
**ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ**
**ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ**
**ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ**
**ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΗ ΒΙΟΙΑΤΡΙΚΗ**

# Το Management στην εποχή του Διαδικτύου των Πραγμάτων (Internet of Things)

## Μέρος Β: Η σημασία του Διαδικτύου των Πραγμάτων στη Διαχείριση Έργων

**Ιωάννης Κ. Επίσκοπος**

**ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ**
**Επιβλέπων**
**Κ. Γεώργιος Σταμούλης**

**Λαμία, Νοέμβριος 2018**

**UNIVERSITY OF THESSALY**

**SCHOOL OF SCIENCE**

**INFORMATICS AND COMPUTATIONAL BIOMEDICINE**

# Management in the era of Internet of Things

## Part B: The importance of Internet of Things in Project Management

**Ioannis K. Episkopos**

**Master thesis**
**Supervisor**
**Mr. George Stamoulis**

**Lamia**
**November of 2018**

**ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ**
**ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ**
**ΔΙΑΤΜΗΜΑΤΙΚΟ ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ**
**ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΗ ΒΙΟΙΑΤΡΙΚΗ**
**ΚΑΤΕΥΘΥΝΣΗ**

**«ΠΛΗΡΟΦΟΡΙΚΗ ΜΕ ΕΦΑΡΜΟΓΕΣ ΣΤΗΝ ΑΣΦΑΛΕΙΑ, ΔΙΑΧΕΙΡΙΣΗ ΜΕΓΑΛΟΥ ΟΓΚΟΥ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΠΡΟΣΟΜΟΙΩΣΗ»**

# Το Management στην εποχή του Διαδικτύου των Πραγμάτων (Internet of Things)

## Μέρος Β: Η σημασία του Διαδικτύου των Πραγμάτων στη Διαχείριση Έργων

**Ιωάννης Κ. Επίσκοπος**

**ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ**

**Επιβλέπων**
**Κ. Γεώργιος Σταμούλης**

**Λαμία, Νοέμβριος 2018**

«Υπεύθυνη Δήλωση μη λογοκλοπής και ανάληψης προσωπικής ευθύνης»

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, και γνωρίζοντας τις συνέπειες της λογοκλοπής, δηλώνω υπεύθυνα και ενυπογράφως ότι η παρούσα εργασία με τίτλο [«τίτλος εργασίας»] αποτελεί προϊόν αυστηρά προσωπικής εργασίας και όλες οι πηγές από τις οποίες χρησιμοποίησα δεδομένα, ιδέες, φράσεις, προτάσεις ή λέξεις, είτε επακριβώς (όπως υπάρχουν στο πρωτότυπο ή μεταφρασμένες) είτε με παράφραση, έχουν δηλωθεί κατάλληλα και ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή. Αναλαμβάνω πλήρως, ατομικά και προσωπικά, όλες τις νομικές και διοικητικές συνέπειες που δύναται να προκύψουν στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής.

Ο ΔΗΛΩΝ

Ημερομηνία

Υπογραφή

# Το Management στην εποχή του Διαδικτύου των Πραγμάτων (Internet of Things)

## Μέρος Β: Η σημασία του Διαδικτύου των Πραγμάτων στη Διαχείριση Έργων

**Ιωάννης Κ. Επίσκοπος**

## Τριμελής Επιτροπή:

Γεώργιος Σταμούλης, Επιβλέπων

Αθανάσιος Λουκόπουλος, Μέλος

Γεώργιος Δημητρίου, Μέλος

# Πίνακας Περιεχομένων

## Συντομογραφίες

IoT: Διαδίκτυο των πραγμάτων

VO: Εικονικά αντικείμενα

CVO: Σύνθετα εικονικά αντικείμενα

RWO: Πραγματικά αντικείμενα

ALG: Device-to-application-layer-Gateway

# Πίνακας εικόνων

# Εισαγωγή

Το Διαδίκτυο (Internet) στη σημερινή εποχή, αποτελεί παγκοσμίως ένα σύγχρονο αγαθό το οποίο χρησιμοποιείται συστηματικά από το μοντέρνο άνθρωπο στις περισσότερες πτυχές της καθημερινότητας του. Αποτελεί το πλέον βασικό βοήθημα για την απόκτηση γνώσης, εκπαίδευσης, οργάνωσης, ενημέρωσης και ψυχαγωγίας, καθώς επίσης και απαραίτητο επαγγελματικό εργαλείο. Ακολουθώντας τις απαιτήσεις αυτές, τα μέσα χρήσης του Internet έχουν εξελιχθεί ως προς τη φορητότητα και το μέγεθος τους, και έχουν προσαρμοστεί έτσι ώστε η πρόσβαση στο διαδίκτυο να είναι εφικτή από τον εκάστοτε χρήστη, ανά πάσα στιγμή ανεξαρτήτως τοποθεσίας. Η ραγδαία εξέλιξη της τεχνολογίας επιτρέπει στο χρήστη να συνδέεται από οπουδήποτε σχεδόν βρίσκεται, μέσω του σταθερού υπολογιστή, του laptop, του tablet, ακόμα και μέσω του κινητού τηλεφώνου του.

Η αναγκαιότητα για την ευκολία στη χρήση και την επικοινωνία από απόσταση, οδηγούν την αγορά σε μια συνεχή ανάπτυξη ιδεών κι εφαρμογών. Σχεδόν για κάθε ηλεκτρονική εφαρμογή ή προϊόν ή υπηρεσία που χρησιμοποιεί κανείς, υπάρχει και το ανάλογο barcode ή QR Code, τα οποία διαβάζονται από ειδικά code scanners, που αναγνωρίζουν τις ετικέτες (tags) που είναι συνδεδεμένες σε αυτά, με σκοπό τη βελτίωση των υπηρεσιών που καλύπτουν καθημερινές ανάγκες. Αυτή η συνδεσιμότητα των δεδομένων (data) οδηγεί στη δημιουργία ενός ατομικού ιστού μέσα στον παγκόσμιο ιστό του internet, εξελίσσοντας με τον τρόπο αυτό τη σύνδεση φυσικού και ηλεκτρονικού κόσμου.

Στα πλαίσια της συνεχούς τεχνολογικής ανάπτυξης, αντιλαμβανόμαστε πως τα καθημερινά μας αγαθά συνδέονται με data, διαβάζονται από μηχανές με αισθητήρες, συλλέγονται πληροφορίες και μας καθοδηγούν σε μια εξατομικευμένη χρήση του παγκόσμιου ιστού. Χρησιμοποιούνται όλο και περισσότερα gadgets για επαγγελματικούς και προσωπικούς σκοπούς, χτίζονται «έξυπνα σπίτια» με αισθητήρες που ρυθμίζονται ακόμα και με απομακρυσμένες εντολές, δημιουργούνται πρωτόκολλα ασφαλείας που αυτορυθμίζουν, για παράδειγμα, μια γραμμή βιομηχανικής παραγωγής. Όλα αυτά αποτελούν μέρος του Internet Of Things, που έρχεται στο τεχνολογικό μέλλον να διευκολύνει και να εξελίξει το μέσο άνθρωπο.

Αν το Internet αποτελεί μια από τις πιο σημαντικές και ισχυρές δημιουργίες στην ανθρώπινη ιστορία, τότε το Internet Of Things είναι η πιο σημαντική μετεξέλιξή του. Δικτυωμένα προϊόντα, συσκευές, αυτοκίνητα, κτίρια με ενσωματωμένα ηλεκτρονικά συστήματα, λογισμικά κι αισθητήρες, μπορούν να «επικοινωνούν» με έξυπνο τρόπο μεταξύ τους, με την προϋπόθεση της δικτύωσης. Συλλέγουν κι ανταλλάσσουν δεδομένα, και χρησιμοποιούνται

για την εξοικονόμηση ενέργειας, τη βελτίωση των υπηρεσιών υγείας, τη αυτοματοποίηση της αγροτικής παραγωγής, τη διανομή των φυσικών αγαθών, την ευχρηστία ηλεκτρονικών συσκευών, τη μετακίνηση του πολίτη, καθώς και σε αμέτρητες άλλες κατηγορίες.

Στην παρούσα εργασία γίνεται μια σε βάθος ανάλυση για την εφαρμογή και διαχείριση του Internet Of Things- καλούμενο εφεξής IoT, τη χρησιμότητά του στο ανά κλάδους Project Management, καθώς και στη συνδυαστική αποτελεσματικότητα αυτών των δύο στην εξέλιξη της ποιότητας του σύγχρονου τρόπου ζωής. Στόχος μας είναι να παραθέσουμε σε βάθος τη χρησιμότητα του IoT ως εργαλείο του Project Management, τόσο στη διαχείριση όσο και στην ανάπτυξη έργων ανάπτυξης βασισμένα στην τεχνολογία.

