εκπομπών της ΕΕ (EU Emissions Trading System – ETS)<sup>9</sup> περιορίζει τις εκπομπές διοξειδίου του άνθρακα και άλλων αερίων σε μεγάλες βιομηχανίες. Οι επιχειρήσεις είναι υποχρεωμένες να αποκτούν δικαιώματα εκπομπών για να καλύπτουν τις εκπομπές τους, ενώ δεσμεύονται την μείωση αυτών με την πάροδο του χρόνου. Ακόμα, το EMAS – Eco-Management and Audit Scheme<sup>10</sup> είναι ένας κανονισμός για την περιβαλλοντική διαχείριση που αναπτύχθηκε από την ΕΕ με σκοπό να βοηθήσει τους οργανισμούς να αξιολογούν, να βελτιώνουν και να αναφέρουν τις περιβαλλοντικές επιπτώσεις τους. Όσες επιχειρήσεις συμμετέχουν στο EMAS πρέπει να συμμορφώνονται με υψηλά περιβαλλοντικά πρότυπα. Σε γενικές γραμμές, οι επιχειρήσεις πρέπει να εφαρμόζουν μέτρα για τη βελτίωση της ενεργειακής απόδοσης σε διάφορες δραστηριότητες, από τη χρήση μηχανημάτων και εξοπλισμού έως τη διαχείριση κτηριακών εγκαταστάσεων. Ένα περιβάλλον IIoT, που διαθέτει πολλά μηχανήματα και μεγάλο εξοπλισμό οφείλει να συμμορφώνεται και να ακολουθεί τις οδηγίες της ΕΕ. Επιπρόσθετα, οι καταναλωτές και οι επενδυτές είναι πλέον ευαισθητοποιημένοι σε περιβαλλοντικά θέματα και η μη συμμόρφωση με τους κανόνες μπορεί να έχει επίπτωση στη φήμη της βιομηχανίας.

**Απαιτήσεις για ασφάλεια:** Οι απαιτήσεις σε ασφάλεια είναι ιδιαίτερα σημαντικές, αφού εάν οι λειτουργίες, τα δεδομένα και οι συσκευές παραβιαστούν μπορεί να δημιουργηθούν επικίνδυνες και ανεπιθύμητες καταστάσεις στους εργαζομένους, οικονομικές ζημιές και περιβαλλοντικά επικίνδυνες καταστάσεις. Συνεπώς, τα δίκτυα στα οποία μεταφέρονται οι πληροφορίες θα πρέπει να είναι ασφαλή από επιθέσεις που μπορούν να πάρουν τον έλεγχο μηχανημάτων ή να διακόψουν την παραγωγή. Επίσης, τα δεδομένα που συλλέγονται και διακινούνται θα πρέπει να είναι προστατευμένα από υποκλοπές και αλλοιώσεις. Επίσης, υπάρχει ανάγκη ταυτοποίησης, ώστε μόνο εξουσιοδοτημένα άτομα να μπορούν να έχουν πρόσβαση στα

---

<sup>9</sup> [https://climate.ec.europa.eu/eu-action/eu-emissions-trading-system-eu-ets/what-eu-ets\\_en](https://climate.ec.europa.eu/eu-action/eu-emissions-trading-system-eu-ets/what-eu-ets_en)

<sup>10</sup> [https://green-business.ec.europa.eu/emas\\_en](https://green-business.ec.europa.eu/emas_en)

δεδομένα και στον έλεγχο των μηχανημάτων. Οποιαδήποτε επίθεση θα πρέπει να εντοπίζεται άμεσα και να αντιμετωπίζεται. Το αντίκτυπο μιας επίθεσης, μπορεί να έχει τεράστιες οικονομικές επιπτώσεις για την επιχείρηση, τραυματισμό εργαζομένων από κακόβουλο χειρισμό των μηχανημάτων αλλά και διαρροή ευαίσθητων δεδομένων.

## ΚΕΦΑΛΑΙΟ 4: ΑΣΦΑΛΕΙΑ ΚΑΙ ΙΔΙΩΤΙΚΟΤΗΤΑ

Το περιβάλλον του IIoT περιλαμβάνει διάφορες τεχνολογίες που επεξεργάζονται, αναλύουν και αποθηκεύουν τεράστιο όγκο πληροφοριών. Τα πληροφοριακά συστήματα χρησιμοποιούν τα δεδομένα, προκειμένου να είναι αποδοτικά. Ωστόσο, όσο προχωράει η τεχνολογία των πληροφοριακών συστημάτων, τόσο μεγαλύτερη σημασία αποκτούν τα δεδομένα αυτά. Η χρήση τους θα πρέπει να γίνεται με υπευθυνότητα και σεβασμό στα ανθρώπινα δικαιώματα και για αυτό το λόγο είναι επιτακτική η ανάγκη για την ύπαρξη ασφαλών μεθόδων προστασίας και διακίνησης των δεδομένων. Στο κεφάλαιο αυτό, αποσαφηνίζονται οι όροι της Ιδιωτικότητας και της Ασφάλειας στην επιστήμη των υπολογιστών, καθώς και πως αυτοί συνδέονται με το Διαδίκτυο των Πραγμάτων και κα επέκταση με το Βιομηχανικό Διαδίκτυο των Πραγμάτων.

### 4.1 Ιδιωτικότητα

Ο όρος της ιδιωτικότητας «privacy» ξεκίνησε να γίνεται ευρέως γνωστός από τους Samuel Warren και Louis Brandeis μέσω του άρθρου τους με τίτλο «The Right to Privacy» (Warren S, Brandeis L, 1890). Υποστήριξαν την αναγνώριση ενός νομικού δικαιώματος στην ιδιωτικότητα για την προστασία των ατόμων από ανεπιθύμητη εισβολή στην ιδιωτική τους ζωή. Αφορμή ήταν οι μεγάλες τεχνολογικές και κοινωνικές αλλαγές της εποχής, όπως η ευρεία χρήση της φωτογραφίας και των εφημερίδων, καθώς και καινούριες κοινωνικές συνθήκες που έφερε η αστικοποίηση μετά τη βιομηχανική επανάσταση. Ο όρος της ιδιωτικότητας συνδέεται με το δικαίωμα για προστασία της προσωπικής ζωής από αδικαιολόγητες επεμβάσεις σε αυτή, στην επικοινωνία και γενικότερα αντιτίθεται στην κυβερνητική παρακολούθηση, αλλά και με το πληροφοριακό απόρρητο που εκτείνεται κυρίως στο ψηφιακό κόσμο. Το πληροφοριακό απόρρητο αφορά τα δικαιώματα και τον έλεγχο πάνω στη συλλογή, χρήση, κοινοποίηση και προστασία των προσωπικών δεδομένων από το κράτος και ιδιωτικούς οργανισμούς. Παραδείγματα τέτοιων δεδομένων είναι χαρακτηριστικά, όπως η ημερομηνία γέννησης ενός ατόμου, η σεξουαλική προτίμηση, η τοποθεσία, η θρησκεία, αλλά και η διεύθυνση IP του υπολογιστή του ή τα μεταδεδομένα («metadata») που αφορούν αυτού του είδους τις πληροφορίες. Επιπλέον, τα προσωπικά δεδομένα μπορούν να είναι πιο έμμεσα, στη μορφή συμπεριφορικών δεδομένων, για παράδειγμα από τα κοινωνικά δίκτυα, τα οποία μπορούν να συνδεθούν με τα άτομα, οι ενέργειες των ατόμων στον ψηφιακό κόσμο που φανερώνουν τις προτιμήσεις τους.

Η εκμετάλλευση των προσωπικών δεδομένων είναι ένα καθημερινό φαινόμενο στον ψηφιακό κόσμο. Κάθε κλικ, αναζήτηση, αγορά ή οποιαδήποτε άλλη δραστηριότητα στον διαδίκτυο αφήνει ένα ψηφιακό αποτύπωμα, το οποίο δύναται να περισυλλεχθεί από εταιρείες, διαφημιστές ή κακόβουλους χρήστες. Το πρόβλημα είναι ότι συνήθως τα δεδομένα συλλέγονται χωρίς κάποια ρητή συγκατάθεση ή η συγκατάθεση βρίσκεται θαμμένη σε μακροσκελείς όρους που λήγει θα διαβάσουν και ακόμα λιγότεροι θα κατανοήσουν (Fowler, 2022). Αυτή η πρακτική έχει κανονικοποιήσει μία κοινωνία παρακολούθησης, όπου τα άτομα βρίσκονται σε συνεχή

παρακολούθηση και τα δεδομένα τους συλλέγονται για διάφορους σκοπούς. Τα δεδομένα αυτά συχνά είναι στόχος για διαφημιστές, αναλυτές δεδομένων, κοινωνικά μέσα και εταιρείες που μπορούν να δημιουργήσουν λεπτομερή προφίλ χρηστών. Ταυτόχρονα η συλλογή των δεδομένων είναι ελκυστική για τους ψηφιακούς εγκληματίες, οι οποίοι συνήθως προσπαθούν να αποσπάσουν ευαίσθητες πληροφορίες όπως αριθμούς ασφαλείας και κωδικούς, οικονομικά στοιχεία, τηλέφωνα και emails. Αυτό μπορεί να έχει ως αντίκτυπο την κλοπή της ταυτότητας του ατόμου, οικονομικές απώλειες και σημαντική εισβολή στην ιδιωτικότητα. Τέλος, τα δεδομένα και οι προτιμήσεις των ατόμων, μπορούν να χρησιμοποιηθούν για την χειραγώγηση της μάζας και την υπονόμευση της δημοκρατίας. Τα δεδομένα που θα συλλεχθούν, μπορεί να φανερώσουν προτιμήσεις, τις οποίες θα εκμεταλλευτούν οι κυβερνήσεις. Συνεπώς, η σημασία της ιδιωτικότητας και των προσωπικών δεδομένων έχει πολλαπλές διαστάσεις.

Η προστασία της ιδιωτικότητας θα πρέπει να γίνεται λαμβάνοντας υπόψη ένα σωρό από προκλήσεις. Αρχικά, η συγκατάθεση στα προσωπικά δεδομένα γίνεται με επίγνωση από τα άτομα προκειμένου να μην υπονομεύεται η ηθική των δεδομένων και η αυτονομία των ατόμων πάνω στα προσωπικά τους στοιχεία. Δεύτερον, τίθενται διάφορα ερωτήματα σχετικά με την παρακολούθηση και κατασκοπεία των κυβερνήσεων, αφού η χρήση εξελιγμένων αλγορίθμων σε δεδομένα μπορεί να δημιουργήσει προβλέψεις για το μέλλον. Επιπροσθέτως, όσο μεγαλώνει ο όγκος των δεδομένων που αποθηκεύονται στο διαδίκτυο, η υποκλοπή της ταυτότητας και ευαίσθητων πληροφοριών αυξάνεται. Επίσης, σε ότι αφορά την αξιοποίηση των δεδομένων και το πως αυτά θα χρησιμοποιηθούν ή που θα διαμοιραστούν τίθενται συχνά διάφορα ερωτήματα. Με άλλα λόγια, η διαφάνεια της εκμετάλλευσης των προσωπικών δεδομένων είναι συχνά ελλιπής. Άλλη μια πρόκληση στην προστασία της ιδιωτικότητας προκύπτει από το διαφορετικό νομοθετικό πλαίσιο της κάθε χώρας. Κάθε χώρα έχει τη δικιά της νομοθεσία, ωστόσο το διαδίκτυο είναι παγκόσμιο και δύσκολο μπορεί να περιοριστεί σε σύνορα. Επιπλέον, οι τεχνολογίες που συνεχώς εξελίσσονται όπως το IoT και το Artificial Intelligence (AI) μπορούν να συλλέγουν και να επεξεργάζονται δεδομένα με τρόπους που είναι δύσκολο να ελεγχθούν ή να υπακούσουν στα υπάρχοντα συστήματα κανόνων. Ακόμη, υπάρχει μεγάλη αδιαφορία και αμάθεια από τους χρήστες των τεχνολογιών σχετικά με τη σημασία της ιδιωτικότητας. Αυτή η έλλειψη επαγρύπνησης, οδηγεί σε υποτίμηση της σημασίας της ιδιωτικότητας, δημιουργώντας περισσότερες συνέπειες από τη διακίνηση των προσωπικών δεδομένων.

## **4.2 Ασφάλεια**

Η έννοια της ασφάλειας στην επιστήμη των υπολογιστών περιλαμβάνει όλες τις πρακτικές, πολιτικές και τεχνολογίες με σκοπό την προστασία των υπολογιστικών συστημάτων, δικτύων και δεδομένων από μη εξουσιοδοτημένη πρόσβαση, ζημιά ή κλοπή. Με άλλα λόγια, προσπαθεί να διασφαλίσει την εμπιστευτικότητα (confidentiality), την ακεραιότητα (integrity) και διαθεσιμότητα (availability) των πληροφοριών (Pfleeger, 2015). Η ασφάλεια κατηγοριοποιείται

προκειμένου να μελετηθεί ξεχωριστά σε διάφορες περιοχές. Έτσι, έχουν δημιουργηθεί οι παρακάτω κατηγορίες:

**Ασφάλεια στο φυσικό επίπεδο:** Περιλαμβάνει την ασφάλεια και μέτρα ασφαλείας από δολιοφθορές και κλοπές υλικού από εισβολείς. Για παράδειγμα, η απόκρυψη ενός σκληρού δίσκου ή καναλιών που περνούν ευαίσθητες πληροφορίες και φύλαξη αυτών σε ασφαλές δωμάτιο, προσβάσιμο σε εξουσιοδοτημένα και έμπιστα άτομα.

**Ασφάλεια δικτύων:** Μέτρα για την προστασία των δεδομένων κατά τη μετάδοση τους μέσω δικτύων. Αυτά στοχεύουν, στην ασφαλή παράδοση του μηνύματος στον εξουσιοδοτημένο χρήστη, καθώς και στην ακεραιότητα του μηνύματος μέχρι να φτάσει στον τελικό παραλήπτη.

**Ασφάλεια πληροφοριών:** Διαβεβαιώνει την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των δεδομένων, που εδρεύουν κυρίως σε βάσεις δεδομένων και στο cloud. Στοχεύει κυρίως στην προστασία των δεδομένων αυτών από πρόσβαση μη εξουσιοδοτημένων ατόμων, χρήση, αλλοίωση και καταστροφή αυτών.

**Ασφάλεια εφαρμογών:** Περιλαμβάνει την προστασία μίας εφαρμογής από απειλές και κακόβουλους ιούς. Συνήθως, οι εφαρμογές απειλούνται από ιούς τύπου δούρειων ίππων. Για αυτό το λόγο, είναι σημαντικό να υπάρχει το λεγόμενο “testing” από ιούς κατά την παραγωγή μίας εφαρμογής, αλλά και υποστήριξη κατά την διατήρηση της.

**Κρυπτογραφία:** Η χρήση της κρυπτογραφίας είναι από τα πιο σημαντικά μέτρα για τη διασφάλιση της εμπιστευτικότητας και ακεραιότητας των δεδομένων. Εξελιγμένοι αλγόριθμοι κωδικοποιούν τα μηνύματα και η αποκωδικοποίηση τους γίνεται εφικτή μονάχα από εξουσιοδοτημένα άτομα.

**Επιχειρησιακή ασφάλεια:** Περιλαμβάνει τις πολιτικές και διαδικασίες για το χειρισμό και την επεξεργασία των δεδομένων.

**Ασφάλεια τελικού χρήστη:** Αφορά κυρίως την εκπαίδευση και επαγρύπνηση του τελικού χρήστη προκειμένου να χρησιμοποιεί με ασφάλεια τις υπηρεσίες. Αυτό περιλαμβάνει, τη χρήση διαφορετικών κωδικών στις εφαρμογές, την πρόσβαση σε αξιόπιστες ιστοσελίδες, την αποφυγή από επιθέσεις τύπου “Phishing” κλπ.

**Ασφάλεια και ιδιωτικότητα:** Από τη στιγμή που η ασφάλεια ασχολείται με την εμπιστευτικότητα και ακεραιότητα των δεδομένων είναι φανερό ότι έχει άμεση σχέση με την προστασία των προσωπικών δεδομένων, δηλαδή την ιδιωτικότητα. Η φύλαξη και προστασία των προσωπικών δεδομένων από τρίτους είναι από τις πιο σημαντικές δικλείδες ασφαλείας της ιδιωτικότητας. Εμπιστοσύνη σχετικά με τα προσωπικά δεδομένα που χρησιμοποιούνται από υπηρεσίες χτίζονται και επικυρώνονται με συμφωνητικά και πολιτικές χρησιμοποίησης. Ο όρος ιδιωτικότητα από το σχεδιασμό («privacy by design»), χρησιμοποιείται στις διεργασίες των μηχανικών συστημάτων. Αυτό περιλαμβάνει την εφαρμογή ελέγχων ασφαλείας από την αρχή για τη διασφάλιση του απορρήτου των δεδομένων καθ' όλη τη διάρκεια του κύκλου ζωής τους, δείχνοντας πώς τα μέτρα ασφαλείας είναι καθοριστικά για την επίτευξη των στόχων απορρήτου.

### 4.3 Κανονιστική συμμόρφωση

Προκειμένου να εντοπιστούν οι απαιτήσεις προστασίας της ιδιωτικότητας σε οποιοδήποτε περιβάλλον θα πρέπει να οριστεί με κάποιο τρόπο το πλαίσιο ελευθερίας διακίνησης ευαίσθητων πληροφοριών, η πρόσβαση και η εξουσιοδότηση της συλλογής δεδομένων, καθώς και η επεξεργασία τους με τη σύμφωνη γνώμη των ενδιαφερόμενων. Στην Ελλάδα όπως και στα υπόλοιπα κράτη της Ευρωπαϊκής Ένωσης, οι κανόνες ιδιωτικότητας ορίζονται από το General Data Protection Regulation (GDPR) της Ευρωπαϊκής Ένωσης (europa.eu, n.d.). Επιπρόσθετα για την Ελλάδα, είναι σε εφαρμογή ο νόμος 4624/2019 (kodiko.gr, 2019). Ο ορισμός του τι θεωρείται προσωπικά δεδομένα μπορεί να γίνει αρκετά περίπλοκος, δεδομένου ότι δεν υπάρχουν ξεκάθαρα όρια, ωστόσο μπορεί να προσδιοριστεί το μεγαλύτερο μέρος αυτών. Πιο συγκεκριμένα, προσωπικά δεδομένα όπως τα στοιχεία που περιέχονται σε ένα διαβατήριο, ειδικές κατηγορίες προσωπικών δεδομένων όπως σεξουαλικότητα, θρησκεία, υγεία και βιομετρικά χαρακτηριστικά καθώς και η επεξεργασία αυτών (αποθήκευση, διακίνηση ή διαγραφή) θα πρέπει να διαχειρίζονται προσεκτικά. Μερικές από τις βασικές αρχές του GDPR περιλαμβάνουν τη διαφάνεια στην επεξεργασία δεδομένων, περιορισμό με βάση το σκοπό, την αρχή της αναλογικότητας και την ασφάλεια των δεδομένων. Ο ιδιώτης έχει δικαίωμα στην πρόσβαση των δεδομένων που συλλέγονται, στη διόρθωση σφαλμάτων, στη διαγραφή και αντίρρηση στην επεξεργασία και διακίνηση αυτών. Οι οργανισμοί είναι υποχρεωμένοι να ορίσουν έναν Υπεύθυνο Προστασίας Δεδομένων (ΥΠΔ) ή Data Protection Officer (DPO) εφόσον είναι αναμεμειγμένοι σε μεγάλης κλίμακας ευαίσθητα δεδομένα ή χρειάζονται συστηματική παρακολούθηση δεδομένων όπως συνηθίζεται σε περιβάλλοντα IIoT.

### 4.4 Πραγματικές περιπτώσεις παραβιάσεων ιδιωτικότητας

Αναλύοντας πραγματικά περιστατικά παραβιάσεων ιδιωτικότητας του Βιομηχανικού Διαδικτύου των Πραγμάτων αποκαλύπτονται κρίσιμα μαθήματα.

**Stuxnet (2010):** Ένα από τα πιο αξιοσημείωτα περιστατικά ασφάλειας στο IIoT είναι η επίθεση με τον ιό Stuxnet (KUSHNER, 2013). Ανακαλύφθηκε αρχικά το 2010 και είχε ως στόχο τους προγραμματιζόμενους λογικούς ελεγκτές (PLCs) που χρησιμοποιούνταν στο ιρανικό πυρηνικό πρόγραμμα. Αυτή η κυβερνοεπίθεση ανέδειξε την ευπάθεια των συστημάτων ελέγχου της βιομηχανίας στο κακόβουλο λογισμικό. Η κρίσιμη σημασία της ασφάλισης των συσκευών IIoT ενάντια σε περίπλοκο κακόβουλο λογισμικό είναι απαραίτητη, καθώς το συγκεκριμένο περιστατικό φανερώνει ένα από τα τρωτά σημεία ενός βιομηχανικού περιβάλλοντος. Με αφορμή αυτό το περιστατικό δόθηκε έμφαση στην ανάγκη για ισχυρά μέτρα κυβερνοασφάλειας σε βιομηχανικά περιβάλλοντα για την προστασία όχι μόνο από την κλοπή δεδομένων, αλλά και από την πιθανή δολιοφθορά.

**Έντουαρντ Σνόουντεν (2013):** Οι αποκαλύψεις του Έντουαρντ Σνόουντεν (Snowden, 2019) έφεραν στο φως ένα σωρό παραβιάσεις ιδιωτικότητας και παρατεταμένης παρακολούθησης

από τις κυβερνητικές υπηρεσίες της Αμερικής όπως την National Security Agency (NSA). Σε αυτές περιλαμβάνονται τεράστιες συλλογές από δεδομένα, προερχόμενα από τηλεφωνικές κλήσεις, emails, και διαδικτυακή δραστηριότητα ατόμων τόσο σε τοπικό όσο και σε διεθνές επίπεδο. Αυτά τα δεδομένα συνοδεύονταν επίσης από σχετικά μεταδεδομένα όπως η διάρκεια κλήσης των τηλεφωνημάτων, τα ονόματα των κατόχων των τηλεφώνων και άλλες ευαίσθητες πληροφορίες. Αυτά εγείρουν τεράστια ερωτήματα για τη χρήση αυτών των δεδομένων και την μαζική παρακολούθηση της κυβέρνησης. Εκτός από αυτό, υπογραμμίζεται η έλλειψη διαφάνειας και νομικών εξουσιοδοτήσεων για αυτές τις δραστηριότητες.

**Επίθεση στο ηλεκτρικό δίκτυο της Ουκρανίας (2015):** Τον Δεκέμβριο του 2015, μια κυβερνοεπίθεση στο ηλεκτρικό δίκτυο της Ουκρανίας άφησε 225,000 κατοίκους χωρίς ηλεκτρική ενέργεια (cisa.gov, 2021). Οι επιτιθέμενοι χρησιμοποίησαν μηνύματα phishing για να εγκαταστήσουν κακόβουλο λογισμικό στα συστήματα ελέγχου του δικτύου. Αυτό το περιστατικό δείχνει το δυναμικό από την εκμετάλλευση των συστημάτων IIoT. Οι εργαζόμενοι που δουλεύουν στις επιχειρήσεις και χειρίζονται τεχνολογικά μηχανήματα θα πρέπει να είναι ενήμεροι και εκπαιδευμένοι όσο αναφορά τους κινδύνους των ηλεκτρονικών επιθέσεων, τις πληροφορίες που διαρρέουν και τη σωστή χρήση των συσκευών και της τεχνολογίας.

**Επίθεση Mirai Botnet (2016):** Το κακόβουλο λογισμικό botnet Mirai μετέτρεψε δικτυωμένες συσκευές που τρέχουν παλιές εκδόσεις του Linux σε απομακρυσμένα ελεγχόμενα "bots" (cloudflare, 2017). Το συγκεκριμένο παράδειγμα αποτελεί ορόσημο στον τομέα του Διαδικτύου των Πραγμάτων (IIoT). Χρησιμοποιήθηκε κυρίως για επιθέσεις σε μεγάλη κλίμακα δικτύων, συμπεριλαμβανομένης της διάσημης κυβερνοεπίθεσης στην εταιρεία Dyn το 2016. Αυτό το περιστατικό υπογραμμίζει τη σημασία της ασφάλισης των συσκευών IIoT. Πολλές από αυτές τις συσκευές είχαν προεπιλεγμένα ονόματα χρήστη και κωδικούς πρόσβασης, τα οποία εκμεταλλεύτηκε εύκολα το κακόβουλο λογισμικό.