# Εννοιολογικό υπόβαθρο σχετικά με το Management και το Internet of Things (IoT)

## 1. Τι είναι Management

### 1.1 Ορισμός του Management

Στην κατά τα άλλα πολύ πλούσια ελληνική γλώσσα δεν μπορεί να αποδοθεί μονολεκτικά ο όρος Management. Ο όρος είναι αγγλικός και στην ελληνική αποδίδεται με τη φράση Οργάνωση και Διοίκηση επιχειρήσεων. Ωστόσο, η μεταγραμματισμένη μορφή της λέξης, Μάνατζμεντ, καθιερώθηκε και χρησιμοποιείται επισήμως πλέον από την επιχειρηματική κι επιστημονική κοινότητα. Πρόσφατα, ο Γεώργιος Μπαμπινιώτης στο Λεξικό της Νέας Ελληνικής Γλώσσας (έκδ. 1998) χρησιμοποιεί έναν νέο ελληνικό όρο για την απόδοση του όρου Management, τον όρο Διοικητική ο οποίος φαίνεται να αποδίδει καλύτερα την έννοια του αγγλικού όρου. Έτσι ο όρος "Μάνατζμεντ" περιλαμβάνει το σύνολο των ενεργειών που είναι απαραίτητες για την αποτελεσματική πηδαλιούχηση των διαδικασιών απόδοσης σε μια επιχείρηση ή οργανισμό.

Το Management περιλαμβάνει ένα σύνολο διαδικασιών που περιγράφουν τη συμπεριφορά διοικητικών στελεχών βάσει των αρχών και των αξιωμάτων της επιστήμης. «Μάνατζμεντ» είναι η πρακτική του να επιτυγχάνονται αποτελέσματα μέσω άλλων ανθρώπων. Ειδικότερα και πιο συγκεκριμένα είναι «Το σύνολο διαδικασιών και ελέγχων με τις οποίες εξασφαλίζεται η διατήρηση της οργανωτικής σύνδεσης και η κατεύθυνση μιας ομάδας ανθρώπων που επιδιώκει ένα συγκεκριμένο αποτέλεσμα» (Massie, 1979).

Η πλήρης εννοιολογική απόδοση του περιεχομένου του όρου «Μάνατζμεντ», παρά τις μακρόχρονες προσπάθειες δεν έχει γίνει μέχρι σήμερα, δυνατό να αποδοθεί επαρκώς με έναν 'ελληνοπρεπή' όρο. Απόδειξη αυτής της αδυναμίας, αποτελεί το γεγονός ότι στη σύγχρονη ελληνική ειδική βιβλιογραφία ο όρος αποδίδεται άλλοτε ως 'Διοίκηση' και άλλοτε ως 'Διαχείριση'. Και τούτο παρά το γεγονός ότι αποτελούν έννοιες διακριτές, καθώς, σύμφωνα με τον Mackenzie (Mackenzie, 1991), Διοίκηση σημαίνει να «*πετυχαίνεις αντικειμενικούς στόχους μέσα από άλλους*», ενώ Διαχείριση «*να διευθύνεις τις λεπτομέρειες της εκτελεστικής δουλειάς*». Η αδυναμία απόδοσης του όρου με σαφήνεια και πληρότητα οδηγεί πολύ συχνά στην ταυτόχρονη επιστράτευση και των δύο αυτών όρων με σκοπό να αποδώσουν από κοινού, ως συμπληρωματικές έννοιες, το περιεχόμενο του ξενικού όρου. Η περιφραστική, όμως, διατύπωση της έννοιας πέραν του ότι είναι μακροσκελής, αποδεικνύεται στην πράξη και ανεπαρκής, καθώς αδυνατεί να εκφράσει τις ποικίλες διαστάσεις του όρου στο σύνολό τους. Πέραν τούτου, είναι δυνατόν να οδηγήσει και σε παρανοήσεις εξαιτίας μιας πιθανής λανθασμένης χρησιμοποίησή της.

Ο σαφής ορισμός με τη χρήση στεγανών του management είναι σχεδόν αδύνατον να γίνει με απλοϊκό τρόπο. Ο λόγος είναι η πολυφασματική έννοια της λέξης, και για προφανείς λόγους, η μόνιμη διαμάχη μεταξύ των θεωρητικών και των επαγγελματικών managers. Στη διοίκηση των επιχειρήσεων οι ξένοι όροι που έχουν δημιουργηθεί, όπως management και administration είναι αδύνατον να αποδοθούν με το υπάρχον λεξιλόγιο, οπότε υιοθετούνται ως έχουν. Είναι εξίσου σημαντικό στο σημείο αυτό να γίνει διαφοροποίηση μεταξύ των εννοιών Διοίκησης και Διεύθυνσης.

Η Διοίκηση (Management) περιλαμβάνει ένα σύνολο διαδικασιών με τα επιμέρους στοιχεία-λειτουργίες τους, που περιγράφουν τη συμπεριφορά των διοικητικών στελεχών βάσει αρχών και αξιωμάτων της επιστήμης. Με αυτή τη σημασία η Διοίκηση είναι ευρύτερη έννοια της Διεύθυνσης. «Μάνατζμεντ» είναι η πρακτική του να επιτυγχάνονται αποτελέσματα μέσω άλλων ανθρώπων (Ζώης, Α.Κ.- Γαρουφάλης, Δ.Κ., 2008). Εδώ γίνεται ο διαχωρισμός ανάμεσα σε Διοίκηση και Διεύθυνση, κι εξηγείται πώς λειτουργεί η ανάθεση έργου σε τρίτους πέραν της Διοίκησης ενός οργανισμού.

Στο πλαίσιο αυτό της διαφοροποίησης μεταξύ Διοίκησης και Διεύθυνσης, είναι σημαντικό να αναφερθεί η ασυμμετρία πληροφόρησης που δημιουργείται, λόγω διαφοροποιημένων συμφερόντων. Η εκάστοτε Διοίκηση προσβλέπει στη βέλτιστη λειτουργία μιας επιχειρηματικής μονάδας- οργανισμού, ενώ η εκάστοτε Διεύθυνση προσβλέπει στη βέλτιστη επίτευξη των προσωπικών της στόχων, μέσα από τον οργανισμό. Το γεγονός αυτό αποτελεί από μόνο του την πηγή της ασσυμετρίας πληροφόρησης. Μάνατζμεντ, λοιπόν, είναι ο

συντονισμός όλων των παραγωγικών πόρων για να επιτευχθούν βέλτιστα αποτελέσματα σε ένα έργο ή έναν οργανισμό, εφόσον έχουν εξομαλυνθεί οι διαφορές και το χάσμα των συμφερόντων, καλούμενο στο εξής Management.

Για να επιτευχθεί σε κάθε περίπτωση η βέλτιστη αποτελεσματικότητα του Management, θα πρέπει να υπάρξει συντονισμός στις εξής λειτουργίες ενός οργανισμού:

- Προγραμματισμός (planning)

  Αποτελεί τον προσδιορισμό των στόχων, της στρατηγικής και των τακτικών που θα χρησιμοποιηθούν για την επίτευξή τους. «Οι Koontz και O Donnell πολύ απλά ορίζουν τον Προγραμματισμό ως τη λειτουργία μέσω της οποίας γεφυρώνεται το χάσμα ή η απόσταση μεταξύ του σημείου που βρίσκεται σήμερα το άτομο ή η κοινωνική οργάνωση και του σημείου στο οποίο θέλει να βρίσκεται στο μέλλον, αποφασίζοντας τι θα γίνει, πώς θα γίνει, πότε θα γίνει και ποιος θα το κάνει» (Morgan, 1993).

- Οργάνωση (organising)

  Είναι εκείνη η λειτουργία του μάνατζμεντ που θέτει μια δομή στον τρόπο που συντονίζονται οι παραγωγικοί πόροι. Όπως και με τον προγραμματισμό, έτσι και με την οργάνωση αυτή δεν υφίσταται ουσιαστικώς, αν πέρα από την ανάθεση των εργασιών στους εργαζομένους, δεν τους δίνεται η ανάλογη εξουσία, τα ανάλογα εργαλεία και η ανάλογη πληροφόρηση ώστε να είναι σε θέση να φέρουν εις πέρας την εργασία που τους έχει ανατεθεί (Ζώης, Α.Κ.- Γαρουφάλης, Δ.Κ., 2008). Οργάνωση είναι η σχεδίαση της οργανωτικής δομής δηλαδή η διαδικασία διαμόρφωσης του οργανογράμματος για την υλοποίηση των στόχων και για την διευθέτηση και συσχέτιση των καθηκόντων μεταξύ των διαφόρων θέσεων εργασίας, ώστε να αποσαφηνισθεί το εσωτερικό περιβάλλον του οργανισμού. Με τον τρόπο αυτό καθορίζονται οι σχέσεις, οι ροές και οι διαδικασίες εκτέλεσης των έργων.