## ΚΕΦΑΛΑΙΟ 5: ΕΝΤΟΠΙΣΜΟΣ ΑΠΑΙΤΗΣΕΩΝ ΠΡΟΣΤΑΣΙΑΣ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΣΕ ΠΕΡΙΒΑΛΛΟΝ IIOT

Οι εμπλεκόμενες τεχνολογίες στο IIoT καθιστούν ιδιαίτερα περίπλοκο το περιβάλλον του. Κάθε τεχνολογία που χρησιμοποιείται κάνει χρήση δεδομένων που πολλές φορές χαρακτηρίζονται ευαίσθητα και ακόμη μπορούν να εξαχθούν ευαίσθητα συμπεράσματα από την επεξεργασία τους. Όπως σε κάθε περιβάλλον που εκτίθενται δεδομένα, υπάρχει ένα πλαίσιο που προστατεύει την ιδιωτικότητα, έτσι και εδώ είναι σαφές πως πρέπει να οριοθετηθεί ένα τέτοιο. Σε αυτό το κεφάλαιο, μελετάται το πλαίσιο της ιδιωτικότητας σε ένα περιβάλλον IIoT και εξετάζονται διάφορα ευπαθή σημεία με σκοπό τον προσδιορισμό και τον καλύτερο έλεγχο τους. Προκειμένου να προσδιοριστούν οι απαιτήσεις και οι ευπάθειες που συνδέονται με τα περιβάλλοντα του IIoT αναλύονται δύο διαφορετικά σενάρια με τη χρήση διαφορετικών εργαλείων που μπορεί να χρησιμοποιήσει ένας αναλυτής συστημάτων.

### 5.1 Υποθετικό σενάριο διαχείρισης δεδομένων σε ένα περιβάλλον IIoT

Όπως έχει ήδη αναλυθεί σε προηγούμενο κεφάλαιο, οι τεχνολογίες του IIoT περιλαμβάνουν την αποθήκευση, διακίνηση και επεξεργασία ευαίσθητων δεδομένων προκειμένου να βελτιστοποιήσουν το κύκλο παραγωγής της επιχείρησης. Αυτό μπορεί να δημιουργήσει αρκετά κενά ασφαλείας που θα πρέπει να ληφθούν υπόψη. Για τη καλύτερη κατανόηση των κενών ασφαλείας που μπορεί να δημιουργηθούν αναλύεται το παρακάτω υποθετικό σενάριο που αφορά το σύστημα μιας κλινικής, που δύναται να μελετηθεί ως ένα περιβάλλον IIoT.

#### 5.1.1 Περιγραφή σεναρίου Α

Έστω ότι υπάρχει μία κλινική η οποία χρησιμοποιεί ποικίλες έξυπνες συσκευές σε ασθενείς για την παρακολούθηση μετρικών όπως ο καρδιακός ρυθμός, η πίεση του αίματος, η θερμοκρασία σώματος και άλλες ζωτικές ενδείξεις. Οι συσκευές αυτές είναι συνδεδεμένες στο δίκτυο του νοσοκομείου και τα δεδομένα που συλλέγουν μεταφέρονται σε πραγματικό χρόνο σε ένα τοπικό εξυπηρετητή (server). Ο εξυπηρετητής αυτός επεξεργάζεται τα δεδομένα, αναλύει τις τάσεις των ενδείξεων και ειδοποιεί για κρίσιμες καταστάσεις, πριν αποθηκεύσει τα δεδομένα στη βάση καταγραφών της κλινικής. Επιπρόσθετα το σύστημα μπορεί να επικοινωνεί με κινητές συσκευές επιτρέποντας στο ιατρικό προσωπικό να λαμβάνει τις ενημερώσεις και τις ειδοποιήσεις οπουδήποτε κι αν βρίσκεται στο χώρο του νοσοκομείου. Επίσης, κλινική διαθέτει ένα σύστημα παρακολούθησης εξοπλισμού, ώστε να γνωρίζει κάθε στιγμή σε ποιες κλίνες βρίσκεται ο εξοπλισμός και αν υπάρχει διαθέσιμος προς χρήση. Αυτό επιτυγχάνεται μέσω ετικετών Radio Frequency Identification (RFID) ή ετικετών WiFi πάνω στον εξοπλισμό. Έτσι, φορητός εξοπλισμός όπως είναι τα αναπηρικά καροτσάκια, οι απινιδωτές κι άλλα μπορούν να κάνουν γνωστά τη θέση τους στο χώρο της κλινικής. Τέλος, η κλινική διαθέτει αυτόματες συσκευές διανομής φαρμάκων, που μεριμνούν για τη σωστή δόσοληψία των φαρμάκων από τους ασθενείς. Αυτές διαθέτουν διάφορα χάπια, και προγραμματίζονται από το ιατρικό προσωπικό

ώστε να απελευθερώνουν τη σωστή δΟΣολογία, την κατάλληλη χρονική στιγμή. Παράλληλα ηχούν ώστε να ειδοποιήσουν τον ασθενή να λάβει την θεραπεία του, μόλις αυτή απελευθερωθεί.

### **5.1.2 Οντότητες σεναρίου A**

Στο παραπάνω σενάριο, μπορούν να προσδιοριστούν οι εξωτερικές οντότητες ασθενείς, ιατρικό προσωπικό και φαρμακεία, τα οποία λειτουργούν σαν εξωτερικοί προμηθευτές. Ακόμα, μπορούν να προσδιοριστούν οι διάφορες διαδικασίες που γίνονται όπως α) η συλλογή των μετρικών υγείας από τις έξυπνες συσκευές, β) η κατάσταση και η θέση του ιατρικού εξοπλισμού, γ) η διανομή των φαρμάκων και η διαχείριση της αποθήκης, δ) η ανάλυση των δεδομένων και η δημιουργία ειδοποιήσεων εάν απαιτείται ε) η επικοινωνία των κινητών του ιατρικού προσωπικού με τις καταγραφές του νοσοκομείου και στ) η ανανέωση και αποθήκευση των δεδομένων στη βάση της κλινικής για ιστορική καταγραφή. Η βάση αποθηκεύει μετρικές σχετικές με την υγεία των ασθενών όπως η πίεση του αίματος και ο καρδιακός ρυθμός, δεδομένα σχετικά με τη θέση και κατάσταση του ιατρικού εξοπλισμού και τη διαθεσιμότητα των φαρμάκων. Τα παραπάνω μπορούν να γίνουν περισσότερα κατανοητά με τη βοήθεια ενός διαγράμματος ροής δεδομένων (ΔΡΔ) ή Data Flow Diagram (DFD). Αρχικά τα ιατρικά δεδομένα που καταγράφονται στους ασθενείς από έξυπνες συσκευές αποθηκεύονται προσωρινά και αναλύονται. Παράλληλα, άλλα δεδομένα σχετικά με την θέση και κατάσταση του ιατρικού εξοπλισμού καταγράφονται και αποθηκεύονται με τη βοήθεια κατάλληλων ετικετών RFID. Ειδοποιήσεις και οδηγίες δημιουργούνται από την ανάλυση των ιατρικών δεδομένων και των δεδομένων εξοπλισμού. Αυτές είναι προσβάσιμες και στέλνονται στο ιατρικό προσωπικό μέσω διεπαφών στα κινητά τους τηλέφωνα. Αυτόματοι διανομείς φαρμάκων καταναλώνουν το απόθεμα το φαρμάκων και τέλος ενημερώνονται τα προφίλ των ασθενών με τα νέα δευτερογενή δεδομένα που παράγονται από το στάδιο της ανάλυσης.

### **5.1.3 Περιγραφή δομής δεδομένων σεναρίου A**

Το ΔΡΔ περιγράφει σε υψηλό επίπεδο τη ροή των δεδομένων μέσα σε μια IIoT κλινική. Ωστόσο μια πιο λεπτομερής περιγραφή των δεδομένων θα βοηθήσει στην ανάλυση του σεναρίου και την εκμείωση των απαιτήσεων αυτού. Για το λόγο αυτό, αναλύεται η δομή των ροών δεδομένων του διαγράμματος.

**Ιατρικά Δεδομένα:** Μεταφέρουν σε πραγματικό χρόνο μετρικές σχετικές με την υγεία των ασθενών. Κύρια πηγή των δεδομένων αυτών είναι συσκευές που φοράει ο ασθενής όπως είναι τα έξυπνα ρολόγια και συλλέγουν τον καρδιακό ρυθμό, την αρτηριακή πίεση, τη θερμοκρασία και το οξυγόνο. Χαρακτηριστικά αυτών των δεδομένων είναι οι πληροφορίες που συλλέγουν καθώς και ένα αναγνωριστικό που αντιστοιχεί στον ασθενή μαζί με την χρονοσφραγίδα συλλογής της πληροφορίας. Τελικός προορισμός είναι μία βάση αποθήκευσης των μετρικών υγείας.

**Ενημέρωση Κατάστασης Εξοπλισμού:** Ενημερώνει την κατάσταση και την τοποθεσία του εξοπλισμού. Πηγή των δεδομένων αυτών αποτελεί το σύστημα παρακολούθησης των συσκευών που βασίζεται σε ετικέτες RFID. Χαρακτηριστικά των δεδομένων αυτών είναι το αναγνωριστικό του εξοπλισμού, η τοποθεσία του, η κατάσταση του (διαθέσιμο/ μη διαθέσιμο) και η χρονική στιγμή από την τελευταία παρατήρηση. Τελικός προορισμός είναι μία βάση αποθήκευσης της κατάστασης εξοπλισμού.

**Ενημέρωση Αποθέματος Διανομής Φαρμάκων:** Αφορά την ενημέρωση των φαρμακευτικών αποθεμάτων, κάθε φορά που χορηγείται ένα φάρμακο. Χαρακτηριστικά των δεδομένων αυτών μπορεί να είναι το αναγνωριστικό του φαρμάκου, το αναγνωριστικό του ασθενή στον οποίο χορηγείται, η χρονοσφραγίδα, η ποσότητα που χορηγείται και το αναγνωριστικό του επιβλέπων ιατρικού προσωπικού. Τα δεδομένα αυτά παράγονται από τους αυτόματους διανομείς φαρμάκων και καταλήγουν σε μία βάση που καταγράφει τα αποθέματα.

**Δευτερογενή δεδομένα:** Τα πρωτογενή ιατρικά δεδομένα έχουν μεταφραστεί σε ιατρικά κατανοητούς όρους. Οι διάφορες μετρικές υγείας, έχουν συσχετιστεί και έχουν δημιουργήσει ένα πόρισμα σχετικά με την κατάσταση υγείας του ασθενή. Χαρακτηριστικά των δεδομένων αυτών μπορεί να είναι, το αναγνωριστικό του ασθενή, η κατάσταση του καρδιακού ρυθμού καθώς και των υπολοίπων μετρικών (κακή, μέτρια, καλή), περιγραφή (μπορεί να περιλαμβάνει εκτενές αλφαριθμητικό κείμενο από τη συσχέτιση των καταστάσεων διαφόρων μετρικών και τη χρονοσφραγίδα).

**Ειδοποίηση Κατάστασης Ασθενούς:** Δημιουργεί προειδοποιητικά μηνύματα προς το ιατρικό προσωπικό σχετικά με την παρακολούθηση της υγείας των ασθενών. Εάν από τα δευτερογενή δεδομένα προκύψει κάτι ανησυχητικό στέλνει μήνυμα στο κινητό του εμπλεκόμενου ιατρικού προσωπικού. Χαρακτηριστικά των δεδομένων αυτών μπορεί να είναι το αναγνωριστικό του ασθενή, η κατάσταση των μετρικών, η περιγραφή, η βαθμός επικινδυνότητας, η χρονοσφραγίδα, το εμπλεκόμενο ιατρικό προσωπικό.

**Ενημέρωση Προφίλ Ασθενών:** Ανανεώνει τις πληροφορίες που είναι αποθηκευμένες στη κεντρική βάση που είναι σχετικές με τον ασθενή. Στη βάση δύναται να υπάρχουν επιπλέον πληροφορίες για τον ασθενή από την πρωταρχική του καταχώρηση (πχ ύψος, ηλικία, βάρος, ιστορικό, κλπ.). Χαρακτηριστικά των δεδομένων αυτών μπορεί να είναι το αναγνωριστικό του ασθενή, πιθανές ειδοποιήσεις από την κακή κατάσταση των μετρικών υγείας του, οι καταστάσεις των μετρικών υγείας (δευτερογενή δεδομένα), το υπεύθυνο ιατρικό προσωπικό, η χρονοσφραγίδα.

Η δομή των δεδομένων μπορεί να αποτυπωθεί σε ένα λεξικό που περιγράφει τα απαραίτητα χαρακτηριστικά των δεδομένων.

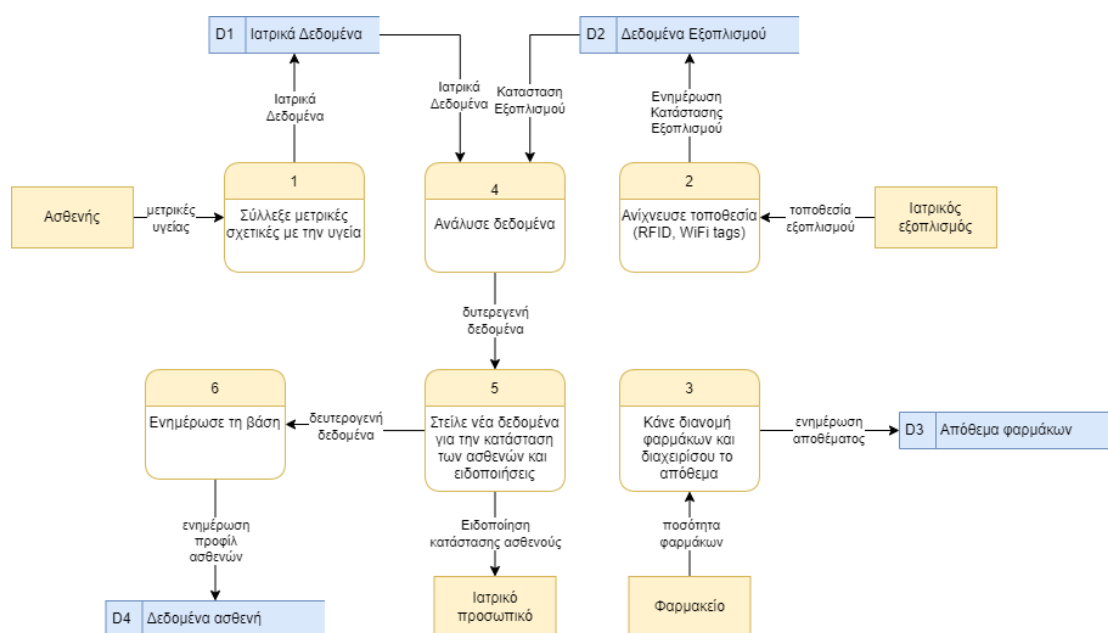


Figure 5 Διάγραμμα ροής δεδομένων ενός συστήματος έξυπνης κλινικής

Table 1 Πίνακας δεδομένων σεναρίου

|                                        |                                                                                                                                                                                                                                                                                    |
|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ιατρικά δεδομένα                       | patientID: Integer<br>timestamp: DateTime<br>heartRate: Integer, μετράται σε beats per minute<br>bloodPressure: String, Συστολική/Διαστολική<br>temperature: Float, θερμοκρασία σώματος σε βαθμούς Κελσίου<br>oxygen: Integer, ποσοστό                                             |
| Ενημέρωση Κατάστασης Εξοπλισμού        | equipmentID: Integer<br>location: String<br>status: String, Διαθέσιμο/ Μη διαθέσιμο<br>lastCheckedTime: DateTime                                                                                                                                                                   |
| Ενημέρωση Αποθέματος Διανομής Φαρμάκων | smartContainerID: Integer<br>medicationID: Integer<br>patientID: Integer<br>timestamp: DateTime<br>dosage: String<br>medicalStaffID: Integer                                                                                                                                       |
| Δευτερογενή Δεδομένα                   | PatientID: Integer<br>description: String, λεπτομερής περιγραφή κινδύνου<br>timestamp: DateTime<br>heartRateStatus: String<br>bloodPressureStatus: String<br>temperatureStatus: String<br>oxygenStatus: String                                                                     |
| Ειδοποίηση Κατάστασης Ασθενούς         | PatientID: Integer<br>alertType: String<br>description: String, λεπτομερής περιγραφή κινδύνου<br>severityLevel: String, βαθμός επικινδυνότητας (χαμηλή, Μέτρια, Υψηλή)<br>timestamp: DateTime<br>targetStaffID: Integer, εμπλεκόμενο ιατρικό προσωπικό που θα λάβει την ειδοποίηση |

|                             |                                                                                                                                                                                                                            |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ενημέρωση<br>προφίλ Ασθενών | PatientID: Integer<br>description: String, λεπτομερής περιγραφή<br>timestamp: DateTime<br>alertType: String<br>heartRateStatus: String<br>bloodPressureStatus: String<br>temperatureStatus: String<br>oxygenStatus: String |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### 5.1.4 Περιγραφή περιπτώσεων και απειλών

Οι οντότητες και η δομή των δεδομένων του σεναρίου βοηθούν στην κατανόηση, ωστόσο δεν φανερώνουν τις ευπάθειες του συστήματος. Προκειμένου να μελετηθεί το σύστημα ως προς την ασφάλεια και ιδιωτικότητα, είναι χρήσιμη οι δημιουργία περιπτώσεων επιθέσεων που αποκαλύπτουν τυχόν ευπάθειες. Για το λόγο αυτό, το σύστημα μελετάται σε διάφορες περιπτώσεις απειλών οι οποίες εξελίσσονται μέσα από UML sequence διαγράμματα και στη συνέχεια αναλύονται οι τρόποι αντιμετώπισης των πιθανών απειλών.

##### Περίπτωση 1 (Fake data)

Στο παρακάτω UML διάγραμμα αλληλουχίας, φαίνεται μία πιθανή επίθεση προσποίησης ταυτότητας από έναν επιτιθέμενο. Αρχικά, η συσκευή που φοράει ο ασθενής, στέλνει ιατρικά δεδομένα μέσω του δικτύου στη βάση. Κάποιος επιτιθέμενος που σχεδιάζει να προσποιηθεί ότι είναι η συσκευή, πρώτα αποκτά πρόσβαση στο δίκτυο εκμεταλλευόμενος κάποια ευπάθεια. Στη συνέχεια σαρώνει το δίκτυο και ψάχνει τα πακέτα που πηγαίνουν στη βάση από τη συσκευή του ασθενή. Με αυτό τον τρόπο μπορεί να μάθει τη δομή των δεδομένων και το token αυθεντικοποίησης. Στη συνέχεια φτιάχνει ένα όμοιο μήνυμα, όπως αυτό που βρήκε, αλλά χρησιμοποιεί ψεύτικο φορτίο. Τα νέα ψεύτικα δεδομένα αποθηκεύονται στη βάση και η εφαρμογή βασισμένη σε αυτά στέλνει μήνυμα κινδύνου στο ιατρικό προσωπικό. Τα αποτελέσματα από μία τέτοια επιτυχημένη επίθεση μπορεί να είναι εξαιρετικά κρίσιμα ακόμα και για την υγεία του ασθενούς, εφόσον το ιατρικό προσωπικό χορηγήσει θεραπεία με βάση αυτά.

##### Περίπτωση 2 (SQL injection)

Στο παρακάτω UML διάγραμμα αλληλουχίας, φαίνεται μία πιθανή επίθεση στη βάση του συστήματος όπου αποθηκεύονται ευαίσθητες πληροφορίες για τους ασθενείς. Ο επιτιθέμενος εκμεταλλευόμενος μία ευπάθεια της βάσης καταφέρνει να κερδίσει πρόσβαση και να διαρρεύσει τα ευαίσθητα ιατρικά και προσωπικά δεδομένα των ασθενών.

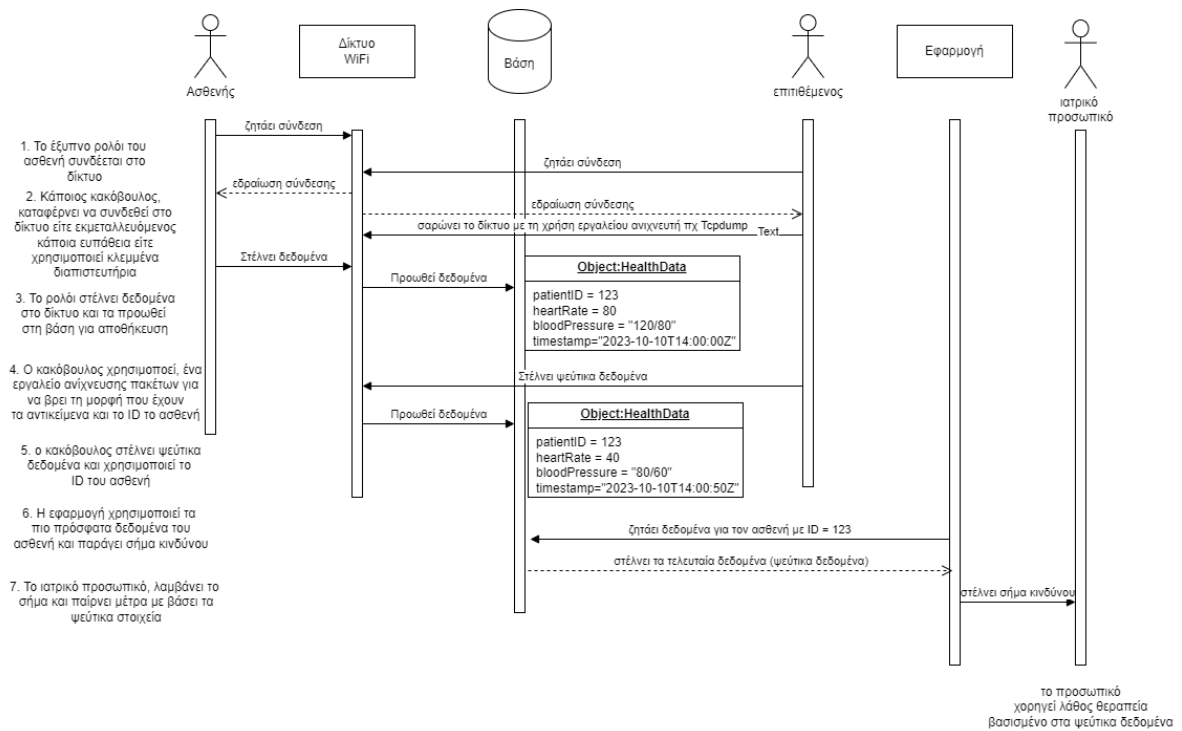


Figure 6 Διάγραμμα αλληλουχίας, περίπτωση προσποίησης ταυτότητας

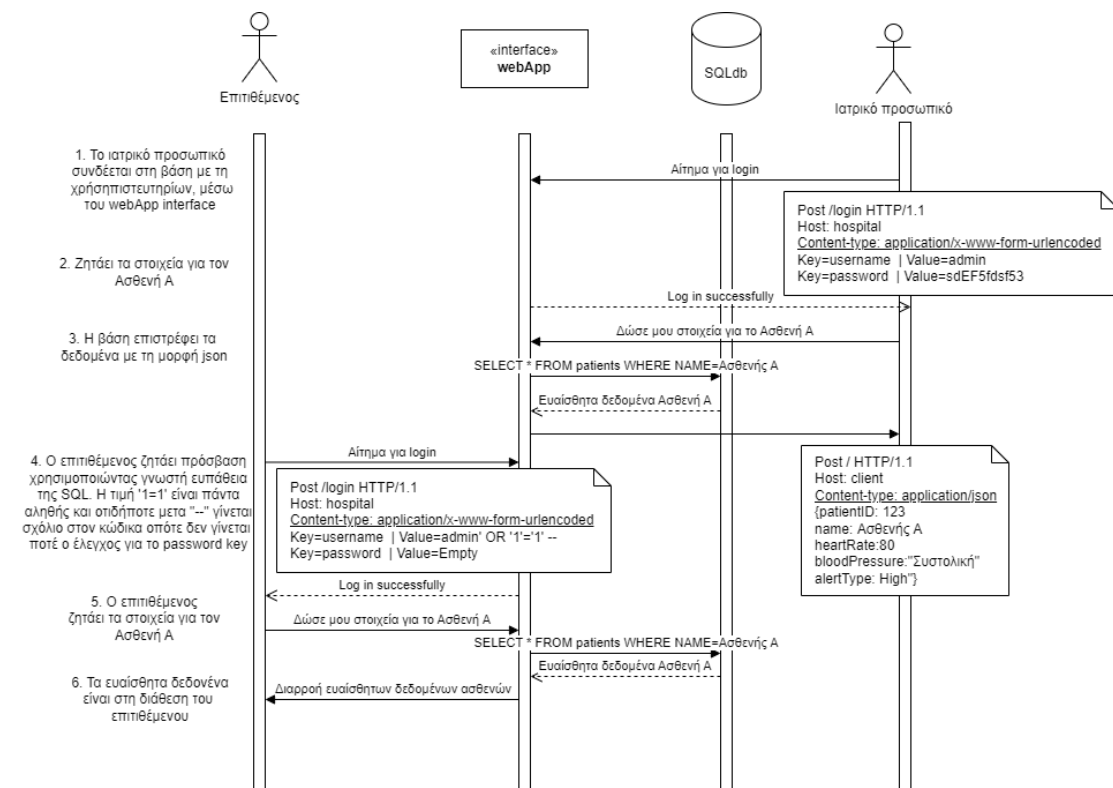


Figure 7 SQL injection στη κεντρική βάση του συστήματος της έξυπνης κλινικής

### Περίπτωση 3 (DDoS)

Στο παρακάτω σχεδιάγραμμα αλληλουχίας φαίνεται μία επίθεση άρνησης υπηρεσιών στο σύστημα της έξυπνης κλινικής. Πρόκειται για μία επίθεση πλημμύρας SYN, όπου κάποιος κακόβουλος στέλνει μια γρήγορη διαδοχή πακέτων SYN, συχνά από πλαστές διευθύνσεις IP (spoofed). Ο εξυπηρετητής επεξεργάζεται κάθε αίτημα, εκχωρεί πόρους στη σύνδεση και στέλνει ένα SYN-ACK πίσω στην πηγαία IP. Ωστόσο, το τελικό ACK από τον πελάτη (επιτιθέμενο) δεν φτάνει ποτέ, αφήνοντας τις συνδέσεις μισάνοιχτες και τελικά εξαντλώντας τους πόρους του διακομιστή. Η εξάντληση των πόρων, καθιστά το δίκτυο αναξιόπιστο και πολλές φορές μη διαθέσιμο. Τα νέα μηνύματα με τα δεδομένα από τους αισθητήρες είναι αδύνατο πια να αξιοποιηθούν, με αποτελέσματα να υποβαθμίζονται οι υπηρεσίες της κλινικής.

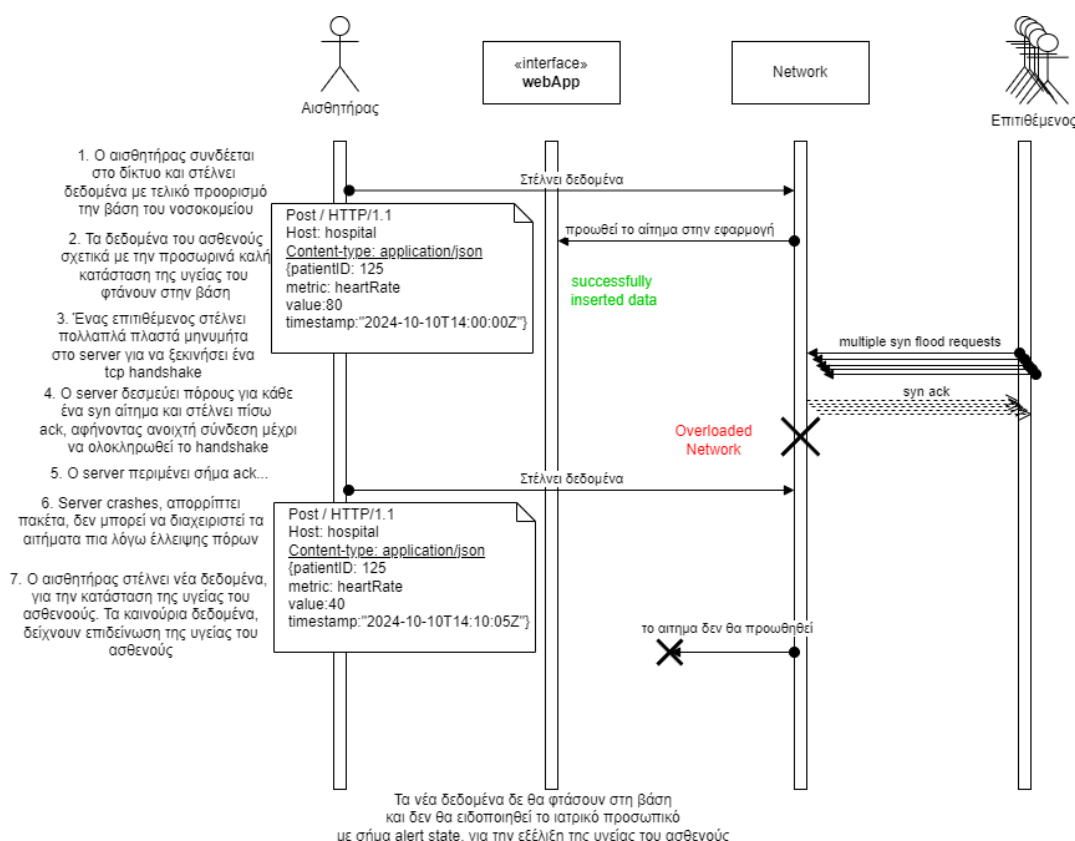


Figure 8 Επίθεση άρνησης υπηρεσιών στο σύστημα της έξυπνης κλινικής

#### 5.1.5 Εκμείωση απαιτήσεων

Οι παραπάνω περιπτώσεις του σεναρίου της έξυπνης κλινικής αναδεικνύουν απαιτήσεις που οφείλει να έχει το σύστημα προκειμένου να είναι λειτουργικό και αποδοτικό:

**Ασφάλεια δεδομένων και Ιδιωτικότητα:** Οι ασθενείς περιμένουν ότι τα ιατρικά τους δεδομένα θα προστατεύονται από αδικαιολόγητη πρόσβαση και χρήση από τρίτους. Η πρόσβαση από τρίτους σε ιδιαίτερα ευαίσθητες πληροφορίες, όπως το ιατρικό ιστορικό, οι διαγνώσεις, οι θεραπείες και άλλες προσωπικές πληροφορίες που συνδέονται με την υγεία και την ευημερία

τους, μπορεί να ελλοχεύει σοβαρούς κινδύνους. Αρχικά, τα ιατρικά δεδομένα είναι εξαιρετικά προσωπικά και ευαίσθητα, και η αποκάλυψή τους μπορεί να προκαλέσει δυσφορία ή ντροπή στους ασθενείς. Η έκθεση αυτών των πληροφοριών σε άτομα που δεν έχουν την εξουσιοδότηση να τα γνωρίζουν μπορεί να επηρεάσει ψυχολογικά τον ασθενή και να μειώσει την εμπιστοσύνη του προς το σύστημα υγείας (παραβίαση της ιδιωτικότητας). Επιπλέον, ορισμένες ασθένειες ή παθήσεις ενδέχεται να φέρουν κοινωνικό ή επαγγελματικό στιγματισμό, ιδιαίτερα αν πρόκειται για χρόνιες, ψυχιατρικές ή μεταδοτικές παθήσεις. Η διαρροή αυτών των δεδομένων μπορεί να οδηγήσει σε διακρίσεις από τον κοινωνικό περίγυρο ή στον χώρο εργασίας, δημιουργώντας πρόσθετα προβλήματα στον ασθενή και στην ποιότητα της κοινωνικής του ζωής. Ακόμη, τα ιατρικά δεδομένα μπορούν να χρησιμοποιηθούν από επιτήδειους για τη δημιουργία πλαστών ασφαλιστικών ή χρηματοπιστωτικών εγγράφων. Για παράδειγμα, άτομα που αποκτούν πρόσβαση σε δεδομένα ασθενών μπορούν να υποβάλουν ψευδείς ασφαλιστικές αξιώσεις, εκμεταλλευόμενοι την ασφάλιση του ασθενούς για δικές τους ιατρικές δαπάνες. Επιπρόσθετα, οι προσωπικές πληροφορίες που συνοδεύουν τα ιατρικά δεδομένα, όπως το ονοματεπώνυμο, η ημερομηνία γέννησης, η διεύθυνση και άλλες ταυτοποιητικές λεπτομέρειες, μπορούν να αξιοποιηθούν για κλοπή της ταυτότητας των ασθενών, που δύναται να χρησιμοποιηθεί ποικιλοτρόπως σε άλλες απάτες. Αυτό μπορεί να επιτρέψει σε τρίτους να αποκτήσουν πρόσβαση σε άλλα ευαίσθητα δεδομένα ή ακόμη και να διαπράξουν και οικονομικές απάτες στο όνομα του ασθενούς. Τέλος, εάν τρίτοι έχουν τη δυνατότητα να τροποποιούν ή να αλλοιώνουν ιατρικά δεδομένα, υπάρχει ο κίνδυνος να επηρεάσουν αρνητικά τις διαγνώσεις και τις θεραπείες. Λανθασμένα ή αλλοιωμένα δεδομένα μπορεί να οδηγήσουν σε εσφαλμένες ιατρικές αποφάσεις, με σοβαρές συνέπειες για την υγεία του ασθενούς.

**Αξιοπιστία:** Οι ασθενείς αναμένουν ότι η κλινική θα παρέχει ιατρική βοήθεια βασισμένη σε δεδομένα και ενέργειες που θα καλυτερεύσουν την υγεία τους. Όταν οι ασθενείς περιμένουν να λαμβάνουν βοήθεια βασισμένη σε ακριβή και ενημερωμένα δεδομένα, τυχόν σφάλματα ή παραλείψεις μπορούν να οδηγήσουν σε σοβαρά προβλήματα, επηρεάζοντας αρνητικά την αξιοπιστία της κλινικής. Πιο συγκεκριμένα, η αξιοπιστία της κλινικής εξαρτάται σε μεγάλο βαθμό από την ακρίβεια και την πληρότητα των ιατρικών δεδομένων. Σε περιπτώσεις όπου τα δεδομένα δεν είναι σωστά καταχωρημένα ή δεν ενημερώνονται τακτικά, οι γιατροί μπορεί να βασιστούν σε εσφαλμένες πληροφορίες. Αυτό μπορεί να οδηγήσει σε εσφαλμένες διαγνώσεις ή ακατάλληλες θεραπείες, κάτι που όχι μόνο βλάπτει την υγεία των ασθενών αλλά επίσης δημιουργεί την αίσθηση αναξιοπιστίας. Επίσης, εάν τα συστήματα IIoT και οι ψηφιακές πλατφόρμες για τη διαχείριση δεδομένων που χρησιμοποιούνται παρουσιάζουν συχνά προβλήματα ή βλάβες, και για παράδειγμα δεν είναι δυνατή η άμεση πρόσβαση σε πληροφορίες ασθενών ή η ακριβής παρακολούθηση της κατάστασής τους, αυτές οι καθυστερήσεις ή τα σφάλματα στα συστήματα μπορούν να δημιουργήσουν την αίσθηση ότι η κλινική δεν είναι οργανωμένη και δεν παρέχει ασφαλείς και γρήγορες υπηρεσίες. Συνεπώς οι τεχνικές βλάβες και οι δυσλειτουργίες του συστήματος από μία επίθεση άρνησης υπηρεσιών,



μπορούν να μειώσουν την αξιοπιστία της κλινικής. Επιπρόσθετα, η διαρροή ευαίσθητων ιατρικών πληροφοριών ή η μη ασφαλής διαχείριση δεδομένων μπορεί να κλονίσει την εμπιστοσύνη των ασθενών. Όταν οι ασθενείς αντιλαμβάνονται ότι τα δεδομένα τους δεν είναι ασφαλή, αμφισβητούν τη συνολική αξιοπιστία της κλινικής και είναι λιγότερο πιθανό να τη θεωρήσουν ως έμπιστο πάροχο φροντίδας.

Διαθεσιμότητα: Οι ασθενείς αναμένουν ότι η κλινική θα παρέχει ιατρική επίβλεψη συνέχεια και αδιάλειπτα για όλο το στάδιο παραμονής τους. Σε περιπτώσεις επιδείνωσης της υγείας, όπως οξεία επεισόδια, αλλεργικές αντιδράσεις ή επιπλοκές μετά από χειρουργική επέμβαση, η γρήγορη ανταπόκριση είναι ζωτικής σημασίας για τη διαφύλαξη της ζωής του ασθενούς. Η καθυστέρηση μπορεί να οδηγήσει σε σοβαρές επιπλοκές ή ακόμα και σε κίνδυνο για τη ζωή του ασθενούς, γεγονός που καθιστά την αδιάλειπτη διαθεσιμότητα απαραίτητη. Επομένως, η άμεση αντιμετώπιση των επειγόντων περιστατικών και η έγκαιρη ειδοποίηση του ιατρικού προσωπικού για την εξέλιξη της υγείας των ασθενών είναι απαραίτητη. Μηνύματα και ειδοποιήσεις από τα συστήματα IIoT που δεν φτάνουν ποτέ στο ιατρικό προσωπικό μπορεί να αποδειχθούν εξαιρετικής σημασίας. Μάλιστα, οι ασθενείς που νοσηλεύονται συχνά βρίσκονται υπό παρακολούθηση για να εντοπιστούν τυχόν μικρές αλλαγές στην κατάσταση τους που θα μπορούσαν να υποδείξουν προβλήματα υγείας. Η συνεχής παρακολούθηση επιτρέπει την πρόληψη σοβαρότερων προβλημάτων και την έγκαιρη παρέμβαση, κάτι που μπορεί να μειώσει τη διάρκεια και το κόστος της νοσηλείας. Τεχνικές βλάβες, αναπροσαρμογές και καθυστερήσεις στην συντήρηση και τη διάθεση του εξοπλισμού, αλλά και κυβερνοεπιθέσεις μπορούν να μειώσουν τη διαθεσιμότητα της κλινικής και χρήζουν ιδιαίτερης προσοχής.

Διαχείριση επιθέσεων: Το ιατρικό προσωπικό και οι ασθενείς απαιτούν την έγκαιρη αντίδραση του συστήματος για κάθε απειλή που αφορά την υπονόμευση των εργαλείων και μέσων της κλινικής. Σε περίπτωση που μια επίθεση επηρεάσει κρίσιμα εργαλεία και συστήματα, υπάρχει κίνδυνος να τεθεί σε κίνδυνο η ασφάλεια των ασθενών. Για παράδειγμα, αν παραβιαστούν τα συστήματα που παρακολουθούν ζωτικά σημεία ή ρυθμίζουν τη δοσολογία φαρμάκων, οι ασθενείς μπορεί να λάβουν εσφαλμένη θεραπεία ή να μην εντοπιστεί έγκαιρα κάποια επιδείνωση της κατάστασής τους. Η άμεση αντίδραση σε τέτοιες απειλές είναι απαραίτητη για να διασφαλιστεί ότι η φροντίδα παρέχεται σωστά και χωρίς παρεμβάσεις. Επίσης, όπως ήδη έχει ειπωθεί, τα συστήματα της κλινικής περιέχουν ευαίσθητες πληροφορίες για την υγεία των ασθενών. Μια επίθεση που στοχεύει αυτά τα δεδομένα μπορεί να οδηγήσει σε διαρροή προσωπικών και ιατρικών πληροφοριών. Αυτό όχι μόνο βλάπτει τους ασθενείς, αλλά επηρεάζει και τη φήμη της κλινικής και την εμπιστοσύνη του κοινού σε αυτή. Η άμεση αντίδραση σε μια απειλή αποτρέπει πιθανές παραβιάσεις δεδομένων και προστατεύει τα προσωπικά στοιχεία των ασθενών. Ακόμη, η έγκαιρη ανίχνευση και αντίδραση μπορεί να αποτρέψει διακοπές στη λειτουργία της κλινικής, διασφαλίζοντας τη συνεχή λειτουργία των εργαλείων και την αδιάλειπτη παροχή φροντίδας στους ασθενείς. Επίσης, το ιατρικό προσωπικό πρέπει να είναι σίγουρο ότι τα συστήματα και τα εργαλεία που χρησιμοποιεί είναι ασφαλή και λειτουργικά. Αν δεν υπάρχει αξιόπιστη διαχείριση επιθέσεων και συνεχείς ενημερώσεις, το προσωπικό μπορεί να αρχίσει

να αμφιβάλλει για την ασφάλεια των εργαλείων που χρησιμοποιεί, κάτι που θα μπορούσε να επηρεάσει την αποτελεσματικότητά του. Οι εργαζόμενοι πρέπει να αισθάνονται ότι η τεχνολογία που έχουν στη διάθεσή τους υποστηρίζεται και προστατεύεται από αποτελεσματικά μέτρα ασφαλείας. Συνολικά, οι κυβερνοεπιθέσεις μπορούν να επιφέρουν σημαντικό οικονομικό κόστος σε μια κλινική. Η διακοπή λειτουργίας, η ανάγκη για αποκατάσταση συστημάτων και η αποζημίωση ασθενών ή συνεργατών είναι μόνο μερικές από τις δαπάνες που μπορεί να προκύψουν. Η άμεση διαχείριση των επιθέσεων μειώνει τον κίνδυνο και την έκταση της ζημιάς, διατηρώντας τα οικονομικά της κλινικής σταθερά.

Συμμόρφωση με την νομοθεσία: Συμμόρφωση με όλες τις εφαρμοζόμενες νομοθεσίες και κανονισμούς για την προστασία δεδομένων και ιδιωτικότητας. Οι ασθενείς έχουν δικαίωμα να γνωρίζουν πώς διαχειρίζονται και προστατεύονται τα προσωπικά τους δεδομένα. Η συμμόρφωση με τη νομοθεσία εξασφαλίζει ότι τα δικαιώματα των ασθενών, όπως η πρόσβαση στα δεδομένα τους, η διόρθωση και η διαγραφή τους, διατηρούνται και εφαρμόζονται με διαφάνεια. Όταν οι ασθενείς γνωρίζουν ότι η κλινική συμμορφώνεται με τα νομικά πρότυπα προστασίας δεδομένων, αισθάνονται πιο ασφαλείς και εμπιστεύονται το σύστημα υγείας. Η συμμόρφωση ενισχύει την εικόνα της κλινικής ως υπεύθυνου και αξιόπιστου παρόχου φροντίδας, γεγονός που βελτιώνει τη σχέση μεταξύ ασθενούς και κλινικής. Η μη συμμόρφωση με τους κανονισμούς μπορεί να οδηγήσει σε αυστηρές κυρώσεις, όπως υψηλά πρόστιμα και νομικές επιπτώσεις. Οι κανονισμοί προστασίας δεδομένων, όπως ο GDPR, επιβάλλουν σημαντικές ποινές σε περιπτώσεις παραβίασης. Η συμμόρφωση βοηθά την κλινική να αποφύγει τέτοιες κυρώσεις, διασφαλίζοντας ταυτόχρονα την καλή οικονομική της κατάσταση. Τέλος, η συμμόρφωση με τους νόμους προστασίας δεδομένων συμβάλλει στη διατήρηση της θετικής φήμης της κλινικής. Οι παραβιάσεις δεδομένων ή η μη συμμόρφωση μπορεί να οδηγήσουν σε αρνητική δημοσιότητα, η οποία θα μπορούσε να αποτρέψει ασθενείς και συνεργάτες από το να εμπιστευθούν την κλινική.

### **5.2.6 Αντιμετώπιση απαιτήσεων**

Οι παραπάνω απαιτήσεις αναδεικνύουν την ανάγκη για περισσότερη ασφάλεια πάνω στο σύστημα της έξυπνης κλινικής. Προκειμένου να λειτουργήσει σωστά το σύστημα και οι ασθενείς να είναι ικανοποιημένοι από την εξυπηρέτηση και τις παροχές της κλινικής θα πρέπει να θεωρακιστεί, ώστε να είναι ασφαλές και να εξάγεται ομαλά η λειτουργία του.

## **5.2 Υποθετικό σενάριο διαχείρισης δεδομένων σε ένα περιβάλλον IIoT**

Όπως έχει ήδη αναλυθεί σε προηγούμενο κεφάλαιο, οι τεχνολογίες του IIoT περιλαμβάνουν την αποθήκευση, διακίνηση και επεξεργασία ευαίσθητων δεδομένων προκειμένου να βελτιστοποιήσουν το κύκλο παραγωγής της επιχείρησης. Αυτό μπορεί να δημιουργήσει αρκετά κενά ασφαλείας που θα πρέπει να ληφθούν υπόψη. Για τη καλύτερη κατανόηση των κενών ασφαλείας που μπορεί να δημιουργηθούν αναλύεται το παρακάτω υποθετικό σενάριο που αφορά το κύκλο παραγωγής μιας επιχείρησης.

### 5.2.1 Περιγραφή σεναρίου

Έστω ότι υπάρχει κάποιο έξυπνο εργοστάσιο που χρησιμοποιεί IIoT συσκευές για να συλλέγει σε πραγματικό χρόνο δεδομένα, σχετικά με την επίδοση των μηχανών, τις περιβαλλοντικές συνθήκες και τη δραστηριότητα του ανθρώπινου δυναμικού κατά τα στάδια του κύκλου παραγωγής. Είναι εμφανές ότι υπάρχουν ευπάθειες όπως η μη εξουσιοδοτημένη πρόσβαση στη συλλογή των ευαίσθητων δεδομένων. Ο αντίκτυπος μίας τέτοιας ευπάθειας μπορεί να έχει οικονομικές αλλά και νομικές επιπτώσεις. Για παράδειγμα, η πρόσβαση σε δεδομένα που αφορούν την κατασκευή ενός καινοτόμου προϊόντος μπορεί να έχει οικονομικό αντίκτυπο στην επιχείρηση από ανταγωνιστές. Επιπρόσθετα, τα προσωπικά στοιχεία του ανθρώπινου δυναμικού δεν θα πρέπει να κοινοποιούνται σε τρίτους χωρίς την συγκατάθεση τους σύμφωνα με τους κανόνες του GDPR. Ακόμα, οι περισσότερες συσκευές μεταφέρουν τις πληροφορίες ασύρματα στο χώρο του εργοστασίου. Σε περίπτωση που υπάρχει έλλειψη κρυπτογραφίας και αδύναμα πρωτόκολλα ταυτοποίησης, ελλοχεύει ο κίνδυνος υποκλοπής των δεδομένων κατά τη μετάδοση τους. Σε πολλές περιπτώσεις, οι επιχειρήσεις και οι οργανισμοί προκειμένου να εξοικονομήσουν χρόνο και πόρους που δαπανούνται από τα συστήματα ασφαλείας των δεδομένων, τα παραλείπουν. Τα δεδομένα έπειτα συγκεντρώνονται και υποβάλλονται για επεξεργασία σε κάποιο «σύννεφο» (cloud). Οι ανησυχίες για την ασφάλεια εδώ περιλαμβάνουν παραβιάσεις δεδομένων στο σύννεφο, ανεπαρκή στοιχεία ελέγχου πρόσβασης και ευπάθειες στις διεπαφές του. Ο έλεγχος και η παρακολούθηση της παραγωγής γίνεται εξ αποστάσεως από μηχανικούς που είναι εξουσιοδοτημένοι να δίνουν εντολές σε διάφορα σημεία πρόσβασης. Και εδώ τίθενται θέματα ασφαλείας σχετικά με την ασφάλεια των απομακρυσμένων σημείων πρόσβασης, την προστασία από κακόβουλα λογισμικά και την κρυπτογράφηση των εντολών. Το εργοστάσιο συνεργάζεται με εξωτερικούς προμηθευτές για τη διαχείριση των αποθεμάτων σε πραγματικό χρόνο. Οποιαδήποτε παρόμοια συνεργασία με τρίτους φορείς βάζει σε κίνδυνο την επιχείρηση δεδομένου ότι τα τρωτά σημεία των συνεργατών του μετατρέπονται σε τρωτά σημεία του οικοσυστήματος που δημιουργεί η συνεργασία τους. Τα δεδομένα αφού συλλεχθούν επεξεργάζονται και αναλύονται με τη βοήθεια διάφορων αλγορίθμων. Συνεπώς, η επιχείρηση θα πρέπει να έχει εξασφαλίσει ότι η επεξεργασία τους δεν εκθέτει ακούσια δεδομένα σε τρίτους. Το σύστημα παρακολούθησης των εργαζομένων διαθέτει έξυπνες φορητές συσκευές όπως έξυπνα ρολόγια που παρακολουθούν την υγεία και την παραγωγικότητα των εργαζομένων. Έτσι, αν κάποιος εργαζόμενος νιώσει κάποια αδιαθεσία, ή έχει αυξημένο σφυγμό λόγω πίεσης, το σύστημα είναι ικανό να βρει γρήγορα αντικαταστάτη να συνεχίσει την εργασία στο πόστο, προκειμένου ο εργαζόμενος να ξεκουραστεί για όσο χρειαστεί. Βέβαια αυτό, εγείρει ανησυχίες σχετικά με το απόρρητο των εργαζομένων, τη συγκατάθεση ιατρικών δεδομένων και την ηθική χρήση των προσωπικών τους δεδομένων.