- Στελέχωση (staffing)

  Αφορά στο ανθρώπινο δυναμικό που θα στελεχώσει και θα επανδρώσει τις εκάστοτε μονάδες. Ιδιαίτερη σημασία θα πρέπει να δοθεί στη συγκεκριμένη λειτουργία του management, καθώς η σωστή στελέχωση αποτελεί καίριο και σημαντικό άξονα της λειτουργίας μιας επιχειρηματικής δομής.

- Διεύθυνση (leading)

Είναι η ροή πληροφορίας από την ηγεσία ενός οργανισμού προς το εργατικό δυναμικό της. Εδώ επαφίεται το σημαντικό των διαπροσωπικών σχέσεων στη διοικητική ικανότητα της ηγεσίας.

Έλεγχος (controlling)

Ένας απλός ορισμός του ελέγχου είναι αυτός που τον θεωρεί ως τη διαδικασία με την οποία η διοίκηση ενός οργανισμού επαληθεύει τη σύμπτωση των επιτευχθέντων αποτελεσμάτων με τα προγραμματισθέντα πρότυπα (Cho, C. S., & Gibson, G. E., 2001). Πιο συγκεκριμένα, ο έλεγχος είναι εκείνη η λειτουργία με την οποία η Διεύθυνση αποτυπώνει τα αποτελέσματα του management και τα συγκρίνει με τα βέλτιστα δυνατά. Στόχος, σε αυτή την περίπτωση, είναι ο απολογιστικός συντονισμός και η αξιολόγηση. Το management έχοντας τα στοιχεία του ελέγχου στα χέρια του, τα χρησιμοποιεί για να επαληθεύσει αν η πορεία των εργασιών κινείται προς τη σωστή κατεύθυνση ή, εάν υπάρχουν σφάλματα, να τα εντοπίσει και εναλλακτικά να προχωρήσει σε διορθωτικές κινήσεις, αποφάσεις, στρατηγικές.

- Συντονισμός (coordination)

  Το αν ο συντονισμός ανήκει στις λειτουργίες του management είναι επιστημονικά αμφισβητούμενο. Ωστόσο, δεν παύει να αποτελεί κλειδί για κάθε μία από τις προαναφερόμενες λειτουργίες του management και χωρίς αυτόν δεν είναι δυνατή η εύρυθμη λειτουργία του οργανισμού.

## 1.2 Εργαλεία Management

Αν και στη σύγχρονη επιστήμη του Management έχουν ήδη αναπτυχθεί τα απαραίτητα εργαλεία για την επιτυχημένη εφαρμογή του, η επιτυχημένη χρήση των εργαλείων αυτών, η οποία βασίζεται στην κατανόησή τους και την ορθή χρήσης τους, προϋποθέτει τη βαθιά γνώση του εκάστοτε εργαλείου.

Ο επιχειρηματικός κόσμος εξελίσσεται συνεχώς και τα εργαλεία αυτά αποτελούν σημαντικό πυλώνα διαχείρισης κι επίλυσης προβλημάτων στην επιχειρηματικότητα. Βοηθούν τον άνθρωπο να πάρει επιχειρηματικές αποφάσεις για τη δημιουργία βελτιωμένων προϊόντων και υπηρεσιών τα οποία θα είναι ικανά να οδηγήσουν την εκάστοτε επιχειρηματική οντότητα σε αυξημένη παραγωγικότητα και κατ' επέκταση σε αυξημένη ανταγωνιστικότητα και κερδοφορία.

Τα βασικότερα εργαλεία του Μάνατζμεντ αναπτύσσονται ακολούθως.

### *1.2.1 Συγκριτική Αξιολόγηση (Benchmarking)*

Αποτελεί ένα από τα πιο χρήσιμα εργαλεία του management. Βελτιώνει την αποδοτικότητα με το να αναγνωρίζει τις βέλτιστες πρακτικές της αγοράς στις διαδικασίες και τις πωλήσεις. Με τη συγκριτική αξιολόγηση χρησιμοποιούνται οι καλύτερες πρακτικές μεγάλων επιχειρήσεων ή ηγετών του εκάστοτε κλάδου και υιοθετούνται από μικρότερες επιχειρήσεις που εκτελούν παρόμοιες εργασίες. Αντικείμενο της συγκριτικής αξιολόγησης είναι να εντοπίσει παραδείγματα ανώτερης απόδοσης και να εντρυφήσει στις πρακτικές τους. Οι επιχειρήσεις μπορούν να εξατομικεύσουν τις πρακτικές αυτές ή να προβούν σε δημιουργία παρόμοιων, επιτυγχάνοντας τη βελτιστοποίηση της αποδοτικότητας, την αύξηση περιθωρίου κέρδους και την απόκτηση στρατηγικού πλεονεκτήματος.

### *1.2.2 Στρατηγικός Σχεδιασμός (Strategic Planning)*

Ο στρατηγικός σχεδιασμός είναι μια περιεκτική διαδικασία σχετικά με το πού θέλει το management να οδηγήσει την επιχείρηση, ποιοι είναι οι στόχοι που θέλει να πετύχει και με ποιους τρόπους θα επιτευχθούν οι στόχοι αυτοί. Ο στρατηγικός σχεδιασμός είναι μια συστηματική διαδικασία για το management κι αποτελεί πρόκληση ως προς τη αφοσίωση στους στόχους. Συχνά χρησιμοποιείται για την ολοκληρωτική αλλαγή στις εργασίες μιας επιχείρησης, για να δημιουργήσει μια εσωτερική κουλτούρα αφοσίωσης στο στόχο, για να καθοδηγήσει σαφώς την επιχείρηση μέσα από έναν προϋπολογισμό και τέλος για να εκπαιδεύσει τους διευθυντές να αξιολογούν την πληροφορία που έχουν στη διάθεσή τους, ώστε να παίρνουν καλύτερες αποφάσεις.

### *1.2.3 Ισορροπημένο Σύστημα Επιδόσεων (Balanced Scorecard)*

Είναι ίσως το πιο σημαντικό από όλα τα εργαλεία management και η ελληνική απόδοση δε θα μπορούσε να είναι ακριβής. Είναι ένα σύστημα, κατά το οποίο τα αριθμητικά μεγέθη μιας επιχείρησης αποτυπώνονται και μετατρέπονται σε ποιοτικά χαρακτηριστικά. Με τον τρόπο αυτό καταγράφονται οι αδυναμίες και τα πλεονεκτήματα του οργανισμού, με σκοπό να προσαρμοστούν εν τέλει στους στρατηγικούς στόχους. Είναι ένα σύστημα μέτρησης επίδοσης, στρατηγικό σύστημα ελέγχου κι εργαλείο επικοινωνίας. Κύρια χαρακτηριστικά του συστήματος είναι οι οικονομική διάσταση, οι εσωτερικές διαδικασίες, οι πελάτες και τέλος η εκπαίδευση και ανάπτυξη.

### *1.2.4 Ανάλυση SWOT*

Προέρχεται από τα αρχικά των λέξεων Strengths, Weaknesses, Opportunities, Threats. Χρησιμοποιείται με τέτοιο τρόπο ώστε να εντοπιστούν οι ευκαιρίες και οι απειλές σε ένα

έργο ή σε έναν οργανισμό, ώστε να μετατραπούν με στρατηγικό τρόπο σε ισχυρά πλεονεκτήματα και να εξαλειφθούν τυχόν αδυναμίες. Είναι ένα εύκολο εργαλείο στη χρήση του, εύκολο να χρησιμοποιηθεί και γρήγορο να δομηθεί. Η ανάλυση των στοιχείων του SWOT οδηγεί σε καταγραφή όχι μόνο των εσωτερικών διαδικασιών, αλλά και των εξωτερικών απειλών.