### 5.2.2 Οντότητες σεναρίου

Ο προσδιορισμός των οντοτήτων είναι το πρώτο και βασικό βήμα για την ανάπτυξη μιας μοντελοποίησης που επιτρέπει την αποτελεσματική ανάλυση και κατανόηση ενός συστήματος. Για κάθε σύστημα και ιδιαίτερα περίπλοκα περιβάλλοντα όπως το βιομηχανικό Internet of Things (IIoT), όπου οι οντότητες μπορεί να είναι συσκευές, αισθητήρες, δεδομένα, και άνθρωποι, είναι κρίσιμος ο προσδιορισμός τους. Κάθε οντότητα αντιπροσωπεύει κάτι πραγματικό ή αφηρημένο που πρέπει να παρακολουθηθεί, να αναλυθεί ή να διαχειριστεί. Μπορεί να είναι οτιδήποτε σχετικό με το σύστημα, όπως φυσικά αντικείμενα (π.χ. μηχανήματα, εργαζόμενοι), αφηρημένες έννοιες (π.χ. παραγγελίες, συμβάσεις), ή ακόμα και διαδικασίες (π.χ. παραγωγή, διανομή). Με άλλα λόγια, οι οντότητες αποτελούν τα θεμέλια της κατανόησης του συστήματος και αν δεν προσδιοριστούν με ακρίβεια, δεν δύναται να κατανοηθούν οι σχέσεις, οι αλληλεπιδράσεις ή τα δεδομένα που σχετίζονται με αυτές. Στο παραπάνω σενάριο μπορούν να προσδιοριστούν οι παρακάτω οντότητες:

**IIoT Συσκευές:** Αυτές οι συσκευές περιλαμβάνουν αισθητήρες, έξυπνα ρολόγια και άλλες φορητές ή σταθερές συσκευές που παρακολουθούν και καταγράφουν δεδομένα σε πραγματικό χρόνο. Για παράδειγμα, αισθητήρες τοποθετημένοι σε μηχανές μπορούν να καταγράφουν τη θερμοκρασία, την ταχύτητα λειτουργίας ή τα επίπεδα κατανάλωσης ενέργειας. Οι φορητές συσκευές των εργαζομένων, όπως έξυπνα ρολόγια, μπορούν να παρακολουθούν τον καρδιακό ρυθμό και τη φυσική κατάσταση των εργαζομένων.

**Ανθρώπινο δυναμικό:** Το προσωπικό της επιχείρησης που εμπλέκεται σε κάθε στάδιο της παραγωγής, όπως οι εργαζόμενοι στη γραμμή παραγωγής, οι υπεύθυνοι συντήρησης και οι διευθυντές παραγωγής. Οι εργαζόμενοι παρακολουθούνται μέσω συσκευών IIoT που καταγράφουν τόσο την αποδοτικότητα τους (π.χ., πόσες μονάδες προϊόντος παράγουν ανά ώρα) όσο και τη φυσική τους κατάσταση. Παράδειγμα: Ένας εργαζόμενος με έξυπνο ρολόι μπορεί να έχει αυξημένο καρδιακό ρυθμό λόγω άγχους ή φυσικής κόπωσης, και το σύστημα μπορεί να ειδοποιήσει τον προϊστάμενό του για να εξεταστεί η κατάσταση.

**Μηχανές Παραγωγής:** Αφορά όλα τα μηχανήματα που εκτελούν τις κρίσιμες διαδικασίες στην παραγωγή του εργοστασίου. Οι IIoT συσκευές συνδέονται με τις μηχανές για να συλλέγουν δεδομένα όπως θερμοκρασία, πίεση, ταχύτητα περιστροφής, κ.λπ. Παράδειγμα: Μία μηχανή που παρακολουθείται μπορεί να έχει αυξημένη θερμοκρασία, και το σύστημα μπορεί να εντοπίσει πιθανή αστοχία ή υπερφόρτωση. Ορισμένες μηχανές παραγωγής μπορεί να χειρίζονται από εργαζομένους.

**Δίκτυο επικοινωνίας:** Ασύρματα ή ενσύρματα δίκτυα που χρησιμοποιούνται για τη μεταφορά δεδομένων από τις συσκευές IIoT στις κεντρικές υποδομές του εργοστασίου. Εάν το δίκτυο δεν είναι επαρκώς ασφαλές, υπάρχει κίνδυνος υποκλοπής δεδομένων. Παράδειγμα: Εάν οι αισθητήρες σε μια μηχανή μεταδίδουν δεδομένα χωρίς κρυπτογράφηση, τότε αυτά τα δεδομένα

θα μπορούσαν να υποκλαπούν από εξωτερικούς επιτιθέμενους. Η περιγραφή αυτής της οντότητας είναι κρίσιμη για να σχεδιαστούν σωστές στρατηγικές ασφαλής επικοινωνίας.

**Υποδομή για το Σύννεφο:** Τα δεδομένα που συλλέγονται από τις συσκευές αποθηκεύονται και επεξεργάζονται στο cloud. Αυτό επιτρέπει την απομακρυσμένη πρόσβαση από τους διαχειριστές και τη χρήση προηγμένων αλγορίθμων για ανάλυση. Παράδειγμα: Τα δεδομένα από τους αισθητήρες που παρακολουθούν τις μηχανές ανεβαίνουν στο cloud για ανάλυση από αλγόριθμους μηχανικής μάθησης, που προσδιορίζουν πότε μια μηχανή πλησιάζει το τέλος της ζωής της και χρειάζεται συντήρηση.

**Εξωτερικοί Προμηθευτές/Συνεργάτες:** Πρόκειται για τους εξωτερικούς συνεργάτες που διαχειρίζονται αποθέματα ή προμήθειες και οι οποίοι έχουν πρόσβαση στα δεδομένα του εργοστασίου. Οι τρωτότητες στα συστήματα των προμηθευτών μπορεί να επηρεάσουν το ίδιο το εργοστάσιο. Παράδειγμα: Ένας προμηθευτής ανταλλακτικών μπορεί να έχει πρόσβαση στα δεδομένα των μηχανών για να παρακολουθεί τη χρήση των ανταλλακτικών και να προβλέψει πότε θα χρειαστούν νέα αποθέματα. Αν το σύστημα του προμηθευτή είναι ανασφαλές, τα δεδομένα του εργοστασίου κινδυνεύουν.

**Εξουσιοδοτημένοι Μηχανικοί:** Είναι μέρος του ανθρώπινου δυναμικού, όμως διαθέτει ιδιαίτερες γνώσεις και έχει κομβικό ρόλο στη διαχείριση των δεδομένων για αυτό και μελετάται σαν ξεχωριστή οντότητα. Οι μηχανικοί είναι υπεύθυνοι για τον έλεγχο της παραγωγής από απομακρυσμένα σημεία, δίνοντας εντολές στα συστήματα μέσω διαδικτύου. Αυτοί οι μηχανικοί είναι αρμόδιοι για τη συντήρηση και τη λειτουργία του εργοστασίου. Παράδειγμα: Ένας μηχανικός από το σπίτι μπορεί να συνδεθεί στο σύστημα του εργοστασίου για να προσαρμόσει τη λειτουργία μιας μηχανής. Ωστόσο, η απομακρυσμένη πρόσβαση δημιουργεί κινδύνους για μη εξουσιοδοτημένη πρόσβαση ή κακόβουλες επιθέσεις, αν δεν είναι καλά προστατευμένη.

**Αλγόριθμοι Επεξεργασίας:** Προηγμένοι αλγόριθμοι που αναλύουν τα δεδομένα που συλλέγονται για τη βελτιστοποίηση της παραγωγικής διαδικασίας. Αυτοί μπορεί να περιλαμβάνουν αλγόριθμους μηχανικής μάθησης που κάνουν προβλέψεις για τη συντήρηση μηχανών ή την αποδοτικότητα των εργαζομένων. Παράδειγμα: Ένας αλγόριθμος μπορεί να αναλύσει δεδομένα από τις μηχανές και να εντοπίσει μοτίβα που υποδεικνύουν μελλοντικές βλάβες, προτείνοντας προληπτική συντήρηση πριν το σύστημα υποστεί σοβαρές ζημιές.

### 5.2.3 Δυναμικές σχέσεις μεταξύ οντοτήτων

Οι σχέσεις των οντοτήτων μεταξύ τους προσδιορίζουν τον τρόπο με τον οποίο αυτές αλληλοεπιδρούν και επηρεάζουν η μία την άλλη μέσα στο σύστημα. Οι δυναμικές σχέσεις αφορούν όχι μόνο στατικές αλληλεπιδράσεις αλλά και αλλαγές που μπορούν να συμβούν με την πάροδο του χρόνου ή λόγω συγκεκριμένων συνθηκών. Σε πολύπλοκα, διασυνδεδεμένα περιβάλλοντα, όπου η συνεργασία των οντοτήτων είναι το κλειδί για την επιτυχία, η κατανόηση των σχέσεων τους είναι απαραίτητη για να βελτιστοποιηθούν διαδικασίες και να γίνει έγκαιρη

προσαρμογή σε μεταβαλλόμενες συνθήκες. Αρχικά, οι οντότητες δεν λειτουργούν απομονωμένα, αλλά αλληλοεπιδρούν μεταξύ τους συνεχώς. Η δυναμική των σχέσεων καθορίζει πώς οι αλλαγές σε μία οντότητα επηρεάζουν τις άλλες. Αυτό είναι σημαντικό για τη διαχείριση πολύπλοκων συστημάτων, όπως ένα IIoT περιβάλλον, όπου οι μεταβολές σε δεδομένα ή σε συμπεριφορές συσκευών μπορούν να έχουν ευρείες επιπτώσεις. Σε συστήματα όπου κυκλοφορούν πληροφορίες ή δεδομένα, όπως ένα βιομηχανικό δίκτυο IIoT, οι σχέσεις μεταξύ οντοτήτων καθορίζουν πώς τα δεδομένα κινούνται μέσα στο σύστημα. Χωρίς αυτές τις σχέσεις, δεν είναι δυνατή η κατανόηση του τρόπου με τον οποίο οι πληροφορίες επεξεργάζονται, μεταφέρονται ή αλλάζουν μορφή. Επιπρόσθετα, ο προσδιορισμός των δυναμικών σχέσεων βοηθάει στη δημιουργία μοντέλων προσομοίωσης προκειμένου να προβλεφθεί πώς το σύστημα θα αντιδράσει σε διάφορες συνθήκες. Εφόσον είναι γνωστό πώς οι οντότητες επηρεάζουν η μία την άλλη με την πάροδο του χρόνου, οι μελλοντικές καταστάσεις του συστήματος μπορούν να προβλεφθούν με μεγαλύτερη ακρίβεια. Παρακάτω περιγράφονται οι δυναμικές σχέσεις μεταξύ των οντοτήτων του σεναρίου:

**IIoT Συσκευές & Ανθρώπινο Δυναμικό:** Στο πλαίσιο της αλληλεπίδρασης μεταξύ IIoT συσκευών και ανθρώπινου δυναμικού, οι συσκευές αυτές λειτουργούν ως εργαλεία παρακολούθησης που συλλέγουν δεδομένα σχετικά με την υγεία και την απόδοση των εργαζομένων. Καταγράφουν μεταβλητές όπως τον καρδιακό ρυθμό και την κίνηση, χρησιμοποιώντας αισθητήρες και έξυπνες συσκευές τοποθετημένες σαν αξεσουάρ στο σώμα, ενώ παρακολουθούν επίσης την παραγωγικότητα μέσω ειδικών εφαρμογών. Τα δεδομένα αναλύονται για να εντοπιστούν ανωμαλίες ή τάσεις, όπως η υπερκόπωση, συγκρίνοντας τα με προκαθορισμένα ή ιστορικά επίπεδα.

Όταν ανιχνεύονται προβληματικά στοιχεία, το σύστημα ειδοποιεί τους διευθυντές για την ανάγκη παρέμβασης, είτε με τη μορφή αντικατάστασης του εργαζομένου ή παροχής διαλείμματος είτε με αλλαγή των εργασιακών συνθηκών. Αυτή η τεχνολογική ενσωμάτωση βελτιώνει τις συνθήκες εργασίας και ενισχύει την αποδοτικότητα, αλλά φέρει μαζί της και σημαντικές προκλήσεις. Τα ζητήματα απορρήτου και η διαχείριση των προσωπικών δεδομένων απαιτούν προσεκτικό χειρισμό, ενώ η ακρίβεια των δεδομένων και οι ψυχολογικές επιπτώσεις της συνεχούς παρακολούθησης απαιτούν συνεχή επαγρύπνηση.

**IIoT Συσκευές & Μηχανές Παραγωγής:** Σε ένα βιομηχανικό σύστημα Internet of Things (IIoT), οι συσκευές IIoT και οι μηχανές παραγωγής συνεργάζονται στενά για τη βελτίωση της λειτουργίας και της συντήρησης των μηχανών. Συσκευές IIoT είναι ενσωματωμένες στις μηχανές παραγωγής με στόχο την παρακολούθηση και την καταγραφή κρίσιμων δεδομένων που αφορούν την απόδοση και την κατάσταση των μηχανών. Τέτοιες συσκευές συλλέγουν δεδομένα όπως η θερμοκρασία, οι κραδασμοί και η κατανάλωση ενέργειας των μηχανών. Κάθε μία από αυτές τις παραμέτρους παρέχει σημαντικές πληροφορίες για την υγεία της μηχανής. Για παράδειγμα, η θερμοκρασία μπορεί να δείξει αν μια μηχανή λειτουργεί σε φυσιολογικά επίπεδα ή αν υπάρχει υπερθέρμανση. Οι κραδασμοί είναι ενδείξεις πιθανών μηχανικών

προβλημάτων ή ανισορροπιών, ενώ η κατανάλωση ενέργειας μπορεί να αποκαλύψει αν η μηχανή λειτουργεί αποδοτικά ή αν υπάρχουν προβλήματα που επηρεάζουν την αποδοτικότητα της. Σε περίπτωση που μια μηχανή παρουσιάσει σημάδια υπερθέρμανσης, οι συσκευές IIoT ανιχνεύουν την αύξηση της θερμοκρασίας και ενεργοποιούν ένα σύστημα ειδοποίησης. Το σύστημα αυτό αποστέλλει άμεσες ειδοποιήσεις στους τεχνικούς συντήρησης, προειδοποιώντας τους για την ανάγκη προληπτικής συντήρησης. Αυτή η διαδικασία προλαμβάνει την εμφάνιση σοβαρών βλαβών που θα μπορούσαν να οδηγήσουν σε διακοπές παραγωγής ή σε βλάβες που απαιτούν δαπανηρές επισκευές, ενώ ταυτόχρονα ειδοποιεί έγκαιρα για τον κατάλληλο προγραμματισμό των συντηρήσεων των μηχανών.

Η συνεχής παρακολούθηση των δεδομένων που καταγράφονται από τις συσκευές IIoT επιτρέπει την ανάλυση τάσεων και την πρόβλεψη πιθανών προβλημάτων πριν γίνουν κρίσιμα. Με τη χρήση δεδομένων από τους αισθητήρες, το σύστημα μπορεί να ανιχνεύσει ανωμαλίες και να εφαρμόσει στρατηγικές συντήρησης βάσει της πραγματικής κατάστασης της μηχανής. Αυτό εξασφαλίζει την αποτελεσματική λειτουργία του εξοπλισμού, μειώνει τον χρόνο διακοπής της παραγωγής και βελτιώνει τη συνολική αποδοτικότητα του βιομηχανικού συστήματος.

**IIoT Συσκευές & Δίκτυο Επικοινωνίας:** Στα βιομηχανικά περιβάλλοντα του Internet of Things (IIoT), οι συσκευές IoT παίζουν καθοριστικό ρόλο στην παρακολούθηση και τη συλλογή δεδομένων από τις διάφορες μηχανές, το ανθρώπινο δυναμικό και τις διαδικασίες παραγωγής. Ωστόσο, η συλλογή αυτών των πληροφοριών είναι μόνο το πρώτο βήμα. Οι πληροφορίες που καταγράφονται από τις συσκευές IoT πρέπει να μεταδοθούν μέσω ενός δικτύου επικοινωνίας σε κεντρικά συστήματα αποθήκευσης και ανάλυσης, προκειμένου να αξιοποιηθούν για τη λήψη αποφάσεων, τη βελτιστοποίηση της παραγωγής και τη συντήρηση του εξοπλισμού. Το δίκτυο επικοινωνίας αναλαμβάνει να συνδέσει τις συσκευές IoT με τους εξυπηρετητές, τις βάσεις δεδομένων ή τα συστήματα cloud, όπου τα δεδομένα αποθηκεύονται και αναλύονται. Ωστόσο, η μετάδοση αυτών των δεδομένων μέσω δικτύου θέτει σημαντικές προκλήσεις για την ασφάλεια. Εάν το δίκτυο δεν είναι επαρκώς ασφαλές, οι πληροφορίες που μεταφέρονται γίνονται ευάλωτες σε υποκλοπή ή κακόβουλη αλλοίωση από τρίτους. Μια βασική ανησυχία αφορά την προστασία των ευαίσθητων δεδομένων που συλλέγονται από τις συσκευές IIoT. Τα δεδομένα αυτά μπορεί να περιλαμβάνουν κρίσιμες πληροφορίες για τη λειτουργία της παραγωγικής διαδικασίας, όπως η απόδοση των μηχανών, οι ενεργειακές απαιτήσεις και οι συνθήκες λειτουργίας. Αν αυτές οι πληροφορίες διαρρεύσουν στα χέρια κακόβουλων παραγόντων, υπάρχει κίνδυνος να χρησιμοποιηθούν για σαμποτάζ και κλοπή βιομηχανικών μυστικών. Ταυτόχρονα, οι πληροφορίες που μεταδίδονται μπορεί να μεταφέρουν ευαίσθητα δεδομένα από το ανθρώπινο δυναμικό.

Επιπλέον, υπάρχει η πιθανότητα κακόβουλης αλλοίωσης των δεδομένων κατά τη διάρκεια της μετάδοσής τους. Αν κάποιος τρίτος καταφέρει να παρέμβει στη ροή των δεδομένων, θα μπορούσε να τροποποιήσει ή να παραποιήσει τις πληροφορίες, επηρεάζοντας έτσι την αξιοπιστία των αναλύσεων και των αποφάσεων που βασίζονται σε αυτά τα δεδομένα. Για

παράδειγμα, μια τέτοια αλλοίωση θα μπορούσε να οδηγήσει σε ψευδείς ειδοποιήσεις συντήρησης ή σε λανθασμένες ενέργειες που θα μπορούσαν να επηρεάσουν την παραγωγική διαδικασία. Γι' αυτόν τον λόγο, είναι ζωτικής σημασίας το δίκτυο επικοινωνίας που χρησιμοποιείται για τη μετάδοση των δεδομένων να είναι πλήρως ασφαλές. Αυτό μπορεί να επιτευχθεί μέσω της κρυπτογράφησης των δεδομένων κατά τη μετάδοση, της χρήσης ασφαλών πρωτοκόλλων επικοινωνίας και της συνεχούς παρακολούθησης για ανωμαλίες στη δικτυακή κίνηση. Η ασφαλής διαχείριση των δικτύων εξασφαλίζει ότι τα δεδομένα που συλλέγονται από τις συσκευές IIoT παραμένουν ακριβή, προστατευμένα και αξιόπιστα, επιτρέποντας την ασφαλή λειτουργία και τη βελτίωση της παραγωγικής διαδικασίας. Συνεπώς, η σχέση των συσκευών IIoT και του δικτύου επικοινωνίας είναι διαρκής και ύψιστης σημασίας για τη μοντελοποίηση του σεναρίου.

**Δίκτυο Επικοινωνίας & Υποδομή για το Σύννεφο:** Η δυναμική της σχέσης μεταξύ του δικτύου επικοινωνίας και της υποδομής για το σύννεφο (cloud) είναι κρίσιμη για την ασφαλή και αποτελεσματική λειτουργία της βιομηχανικής παραγωγής. Το δίκτυο επικοινωνίας λειτουργεί σαν "γέφυρα" που επιτρέπει τη μεταφορά δεδομένων από τις IIoT συσκευές προς την cloud υποδομή, όπου τα δεδομένα αποθηκεύονται και αναλύονται. Σε ένα τυπικό βιομηχανικό περιβάλλον, οι IIoT συσκευές συλλέγουν τεράστιες ποσότητες δεδομένων σε πραγματικό χρόνο, όπως δεδομένα για την παραγωγική απόδοση, την κατανάλωση ενέργειας, τις συνθήκες λειτουργίας των μηχανών, και άλλες κρίσιμες πληροφορίες. Αυτά τα δεδομένα μεταδίδονται μέσω του δικτύου επικοινωνίας στο cloud, όπου μπορούν να επεξεργαστούν για να εξαχθούν πολύτιμα συμπεράσματα, να παρακολουθηθεί η απόδοση της παραγωγής, και να προγραμματιστούν ενέργειες συντήρησης ή βελτιστοποίησης.

Ωστόσο, αυτή η διαδικασία μεταφοράς δεδομένων ενέχει σοβαρούς κινδύνους αν το δίκτυο επικοινωνίας δεν είναι σωστά ασφαλισμένο. Το δίκτυο επικοινωνίας πρέπει να προστατεύεται από εξωτερικές επιθέσεις, καθώς αποτελεί το μέσο μέσω του οποίου τα δεδομένα κινούνται από το φυσικό περιβάλλον της παραγωγής σε μια ψηφιακή υποδομή cloud, η οποία μπορεί να βρίσκεται σε απομακρυσμένη τοποθεσία. Αν το δίκτυο δεν είναι κρυπτογραφημένο, υπάρχει κίνδυνος ένας κακόβουλος επιτιθέμενος να υποκλέψει τα δεδομένα κατά τη διάρκεια της μετάδοσης. Επιπλέον, εκτός από την υποκλοπή, υπάρχει και ο κίνδυνος κακόβουλης αλλοίωσης των δεδομένων κατά τη μεταφορά τους. Οι ίδιες απειλές που ισχύουν για τη σχέση μεταξύ δικτύου επικοινωνίας και συσκευών IIoT, ισχύουν και σε αυτή την περίπτωση.