Αναφέραμε παραπάνω μερικά από τα πιο χαρακτηριστικά και σύγχρονα εργαλεία του management. Επιπροσθέτως, στη λειτουργία τους οι οργανισμοί χρησιμοποιούν επιπλέον εργαλεία σημαντικά για τη λήψη αποφάσεων, όπως για παράδειγμα το δέντρο αποφάσεων, το προφίλ κινδύνου, τις στρατηγικές συμμαχίες κλπ. Είναι σημαντικό για τη διοίκηση ενός οργανισμού να γνωρίζει ποιο εργαλείο θα χρησιμοποιήσει για να εφαρμόσει τη στρατηγική της. Σε κάθε περίπτωση, αυτό απαιτεί καλή γνώση τόσο των εργαλείων, όσο και της στοχοθέτησης του management, για το βέλτιστο συνδυασμό των δύο αυτών χαρακτηριστικών.

## 1.3 Τι είναι το Project Management

Το Project Management, ή αλλιώς Διοίκηση Έργου στην Ελληνική, είναι η εφαρμογή γνώσεων, ικανοτήτων, εργαλείων, και τεχνικών διοίκησης στην ανάπτυξη και στις δραστηριότητες ενός έργου (PMBOK Guide, 2000). Το Project Management επιτυγχάνεται με τις ίδιες λειτουργίες του management, εμπλουτισμένο ωστόσο με χρονικές σταθερές: έναρξη, σχεδιασμός, εκτέλεση, έλεγχος και κλείσιμο ή λήξη.

Ο όρος Project Management χρησιμοποιείται συχνά για να περιγράψει το management σε συνεχιζόμενες δραστηριότητες. Αυτή η προσέγγιση καλύπτει περισσότερες οπτικές του management κι έχει εφαρμογή σε αμέτρητες τεχνικές ανάπτυξης έργων σε έναν οργανισμό.

Το Project Management δομικά περιλαμβάνει:

1) Τον προσδιορισμό των απαιτήσεων του έργου
2) Τον καθορισμό των επιτεύξιμων στόχων
3) Την εξισορρόπηση των αιτημάτων για φυσικούς πόρους, ποιότητα, χρόνο και κόστος και
4) Την προσαρμογή προδιαγραφών, σχεδίων και προσεγγίσεων στις διαφορετικές ανάγκες και προσδοκίες των συμμετεχόντων.

Σε κάθε περίπτωση, στην εφαρμογή του Project Management, υπάρχει πάντοτε ο διαχειριστής έργου, ο οποίος πρέπει να είναι σε θέση να εφαρμόσει τις απαραίτητες τεχνικές

και να προχωρήσει στις αναγκαίες ενέργειες, ώστε το εκάστοτε έργο να υλοποιηθεί σε απόλυτη ισορροπία πόρων, ποιότητας, χρόνου και χρήματος.

# 2. Η έννοια του Internet Of Things και ορισμοί

## 2.1 Εννοιολογική Θεμελίωση

Η τεχνολογία είναι ο πλέον αναπτυσσόμενος τομέας των τελευταίων εκατό ετών και το Internet αποτελεί σημαντικό παράγοντα στην εξέλιξή της. Οι νέες τεχνολογίες έχουν ως προϋπόθεση τη συνδεσιμότητα ανάμεσα σε διαφορετικά ψηφιακά περιβάλλοντα, ακόμα κι αν χρησιμοποιούνται διαφορετικές γλώσσες προγραμματισμού. Από εκεί προκύπτει και ο όρος Internet of Things (IoT). Αν αναλύσουμε τη φράση προκύπτει η εννοιολογική βάση του IoT, κοινώς είναι η σύνδεση φυσικών πραγμάτων μέσω του Παγκοσμίου Ιστού. Ειδικότερα, είναι η σύνδεση ηλεκτρονικών συσκευών, οι οποίες με τη βοήθεια ενσωματωμένων τεχνολογιών, δίνουν τη δυνατότητα επικοινωνίας και καταγραφής μεγεθών του εξωτερικού περιβάλλοντος και της εσωτερικής τους λειτουργίας.

Η εξέχουσα σημασία του IoT είναι η εφαρμογή του στην καθημερινή ζωή, είτε αναφερόμαστε σε άτομα, είτε σε επιχειρήσεις. Στην περίπτωση των ατόμων, η εφαρμογή του IoT μπορεί να έχει άμεσα αποτελέσματα στη βελτίωση της εργασίας και του τρόπου ζωής, μάθησης και παροχών υγείας. Στην περίπτωση των επιχειρήσεων, αποτελεί σύγχρονο εργαλείο στη βιομηχανική παραγωγή και δη στη διαχείριση επιχειρησιακών διαδικασιών για τη μεταφορά αγαθών και ανθρώπων. Συμπερασματικά καταλήγουμε πως το IoT θα είναι στο εξής το βασικό κλειδί για την ανάπτυξη και βελτίωση του τρόπου ζωής και της επιχειρησιακής οργάνωσης, συντελώντας από κοινού στη βελτίωση της παγκόσμιας οικονομίας.

Η συνδεσιμότητα με μοναδικό τρόπο συσκευών μέσω του διαδικτύου απαιτεί τη συνεχή ανάπτυξη τεχνολογιών που μπορούν να υποστηρίξουν με ασφαλή τρόπο τα διαχειριζόμενα δεδομένα. Αναγνωρίζουμε στο σημείο αυτό την αλληλεπίδραση μεταξύ τεχνολογίας και συνδεσιμότητας, ώστε ο ένας κλάδος να προωθεί και να μετέχει στην ανάπτυξη του άλλου. Οι συσκευές τείνουν να γίνονται όλο και πιο «έξυπνες» με τη συλλογή και τη διαχείριση δεδομένων, ωστόσο είναι απαραίτητο να διασφαλίζεται σε κάθε περίπτωση η ιδιωτικότητα του χρήστη.

Η ανθεκτικότητα ενός συστήματος IoT σε πιθανές κυβερνο-επιθέσεις και η ασφαλής διατήρηση των δεδομένων αποτελούν τη πιο βασική και κατά προτεραιότητα πρόκληση, στην οποία καλείται ο χειριστής του IoT να ανταποκριθεί αποτελεσματικά και με συνέπεια.

Κερδίζοντας με τον τρόπο αυτό την εμπιστοσύνη του χρήστη, το IoT μπορεί να κερδίσει τη διεισδυτικότητα για την οποία προορίζεται. Με τη δημιουργία δικλείδων ασφαλείας απαιτούνται τεχνολογίες που ενισχύουν την ασφάλεια, Privacy Enhancing Technologies, μεταξύ των οποίων το VPN (Virtual Private Networks), TLC (Transport Layer Security) και Onion Routing.

### 2.1.1 Έξυπνες Συσκευές

Έξυπνη συσκευή ονομάζουμε κάθε ηλεκτρονική συσκευή που συνδέεται με διάφορους αποδεκτούς τρόπους με το internet για λειτουργικούς σκοπούς. Αποτελείται από έναν τροφοδότη ρεύματος, αισθητήρες ή ενεργοποιητές (sensors- actuators), έναν επεξεργαστή και μια συσκευή επικοινωνίας (Wi-Fi- Bluetooth). Ο τροφοδότης ρεύματος είναι η πηγή ενέργειας της συσκευής. Οι αισθητήρες λαμβάνουν πληροφορίες από το φυσικό περιβάλλον και οι ενεργοποιητές ορίζουν τη λειτουργία της συσκευής με βάση τις πληροφορίες αυτές. Η συσκευή επικοινωνίας μεταδίδει τις πληροφορίες λειτουργίας και συνδέει την έξυπνη συσκευή με άλλες μέσω δικτύου.

### 2.1.2 Χώροι Εφαρμογής

Έχει ήδη γίνει μια περιληπτική αναφορά για την εφαρμογή του IoT στη σύγχρονη ζωή. Προϋπόθεση της αποτελεσματικότητας των εφαρμογών του είναι οι δομές στις οποίες θεωρούμε χρήσιμο να αναπτυχθεί να συνδέονται μεταξύ τους με κάποιο τρόπο, οι πληροφορίες και τα δεδομένα του περιβάλλοντος να μπορούν να συλλεχθούν ώστε τα αντικείμενα να αισθάνονται, να επικοινωνούν και να αλληλοεπιδρούν. Παρακάτω παρατίθενται ορισμένοι τομείς οι οποίοι μπορούν να επηρεαστούν άμεσα από το IoT και αναλύονται περεταίρω στο δεύτερο μέρος:

- Αστική χρήση: Είναι πλέον πιθανή η προσθήκη εξυπνάδας σε κτίρια και περιβάλλοντα που αφορούν σε εργασία, προσωπικούς χώρους, εκπαίδευση και βιομηχανικές εγκαταστάσεις. Σε σπίτια και γραφεία μπορεί να επιτευχθούν λύσεις όπως αυτόματος φωτισμός, συστήματα συναγερμού, προσαρμόσιμα συστήματα θέρμανσης και άλλα με στόχο την διευκόλυνση του ανθρώπου όπως τη μείωση του κόστους και την εξοικονόμηση ενέργειας. Ήδη τα περισσότερα από αυτά είναι τεχνολογίες ενσωματωμένες στα σύγχρονα αυτοκίνητα.

- Βιομηχανοποίηση: Μια άλλη εφαρμογή που μπορεί να έχει το IoT είναι σε βιομηχανικές εγκαταστάσεις. Σε βιομηχανικά περιβάλλοντα μπορεί να γίνει χρήση της τεχνολογίας RFID στα μέρη της παραγωγής για αυτοματοποίηση των διαδικασιών, τη διαχείριση της αποθήκης και των αποθεμάτων, καθώς και την αποτελεσματική παραγωγικότητα των μηχανών.

- Υγεία: Με τη χρήση αισθητήρων που μπορεί να τοποθετήσει ένας χρήστης σε εφαρμογή με το σώμα του, καταγράφεται η φυσική του δραστηριότητα και η αντίδραση βασικών λειτουργιών του σώματος. Με τον τρόπο αυτό μπορεί να διατηρηθεί ένα ιστορικό υγείας με μοναδική κωδικοποίηση ανά άτομο, ώστε ανά πάσα ώρα και στιγμή τα δεδομένα να είναι διαθέσιμα στον ιατρό.

- Μεταφορές: Οι περισσότεροι από μας έχουμε στα κινητά μας τηλέφωνα ενσωματωμένα GPS που μας δείχνουν τη θέση μας, την κίνηση στους δρόμους, μετρούν την απόσταση και το χρόνο που θα χρειαστεί για να μεταβεί κάποιος στο σημείο προορισμού του, καθώς και δρομολογούν διαφορετικές διαδρομές αναλόγως κίνησης ή/ και κυκλοφοριακών ανά περίπτωση ρυθμίσεων (π.χ. κλειστοί δρόμοι, πορείες κλπ).

Οι εφαρμογές του IoT μπορούν να είναι άπειρες και σε αμέτρητους κλάδους της καθημερινότητάς μας. Το μέλλον είναι πολλά υποσχόμενο από τις σύγχρονες τεχνολογίες και οι απαιτήσεις του ανθρώπου υψηλές.

## 2.2 Σύντομη Ιστορική Ανασκόπηση του Internet of Things

Ο όρος Internet of Things χρησιμοποιήθηκε για πρώτη φορά το 1999 από το Βρετανό Kevin Ashton, με σκοπό να περιγράψει ένα σύστημα όπου θα ήταν δυνατή η σύνδεση φυσικών αντικειμένων με το internet μέσω αισθητήρων προχωρημένης τεχνολογίας. Έναυσμα αποτέλεσαν τα ήδη ανεπτυγμένα συστήματα ταυτοποίησης μέσω ραδιοσυχνοτήτων, RFID (Radio Frequency Identification), που χρησιμοποιούνται κυρίως από εταιρικές ανεφοδιαστικές αλυσίδες, προκειμένου να μετρήσουν και να παρακολουθούν τα αποθέματα της αποθήκης τους χωρίς την ανθρώπινη παρέμβαση.

Τα πρώτα σημάδια του Διαδικτύου των πραγμάτων (Internet of Things, IoT) μπορούν να εντοπιστούν ήδη από το 1932. Ο Jay B. Nash γράφει στον Spectatoritis (Nash, 1932): *«Μέσα στις δυνατότητές μας είναι η ψυχαγωγία του Έλληνα πολίτη, που κατέστη δυνατή με μηχανικά σκλάβους μας, που υπερτερούν κατά πολύ του δώδεκα έως δεκαπέντε των ελεύθερων*

*ανθρώπων... Καθώς μπαίνουμε σε ένα δωμάτιο, με το πάτημα ενός κουμπιού δώδεκα σκλάβοι φωτίζουν το δρόμο μας. Ένας άλλος σκλάβος κάθεται είκοσι τέσσερις ώρες την ημέρα στο θερμοστάτη μας, ρυθμίζοντας τη θερμοκρασία του σπιτιού μας. Ένας άλλος κάθεται νύχτα και μέρα στο αυτόματο ψυγείο μας. Ξεκινούν το αυτοκίνητό μας, κινούν τους κινητήρες μας, γυαλίζουν τα παπούτσια μας, και περιποιούνται τα μαλλιά μας. Καταργούν σχεδόν το χρόνο και το χώρο με την ταχύτητά τους.»* [1]. Το 1949, ο γραμμικός κώδικας σχεδιάστηκε από τον Norman Joseph Woodland, όταν σχεδίασε τέσσερις γραμμές στην άμμο σε μια παραλία του Μαϊάμι (Woodland). Αυτό οδήγησε στην εφεύρεση του Universal Product Code (UPC), του πανταχού παρόντος bar code που χρησιμοποιείται σε όλα τα προϊόντα. Το 1967, ο Hubert Upton εφευρίσκει έναν αναλογικό φορετό (wearable) υπολογιστή με οθόνες που τοποθετούνται σε γυαλιά για να βοηθήσουν στην ανάγνωση των χειλιών (M. L. HEILIG). Το 1969, το πρώτο μήνυμα αποστέλλεται μέσω του ARPANET, του προκατόχου του Διαδικτύου (internet_first_words.html, 2018).

Το 1973, ο Mario Cardullo έλαβε το πρώτο δίπλωμα ευρεσιτεχνίας για τη παθητική ετικέτα RFID ανάγνωσης και εγγραφής (Cardullo, 2003). Στις αρχές της δεκαετίας του 1980, τα μέλη του τμήματος πληροφορικής Carnegie -Mellon εγκατέστησαν μικροδιακόπτες στην αυτόματη μηχανή πώλησης οπτανθρακοποίησης, ώστε να δουν πόσα μπουκάλια ήταν παρόντα στη μηχανή και αν ήταν κρύα ή όχι (CMU SCS Coke Machine, 2018). Το 1991, ο Mark Weiser της Xerox PARC δημοσιεύει στον επιστημονικό αμερικανικό χώρο "Ο υπολογιστής στον 21ο αιώνα", όπου χρησιμοποιήθηκαν για πρώτη φορά οι όροι "πανταχού παρούσα υπολογιστική" και "ενσωματωμένη εικονικότητα" (Weiser, 1991). Το 1994, ο Mik Lamming και ο Mike Flynn της Xerox EuroPARC καταδεικνύουν το Forget-Me-Not, μια wearable συσκευή που καταγράφει τις αλληλεπιδράσεις μεταξύ ανθρώπων και συσκευών, αποθηκεύοντας τις πληροφορίες σε μια βάση δεδομένων (M. Lamming and M. Flynn, 1994.). Τον Σεπτέμβριο του ίδιου έτους, ο όρος "συνειδητό περιβάλλον" χρησιμοποιήθηκε για πρώτη φορά από τον B.N. Schilit και M.M Theimer στο "Διάδοση ενεργών πληροφοριών χαρτών σε φορητούς υπολογιστές", (B. N. Schilit and M. M. Theimer, 1994).

Στις 13-14 Οκτωβρίου 1997, οι Carnegie-Mellon, MIT και Georgia Tech φιλοξένησαν το πρώτο διεθνές συμπόσιο IEEE για τους Wearable υπολογιστές, στο Cambridge, MA. Το 1999, το κέντρο αυτόματης αναγνώρισης (Auto-ID) ιδρύθηκε στο MIT. Ο Sanjay Sarma, ο David Brock

[1] *"Within our grasp is the leisure of the Greek citizen, made possible by our mechanical slaves, which far outnumber his twelve to fifteen per free man… As we step into a room, at the touch of a button a dozen light our way. Another slave sits twenty-four hours a day at our thermostat, regulating the heat of our home. Another sits night and day at our automatic refrigerator. They start our car; run our motors; shine our shoes; and cult our hair. They practically eliminate time and space by their very fleetness."*

και ο Kevin Ashton μετέτρεψαν την RFID τεχνολογία, σε τεχνολογία δικτύωσης συνδέοντας αντικείμενα με το Διαδίκτυο μέσω της ετικέτας RFID (S. Sarma, D. L. Brock, and K. Ashton). Δύο χρόνια αργότερα, το Κέντρο Auto-ID θα εισήγαγε ένα νέο σχήμα αναγνώρισης αντικειμένων, τον Ηλεκτρονικό Κωδικό Προϊόντος (EPC). Το 2005, μια ομάδα μελών διδακτικού προσωπικού στο Ινστιτούτο Σχεδίασης Αλληλεπιδράσεων Ivrea στην Ivrea της Ιταλίας ανέπτυξε αντίκτυπο στον κόσμο της φυσικής πληροφορικής.