**Εξουσιοδοτημένοι Μηχανικοί & Υποδομή για το Σύννεφο:** Η σχέση μεταξύ της υποδομής για το Σύννεφο (cloud) και των εξουσιοδοτημένων μηχανικών που παρακολουθούν και διαχειρίζονται τις βιομηχανικές μηχανές εξ αποστάσεως είναι εξαιρετικά σημαντική για τη διασφάλιση της αποτελεσματικής λειτουργίας της παραγωγικής διαδικασίας. Οι μηχανικοί βασίζονται στην υποδομή cloud για να αποκτούν πρόσβαση σε πραγματικό χρόνο στα δεδομένα της παραγωγής, να παρακολουθούν τη λειτουργία των μηχανών και, σε πολλές περιπτώσεις, να προβαίνουν σε ρυθμίσεις ή τροποποιήσεις διασφαλίζοντας τη βέλτιστη



απόδοση των μηχανημάτων. Για παράδειγμα, ένας μηχανικός που εργάζεται εξ αποστάσεως μπορεί να χρειαστεί να συνδεθεί στο cloud από το σπίτι του, προκειμένου να αλλάξει τις ρυθμίσεις μιας μηχανής που δείχνει σημάδια ανώμαλης λειτουργίας ή υπολειτουργίας. Αυτό μπορεί να περιλαμβάνει την προσαρμογή της ταχύτητας, την αλλαγή των θερμοκρασιών λειτουργίας ή ακόμα και την επανεκκίνηση της μηχανής. Η δυνατότητα να πραγματοποιηθούν αυτές οι ενέργειες εξ αποστάσεως αποτελεί σημαντικό πλεονέκτημα για τη σύγχρονη βιομηχανική παραγωγή, επιτρέποντας την άμεση αντιμετώπιση προβλημάτων χωρίς να χρειάζεται φυσική παρουσία στον χώρο της παραγωγής.

Ωστόσο, αυτή η διαδικασία ενέχει και σημαντικούς κινδύνους αν δεν υπάρχει επαρκής προστασία στο σύστημα. Όταν οι μηχανικοί συνδέονται στην cloud υποδομή από απομακρυσμένα σημεία, υπάρχει ο κίνδυνος να γίνουν στόχος κακόβουλων λογισμικών ή επιθέσεων τύπου phishing που μπορούν να επηρεάσουν την ασφάλεια των δεδομένων και την ακεραιότητα των εντολών που αποστέλλονται στις μηχανές. Για παράδειγμα, αν ένας μηχανικός προσπαθήσει να αλλάξει τις ρυθμίσεις μιας μηχανής χωρίς να υπάρχει ασφαλής σύνδεση ή κατάλληλη κρυπτογράφηση, οι εντολές του θα μπορούσαν να παραποιηθούν από έναν επιτιθέμενο. Αυτή η παραποίηση μπορεί να έχει καταστροφικές συνέπειες, καθώς τροποποιημένες εντολές μπορεί να οδηγήσουν σε λανθασμένες ρυθμίσεις στις μηχανές, προκαλώντας βλάβες, διακοπές στην παραγωγή ή ακόμα και ζημιές στα ίδια τα μηχανήματα. Σε άλλη περίπτωση, κακόβουλο λογισμικό θα μπορούσε να αποκτήσει τον έλεγχο των μηχανών και να τις θέσει σε κατάσταση εκτός λειτουργίας, εκβιάζοντας την επιχείρηση ή προκαλώντας σοβαρές οικονομικές απώλειες.

Για αυτό το λόγο, είναι κρίσιμη η εφαρμογή αυστηρών μέτρων ασφαλείας σε κάθε στάδιο της διαδικασίας. Πρώτον, η σύνδεση μεταξύ των εξουσιοδοτημένων μηχανικών και της cloud υποδομής πρέπει να είναι κρυπτογραφημένη και να χρησιμοποιεί ασφαλή πρωτόκολλα επικοινωνίας (όπως VPNs ή SSL/TLS), ώστε να αποτρέπεται η υποκλοπή δεδομένων ή εντολών από τρίτους. Δεύτερον, οι μηχανικοί θα πρέπει να χρησιμοποιούν μηχανισμούς ελέγχου ταυτότητας πολλαπλών παραγόντων [multi-factor authentication (MFA)] για να εξασφαλιστεί ότι μόνο εξουσιοδοτημένοι χρήστες μπορούν να έχουν πρόσβαση στα δεδομένα και να εκτελούν ενέργειες στις μηχανές. Επιπλέον, η τακτική ενημέρωση του λογισμικού ασφαλείας και η ευαισθητοποίηση των μηχανικών σχετικά με τις κυβερνοαπειλές είναι κρίσιμα στοιχεία για τη διατήρηση της ασφάλειας του συστήματος. Οι μηχανικοί πρέπει να είναι εξοικειωμένοι με τις πρακτικές ασφαλούς σύνδεσης και να αποφεύγουν την πρόσβαση στο cloud από μη ασφαλή δίκτυα, όπως δημόσια WiFi, τα οποία είναι ευάλωτα σε επιθέσεις.

Συνοψίζοντας, η σχέση μεταξύ της cloud υποδομής και των εξουσιοδοτημένων μηχανικών είναι δυναμική και εξαιρετικά σημαντική για την αποδοτική λειτουργία της βιομηχανικής παραγωγής. Ωστόσο, για να είναι αποτελεσματική και ασφαλής, απαιτείται η εφαρμογή ισχυρών μέτρων προστασίας, καθώς και η σωστή εκπαίδευση των μηχανικών.

**Αλγόριθμοι Επεξεργασίας & Υποδομή για το Σύννεφο:** Η σχέση μεταξύ της cloud υποδομής και των αλγορίθμων επεξεργασίας αποτελεί τον πυρήνα της ανάλυσης και της αξιοποίησης των δεδομένων που συλλέγονται από τις συσκευές IIoT στη βιομηχανική παραγωγή. Αυτή η δυναμική σχέση είναι καθοριστική για την επίτευξη αυτοματοποιημένης ανάλυσης δεδομένων και τη λήψη στρατηγικών αποφάσεων με βάση τα δεδομένα που καταγράφονται. Τα δεδομένα που συλλέγονται από τις μηχανές παραγωγής και μεταφέρονται στην cloud υποδομή είναι σε ακατέργαστη μορφή. Αυτά τα δεδομένα αφορούν παραμέτρους όπως η απόδοση των μηχανών, οι ώρες λειτουργίας, οι θερμοκρασίες, οι κραδασμοί και η κατανάλωση ενέργειας. Ωστόσο, για να αποκτηθεί μια σαφής εικόνα των τάσεων παραγωγής και για να ληφθούν έγκαιρες αποφάσεις, τα δεδομένα αυτά χρειάζεται να υποβληθούν σε επεξεργασία μέσω αλγορίθμων. Η cloud υποδομή προσφέρει την απαραίτητη υπολογιστική ισχύ και τις υποδομές αποθήκευσης για να γίνει αυτή η επεξεργασία αποτελεσματική και σε μεγάλη κλίμακα. Οι αλγόριθμοι επεξεργασίας δεδομένων εφαρμόζουν σύνθετες αναλύσεις στα δεδομένα, όπως αναγνώριση προτύπων, στατιστική ανάλυση και μηχανική μάθηση. Αυτές οι τεχνικές επιτρέπουν στους αλγόριθμους να εντοπίζουν κρίσιμα μοτίβα και τάσεις που δεν είναι άμεσα ορατά. Για παράδειγμα, ένας τέτοιος αλγόριθμος μπορεί να αναλύσει δεδομένα από όλες τις μηχανές σε ένα εργοστάσιο και να προβλέψει σε ποια από αυτές πρέπει να δοθεί προτεραιότητα για άμεση συντήρηση. Με τη χρήση δεδομένων ιστορικού καθώς και τα στοιχεία που αντλεί σε πραγματικό χρόνο, ο αλγόριθμος μπορεί να εντοπίσει ενδείξεις φθοράς ή ανωμαλιών, όπως μικρές αυξήσεις στη θερμοκρασία ή ανωμαλίες στους κραδασμούς. Αυτός ο τύπος ανάλυσης δεν θα ήταν δυνατός αν οι αλγόριθμοι δεν είχαν πρόσβαση στα δεδομένα σε πραγματικό χρόνο, τα οποία παρέχει η cloud υποδομή.

Η σχέση μεταξύ της cloud υποδομής και των αλγορίθμων επεξεργασίας δεδομένων είναι τόσο διαδραστική όσο και εξαρτώμενη. Η cloud υποδομή παρέχει το περιβάλλον μέσα στο οποίο οι αλγόριθμοι μπορούν να εκτελούνται αποδοτικά, αξιοποιώντας την κλίμακα και την ευελιξία του cloud για να επεξεργάζονται τεράστιες ποσότητες δεδομένων ταυτόχρονα. Χωρίς αυτή την υποδομή, η επεξεργασία των δεδομένων θα απαιτούσε σημαντικούς τοπικούς πόρους, κάτι που θα περιοριζε την κλίμακα και την ταχύτητα ανάλυσης. Από την άλλη πλευρά, οι αλγόριθμοι δίνουν νόημα στα δεδομένα που φιλοξενούνται στο cloud, ερμηνεύοντας την ακατέργαστη πληροφορία σε πολύτιμες γνώσεις. Μέσω της ανάλυσης των δεδομένων, οι αλγόριθμοι επιτρέπουν την πρόβλεψη προβλημάτων πριν αυτά εμφανιστούν, τη βελτιστοποίηση της παραγωγής, και τη μείωση των απρογραμματίστων διακοπών λειτουργίας, κάτι που μπορεί να βελτιώσει σημαντικά την αποδοτικότητα της παραγωγικής διαδικασίας.

Παράλληλα, όμως, υπάρχουν και προκλήσεις που συνοδεύουν αυτή τη σχέση. Αν οι αλγόριθμοι επεξεργασίας δεν έχουν κατασκευαστεί ή εκπαιδευτεί σωστά, μπορεί να οδηγήσουν σε λανθασμένα αποτελέσματα και κακές αποφάσεις. Επίσης, η ακεραιότητα και η ασφάλεια των δεδομένων είναι κρίσιμα σημεία προσοχής. Τα δεδομένα που επεξεργάζονται οι αλγόριθμοι πρέπει να προστατεύονται από εξωτερικές επιθέσεις και κακόβουλη αλλοίωση, καθώς αυτό θα μπορούσε να επηρεάσει τη λειτουργία της παραγωγής.

**Εξωτερικοί Προμηθευτές & Υποδομή για το Σύννεφο:** Η σχέση μεταξύ των εξωτερικών προμηθευτών και της cloud υποδομής στο πλαίσιο της βιομηχανικής παραγωγής είναι καίρια για την εξασφάλιση της ομαλής ροής των ανταλλακτικών και των πρώτων υλών που απαιτούνται για τη λειτουργία των μηχανών και των παραγωγικών γραμμών. Αυτή η σχέση επιτρέπει στους προμηθευτές να έχουν πρόσβαση σε δεδομένα αποθεμάτων, προγραμματισμού παραγωγής και κατανάλωσης υλικών μέσω της cloud υποδομής του εργοστασίου. Η πρόσβαση των προμηθευτών στα δεδομένα που αποθηκεύονται στο cloud εξυπηρετεί στη βελτίωση της εφοδιαστικής αλυσίδας. Για παράδειγμα, οι προμηθευτές μπορούν να ελέγχουν σε πραγματικό χρόνο τα αποθέματα τους σε ανταλλακτικά και πρώτες ύλες στο εργοστάσιο, και να προγραμματίζουν τις αποστολές τους με βάση τις ανάγκες του εργοστασίου. Αυτό διασφαλίζει ότι τα απαιτούμενα ανταλλακτικά θα είναι διαθέσιμα πριν εξαντληθούν τα αποθέματα, αποτρέποντας καθυστερήσεις στην παραγωγή και απρογραμμάτιστες διακοπές. Ένας προμηθευτής μπορεί, για παράδειγμα, να χρησιμοποιεί τα δεδομένα από την cloud υποδομή για να εντοπίζει τότε ένα συγκεκριμένο ανταλλακτικό ή υλικό πλησιάζει τα ελάχιστα αποθέματα, και να στέλνει άμεσα τις απαραίτητες προμήθειες. Αυτή η προσέγγιση, που βασίζεται στη συνεργασία και την ανταλλαγή δεδομένων, βελτιώνει την απόδοση της εφοδιαστικής αλυσίδας και μειώνει την ανάγκη για υπερβολικά αποθέματα, εξοικονομώντας κόστος και αυξάνοντας την αποδοτικότητα. Ωστόσο, όπως έχει γίνει ήδη φανερό, η χρήση των υποδομών cloud συνοδεύεται από κάποιους κινδύνους, που αφορούν την ασφάλεια των δεδομένων. Εάν οι προμηθευτές έχουν πρόσβαση σε κρίσιμες πληροφορίες, όπως τα αποθέματα και τα σχέδια παραγωγής, η ασφάλεια αυτών των δεδομένων πρέπει να διασφαλιστεί για να μην υπονομεύεται η λειτουργία του εργοστασίου. Σε περίπτωση που οι προμηθευτές δεν προστατεύουν σωστά τα δεδομένα που ανταλλάσσουν με την cloud υποδομή, υπάρχει σοβαρός κίνδυνος κυβερνοεπιθέσεων, οι οποίες μπορούν να οδηγήσουν σε διαρροή βιομηχανικών μυστικών ή ακόμα και σε παραβιάσεις της αλυσίδας εφοδιασμού. Πιο συγκεκριμένα, εάν η υποδομή ενός προμηθευτή δεν είναι σωστά ασφαλισμένη, κακόβουλοι παράγοντες θα μπορούσαν να υποκλέψουν δεδομένα σχετικά με τα αποθέματα του εργοστασίου, τα οποία θα μπορούσαν να χρησιμοποιηθούν για ανταγωνιστικούς σκοπούς ή ακόμα και για κυβερνοεπιθέσεις που θα στόχευαν τη διακοπή της παραγωγής. Επιπλέον, εάν οι προμηθευτές είναι επιρρεπείς σε επιθέσεις μέσω κακόβουλου λογισμικού, υπάρχει ο κίνδυνος τα μολυσμένα δεδομένα να διεισδύσουν στο σύστημα του εργοστασίου μέσω της cloud υποδομής, προκαλώντας σοβαρά προβλήματα ασφάλειας.

Αυτοί οι κίνδυνοι καθιστούν απαραίτητη την εφαρμογή αυστηρών πρωτοκόλλων ασφαλείας σε όλη τη διαδικασία ανταλλαγής δεδομένων μεταξύ της cloud υποδομής του εργοστασίου και των εξωτερικών προμηθευτών. Αυτό περιλαμβάνει τη χρήση κρυπτογράφησης για την προστασία των δεδομένων κατά τη μετάδοσή τους, καθώς και την εφαρμογή ισχυρών μηχανισμών ελέγχου ταυτότητας και ελέγχου πρόσβασης. Επιπλέον, πρέπει να υπάρχει συνεχής παρακολούθηση και έλεγχος της ασφάλειας των συστημάτων των προμηθευτών για να διασφαλιστεί ότι δεν αποτελούν αδύναμο κρίκο στην αλυσίδα εφοδιασμού. Η αποτελεσματική συνεργασία μεταξύ

του εργοστασίου και των προμηθευτών βασίζεται σε μεγάλο βαθμό στην εμπιστοσύνη και την ασφάλεια. Οι προμηθευτές πρέπει να διαχειρίζονται τα δεδομένα που λαμβάνουν από την cloud υποδομή με απόλυτη διακριτικότητα και επαγγελματισμό, ενώ το εργοστάσιο πρέπει να διασφαλίζει ότι παρέχει πρόσβαση μόνο στα απαραίτητα δεδομένα. Η ισχυρή συνεργασία που βασίζεται στην ασφαλή ανταλλαγή πληροφοριών μπορεί να βοηθήσει στην εξασφάλιση της απρόσκοπτης ροής υλικών και ανταλλακτικών, βελτιώνοντας τη συνολική απόδοση της παραγωγής.

#### **5.2.4 Σχεδίαση Σεναρίου**

Οι οντότητες του σεναρίου καθώς και οι δυναμικές σχέσεις μεταξύ τους μπορούν να συνδυαστούν και να συνθέσουν ένα διάγραμμα οντοτήτων-σχέσεων ή αλλιώς Entity Relation Diagrams (ERDs). Η οπτική αναπαράσταση των βασικών οντοτήτων που εμπλέκονται στο σύστημα του σεναρίου βοηθάει στην κατανόηση των βασικών στοιχείων του σεναρίου. Στην παρακάτω εικόνα αποτυπώνεται το ERD διάγραμμα του σεναρίου, όπως αυτό σχεδιάστηκε με το εργαλείο Lucidchart<sup>11</sup>. Στο διάγραμμα παρουσιάζονται οι οντότητες με του συστήματος (Ανθρώπινο Δυναμικό, Μηχανές Παραγωγής κλπ.) με ορθογώνια παραλληλόγραμμα. Οι σχέσεις μεταξύ αυτών περιγράφονται από βέλη που δείχνουν τη ροή πληροφορίας και ρόμβους που περιγράφουν τη δυναμική αλληλεπίδραση τους. Η καρδιναλιότητα των σχέσεων φαίνεται με ειδικά σύμβολα που υποδεικνύουν τη μορφή της σχέσης μεταξύ των οντοτήτων (πχ ένας προς ένα, ένα προ πολλά κλπ). Για τον συμβολισμό χρησιμοποιήθηκαν οι συμβολισμοί του Chen (Team, 2024). Στο διάγραμμα, φαίνονται ότι πολλές συσκευές IIoT παρακολουθούν ένα ή περισσότερους εργαζομένους ταυτόχρονα, καταγράφοντας διάφορους παραμέτρους σχετικά με την υγεία, την ασφάλεια και την απόδοση τους. Τέτοιες συσκευές μπορεί να είναι αισθητήρες που καταγράφουν τη θερμοκρασία ή τα επίπεδα του θορύβου στο χώρο, ακόμα και έξυπνα ρολόγια που φορούν οι εργαζόμενοι και συλλέγουν πληροφορίες σχετικές με τον καρδιακό τους ρυθμό. Αντίστοιχα υπάρχουν αισθητήρες τοποθετημένοι στις μηχανές παραγωγής και συλλέγουν δεδομένα σχετικά με την κατάσταση, τη λειτουργία και την απόδοση των μηχανών. Για παράδειγμα αισθητήρες δόνησης μπορεί να καταγράφουν τυχόν μη φυσιολογικές δονήσεις, οι οποίες υποδεικνύουν πιθανόν προβλήματα στους κινητήρες ή τα ρουλεμάν των μηχανών. Ακόμα, αισθητήρες πίεσης, μπορεί να μετρούν την πίεση των υδραυλικών υγρών των μηχανών, ώστε να εξασφαλιστεί η ομαλή λειτουργία τους και να αποκλειστούν βλάβες όπως είναι οι διαρροές που αν δεν αντιμετωπιστούν έγκαιρα μπορεί να οδηγήσουν σε εκτεταμένη φθορά των μηχανών. Τα πρωτογενή αυτά δεδομένα που συλλέγονται από τις IIoT συσκευές πρέπει να μεταφερθούν για ανάλυση. Όπως φαίνεται και στο σχήμα, οι συσκευές αυτές συνδέονται με την οντότητα του δικτύου επικοινωνίας. Αυτή η οντότητα θα μπορούσε να περιλαμβάνει τη φυσική υποδομή του δικτύου (πχ καλωδιωμένα συστήματα Ethernet και ασύρματες τεχνολογίες WiFi,

---

<sup>11</sup> <https://lucid.app/documents>

LoRa) μαζί με τα πρωτόκολλα που χρησιμοποιούν. Επίσης, το δίκτυο επικοινωνίας θα μπορούσε να είναι ιεραρχημένο με διαφορετικά επίπεδα, από τοπικές πύλες που συνδέουν τους αισθητήρες με το δίκτυο μέχρι κεντρικά συστήματα επεξεργασίας σε τοπικούς εξυπηρετητές (servers) της βιομηχανίας. Για την διασφάλιση της ακεραιότητας της μετάδοσης των δεδομένων μπορεί η οντότητα αυτή να εμπεριέχει τεχνολογίες κρυπτογράφησης και πιστοποίησης ταυτότητας. Πρωτόκολλα όπως το TLS και το VPN μπορούν να προστατέψουν τα δεδομένα κατά τη μεταφορά τους. Τελικός στόχος του δικτύου επικοινωνίας είναι η αποθήκευση των δεδομένων στην υποδομή του σύννεφου. Όπως φαίνεται στο σχήμα μία υποδομή cloud διατηρεί τα δεδομένα ενώ ταυτόχρονα επεξεργάζεται τα πρωτογενή δεδομένα για να παράγει αναλυτικά στοιχεία μέσω έξυπνων αλγορίθμων. Οι εξουσιοδοτημένοι μηχανικοί όπως απεικονίζεται και στο διάγραμμα, έχουν πρόσβαση στο δίκτυο και μέσω αυτού στα πρωτογενή και δευτερογενή δεδομένα που βρίσκονται στο σύννεφο. Με τη βοήθεια του δικτύου, αυτοί είναι εξουσιοδοτημένοι να επηρεάσουν και να ελέξουν τις μηχανές παραγωγής. Για παράδειγμα, εάν από τα αναλυτικά στοιχεία υπάρχει υποψία διαρροής υδραυλικών, μπορούν να απενεργοποιήσουν την συγκεκριμένη μηχανή, προκειμένου να προλάβουν μία εκτεταμένη φθορά που μπορεί να προκληθεί. Μετά την αποκατάσταση της βλάβης μπορούν εκ νέου να τη θέσουν σε λειτουργία.

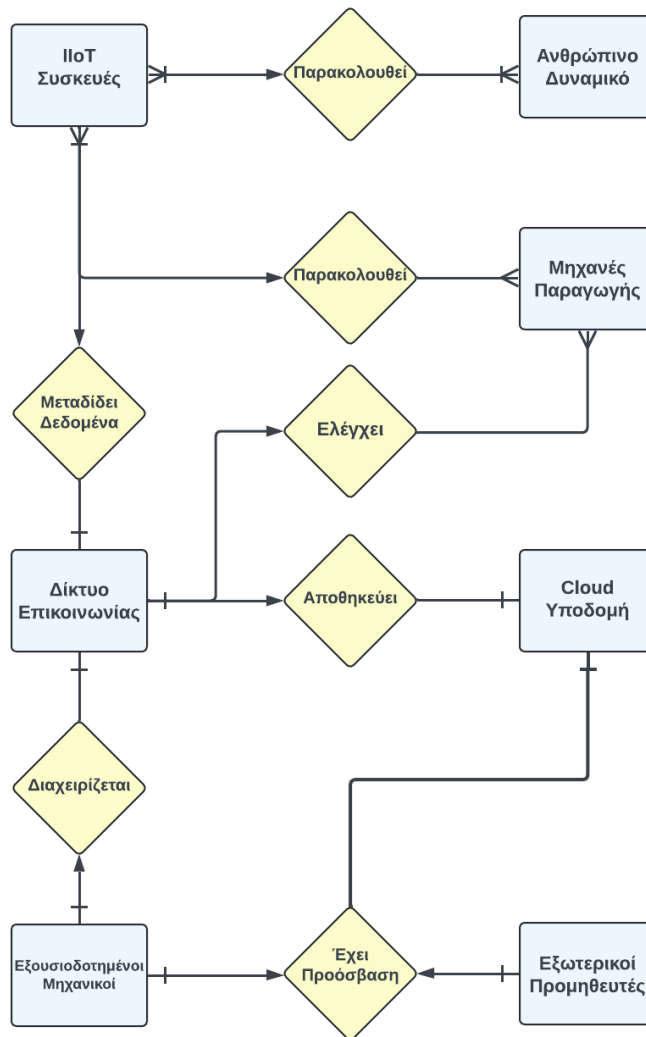


Figure 9 ERD διάγραμμα ενός IIoT εργοστασίου

### 5.2.5 Μοντελοποίηση Σεναρίου

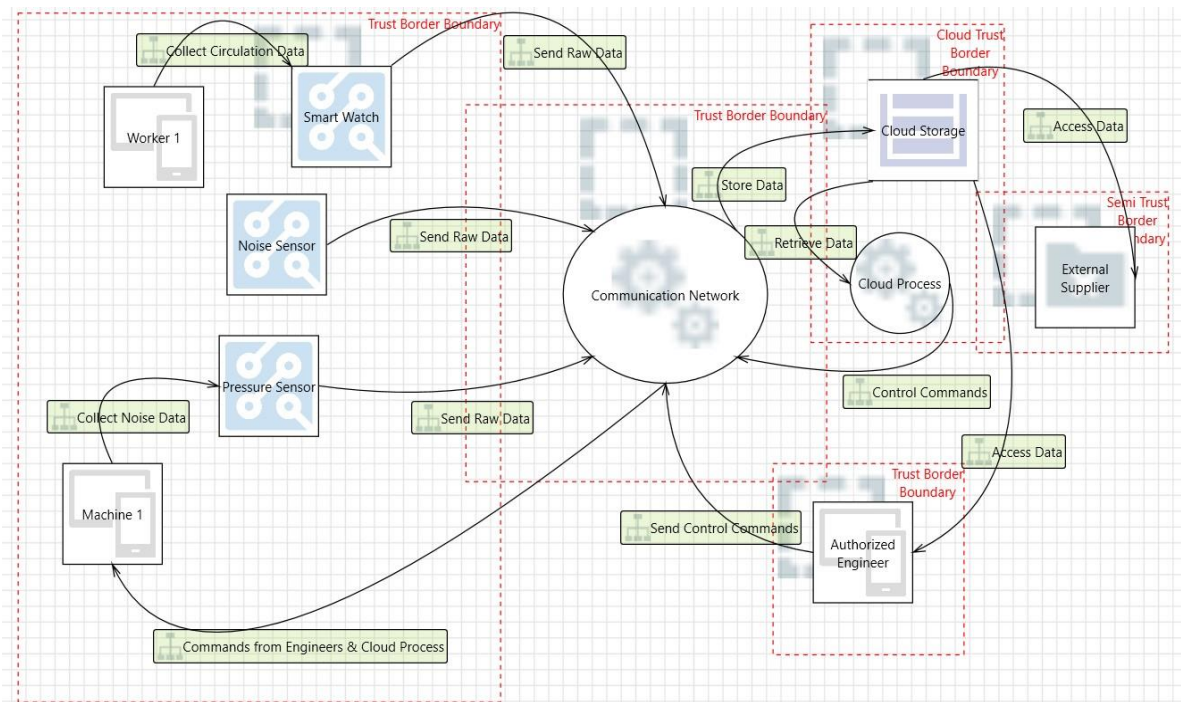
Η σχεδίαση του διαγράμματος οντοτήτων-σχέσεων αποτελεί μία επισκόπηση σε υψηλό επίπεδο σχετικά με την οργάνωση, δομή και τις ροές δεδομένων ενός IIoT εργοστασίου. Το ERD διάγραμμα είναι αρκετά βοηθητικό για την κατανόηση του σεναρίου, ωστόσο είναι ελλιπής όσο αφορά την περιγραφή πιθανών απειλών ασφαλείας και ευπαθειών μεταξύ των οντοτήτων. Σε ένα περιβάλλον IIoT όπου αισθητήρες, υποδομές cloud και εξωτερικοί προμηθευτές συμμετέχουν ενεργά, η ασφάλεια των δεδομένων και η ακεραιότητα αυτών είναι βασική προϋπόθεση. Για αυτό το λόγο είναι απαραίτητη η μοντελοποίηση των απειλών του σεναρίου, με σκοπό την ανάδειξη των συνόρων εμπιστοσύνης (Trust Borders) και την επισήμανση των κενών ασφαλείας καθώς τα δεδομένα μεταφέρονται μέσα στο πολύπλοκο αυτό οικοσύστημα.