## 2.3 Ορισμοί του Διαδικτύου των Πραγμάτων (IoT)

Οι σύγχρονες ασύρματες επικοινωνίες προωθούν συνεχώς την αναγκαιότητα για την ανάπτυξη του IoT. Με κύρια εφαρμογή τους τις ετικέτες ραδιοσυχνότητας RFID, αισθητήρες, ενεργοποιητές κλπ, οι συσκευές αλληλοεπιδρούν και επικοινωνούν μεταξύ τους μέσω μοναδικών συστημάτων διευθυνσιοδότησης (D. Giusto, A. Iera, G. Morabito, and L. Atzori,, 2010.). Σχετικά με την εφαρμογή του IoT και ανάλογα με τον τρόπο χρήσης του μπορούν να προσδιοριστούν οι εξής ορισμοί (L. Atzori, A. Iera, and G. Morabito, 2010.):

- Οπτική προσανατολισμένη στα πράγματα (Things oriented)
- Οπτική προσανατολισμένη στο Διαδίκτυο (Internet oriented)
- Σημασιολογική οπτική (Semantics oriented)

Στον πρώτο ορισμό του IoT δίνεται περισσότερη βάση στα φυσικά αντικείμενα, δηλ. Ετικέτες αναγνώρισης ραδιοσυχνοτήτων (RFID) (M. Presser and A. Gluhak,, 2009.). Παρόλο που η RFID εξακολουθεί να είναι η κορυφαία τεχνολογία στην Things Oriented προοπτική, λόγω της ωριμότητας, του χαμηλού κόστους και της ισχυρής υποστήριξης από την επιχειρηματική κοινότητα, αναπτύσσεται σήμερα ένα ευρύ φάσμα συσκευών, δικτύων και υπηρεσιών τεχνολογίας, όπως η Near Field Communications (NFC) και ασύρματα δίκτυα ενεργοποιητών αισθητήρων (WSAN).

Η προσανατολισμένη στο Internet προοπτική, απαιτεί μια παγκόσμια υποδομή που να συνδέει τόσο εικονικά όσο και φυσικά γενικά αντικείμενα και υπογραμμίζει τη σημασία της συμπερίληψης των υφιστάμενων και εξελισσόμενων εξελίξεων στο δίκτυο και το Διαδίκτυο (J. P. Vasseur and A. Dunkels, 2008.). Ένα παράδειγμα της Προσανατολισμού στο Διαδίκτυο μπορεί να βρεθεί στο IP για τα Smart Objects (IPSO), ένα φόρουμ που δημιουργήθηκε το Σεπτέμβριο του 2008 για να προωθήσει το Internet Protocol ως τεχνολογία δικτύου για τη σύνδεση Smart Objects σε όλο τον κόσμο. Η αιτιολόγηση για το IPSO έγκειται στην ιδέα ότι η στοίβα IP (IP stack) είναι ένα ελαφρύ πρωτόκολλο που ήδη συνδέει ένα τεράστιο αριθμό

συσκευών επικοινωνίας και τρέχει σε μικροσκοπικές ενσωματωμένες συσκευές που λειτουργούν με μπαταρία. Αυτό εγγυάται ότι η IP έχει όλες τις ιδιότητες για να γίνει πραγματικότητα το IoT.

Τέλος, η ιδέα πίσω από τη Σημασιολογική Προοπτική είναι ότι ο αριθμός των αντικειμένων που εμπλέκονται στο Μελλοντικό Διαδίκτυο προορίζεται να γίνει εξαιρετικά υψηλός, δημιουργώντας έτσι ζητήματα σχετικά με την οργάνωση, την αναζήτηση, την αντιπροσώπευση και την αποθήκευση των πληροφοριών του IoT (I. Toma, E. Simperl, and G. Hench, 2009.). Οι σημασιολογικές τεχνολογίες μπορούν να εκμεταλλευτούν τις κατάλληλες λύσεις μοντελοποίησης για την περιγραφή των πραγμάτων, τη συλλογιστική σχετικά με τα δεδομένα, τα σημασιολογικά περιβάλλοντα εκτέλεσης και τις αρχιτεκτονικές, καθώς και την κλιμακωτή υποδομή αποθήκευσης και επικοινωνίας.

## 2.4 Διαδίκτυο των Πραγμάτων (IoT): Τεχνολογίες

Οι κύριες τεχνολογίες που χρησιμοποιούνται στη θεμελίωση του IoT είναι τα RFID συστήματα και τα ασύρματα δίκτυα αισθητήρων.

Ένα σύστημα ταυτοποίησης μέσω ραδιοσυχνοτήτων RFID αποτελείται από RFID αναγνώστες (readers) και ετικέτες (tags). Οι ετικέτες είναι μικρά ηλεκτρονικά chips στα οποία αποθηκεύεται συγκεκριμένος όγκος δεδομένων και μια κεραία. Κάθε ετικέτα αποτελεί μοναδικό αναγνωριστικό δεδομένο που εφαρμόζεται στα αντικείμενα κι ενεργοποιείται όταν σκανάρεται από έναν RFID reader (Vogt, 2002,). Η κεραία της ετικέτας μεταδίδει στον αναγνώστη όλες τις πληροφορίες που έχουν αποθηκευτεί σε αυτή. Τα αντικείμενα που φέρουν την ετικέτα δεν είναι υποχρεωτικό να βρίσκονται πλήρως ευθυγραμμισμένα με τον reader, η ανάγνωση της ετικέτας μπορεί να πραγματοποιηθεί και υπό γωνία, αρκεί η ετικέτα να βρίσκεται εντός των πλαισίων εκπομπής σήματος του RFID αναγνώστη.

Οι ετικέτες, αναλόγως με τον τρόπο λειτουργίας τους, κατατάσσονται σε τρεις κατηγορίες. Είναι πιθανό να είναι παθητικές, δηλαδή δεν είναι απαραίτητο να είναι συνδεδεμένες με πηγή ενέργειας, αλλά ενεργοποιούνται από ραδιοκύματα που στέλνει ο ηλεκτρονικός αναγνώστης που βρίσκεται κοντά. Εξίσου πιθανό είναι να χρησιμοποιούν ενέργεια για να λειτουργήσουν, όπως μπαταρίες, γεγονός που τις κατατάσσει στις ημι-αυτόνομες και στις αυτόνομες ή ενεργές. Στην περίπτωση της μερικής αυτονομίας, η μπαταρία τροφοδοτεί το chip με ηλεκτρική ενέργεια τη στιγμή που λαμβάνουν το σήμα του RFID reader. Στην τρίτη περίπτωση, αυτή των ενεργών ετικετών, οι μπαταρίες τροφοδοτούν τη συνεχή εκπομπή

σήματος. Είναι προφανές ότι η εμβέλεια της ραδιοσυχνότητας είναι βέλτιστη στις αυτόνομες ετικέτες, ακόμα κι αν αυτό συνεπάγεται μεγαλύτερη κατανάλωση ενέργειας και κόστος παραγωγής.

Στα ασύρματα δίκτυα αισθητήρων που συνεργάζονται και υποστηρίζουν την επικοινωνία με FRID συστήματα είναι πιο αποτελεσματικός ο προσδιορισμός της κατάστασης των πραγμάτων, όπως για παράδειγμα η θέση ή η θερμοκρασία, ενεργώντας ως γέφυρα μεταξύ του φυσικού και του ψηφιακού κόσμου. Τα εν λόγω δίκτυα αποτελούνται από ένα συγκεκριμένο αριθμό αισθητηριακών κόμβων, οι οποίοι επικοινωνούν μέσω ασύρματης multihop τεχνολογίας. Συνήθως, οι κόμβοι αναφέρουν τα αποτελέσματα των αισθητήρων ώστε η λειτουργία του συστήματος να βασίζεται σε βέλτιστη λειτουργία, όπως για παράδειγμα η ενεργειακή απόδοση, η επεκτασιμότητα του δικτύου, η αξιοπιστία για την αποφυγή εκτάκτων συναγερμών και η ευρωστία για την αποφυγή κατάρρευσης του δικτύου (I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, 2002.).