### Περιγραφή Διαγράμματος

Η εταιρεία της Microsoft προσφέρει το εργαλείο Microsoft Threat Modeling Tool<sup>12</sup> για την αναπαράσταση των συνιστωσών ενός πολύπλοκου συστήματος που περιλαμβάνει διαδικασίες, αποθηκευτικά μέσα, επικοινωνιακά κανάλια, εξωτερικά συστήματα κλπ. Αποτελεί μέρος του Security Development Lifecycle (SDL), μίας προσέγγισης που χρησιμοποιεί η Microsoft για να ενσωματώνει την ασφάλεια στις DevOps (Development & Operations) διαδικασίες. Έτσι επιτρέπει στους αρχιτέκτονες λογισμικού να εντοπίζουν και να μετριάζουν πιθανά ζητήματα ασφάλειας έγκαιρα, όταν είναι σχετικά εύκολο και οικονομικά αποδοτικό να επιλυθούν. Ως αποτέλεσμα, μειώνει σημαντικά το συνολικό κόστος ανάπτυξης. Επίσης, μετά το σχεδιασμό με το Microsoft Threat Modeling Tool, μπορούν να εφαρμοστούν διάφορες μεθοδολογίες όπως είναι η STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) προκειμένου να αναλυθούν να αναδειχθούν πιθανά κενά ασφαλείας. Στη μοντελοποίηση που ακολουθεί φαίνεται το σενάριο του IIoT εργοστασίου. Η μοντελοποίηση του σεναρίου περιλαμβάνει, έναν εργαζόμενο, μία μηχανή, τρεις αισθητήρες, ένα δίκτυο επικοινωνίας, μία υποδομή cloud για την αποθήκευση και επεξεργασία των δεδομένων, έναν εξωτερικό προμηθευτή και έναν εξουσιοδοτημένο μηχανικό. Όπως έχει ήδη περιγραφεί στο διάγραμμα οντοτήτων-σχέσεων, δύναται να υπάρχουν πολλοί περισσότεροι αισθητήρες, εργαζόμενοι, μηχανικοί, μηχανές και εξωτερικοί προμηθευτές, ωστόσο κάτι τέτοιο θα έκανε τη μοντελοποίηση πολύ περίπλοκη χωρίς να αλλάζει κάτι στις διαδικασίες που περιγράφονται από το μοντέλο. Για την αναπαράσταση των εργαζομένων, των μηχανών και των εξουσιοδοτημένων μηχανικών χρησιμοποιήθηκε ο συμβολισμός του πολυγράφου Client που αποτελεί υποκατηγορία του External Interactor, αφού η διεπαφή που χρησιμοποιείται από αυτές τις οντότητες είναι κάποιου είδους λογισμικού. Για τους αισθητήρες χρησιμοποιήθηκε ο συμβολισμός του πολυγράφου IoT Devices, αφού πρόκειται για τέτοιες συσκευές, για τον εξωτερικό προμηθευτή χρησιμοποιήθηκε το Generic External Interactor και για την αποθήκευση στο cloud η δομή Generic Data Storage. Τέλος, η επεξεργασία των δεδομένων στο cloud και το δίκτυο επικοινωνίας αναπαριστώνται Generic Processes, αφού επεξεργάζονται δεδομένα και λειτουργούν σαν Gateways αντίστοιχα. Ακόμη, Trust Boundaries, περιγράφουν τις δομές εμπιστοσύνης μέσα στο σύστημα. Οι μηχανές, οι εργαζόμενοι και οι αισθητήρες βρίσκονται όλοι κάτω από το ίδιο τοπικό δίκτυο, οπότε μπορούν να συμπεριληφθούν σαν ένα κοινό δίκτυο εμπιστοσύνης. Η υποδομή Cloud υλοποιείται από ένα εξωτερικό συνεργάτη και αποτελεί ένα διαφορετικό όριο εμπιστοσύνης όπως επίσης και το δίκτυο επικοινωνίας του συστήματος. Το ίδιο ισχύει και για κάθε εξωτερικό προμηθευτή που υπάρχει στο σύστημα. Τέλος, κάθε εξουσιοδοτημένος μηχανικός, δεδομένου ότι μπορεί να διαχειρίζεται απομακρυσμένα το περιβάλλον, είναι ένα ξεχωριστό όριο εμπιστοσύνης.

---

<sup>12</sup> <https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool>



**Figure 10 Μοντελοποίηση απειλών ενός IIoT εργοστασίου**

### STRIDE METHODOLOGY

Η μοντελοποίηση απειλών του σεναρίου, επιτρέπει την εφαρμογή της μεθοδολογίας STRIDE για την ανάδειξη των ευπαθειών ασφαλείας. Η μεθοδολογία STRIDE χωρίζεται σε έξι (6) κατηγορίες απειλών. Αναλύοντας κάθε στοιχείο ενός συστήματος σε καθεμία από τις κατηγορίες αυτές είναι δυνατό να αναγνωριστούν αδυναμίες του συστήματος και να μετριάστούν τα ρίσκα από επιθέσεις ασφαλείας.

Η πρώτη κατηγορία της μεθοδολογίας αφορά την απόπειρα πλαστογράφησης ταυτότητας (**Spoofing**). Αρχικά, στόχος σε αυτή την κατηγορία μπορεί να είναι οι οντότητες των εργαζομένων, εξουσιοδοτημένων μηχανικών ή εξωτερικών προμηθευτών. Κάποιος κακόβουλος μπορεί να προσποιηθεί ότι είναι εργαζόμενος, προμηθευτής ή μηχανικός για να αποκτήσει πρόσβαση σε κρίσιμα συστήματα και δεδομένα. Για παράδειγμα, κάποιος κακόβουλος αποκτά πρόσβαση σε ταυτότητες RFID εργαζομένων και εισέρχεται στο δίκτυο του εργοστασίου. Σε αυτή την περίπτωση, προτείνεται η πολυπαραγοντική ταυτοποίηση με τη χρήση βιομετρικών χαρακτηριστικών, ώστε να μην είναι τόσο εύκολη η πρόσβαση σε κρίσιμα συστήματα. Ακόμα, πλαστογράφηση ταυτότητας μπορεί να γίνει και σε συσκευές IIoT. Είναι εφικτό, ένας κακόβουλος να προσποιηθεί ότι είναι ένας αισθητήρας (πχ θερμοκρασίας) για να εισάγει ψευδή δεδομένα στο σύστημα. Για την αντιμετώπιση μίας τέτοιας απειλής θα ήταν αναγκαία η ταυτοποίηση των συσκευών μέσω μοναδικών πιστευτηρίων (credentials) και την επιβεβαίωση των δεδομένων από πολλαπλούς αισθητήρες. Επιπλέον, θα ήταν ωφέλιμο να γίνεται χρήση πιστοποιητικών και ασφαλών πρωτοκόλλων επικοινωνίας όπως η χρήση του TLS.



Η δεύτερη κατηγορία της μεθοδολογίας αφορά την αλλοίωση δεδομένων (**Tampering**), όπου μη εξουσιοδοτημένοι χρήστες τροποποιούν τα δεδομένα, πράγμα το οποίο μπορεί να έχει ολέθριες οικονομικές συνέπειες για ένα οικοσύστημα εργοστασίου. Το κεντρικό κανάλι επικοινωνίας στο οποίο μεταφέρονται τα δεδομένα μεταξύ των οντοτήτων αποτελεί ένα δελεαστικό στόχο για τέτοιου είδους επιθέσεις. Συνεπώς, μία επίθεση θα μπορούσε να εστιάζει στο δίκτυο επικοινωνιών και τα δεδομένα που μεταδίδονται από τους αισθητήρες. Πιο συγκεκριμένα, επιτιθέμενοι που έχουν εισχωρήσει στο δίκτυο τροποποιούν τα πρωτογενή δεδομένα που στέλνουν οι αισθητήρες πίεσης, ώστε να πυροδοτήσουν μία σειρά λανθασμένων αντιδράσεων στο σύστημα. Και σε αυτή την περίπτωση, συστήνεται η χρήση ασφαλών πρωτοκόλλων για την κρυπτογραφημένη μεταφορά των δεδομένων (πχ TLS) καθώς και ο έλεγχος της ακεραιότητας των δεδομένων που μπορεί να πραγματοποιηθεί με τις συναρτήσεις κατακερματισμού (hash functions). Όταν εφαρμόζονται αυτές οι συναρτήσεις, δημιουργούν μια σειρά χαρακτήρων σταθερού μήκους. Έτσι κάθε πιθανή αλλοίωση των δεδομένων θα δημιουργήσει διαφορετικές σειρές χαρακτήρων, που δεν επαληθεύουν την ακεραιότητα των δεδομένων. Τέλος, ένα πρόσθετο μέτρο προστασίας που εφαρμόζεται στα δίκτυα είναι αυτό της χρήσης ανίχνευσης εισβολών συστήματος - Intrusion Detection Systems (IDS). Συστήματα IDS παρακολουθούν και αναλύουν την κίνηση ενός δικτύου σε πραγματικό χρόνο και συγκρίνουν τα δεδομένα με γνωστά πρότυπα επιθέσεων αναζητώντας ανώμαλες συμπεριφορές. Εφόσον εντοπιστεί η απειλή μπορεί να της αποτραπεί καθε μέλλοντική προσπάθεια για συμμετοχή στο δίκτυο ή να ειδοποιηθεί το κατάλληλο κλιμάκιο ασφαλείας για να λάβει μέτρα προστασίας. Πέρα από τα δεδομένα που μεταφέρονται στο δίκτυο, υπάρχουν και δεδομένα που βρίσκονται στις βάσεις δεδομένων. Στο παράδειγμα που εξετάζεται σε αυτό το κεφάλαιο, τα δεδομένα του οικοσυστήματος βρίσκονται στη δομή του συνέφου. Εάν κάποιος κακόβουλος αποκτήσει πρόσβαση στα δεδομένα αυτά και τα αλλοιώσει, μπορεί να τροποποιήσει παραμέτρους που αφορούν τη λειτουργία των μηχανών. Σε αυτή τη περίπτωση, θα πρέπει τα δεδομένα να αποθηκεύονται σε κρυπτογραφημένη μορφή να εφαρμόζονται πολιτικές ελέγχου πρόσβασης (access control policies). Ουσιαστικά πρόκειται για διαβαθμισμένο έλεγχο χρηστών που καθορίζουν ποιοι χρήστες και υπό ποιες συνθήκες είναι εξουσιοδοτημένοι να έχουν πρόσβαση, έλεγχο και επεξεργασία στα δεδομένα. Για παράδειγμα, κάποιος χρήστη μπορεί να έχει δικαιώματα ανάγνωσης των δεδομένων, αλλά όχι επεξεργασίας ή διαγραφής. Ακόμα, η δημιουργία μητρώων δραστηριότητας (logs) που θα καταγράφουν όλες τις ενέργειες που πραγματοποιούνται στα δεδομένα μπορεί να βοηθήσει στην προστασία από επιθέσεις αλλοίωσης δεδομένων. Οι καταγραφές, μπορούν να αναλυθούν για να εντοπιστούν ασυνήθιστες ή μη εξουσιοδοτημένες αλλαγές.

Η τρίτη κατηγορία της μεθοδολογίας Stride αφορά την άρνηση ευθύνης (**Repudiation**). Μία οντότητα αρνείται ότι έκανε μία ενέργεια και δεν υπάρχει τρόπος να αποδειχθεί ότι πράγματι την έκανε. Για παράδειγμα, ένας εξουσιοδοτημένος μηχανικός τροποποιεί παραμέτρους σε μία μηχανή και αρνείται ότι το έκανε. Σε αυτή την περίπτωση, θα μπορούσαν να χρησιμοποιούνται

μοναδικά ψηφιακά κλειδιά για κάθε χρήστη/μηχανικό που θα υπογράφουν ψηφιακά τα δεδομένα, ώστε να είναι σαφές ποιος εκτελεί την κάθε ενέργεια. Ασφαλώς, και εδώ θα πρέπει να καταγράφονται όλες οι ενέργειες μέσω logs που περιλαμβάνουν χρονικές σφραγίδες (timestamps). Παρόμοιο περιστατικό μπορεί να συμβεί και με τις συσκευές IIoT. Πιο συγκεκριμένα, μια συσκευή αισθητήρας σταματά να λειτουργεί προσωρινά για κάποιο μικρό χρονικό διάστημα, με αποτέλεσμα να μην καταγράφονται κρίσιμα δεδομένα. Ο πάροχος του αισθητήρα, αρνείται να πάρει την ευθύνη και ισχυρίζεται ότι ο αισθητήρας δεν σταμάτησε να λειτουργεί. Σε αυτή την περίπτωση θα μπορούσαν να τηρηθούν καταγραφές logs στο δίκτυο επικοινωνιών που θα λειτουργούν σαν μαρτυρίες. Τέλος, προκειμένου να υπάρχει μεγαλύτερη εφεδρικότητα θα μπορούσε να υπάρχουν και εφεδρικές καταγραφές σε περίπτωση διακοπής.

Η τέταρτη κατηγορία αφορά την αποκάλυψη πληροφοριών (**Information Disclosure**). Αυτή η μορφή απειλής περιλαμβάνει την έκθεση πληροφορίας σε τρίτες μη εξουσιοδοτημένες οντότητες. Επειδή και αυτή η μορφή απειλής αφορά δεδομένα, οι κύριες οντότητες που πρέπει να θωρακιστούν είναι το δίκτυο επικοινωνιών και το σύννεφο που αποθηκεύονται τα δεδομένα. Εάν πραγματοποιηθεί κάποια επιτυχημένη επίθεση και τα δεδομένα μιας παραγωγικής μηχανής γίνουν προσβάσιμα στον επιτιθέμενο, ο οποίος μπορεί να είναι ένας εξωτερικός προμηθευτής. Αυτός μπορεί να προσαρμόσει τις υπηρεσίες του με βάση αυτές τις πληροφορίες προκειμένου να αποκτήσει ανταγωνιστικό πλεονέκτημα. Σαν μέτρο αντιμετώπιση προτείνονται πρακτικές που έχουν προταθεί και σε άλλες κατηγορίες. Αυτές είναι η καθολική κρυπτογράφηση των δεδομένων και ο αυστηρός έλεγχος των δικαιωμάτων πρόσβασης. Τα δικαιώματα πρόσβασης θα πρέπει να δίνονται με όσο τον δυνατό περισσότερους περιορισμούς. Με άλλα λόγια, καμία οντότητα δεν πρέπει να έχει δικαιώματα, που περισσεύουν ή δεν είναι απαραίτητα για να ασκήσει το έργο της. Σχετικά με την προστασία υποκλοπής των δεδομένων κατά τη μεταφορά τους στο δίκτυο επικοινωνίας, θα μπορούσε να τηρούνται ασφαλή πρωτόκολλα όπως VPN και TLS και να γίνεται τακτικός έλεγχος για να εντοπίζονται πιθανές παραβιάσεις στο δίκτυο.

Η πέμπτη κατηγορία είναι αυτή της άρνησης παροχής υπηρεσιών (**Denial of Service**). Αυτή η κατηγορία απειλής έχει στόχο την αδυναμία εξυπηρέτησης των νόμιμων χρηστών ενός δικτύου ή μιας υπηρεσίας. Συνήθως επιτυγχάνεται με την υπερφόρτωση του στόχου με αδικαιολόγητες αιτήσεις ή την εκμετάλλευση ευπαθειών, καθιστώντας έτσι αδύνατη τη φυσιολογική λειτουργία του λόγω εξάντλησης των πόρων. Η εξάντληση των πόρων μπορεί να αφορά το εύρος ζώνης, τη μνήμη ή την υπολογιστική ισχύ. Μια επίθεση άρνησης υπηρεσιών δεν είναι απαραίτητο να καταστήσει αδύνατη την εξυπηρέτηση για να θεωρηθεί επιτυχημένη. Ακόμη και η υποβάθμιση της ποιότητας της υπηρεσίας μέσω της πολύωρης εξυπηρέτησης για απλές διεργασίες, μπορεί να είναι κρίσιμη για την εξέλιξη μίας ροής εργασιών που γίνονται σε πραγματικό χρόνο. Σε μία υποτιθέμενη μεγάλης κλίμακας άρνησης παροχής υπηρεσιών επίθεσης με στόχο το δίκτυο του εργοστασίου, θα διακοπεί η επικοινωνία μεταξύ αισθητήρων και υποδομής σνέφου. Σε αυτές τις περιπτώσεις είναι απαραίτητη η χρήση τοίχου προστασίας και συστημάτων IDS που

αναγνωρίζουν τα μοτίβα των επιθέσεων αυτών και μπορούν να αποκόψουν αιτήσεις από επιτιθέμενους που σκοπεύουν να εξαντλήσουν τους πόρους του δικτύου. Σαν επιπρόσθετο μέτρο θα μπορούσαν να κατανεμηθούν τα δεδομένα σε πολλαπλές διαδρομές κάνοντας χρήση των load balancing τεχνικών, αποσκοπώντας στη μείωση της επιβάρυνσης σε ένα μοναδικό σημείο. Σε μία άλλη επίθεση, έστω ότι γίνεται στόχος ένας αισθητήρας θερμοκρασίας και ένας κακόβουλος ή μία κακόβουλη συσκευή πλησίον του αισθητήρα στέλνει χιλιάδες ψεύτικα αιτήματα, προκαλώντας τη υπερφόρτωση και διακοπή της λειτουργίας του. Με αποτέλεσμα, να μην συλλέγονται κρίσιμα δεδομένα, θέτοντας σε κίνδυνο την ασφάλεια των μηχανών και του εργοστασίου. Και σε αυτήν την περίπτωση θα μπορούσαν να χρησιμοποιηθούν τεχνικές ανίχνευσης ανωμαλιών στις ροές δεδομένων προς τους αισθητήρες αλλά και εφαρμογή του rate-limiting, δηλαδή προκαθορισμένο αριθμό αιτημάτων που μπορεί να δεχθεί μία συσκευή σε συγκεκριμένο χρονικό διάστημα.

Η έκτη και τελευταία κατηγορία της μεθοδολογίας έχει να κάνει με την αύξηση των δικαιωμάτων πρόσβασης (**Elevation of Privilege**). Ουσιαστικά, αναφέρεται σε καταστάσεις όπου μία οντότητα αποκτά υψηλότερα δικαιώματα πρόσβασης από αυτά που κανονικά δικαιούται. Αυτό μπορεί να συμβεί είτε γιατί δόθηκαν εξ αρχής λανθασμένα δικαιώματα είτε γιατί η οντότητα εκμεταλλεύτηκε ευπάθειες στο σύστημα. Σε ένα σύστημα IIoT, η αύξηση δικαιωμάτων πρόσβασης είναι ιδιαίτερα επικίνδυνη, καθώς επιτρέπει σε κακόβουλους παράγοντες να έχουν πρόσβαση σε κρίσιμα δεδομένα ή να έχουν έλεγχο σε σημαντικές διαδικασίες, πράγμα που μπορεί να οδηγήσει σε διακοπές στην παραγωγή, σε διαρροές δεδομένων, ακόμα και σε σωματικές βλάβες λόγω εσφαλμένου χειρισμού των μηχανών. Για παράδειγμα, εάν κάποιος εξουσιοδοτημένος μηχανικός, υπεύθυνος για την συντήρηση των μηχανών παραγωγής αποκτήσει δικαιώματα διαχειριστή στο σύστημα παραγωγής, ο μηχανικός μπορεί να αλλάξει τις ρυθμίσεις των μηχανών, να τροποποιήσει ή να διαγράψει δεδομένα, ή να αποκτήσει πρόσβαση σε εμπιστευτικές πληροφορίες. Αποτέλεσμα των παραπάνω, θα μπορούσε να είναι, η πρόκληση φθοράς στο σύστημα με σκοπό την τακτική του συντήρησης, η διαρροή πληροφοριών σε ανταγωνιστές ή η απώλεια σημαντικών δεδομένων που θα οδηγήσει σε μη αποτελεσματική παραγωγή. Τα αυξημένα δικαιώματα θα μπορούσαν να χορηγηθούν είτε από αμέλεια είτε εκμεταλλευόμενος ο ίδιος γνωστές ευπάθειες σε παλαιότερες εκδόσεις του συστήματος. Για την αντιμετώπιση τέτοιων περιστατικών, συστήνεται η χρήση των αρχών του ελάχιστου προνομίου (least privilege). Κατά την αρχή αυτή, κάθε χρήστης πρέπει να έχει τα απαραίτητα δικαιώματα για τις εργασίες του και μόνο αυτά. Επίσης, συστήνεται η ενημέρωση και αναβάθμιση των συστημάτων ασφαλείας και ο έλεγχος δικαιωμάτων πρόσβασης, καθώς και η ενεργή παρακολούθηση και καταγραφή όλων των ενεργειών που σχετίζονται με την αύξηση δικαιωμάτων πρόσβασης. Επιπρόσθετα, χρειάζεται ιδιαίτερη προσοχή στα δικαιώματα των εξωτερικών συνεργατών. Σε ένα υποθετικό σενάριο, κάποιος εξωτερικός προμηθευτής αποκτά πρόσβαση σε στοιχεία που αφορούν τις μηχανές και είναι αποθηκευμένα στην υποδομή cloud. Ο προμηθευτής μπορεί να αλλοιώσει δεδομένα παραγωγής ή να διαρρεύσει

ευαίσθητες πληροφορίες σε ανταγωνιστές. Είναι επιτακτική η ανάγκη για καθιέρωση ισχυρών κανόνων ρόλων για εξωτερικούς συνεργάτες (role-based access control – RBAC). Πρόκειται για ένα σύστημα διαχείρισης δικαιωμάτων πρόσβασης, όπου οι χρήστες αποκτούν δικαιώματα και άδειες βάσει των ρόλων που τους αποδίδονται εντός του συστήματος. Κάθε ρόλος αντιπροσωπεύει ένα σύνολο δικαιωμάτων και μπορεί να σχετίζεται με μια ομάδα εργασιών ή ένα σύνολο ευθυνών που κατέχει ο χρήστης. Σε ένα διαφορετικό σενάριο, ένας αισθητήρας θερμοκρασίας, που έχει περιορισμένη πρόσβαση μόνο για την αποστολή δεδομένων, εκμεταλλεύεται μία ευπάθεια του πρωτοκόλλου επικοινωνίας και αποκτά δικαιώματα που του επιτρέπουν να στέλνει εντολές σε άλλες συσκευές. Ο κακόβουλος αισθητήρας θερμοκρασίας μπορεί τώρα να στείλει λάθος δεδομένα και να ελέγξει τη λειτουργία άλλων συσκευών. Για την αντιμετώπιση τέτοιων περιστατικών, θα πρέπει να γίνεται χρήση ασφαλών πρωτοκόλλων επικοινωνίας και πιστοποιητικών ταυτοποίησης για όλες τις συσκευές, καθώς και διαχωρισμός δικαιωμάτων στις συσκευές.