## 2.5 Προκλήσεις και προβλήματα

Μια σειρά ερωτημάτων που θα πρέπει να επιλυθούν εγείρονται στην περίπτωση του IoT (L. Atzori, A. Iera, and G. Morabito, 2010.). Αυτά περιλαμβάνουν:

- Τυποποίηση
- Υποστήριξη κινητικότητας
- Ονομασία
- Πρωτόκολλο μεταφοράς
- Χαρακτηρισμό κυκλοφορίας και υποστήριξη Quality of Service (QoS)
- Αυθεντικοποίηση
- Προστασία προσωπικών δεδομένων
- Ψηφιακή παραχάραξη

Τα προβλήματα που αφορούν στην τυποποίηση πηγάζουν από το γεγονός ότι υπάρχουν αρκετά πρότυπα μέχρι σήμερα, ωστόσο δεν έχει επιτευχθεί η ενσωμάτωση σε ένα ολοκληρωμένο πλαίσιο. Υπάρχον επιπλέον αρκετές προτάσεις για την κατηγοριοποίηση αντικειμένων, αλλά καμία υποστήριξη ή πρωτόκολλο της μεταφοράς τους στο σενάριο του IoT, όπου η κατηγοριοποίηση και η προσαρμοστικότητα σε ετερογενείς τεχνολογίες αποτελούν κρίσιμα προβλήματα. Όσον αφορά στην ονομασία, απαιτείται η υπηρεσία ονομασίας αντικειμένου (Object Name Services) για να χαρτογραφηθεί μια αναφορά στην

περιγραφή ενός συγκεκριμένου αντικειμένου και του σχετικού αναγνωριστικού και αντιστρόφως.

Τα υπάρχοντα πρωτόκολλα μεταφοράς αποτυγχάνουν στα σενάρια του IoT, δεδομένου ότι η εγκατάσταση της σύνδεσης και οι μηχανισμοί ελέγχου συμφόρησης ενδέχεται να αποδειχθούν αναποτελεσματικοί. Επιπλέον, απαιτούν μεγάλο χώρο αποθήκευσης προσωρινών δεδομένων, για να εφαρμοστούν σε αντικείμενα. Το IoT θα δημιουργήσει συμφόρηση δεδομένων με μοντέλα που ενδέχεται να είναι διαφορετικά από αυτά που υπάρχουν ήδη στο διαδίκτυο. Κατά συνέπεια, θα είναι επίσης απαραίτητο να καθοριστούν νέες προδιαγραφές QoS και συστήματα υποστήριξης.

Ο έλεγχος ταυτότητας είναι δύσκολος στο IoT καθώς απαιτεί κατάλληλες υποδομές ελέγχου ταυτότητας, ο οποίες δεν είναι διαθέσιμες στα σενάρια του IoT. Επιπλέον, τα αντικείμενα έχουν περιορισμένους πόρους σε σύγκριση με τις υπάρχουσες συσκευές επικοινωνίας και ηλεκτρονικών υπολογιστών. Πέραν τούτου ελλοχεύει ο κίνδυνος της ανθρώπινης παρέμβασης. Η ασφάλεια των δεδομένων εξασφαλίζεται συνήθως με την εφαρμογή κωδικών πρόσβασης. Ωστόσο, το μέγεθος του κωδικού πρόσβασης που υποστηρίζεται από IoT τεχνολογία στις περισσότερες περιπτώσεις είναι μικρό για να παρέχει τα αναγκαία ισχυρά επίπεδα προστασίας.

Το ηθικό δίλημμα που δημιουργείται είναι η συγκέντρωση πληροφορίας προσωπικών δεδομένων ενός χρήστη, χωρίς ο ίδιος να το γνωρίζει. Ο έλεγχος σχετικά με τη διάδοση τέτοιου είδους πληροφορίας είναι αδύνατος σύμφωνα με τις ισχύουσες πρακτικές. Τέλος, όσον αφορά στη ψηφιακή παραχάραξη, όλες οι πληροφορίες που συλλέγονται από το IoT σχετικά με το άτομο μπορούν να διατηρηθούν επ’ αόριστον, καθώς το κόστος αποθήκευσης μειώνεται. Με τη διαδικασία της «εξόρυξης δεδομένων» μπορούν να ανακτηθούν ακόμη και μετά από χρόνια.

## 2.6 Κύρια Χαρακτηριστικά του IoT

Όπως έχει ήδη γίνει κατανοητό, το Internet of Things (IoT) είναι ένα δίκτυο φυσικών αντικειμένων, συσκευών, οχημάτων, κτιρίων αλλά και άλλων αντικειμένων τα οποία περιέχουν ενσωματωμένα ηλεκτρονικά συστήματα, λογισμικά, αισθητήρες και διαδικτυακή δυνατότητα σύνδεσης – κάτι που επιτρέπει σε αυτά τα αντικείμενα να συλλέγουν και να ανταλλάσσουν δεδομένα. Το IoT δίνει την δυνατότητα στα αντικείμενα αυτά να ελέγχονται απομακρυσμένα μέσω της υπάρχουσας δικτυακής υποδομής δημιουργώντας ευκαιρίες άμεσης ενσωμάτωσης του φυσικού κόσμου με τα

υπολογιστικά συστήματα, έχοντας ως αποτέλεσμα τη βελτίωση της αποτελεσματικότητας και της ακρίβειας αλλά και τη μείωση του κόστους. Από την στιγμή μάλιστα που το IoT εξοπλίζεται με αισθητήρες και ενεργοποιητές αποτελεί μέρος έξυπνων συστημάτων της καθημερινότητας όπως είναι τα έξυπνα σπίτια, οχήματα και πόλεις. Κάθε αντικείμενο αναγνωρίζεται μοναδικά από το ενσωματωμένο υπολογιστικό σύστημα και μπορεί να λειτουργεί τόσο αυτόνομα όσο και σε συνεργασία με την υπόλοιπη διαδικτυακή υποδομή.

Ο όρος Internet of Things προτάθηκε από τον Kevin Ashton το 1999, αν και ήταν υπό συζήτηση τουλάχιστον από το 1991. Η ιδέα του Internet of Things αρχικά έγινε δημοφιλής μέσω του Auto-ID Center στο MIT αλλά και μέσω σχετικών δημοσιεύσεων ανάλυσης της αγοράς. Εκείνες τις ημέρες η ταυτοποίηση ραδιοσυχνοτήτων (RFID) θεωρήθηκε ως προϋπόθεση για το Internet of Things, αφού αν όλα τα αντικείμενα και οι άνθρωποι ήταν εξοπλισμένοι στην καθημερινότητα με αναγνωριστικά, θα μπορούσαν να διαχειρίζονται και να απογράφονται από υπολογιστές. Εκτός από την χρήση RFID, η σήμανση των πραγμάτων μπορεί να επιτευχθεί μέσα από τεχνολογίες όπως η κοντινού τύπου επικοινωνία, οι κώδικες QR, τα barcodes και η ψηφιακή υδατογράφηση.

Σήμερα ο όρος Internet of Things (το Διαδίκτυο των Πραγμάτων), χρησιμοποιείται για να υποδηλώσει την προηγμένη συνδεσιμότητα συσκευών, συστημάτων και υπηρεσιών, πέρα από επικοινωνία μεταξύ μηχανών, αφού καλύπτει μία ποικιλία από πρωτόκολλα, τομείς και εφαρμογές.

Σύμφωνα με τη Gartner, θα υπάρχουν σχεδόν 26 δισεκατομμύρια συσκευές στο Internet of Things μέχρι το 2020. Σύμφωνα με το ABI Research, πάνω από 30 δισεκατομμύρια συσκευές θα συνδέονται ασύρματα από το Διαδίκτυο των πραγμάτων (Διαδίκτυο των πάντων) μέχρι το 2020.

Η Cisco δημιούργησε έναν δυναμικό "μετρητή συνδέσεων" προκειμένου να παρακολουθεί τον εκτιμώμενο αριθμό συνδεδεμένων αντικειμένων από τον Ιούλιο του 2013 μέχρι τον Ιούλιο του 2020. Η ιδέα αυτή, όπου οι συσκευές συνδέονται στο Διαδίκτυο/Παγκόσμιο Ιστό μέσω χαμηλής ισχύος ραδιοσήματα, είναι η πιο ενεργή περιοχή έρευνας στο IoT. Τα ραδιοσήματα χαμηλής ισχύος δεν χρειάζεται να χρησιμοποιούν Wi-Fi ή Bluetooth. Χαμηλότερης ενέργειας και χαμηλότερου κόστους εναλλακτικές διερευνώνται υπό την κατηγορία του Chirp Networks.