**Table 4 Συνοπτικός πίνακας με τα αποτελέσματα της μεθοδολογίας STRIDE**

| ENTITY<br>STRIDE          | Εργαζόμενοι/<br>Μηχανικοί | Εξωτερικοί<br>Προμηθευτές | Συσκευές<br>IIoT/Μηχανές | Δίκτυο<br>Επικοινωνίας | Υποδομή<br>Σύννεφο |
|---------------------------|---------------------------|---------------------------|--------------------------|------------------------|--------------------|
| Spoofing                  | ✓                         | ✓                         |                          |                        |                    |
| Tampering                 | ✓                         | ✓                         | ✓                        | ✓                      | ✓                  |
| Repudiation               | ✓                         | ✓                         | ✓                        |                        |                    |
| Information<br>Disclosure | ✓                         | ✓                         | ✓                        | ✓                      | ✓                  |
| DoS                       | ✓                         | ✓                         | ✓                        | ✓                      | ✓                  |
| Elevation of<br>Privilege | ✓                         | ✓                         | ✓                        |                        | ✓                  |

#### 5.2.6 Καλές πρακτικές προστασίας προσωπικών δεδομένων

Το παραπάνω σενάριο φανέρωσε πολλές αδυναμίες που ενδέχεται να έχει μία επιχείριση ή οργανισμός που λειτουργεί σε ένα περιβάλλον βιομηχανικού διαδικτύου των πραγμάτων:

**Μετάδοση δεδομένων:** Σε περιπτώσεις επιθέσεων όπως επιθέσεις παράπλευρου καναλιού (side channel attacks), κατάληψης κόμβου (node capture), εισαγωγής ψεύτικου κόμβου (fake node insertion), επανάληψης (replay) και επιθέσεις δρομολόγησης (routing attacks) είναι απαραίτητη η χρήση κρυπτογράφησης των δεδομένων και ασφαλών καναλιών επικοινωνίας.

**Σημεία ελέγχου:** Η μετάδοση των δεδομένων οφείλει να γίνεται με ασφάλεια. Ο Γκάι και οι συνεργάτες του (Gai, 2019) εισήγαγαν μία καινοτόμα προσέγγιση που ενσωματώνει το Διαδίκτυο των Πραγμάτων με την υπολογιστική ικανότητα αιχμής (edge computing) και την τεχνολογία blockchain. Στόχος είναι η δημιουργία ενός περιβάλλοντος που διασφαλίζει την ιδιωτικότητα για την ανάθεση εργασιών στο Διαδίκτυο των Πραγμάτων (IIoT) και συνδυάζει το

blockchain και την υπολογιστική ικανότητα αιχμής (edge computing) για να ενισχύσει την εμπιστοσύνη στους κόμβους αιχμής, να ασφαλίσει τις επικοινωνίες και να επιτύχει βέλτιστη ανάθεση εργασιών. Το μοντέλο ενσωματώνει διαφορεική ιδιωτικότητα για την προστασία ταυτοτήτων προσθέτοντας θόρυβο στα δεδομένα που αποθηκεύονται στα μπλοκ, αντιμετωπίζοντας έτσι την πρόκληση των επιθέσεων εξόρυξης δεδομένων.

**Αποθήκευση δεδομένων στο σύννεφο:** Η εξασφάλιση της ιδιωτικότητας στο σύννεφο δεδομένου ότι υλοποιείται από τρίτες υπηρεσίες cloud, ανοίγει ένα άλλο φάσμα επιθέσεων για την αντιμετώπιση των οποίων η επιχείρηση δεν έχει πολλές επιλογές. Η επιχείρηση θα πρέπει να λάβει υπόψη της τα πρωτόκολλα ασφαλείας που διαφέρουν οι διάφορες υπηρεσίες cloud μεταξύ των διαφορετικών παρόχων. Ένας ακόμη τρόπος είναι να υιοθετήσει διάφορα βιομηχανικά πρότυπα και πλαίσια και οδηγίες ασφάλειας. Η επιχείρηση μπορεί να εξασφαλίσει ότι τα δεδομένα που αποθηκεύονται στις IIoT συσκευές, αποθηκεύονται με ασφάλεια. Ακόμα σχετικά με την αποθήκευση θα μπορούσε η πληροφορία να αποθηκεύεται με τη μορφή του K-Anonymity (Sweeney, 2002) όπου είναι εφικτό και απαραίτητο. Χρησιμοποιώντας αυτή την τεχνική, τα δεδομένα επεξεργάζονται με τρόπο ώστε κάθε άτομο να είναι αδιάκριτο από τουλάχιστον k-1 άλλα άτομα στο σύνολο δεδομένων. Αυτό σημαίνει ότι οι πληροφορίες για κάθε πρόσωπο δεν μπορούν να διακριθούν από τουλάχιστον k-1 άτομα, διατηρώντας έτσι την ιδιωτικότητα. Άλλες παρόμοιες μέθοδοι είναι οι L-diversity (Kifer, 2006) και T-closeness (Li, 2007).

**Ευαίσθητα δεδομένα:** Είναι σημαντικό η επιχείρηση και ο οργανισμός να διαφυλάξει τα προσωπικά δεδομένα που παίρνει από το ανθρώπινο δυναμικό του σύμφωνα με τους κανονισμούς του GDPR. Τα δεδομένα που συλλέγονται θα πρέπει να είναι διάφανα στους εργαζομένους, με τη σύμφωνη γνώμη τους και να περιορίζονται στα ελάχιστα δυνατά και απολύτως απαραίτητα για τους σκοπούς της επιχείρησης. Τα αχρείατα δεδομένα θα πρέπει να διαγράφονται και θα πρέπει να υπάρχουν διασφαλίσεις στη πρόσβαση των δεδομένων από τους διαχειριστές. Στην περίπτωση που η διαφάνεια των δεδομένων δεν μπορεί να εφικτή για λόγους που εξυπηρετούν την απόκρυψη πληροφοριών του εργοδότη στον εργαζόμενο, θα πρέπει να υπάρχει ειδικό συμφωνητικό μεταξύ των δύο πλευρών που να καλύπτει νομικά την αντίστοιχη διαχείριση αυτών. Ευαίσθητα δεδομένα για την υγεία των εργαζομένων όπως χρόνια προβλήματα υγείας θα πρέπει να αποφεύγονται και η συλλογή τους θα πρέπει να γίνεται μόνο εφόσον υπάρχει πολύ σοβαρός λόγος. Όλες οι συσκευές παρακολούθησης που χρησιμοποιεί η επιχείρηση θα πρέπει να είναι φανερές και το προσωπικό ενήμερο για τη θέση που είναι τοποθετημένες, καθώς και για την ικανότητα τους να συλλέγουν δεδομένα.

### 5.3 Ασφάλεια και Ιδιωτικότητα στο IIoT

Η ασφάλεια και η ιδιωτικότητα είναι αλληλεξαρτώμενες έννοιες όπως συζητήθηκε στο Κεφάλαιο 4. Εάν δεν εφαρμοστούν η πλειοψηφία από τις αρχές της ασφάλειας, τότε η προστασία των προσωπικών δεδομένων είναι αβέβαιη. Δεδομένη της πολυπλοκότητας διαχείρισης του IIoT, η

διατήρηση της ασφάλειας και της ιδιωτικότητας σε αυτά τα περιβάλλοντα είναι μία από τις μεγαλύτερες προκλήσεις του Industry 4.0. Ο εντοπισμός των απαιτήσεων για την προστασία των προσωπικών δεδομένων είναι απαραίτητη προϋπόθεση για τη δημιουργία μίας σειράς από κανόνων και μεθόδων που θα πρέπει να λαμβάνει υπόψη του κάθε περιβάλλον του IIoT. Το υποθετικό σενάριο που χρησιμοποιήθηκε, φανέρωσε πολλές από τις απαιτήσεις για την προστασία της ιδιωτικότητας σε περιβάλλοντα IIoT, ωστόσο ένα και μοναδικό παράδειγμα δεν αρκεί για να καλύψει όλες τις απαιτήσεις που δημιουργούνται από το σχεδιασμό αυτών των περιβαλλόντων. Οι καλές πρακτικές, που συζητήθηκαν μπορούν να εμπλουτιστούν προκειμένου να δημιουργηθεί ένας πλήρης οδηγός με μεθόδους και κανόνες που πρέπει να τηρούν τα Βιομηχανικά περιβάλλοντα Διαδικτύου των Πραγμάτων για την προστασία της ιδιωτικότητας. Μία επιχείρηση προκειμένου να προστατευτεί από τις εξωτερικές απειλές, θα πρέπει πρώτα να περιορίσει τις εσωτερικές απειλές. Η διαρροή των πληροφοριών μπορεί να γίνει από εσωτερικά, από τον ίδιο τον οργανισμό, δηλαδή από τους ίδιους τους εργαζομένους. Ένας τέτοιος τύπος διαρροής μπορεί να προκύψει είτε από αμέλεια είτε από ενδεχόμενο δόλο. Τρανταχτό παράδειγμα είναι οι αποκαλύψεις του Έντουαρντ Σνόουντεν. Συνεπώς, οι πρόσβαση στους φυσικούς και ψηφιακούς χώρους θα πρέπει να γίνεται από εξουσιοδοτημένα άτομα και θα πρέπει να υπάρχουν διαφορετικές διαβαθμίσεις ανάλογα με τα καθήκοντα και την αξιοπιστία του κάθε εργαζομένου. Ακόμα, θα πρέπει να υπάρχουν αποτρεπτικά μέτρα που να καθιστούν δύσκολη και αδύνατη την κλοπή πληροφοριών. Τέτοιου είδους μέτρα, θα μπορούσε να είναι, η συστηματική παρακολούθηση του δικτύου, η απαγόρευση εξόδου ηλεκτρονικών μέσων αποθήκευσης από τους εργαζομένους ή και χρήση έξυπνων τηλεφώνων μέσα σε συγκεκριμένους χώρους. Επιπρόσθετα, θα πρέπει να υπάρχει διαφάνεια σχετικά με τις πληροφορίες και τα δεδομένα των εργαζομένων που συλλέγονται. Οι εργαζόμενοι έχουν δικαίωμα να είναι ενήμεροι για την διακίνηση των δεδομένων τους και την αξιοποίηση αυτών. Στον παρακάτω πίνακα συνοψίζονται οι απαιτήσεις προστασίας της ιδιωτικότητας σε περιβάλλοντα του IIoT και ενέργειες που πρέπει να γίνουν για να διαφυλαχθεί η ιδιωτικότητα.

**Table 5 Απαιτήσεις προστασίας της ιδιωτικότητας σε IIoT περιβάλλοντα**

| Απαιτήσεις                 | Περιγραφή                                                                                                                                                                                       |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Αυστηρός έλεγχος πρόσβασης | Η πρόσβαση στα δεδομένα και στις πλατφόρμες θα πρέπει να γίνεται με αυθεντικοποίηση και τη διαδικασία επαλήθευσης ταυτότητας του χρήστη. Μόνο εξουσιοδοτημένα άτομα θα πρέπει να έχουν πρόσβαση |

|                                  |                                                                                                                                                                                                                                                                                   |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Πολιτικές ελέγχου εισόδου/εξόδου | Αναφορά στα λεγόμενα «access control policies» που οφείλει να έχει μια επιχείρηση. Θα πρέπει να θεσπιστούν κανόνες και διαδικασίες που θα ορίζουν πως και ποιος εργαζόμενος μπορεί να έχει πρόσβαση σε δεδομένα και πόρους εντός του οργανισμού                                   |
| Διαχείριση αποθήκευσης δεδομένων | Τα δεδομένα θα πρέπει να αποθηκεύονται σε βάσεις στις οποίες μπορούν τηρούνται πρακτικές όπως η K-Anonymity και η χρήση αυτών να γίνεται κοντά στις πηγές παραγωγής τους (πχ αισθητήρες)                                                                                          |
| Ασφάλεια επικοινωνίας            | Η επικοινωνία μεταξύ των μηχανημάτων και συσκευών θα πρέπει να γίνεται μέσα από κρυπτογραφημένα κανάλια                                                                                                                                                                           |
| Πρόσβαση σε χώρους               | Κάθε εργαζόμενος, θα πρέπει να έχει πρόσβαση σε συγκεκριμένους φυσικούς χώρους, στους οποίους εργάζεται.                                                                                                                                                                          |
| Εκπαίδευση εργαζομένων           | Οι εργαζόμενοι θα πρέπει να είναι εκπαιδευμένοι για τους κινδύνους ασφαλείας και τις απειλές του διαδικτύου όπως επιθέσεις τύπου Phishing                                                                                                                                         |
| Ενημέρωση εργαζομένων            | Οι εργαζόμενοι θα πρέπει να είναι ενήμεροι για τις απειλές για την ιδιωτικότητα που σχετίζονται με τη χρήση των τεχνολογιών IIoT όπως τι είδους δεδομένα καταγράφονται από συσκευές που φέρουν πάνω τους π.χ. έξυπνα ρολόγια και πως αυτά τα δεδομένα δύναται να χρησιμοποιηθούν. |
| Φυσική ασφάλεια συσκευών         | Συσκευές αποθήκευσης και παραγωγής ευαίσθητων δεδομένων θα πρέπει να βρίσκονται σε μη προσβάσιμα μέρη, ώστε οποιαδήποτε ενέργεια κλοπής και αντιγραφής δεδομένων να περιορίζεται                                                                                                  |
| Καταγραφή και παρακολούθηση      | Η καταγραφή και παρακολούθηση συμβάντων δεν θα πρέπει να γίνεται με γνώμονα την κατασκοπεία. Κλειστά κυκλώματα                                                                                                                                                                    |

|                                         |                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                         | ασφαλείας θα πρέπει να είναι τοποθετημένα σε περιοχές όπου υπάρχει απόλυτη ανάγκη.                                                                                                                                                                                                                                                                                               |
| Συμμόρφωση με τις διεθνείς προδιαγραφές | Οι επιχειρήσεις που χρησιμοποιούν τεχνολογίες IIoT θα πρέπει να εφαρμόζουν τις απαιτήσεις ασφαλείας και ιδιωτικότητας που καθορίζονται από τις νομοθεσίες όπως το GDPR                                                                                                                                                                                                           |
| Προστασία δικτύου                       | Τείχη προστασίας και συνεχής παρακολούθηση του δικτύου θα βοηθήσουν στην έγκαιρη ανίχνευση απειλών                                                                                                                                                                                                                                                                               |
| Διαχείριση ταυτοτήτων και πρόσβασης     | Identity and Access Management (IAM) δομές θα διαβεβαιώνουν ποιος υπάλληλος έχει δικαίωμα πρόσβασης στις πηγές πληροφοριών                                                                                                                                                                                                                                                       |
| Ασφάλεια εφαρμογών                      | Οι εφαρμογές που χρησιμοποιεί η επιχείρηση θα πρέπει να είναι έμπιστες και ασφαλείς, χωρίς κακόβουλα λογισμικά για να αποφευχθεί η βιομηχανική κατασκοπεία και οποιαδήποτε διαρροή δεδομένων σε τρίτους. Πρότυπα όπως ISO/IEC27001 <sup>13</sup> και ISO/IEC 15408 <sup>14</sup> διασφαλίζουν ότι οι εφαρμογές τηρούν διάφορα πρωτόκολλα κατά την παραγωγή των προγραμμάτων τους |

<sup>13</sup> <https://www.iso.org/standard/88435.html>

<sup>14</sup> <https://www.iso.org/standard/72891.html>



## ΚΕΦΑΛΑΙΟ 6: ΣΥΜΠΕΡΑΣΜΑΤΑ

### 6.1 Οδηγίες για την δημιουργία ασφαλών συστημάτων

Για τον σχεδιασμό ενός ασφαλούς και αξιόπιστου περιβάλλοντος IIoT, ειδικά σε εφαρμογές όπως οι βιομηχανικές κλινικές, ο αναλυτής μηχανικός ασφάλειας μπορεί να ακολουθήσει τις παρακάτω γενικές οδηγίες ή βήματα, που βασίζονται κυρίως σε όσα αναλύθηκαν στα Κεφάλαια 4 και 5 του εγγράφου:

#### Βήμα 1 – Καθορισμός Απαιτήσεων Ασφάλειας και Ιδιωτικότητας

Σε πρώτο στάδιο, θα πρέπει να γίνει ανάλυση των νομικών και κανονιστικών απαιτήσεων (GDPR, HIPAA <sup>15</sup> κ.λπ.), ώστε να ενσωματωθούν στον σχεδιασμό εξ' αρχής. Ακόμη, πρέπει να σχεδιαστεί ένα σύστημα ελέγχου ταυτότητας και διαχείρισης πρόσβασης (IAM) για τον έλεγχο πρόσβασης στα δεδομένα και στα συστήματα. Ο καθορισμός ρόλων και εξουσιοδοτήσεων θα βοηθήσει στον περιορισμό της πρόσβασης μόνο σε εξουσιοδοτημένους χρήστες, μειώνοντας την πιθανότητα μη εξουσιοδοτημένης πρόσβασης ή παραβίασης. Κρίσιμα πόστα όπως διαχειριστές (IT και ασφάλειας), ιατρικό προσωπικό, τεχνικό προσωπικό, εξωτερικοί συνεργάτες θα πρέπει να διαχωριστούν. Επίσης, θα πρέπει να ληφθεί υπόψη η δυνατότητα πολυπαραγοντικής ταυτοποίησης, ώστε να αποφευχθούν επιθέσεις προσποίησης ταυτότητας.

Μερικές βοηθητικές ερωτήσεις για το σχεδιασμό των δεδομένων που θα διαχειρίζεται το IIoT και τη δημιουργία των ρόλων μπορούν να είναι: «Τι δεδομένα συλλέγονται;», «Πώς αποθηκεύονται και πώς διαμοιράζονται;», «Ποιες είναι οι ανάγκες ιδιωτικότητας για κάθε τύπο δεδομένων;», «Ποιοι χρήστες χρειάζονται πρόσβαση σε ποια δεδομένα και γιατί;», «Τι περιορισμοί πρέπει να υπάρχουν για να μειωθεί η πιθανότητα εσωτερικών απειλών;», «Ποιες δραστηριότητες απαιτούν παρακολούθηση και logging;».

#### Βήμα 2 – Σχεδιασμός Αντίδρασης σε Απειλές και Διαχείριση Επιδόσεων

Σε αυτό το στάδιο, θα πρέπει να καθοριστούν τα βασικά χαρακτηριστικά του συστήματος ανίχνευσης και απόκρισης σε απειλές (SIEM<sup>16</sup>, IDS) για την έγκαιρη ανίχνευση ανωμαλιών. Υπάρχουν εργαλεία που συλλέγουν δεδομένα από διάφορες πηγές και παρέχουν ειδοποιήσεις όταν εντοπίζουν ύποπτες δραστηριότητες. Επίσης, η αρχιτεκτονική του συστήματος θα πρέπει να σχεδιαστεί, έτσι ώστε να υποστηρίζει επεκτασιμότητα και απαιτήσεις πραγματικού χρόνου, κυρίως με τη χρήση υπολογιστικού νέφους ή τεχνολογιών edge computing. Η επεκτασιμότητα του συστήματος είναι ζωτική για την προστασία δεδομένων, καθώς αποτρέπει διακοπές που

---

<sup>15</sup> HIPAA – Health Insurance Portability and Accountability Act: νόμος στις ΗΠΑ για την προστασία των προσωπικών και ιατρικών δεδομένων

<sup>16</sup> SIEM – Security Information and Event Management

μπορεί να θέσουν τα δεδομένα σε κίνδυνο. Χρησιμοποιώντας τεχνολογίες υπολογιστικού νέφους και edge computing, βελτιώνεται η διαθεσιμότητα και μειώνονται τα σημεία αποτυχίας.

Μερικές βοηθητικές ερωτήσεις για το κομμάτι της σχεδίασης συστημάτων ανίχνευσης απειλών και διαχείρισης των επιδόσεων είναι: «Ποιες είναι οι πιο πιθανές και σοβαρές απειλές για τα δεδομένα;», «Ποια τμήματα του συστήματος είναι πιο ευάλωτα;», «Ποιοι είναι οι δείκτες που θα δείξουν πιθανές επιθέσεις;», «Πόσο καλά αντέχει το σύστημα στην αύξηση των χρηστών και των δεδομένων;», «Υπάρχουν διαθέσιμα πλεονάζοντα συστήματα (redundancy) για την αποφυγή διακοπών;».

### Βήμα 3 – Επεξεργασία και Αποθήκευση με Ασφάλεια

Ο μηχανικός ασφαλείας οφείλει να επιλέξει μεθόδους ασφαλούς αποθήκευσης, που συμμορφώνονται με τις κανονιστικές απαιτήσεις, όπως η κρυπτογράφηση. Κρυπτογραφημένες βάσεις δεδομένων, όπως Microsoft SQL Server ή MongoDB Atlas, που υποστηρίζουν κρυπτογράφηση τόσο σε μεταφορά όσο και σε στατική αποθήκευση (encryption at rest) θωρακίζουν το σύστημα από απειλές όπως SQL injection. Επιπρόσθετα, πρέπει να ασφαλιστούν και να προστατευτούν τα δεδομένα κατά τη μεταφορά τους. Η εφαρμογή πρωτοκόλλων όπως το TLS/SSL και VPN μπορούν να διασφαλίσουν τη προστασία των δεδομένων από πιθανές παραβιάσεις.

Μερικές βοηθητικές ερωτήσεις πάνω στην επεξεργασία, αποθήκευση και μεταφορά των δεδομένων με ασφάλεια είναι: «Ποια δεδομένα πρέπει να κρυπτογραφούνται;», «Πώς γίνεται η διαχείριση των κλειδιών κρυπτογράφησης;», «Πώς γίνεται η διαδικασία της εφεδρείας (backup) και πώς αυτή προστατεύεται;», «Πώς διασφαλίζεται η προστασία των δεδομένων από υποκλοπές κατά τη μεταφορά;», «Υπάρχουν κατάλληλα πιστοποιητικά ασφαλείας για το TLS/SSL;».

### Βήμα 4 – Διαχείριση και Βελτιστοποίηση Πρωτοκόλλων Συνδεσιμότητας

Ανάλογα με το περιβάλλον του IIoT, πρέπει να επιλεγθούν ασύρματες ή ενσύρματες τεχνολογίες (π.χ., WiFi, Ethernet) και βιομηχανικά πρωτόκολλα επικοινωνίας που θα χρησιμοποιηθούν. Επιπλέον, η διασύνδεση των συσκευών μεταξύ τους, θα πρέπει να γίνεται με ασφαλή πρωτόκολλα όπως το MQTT με TLS για IoT εφαρμογές, ή το Modbus TCP με κρυπτογράφηση για βιομηχανικές συνδέσεις. Κατά το σχεδιασμό του δικτύου, πρέπει να προβλεφθεί η αυξανόμενη κίνηση και να υποστηρίζονται οι απαιτήσεις ασφαλείας, ελαχιστοποιώντας τα ευπαθή σημεία που θα μπορούσαν να εκτεθούν σε επιθέσεις. Υπάρχουν λογισμικά όπως το Cisco Secure Network Analytics για τη συνεχή παρακολούθηση και τον έλεγχο των επικοινωνιών του δικτύου.

Μερικές βοηθητικές ερωτήσεις για τη διαχείριση της συνδεσιμότητας είναι: «Ποια πρωτόκολλα προσφέρουν ασφάλεια και ευελιξία;», «Τι ρυθμίσεις ασφαλείας υποστηρίζουν τα πρωτόκολλα που χρησιμοποιούνται;», «Υπάρχουν δυνατότητες για έλεγχο ταυτότητας και εξουσιοδότηση;»,

«Πώς διασφαλίζεται ότι το δίκτυο είναι ανθεκτικό σε κυβερνοεπιθέσεις;», «Υπάρχουν μηχανισμοί τμηματοποίησης (segmenting) για την απομόνωση των κρίσιμων συσκευών IIoT;».

#### Βήμα 5 – Συντήρηση και Πρόληψη

Είναι απαραίτητο να καθοριστούν διαδικασίες για την προληπτική και τη διαγνωστική συντήρηση του IIoT εξοπλισμού, ώστε να μειωθούν οι απρογραμμάτιστες βλάβες. Δεδομένα από ειδικούς αισθητήρες τοποθετημένους και ενσωματωμένους στα μηχανήματα και μέσα της βιομηχανίας, μπορούν να αξιοποιηθούν από αλγορίθμους για την έγκαιρη πρόγνωση βλαβών. Παράλληλα μπορούν να σχεδιαστούν εργαλεία για την παρακολούθηση της απόδοσης του εξοπλισμού και του δικτύου, ώστε να βελτιστοποιούνται οι πόροι σε πραγματικό χρόνο.

Μερικές βοηθητικές ερωτήσεις είναι: «Ποια δεδομένα πρέπει να παρακολουθούνται για την πρόληψη βλαβών;», «Πόσο συχνά πρέπει να γίνονται έλεγχοι και συντήρηση;», «Υπάρχει σχέδιο για την αντικατάσταση ή επισκευή εξοπλισμού;», «Ποιες μετρικές απόδοσης πρέπει να παρακολουθούνται;», «Υπάρχουν αποθέματα και εφεδρείες για αποτροπή του downtime;».

#### Βήμα 6 – Εκπαίδευση και Βελτίωση

Είναι δυνατό να δημιουργηθεί ένα πρόγραμμα συνεχούς επίβλεψης και βελτίωσης των συστημάτων και των διαδικασιών ασφαλείας για να παρακολουθείτε και να βελτιώνεται η ασφάλεια μακροπρόθεσμα. Παράλληλα, η εκπαίδευση εξασφαλίζει ότι οι εργαζόμενοι κατανοούν και εφαρμόζουν πρακτικές ασφαλείας, προφυλάσσοντας τα δεδομένα από λάθη (πχ επιθέσεις τύπου phishing). Εκπαιδευτικά σεμινάρια και εργαλεία εκπαίδευσης σε θέματα ασφαλείας θα αφυπνίσουν τους εργαζομένους πάνω σε θέματα ασφαλείας. Η εκπαίδευση θα πρέπει να εστιάζει στην διαχείριση ευαίσθητων δεδομένων και την αντίδραση σε περιστατικά ασφαλείας.

Μερικές βοηθητικές ερωτήσεις είναι: «Ποιες αναφορές είναι απαραίτητες για τη συνεχή βελτίωση;», «Υπάρχει σχέδιο για περιοδική αναθεώρηση των πολιτικών ασφαλείας;», «Ποιες διαδικασίες πρέπει να αναβαθμιστούν για βελτιωμένη ασφάλεια;», «Το προσωπικό γνωρίζει τις ευθύνες του στη διαχείριση δεδομένων;», «Είναι ενημερωμένο για τις τελευταίες απειλές;», «Τι μπορεί να γίνει ώστε η εκπαίδευση να είναι συνεχής;».

### **6.2 Συζήτηση και μελλοντική εργασία**

Η παρούσα εργασία πραγματεύεται ένα από τα πλέον σημαντικά ζητήματα της σύγχρονης βιομηχανικής τεχνολογίας, δηλαδή την προστασία δεδομένων και την ασφάλεια στο περιβάλλον του Βιομηχανικού Διαδικτύου των Πραγμάτων (IIoT). Καθώς η τεχνολογία IIoT ενσωματώνεται όλο και περισσότερο στον βιομηχανικό τομέα, οι απειλές αυξάνονται και καθίσταται αναγκαία η ανάπτυξη προσεγγίσεων που διασφαλίζουν την ασφάλεια και την αξιοπιστία των συστημάτων. Η καταγραφή των πραγματικών και αυξανόμενων απειλών που αντιμετωπίζουν τα περιβάλλοντα IIoT, αποδεικνύουν ότι τα παραδοσιακά μέτρα ασφαλείας δεν αρκούν. Πραγματικές επιθέσεις και περιστατικά ασφαλείας που έχουν επηρεάσει βιομηχανίες σε διάφορους τομείς, όπως η παραγωγή, η διαχείριση ενέργειας και η μεταφορά,

υπογραμμίζουν τη σημασία της ασφάλειας στα περιβάλλοντα IIoT και φανερώσουν ότι η ανάγκη είναι υπαρκτή στη σύγχρονη εποχή. Για παράδειγμα, επιθέσεις DDoS μπορούν να θέσουν εκτός λειτουργίας συσκευές και να επιφέρουν σημαντικές καθυστερήσεις στη βιομηχανική παραγωγή, κυβερνοεπιθέσεις τύπου ransomware έχουν στοχοποιήσει συστήματα ελέγχου, εκβιάζοντας οργανισμούς για να αποκτήσουν εκ νέου πρόσβαση στα δεδομένα τους με το αντίστοιχο αντίτιμο. Ακόμα, απειλές από κακόβουλους εσωτερικούς χρήστες παραμένουν μια σοβαρή πρόκληση, ιδίως όταν δεν υπάρχει κατάλληλη διαχείριση ταυτοτήτων και πρόσβασης. Παρακάτω, ανακεφαλαιώνονται διάφορα σημεία από την παρούσα μελέτη και δίνονται κατευθύνσεις για μελλοντικές εργασίες.

### Οργάνωση και Δομή του IIoT

Η παρούσα εργασία ασχολήθηκε με την κατανόηση του τρόπου με τον οποίο είναι οργανωμένο το οικοσύστημα IIoT και πώς αυτό διαφοροποιείται από τις παραδοσιακές τεχνολογίες IoT. Οι τεχνολογίες του IIoT συνδυάζουν συσκευές, αισθητήρες, διαχειριστικά συστήματα και εργαλεία ανάλυσης δεδομένων σε ένα ενιαίο οικοσύστημα που επιτρέπει τον έλεγχο και τη βελτιστοποίηση των βιομηχανικών διαδικασιών σε πραγματικό χρόνο. Βασικές έννοιες που βοηθούν τους αναλυτές να κατανοήσουν την πολυπλοκότητα του IIoT όπως είναι το οικοσύστημα IIoT και το Industry 4.0 αλλά και άλλοι όροι που πολλές φορές συγχέονται αναλύθηκαν σε προηγούμενα κεφάλαια.. Πέρα από τις τεχνικές προδιαγραφές, η μελέτη επιχείρησε να προσδιορίσει και να ξεκαθαρίσει τους όρους και τις τεχνολογικές απαιτήσεις που καθορίζουν τη λειτουργία των IIoT συστημάτων. Ο προσδιορισμός αυτών των εννοιών και των παραμέτρων είναι ζωτικός για την υιοθέτηση ενός κοινού πλαισίου που θα επιτρέψει στους αναλυτές να προσεγγίσουν την ασφάλεια πιο αποτελεσματικά.

### Ανάλυση Απαιτήσεων Ασφαλείας

Η εργασία εισήγαγε δύο διαφορετικά σενάρια ασφάλειας, τα οποία αντανakλούν τις διαφορετικές απαιτήσεις και ευπάθειες των βιομηχανικών συστημάτων IIoT. Το πρώτο σενάριο αφορούσε ένα σταθερό περιβάλλον δεδομένων με λιγότερες μεταβλητές και περιορισμένες ανάγκες διασυνδεσιμότητας. Το δεύτερο σενάριο ασχολείται με πιο δυναμικές συνθήκες, όπου οι ανάγκες των δεδομένων και οι λειτουργίες των συσκευών είναι περισσότερο ευέλικτες και απαιτούν προσαρμοσμένες στρατηγικές ασφάλειας. Χρησιμοποιήθηκαν διαγράμματα use cases της UML και οντοτήτων σχέσεων για την περιγραφή και κατανόηση των σεναρίων. Ακόμη, έγινε ανάλυση των δυναμικών σχέσεων των οντοτήτων, εφαρμογή της μεθοδολογίας STRIDE και χρήση του Microsoft Threat Modeling Tool, εκμαίευση των απαιτήσεων των παραπάνω σεναρίων και συζητήθηκαν τα δυνατά μέτρα για την προστασία των συστημάτων.

### Κατευθύνσεις και Οδηγίες για Αναλυτές

Η παρούσα μελέτη παρουσιάζει ένα δομημένο σύνολο οδηγιών και κατευθύνσεων για την υλοποίηση ασφαλών IIoT συστημάτων. Το τμήμα αυτό της εργασίας είναι ιδιαίτερα χρήσιμο για τους αναλυτές ασφάλειας, καθώς παρέχει πρακτικές προτάσεις και συγκεκριμένα βήματα που

μπορούν να εφαρμοστούν στο σχεδιαστικό κομμάτι ενός περιβάλλον ΙΙoT. Μέσα από πίνακες, ερωτήσεις και βήματα, ο αναλυτής μπορεί να βοηθηθεί στην ανάλυση του και να συμβουλευτεί την παρούσα εργασία.

#### Μελλοντικές Προοπτικές

Η εργασία καταλήγει στο συμπέρασμα ότι η ασφάλεια στα περιβάλλοντα ΙΙoT είναι μια πολυδιάστατη πρόκληση που απαιτεί τη συνεργασία τεχνολογίας, διαδικασιών και ανθρώπων. Η επιτυχής υλοποίηση των στρατηγικών που προτάθηκαν μπορεί να δημιουργήσει ένα ανθεκτικό και ασφαλές περιβάλλον, διασφαλίζοντας τα δεδομένα και τις διαδικασίες από τις σύγχρονες απειλές. Η ανάγκη για συνεχή προσαρμογή στις τεχνολογικές αλλαγές και στις νέες μορφές επιθέσεων καθιστά σαφές ότι η ασφάλεια των δεδομένων στο ΙΙoT θα είναι ένα διαρκές αντικείμενο εξέλιξης και προσοχής. Κάθε περιβάλλον ΙΙoT έχει τη δική του πολυπλοκότητα και τις δικές του ανάγκες, οπότε οι στρατηγικές και ο σχεδιασμός για την ασφάλεια και ιδιωτικότητα του οφείλει να προσαρμόζεται σε αυτές. Με τις οδηγίες της παρούσας εργασίας δύναται να δημιουργηθεί ένα checklist για αναλυτές που θα τους βοηθάει στο σχεδιασμό και στη συνέχεια θα μπορούσε να αξιολογηθεί και να τροποποιηθεί αφού εφαρμοστεί και δοκιμαστεί σε πιο ρεαλιστικά σενάρια. Παράλληλα, η ανάλυση που έγινε στην συγκεκριμένη εργασία, αποτελεί αντικείμενο μελέτης που μπορεί να συμβάλλει μελλοντικά στη δημιουργία ολοκληρωμένων πλαισίων συμμόρφωσης με κανονισμούς όπως το GDPR.

## ΒΙΒΛΙΟΓΡΑΦΙΑ

- Industrial Technology*. (2024). Ανάκτηση από advancedtech: <https://www.advancedtech.com/blog/iiot-vs-industry-4-0/>
- Behnke, I. &. (2023). Real-Time Performance of Industrial IoT Communication Technologies. *IEEE Internet of Things Journal*. doi:<https://doi.org/10.1109/JIOT.2023.3332507>
- Bong, N. (2022, 4 26). Ανάκτηση από progressiveautomations: <https://www.progressiveautomations.com/blogs/news/the-evolution-of-automation>
- Cai, Z. &. (2020). A private and efficient mechanism for data uploading in smart cyber-physical systems. *IEEE Transactions on Network Science and Engineering* (σσ. (2) 766-775). IEEE.
- cisa.gov. (2021, july 21). Ανάκτηση από cisa.gov: <https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01>
- cloudflare. (2017, 12 14). Ανάκτηση από blog.cloudflare: <https://blog.cloudflare.com/inside-mirai-the-infamous-iiot-botnet-a-retrospective-analysis>
- Consortium, I. I. (2018). *Introduction to edge computing in IIoT*. doi:IIC:WHT:IN24
- Desjardins, J. (2018, 1 9). *Timeline: The History of the Industrial Internet of Things*. Ανάκτηση από [https://www.visualcapitalist.com/timeline-industrial-internet-things/#google\\_vignette](https://www.visualcapitalist.com/timeline-industrial-internet-things/#google_vignette)
- desouttertools. (2024, 4 1). Ανάκτηση από <https://www.desouttertools.com/your-industry/news/503/industrial-revolution-from-industry-1-0-to-industry-4-0>
- Dian, F. a. (2020). *IoT Use Cases and Technologies*. British Colombia IT. doi:ISBN 978-1-990132-00-1
- Drosatos, G. R. (2020). Privacy-preserving solutions in the Industrial Internet of Things. *16th International Conference on Distributed Computing in Sensor Systems (DCOSS)*. doi:doi:10.1109/dcoss49796.2020.00044
- E. Sisinni, A. S. (2018). Industrial internet of things: Challenges, opportunities, and directions. *IEEE Transactions on Industrial Informatics* (σσ. 14(11), 4724–4734). IEEE .
- europa.eu. (n.d.). Ανάκτηση από europa.eu: [https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index\\_en.htm#:~:text=The%20GDPR%20sets%20out%20detailed,people%20living%20in%20the%20EU.](https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_en.htm#:~:text=The%20GDPR%20sets%20out%20detailed,people%20living%20in%20the%20EU.)

- Fowler, G. A. (2022). I tried to read all my app privacy policies. It was 1 million words. *The Washington Post*.
- Gai, Y. W. (2019). Differential Privacy-Based Blockchain for Industrial Internet-of-Things. *IEEE Transactions on Industrial Informatics*.
- geeksforgeeks. (2024, 8 9). Ανάκτηση από geeksforgeeks:  
<https://www.geeksforgeeks.org/what-is-vpn-and-how-it-works/>
- Gillis, A. S. (n.d.). *TechTarget*. Ανάκτηση από  
<https://www.techtarget.com/iotagenda/definition/Industrial-Internet-of-Things-IIoT>
- Gong C., L. F. (2020). Intelligent cooperative edge computing in the internet of things. *IEEE Internet of Things Journal*, 1-1.
- Hui, H. Z. (2020). A novel secure data transmission scheme in industrial internet of things. *China Communications*, 17(1), 73-88.
- Huo, Y. M. (2020). An Overview of Privacy Preserving Schemes for Industrial Internet of Things. *China Communication*, 17(10), 1-18.
- IoTNow. (n.d.). *5G for industrial internet of things: Opportunities and challenges*. Ανάκτηση από IoTNow: <https://www.iot-now.com/2023/07/31/133650-5g-for-industrial-internet-of-things-opportunities-and-challenges/>
- Jaidka, H. e. (2020). Evolution of IoT to IIoT: Applications & Challenges. *SSRN Electronic Journal*. doi:<https://doi.org/10.2139/ssrn.3603739>
- Kifer, D. a. (2006). l-Diversity: Privacy Beyond k-Anonymity. *In ICDE*, 24.
- kodiko.gr. (2019). *kodiko.gr*. Ανάκτηση από  
<https://www.kodiko.gr/nomothesia/document/552084/nomos-4624-2019>
- Kumar, J. S. (2014). A survey on internet of things: Security and privacy issues. *International Journal of Computer Applications*, 90(11).
- KUSHNER, D. (2013, FEB 26 ). *the-real-story-of-stuxnet*. Ανάκτηση από spectrum.ieee:  
<https://spectrum.ieee.org/the-real-story-of-stuxnet>
- Li, N. a. (2007). t-Closeness: Privacy Beyond k-Anonymity and l-Diversity. *23rd International Conference on Data Engineering (ICDE 2007)*.
- LTE Cellular Technology—The Future of the IIoT*. (2016, 12 6). Ανάκτηση από moxa:  
<https://moxa.com/en/articles/lte-cellular-technology-the-future-of-the-iiot>
- Mao J., Z. Y. (2017). A position-aware Merkle tree for dynamic cloud data integrity verification. *Soft Computing*, 21(8), 2151-2164.

- mckinsey. (2023, 7 12). Ανάκτηση από <https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-digital-twin-technology>
- moxa. (2016, 12 6). *LTE Cellular Technology—The Future of the IIoT*. Ανάκτηση από moxa: <https://moxa.com/en/articles/lte-cellular-technology-the-future-of-the-iiot>
- Newth, A. (2011). *InfoBloom*. Ανάκτηση October 2011, από <https://www.infobloom.com/what-is-an-experience-good.htm#comments>
- opcfoundation. (n.d.). Ανάκτηση από opcfoundation: <https://opcfoundation.org/about/opc-technologies/opc-ua/>
- Pfleeger, C. P. (2015). *Security in Computing* (5th εκδ.). Prentice Hall.
- S., N. (2024, 1 11). *SSL vs TLS key differences*. Ανάκτηση από cloudpanel: <https://www.cloudpanel.io/blog/ssl-vs-tls-certificates/>
- Sadeghi, A.-R. W. (2015). Security and privacy challenges in industrial internet of things. *Proceedings of the 52nd Annual Design Automation Conference on* . doi:doi:10.1145/2744769.2747942
- Shi W., C. J. (2016). Edge computing: Vision and challenges. *IEEE Internet of Things Journal* (σσ. 3(5), 637- 646). IEEE .
- Snowden, E. (2019). *Permanent record*. Metropolitan Books.
- Subramanyan, R. (2024, 4 5). *5 Benefits of Using MQTT for IIoT in Tracking and Analyzing Unplanned Manufacturing Downtime*. Ανάκτηση από hivemq: <https://www.hivemq.com/blog/5-benefits-mqtt-iiot-analyzing-unplanned-manufacturing-downtime/>
- Suman, M. J. (2021). Significance of sensors for industry 4.0: Roles, capabilities, and applicationsSensors International. *Sensors International*.
- supplychain. (2024, 1 1). *supplychaingamechanger*. Ανάκτηση από <https://supplychaingamechanger.com/industry-4-0-ecosystem-infographic/>
- Sweeney, L. (2002). k-ANONYMITY: A MODEL FOR PROTECTING PRIVACY. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*.
- Tasmiha Khan, M. G. (2024, 4 2). *What is a green data center?* Ανάκτηση από <https://www.ibm.com/topics/green-data-center>
- Team, E. C. (2024, 9 1). Ανάκτηση από edrawsoft: <https://www.edrawsoft.com/er-diagram-symbols.html>



- Terzo, G. (2011). *WiseGeek*. Ανάκτηση 2011, από <https://www.wise-geek.com/what-is-a-search-good.htm>
- Warren S, Brandeis L. (1890). The Right to Privacy. *Harvard Law Review*, 4, 193.
- wemakeiot. (n.d.). *wemakeiot*. Ανάκτηση από <https://www.wemakeiot.com/importance-modbus-iot/>
- Yu, L. S. (2017). CoRE: cooperative end-to-end traffic redundancy elimination for reducing cloud bandwidth cost. *IEEE Transactions on Parallel and Distributed Systems* (σσ. 28(2), 446-461). IEEE .
- Yu, W. D. (2020). A global manufacturing big data ecosystem for fault detection in predictive maintenance. *IEEE Transactions on Industrial Informatics* (σσ. 16(1), 183-192). IEEE .
- Zheng, X. &. (2020). Privacy-preserved data sharing towards multiple parties in industrial IoTs. *IEEE Journal on Selected Areas in Communications*, 38(5), 968-979.
- Zheng, X. C. (2018). Data linkage in smart internet of things systems: A consideration from a privacy perspective. *IEEE Communications Magazine*, 56(9), 55-61.
- IBM. (2024, 4 19). *IBM*. Ανάκτηση από <https://www.ibm.com/topics/industry-4-0>

## ΠΑΡΑΡΤΗΜΑ Α

Στο παράρτημα αυτό απεικονίζονται οι συμβολισμοί που χρησιμοποιήθηκαν για τη σχεδίαση του διαγράμματος Οντοτήτων-Σχέσεων (ERD).

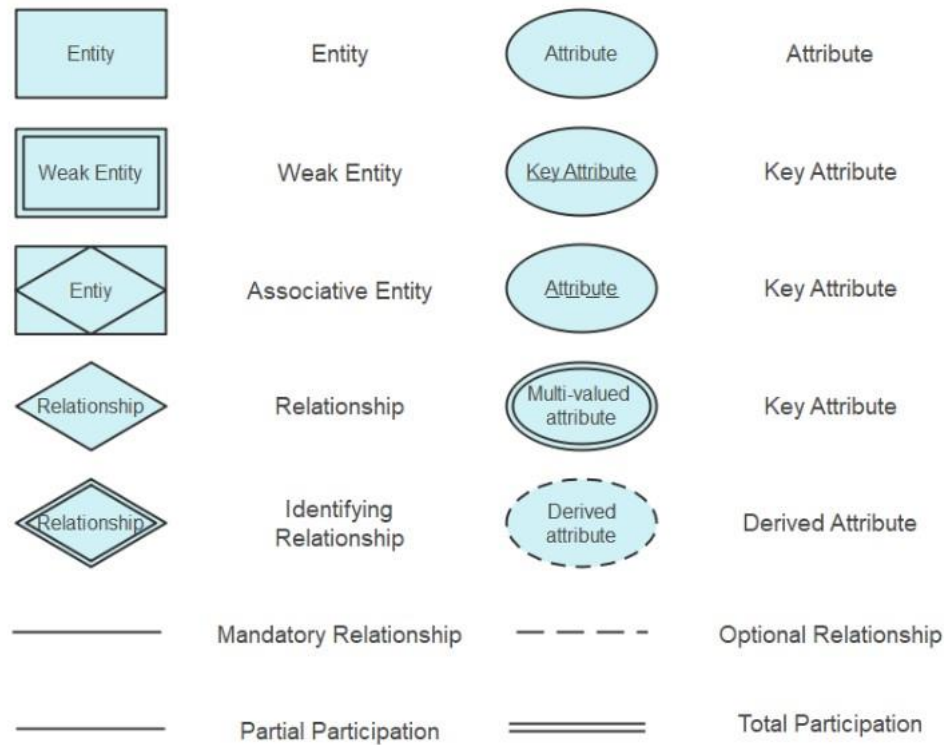


Figure 11 Συμβολισμοί Οντοτήτων-Σχέσεων

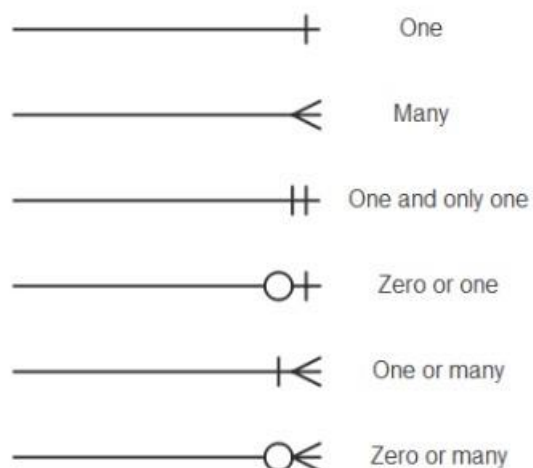


Figure 12 Συμβολισμοί καρδιναλιότητας στις οντολογικές σχέσεις