Σύμφωνα με μία έρευνα και μελέτη που διεξήχθη από το Pew Research Internet Project, μία μεγάλη πλειοψηφία των ειδικών της τεχνολογίας και των χρηστών του Internet που

εμπλέκονταν οι οποίοι ανταποκρίθηκαν (περίπου το 83%) συμφώνησαν με την ιδέα ότι το Διαδίκτυο των πραγμάτων και των ενσωματωμένων υπολογιστών θα έχει διαδεδομένα και ευεργετικά αποτελέσματα έως το 2025. Φαίνεται ότι η επόμενη εξέλιξη του Διαδικτύου αλλάζει τα πάντα. Το Internet of Things (IoT), κάποιες φορές αναφέρεται ως το Διαδίκτυο των αντικειμένων και υπόσχεται να αλλάξει τα πάντα συμπεριλαμβανομένων και των φυσικών προσώπων. Αυτό μπορεί να μοιάζει σαν μία τολμηρή δήλωση αλλά λαμβάνοντας υπόψη τον αντίκτυπο που έχει στην εκπαίδευση, την επικοινωνία, τις επιχειρήσεις, την επιστήμη αλλά και την ανθρωπότητα, αναμφισβήτητα το Διαδίκτυο είναι ένα από τα πιο σημαντικά και ισχυρά δημιουργήματα σε όλη την ανθρώπινη ιστορία. Έτσι, θεωρώντας ότι το IoT αντιπροσωπεύει την εξέλιξη του Διαδικτύου, δημιουργείται ένα τεράστιο άλμα στην ικανότητά του διαδικτύου να συγκεντρώνει, να αναλύει και να διανέμει δεδομένα τα οποία μπορούν να μετατραπούν σε πληροφορίες, γνώσεις και τελικά σοφία. Στο πλαίσιο αυτό το IoT γίνεται ιδιαίτερα σημαντικό και χρήσιμο.

Ήδη, καθώς οι εργασίες του IoT βρίσκονται σε εξέλιξη, παρατηρείται βελτίωση στην κατανομή των διαθέσιμων πόρων, κάτι το οποίο θα μπορούσε να οδηγήσει και στην πάρα πολύ αισιόδοξη, αν όχι ουτοπική, πρόβλεψη ότι η χρήση των εφαρμογών του IoT και η ενσωμάτωσή του στον σύγχρονο τρόπο ζωής θα μπορέσει μελλοντικά να οδηγήσει σε βελτίωση της κατανομής των παγκόσμιων πόρων σε εκείνους που τα χρειάζονται περισσότερο, οδηγώντας έτσι στην μείωση του χάσματος μεταξύ φτώχειας και πλούτου. Παρόλα αυτά υπάρχουν πολλά εμπόδια που απειλούν να επιβραδύνουν την ανάπτυξη του IoT, συμπεριλαμβανομένης της μετάβασης στο IPv6, έχοντας ένα κοινό σύνολο προτύπων και ανάπτυξης των πηγών ενέργειας για εκατομμύρια, ακόμη και δισεκατομμύρια μικροσκοπικούς αισθητήρες. Ωστόσο καθώς οι επιχειρήσεις, οι κυβερνήσεις, οι οργανισμοί τυποποίησης και η ακαδημαϊκή κοινότητα λύνουν τις προκλήσεις αυτές, το IoT θα συνεχίσει να προοδεύει.

Από τεχνικής άποψης, το Internet of Things δεν είναι το αποτέλεσμα μιας μόνο πρωτότυπης τεχνολογίας. Αντιθέτως, διάφορες συμπληρωματικές τεχνικές εξέλιξης παρέχουν δυνατότητες που συνεργάζονται για να γεφυρωθεί το χάσμα μεταξύ του εικονικού και του φυσικού κόσμου. Οι δυνατότητες αυτές περιλαμβάνουν:

- Επικοινωνία και συνεργασία: Τα αντικείμενα έχουν την δυνατότητα να δικτυώνονται με τους πόρους του Διαδικτύου ή ακόμη και το ένα με το άλλο, να κάνουν χρήση των δεδομένων και των υπηρεσιών και να ενημερώνουν την κατάστασή τους. Οι ασύρματες τεχνολογίες, όπως το GSM και UMTS, Wi-Fi, Bluetooth, ZigBee και διάφορα άλλα ασύρματα πρότυπα δικτύωσης που είναι αυτή τη στιγμή υπό

ανάπτυξη, ιδιαίτερα εκείνων που σχετίζονται με τα προσωπικά ασύρματα δίκτυα (WPANs), έχουν πρωταρχική σημασία εδώ.

- Διευθυνσιοδότηση: Σε ένα IoT, τα αντικείμενα μπορούν αν τοποθετούνται και να διευθυνσιοδοτούνται μέσω της ανεύρεσης ή το όνομα των υπηρεσιών κι έτσι έχουν την δυνατότητα να επιβεβαιώνονται ή να ρυθμίζονται εξ αποστάσεως.

- Ταυτοποίηση: Τα αντικείμενα είναι μοναδικά αναγνωρίσιμα. Οι τεχνολογίες RFID, NFC (Near Field Communication) και οι οπτικά αναγνωρίσιμοι κώδικες (bar codes) είναι παραδείγματα τεχνολογιών με τις οποίες μπορούν αν εντοπιστούν ακόμη και παθητικά αντικείμενα που δεν έχουν ενσωματωμένους ενεργειακούς πόρους και να αναγνωριστούν με τη βοήθεια ενός «διαμεσολαβητή» όπως μία συσκευή αναγνώρισης RFID ή ένα κινητό τηλέφωνο. Η ταυτοποίηση επιτρέπει στα αντικείμενα να συνδέονται με πληροφορίες που σχετίζονται με το συγκεκριμένο αντικείμενο και μπορούν να ανακτηθούν από έναν διακομιστή, υπό τον όρο ο μεσολαβητής να είναι συνδεδεμένος στο δίκτυο.

- Ανίχνευση: Τα αντικείμενα διαθέτουν αισθητήρες με την βοήθεια των οποίων συλλέγουν πληροφορίες σχετικά με το περιβάλλον τους, καταγράφοντας διαβιβάζοντας ή αντιδρώντας άμεσα σε αυτό.

- Ενεργοποίηση: Τα αντικείμενα περιέχουν ενεργοποιητές προκειμένου να χειριστούν το περιβάλλον τους. Για παράδειγμα, μετατρέποντας τα ηλεκτρικά σήματα σε μηχανική κίνηση. Τέτοιοι ενεργοποιητές μπορούν να χρησιμοποιηθούν για να ελέγξουν εξ αποστάσεως διεργασίες στον πραγματικό κόσμο μέσω του Διαδικτύου.

- Ενσωματωμένη επεξεργασία πληροφοριών: Έξυπνα αντικείμενα διαθέτουν έναν επεξεργαστή ή μικροελεγκτή, καθώς και την ικανότητα αποθήκευσης. Αυτοί οι πόροι μπορούν αν χρησιμοποιηθούν για παράδειγμα, για να επεξεργάζονται και να ερμηνεύουν πληροφορίες των αισθητήρων ή ακόμη και να παρέχουν στα προϊόντα μία μνήμη για το πως έχουν χρησιμοποιηθεί.

- Εντοπισμός: Τα έξυπνα αντικείμενα έχουν επίγνωση της φυσικής τους θέσης ή μπορούν να εντοπίζονται. Το GPS ή το δίκτυο κινητής τηλεφωνίας είναι κατάλληλες τεχνολογίες για την επίτευξη αυτού του στόχου, καθώς οι

ραδιοφάροι (π.χ. γειτονικοί WLAN σταθμοί βάσεις ή αναγνώστες RFID με γνωστές συντεταγμένες) όπως επίσης και οι οπτικές ίνες.

- Διεπαφές χρήστη: Τα έξυπνα αντικείμενα μπορούν αν επικοινωνούν με τους ανθρώπους με κατάλληλο τρόπο (είτε άμεσα είτε έμμεσα, για παράδειγμα μέσω ενός smart phone). Καινοτόμα παραδείγματα αλληλεπίδρασης είναι: χειροπιαστές διεπαφές χρήστη, ευέλικτες πολυμερείς βάσεις εικόνας και φωνής ή μέθοδοι αναγνώρισης χειρονομιών

Οι περισσότερες ειδικές εφαρμογές χρειάζονται μόνο ένα υποσύνολο αυτών των δυνατοτήτων, ιδιαίτερα μετά την εφαρμογή όλων αυτών είναι συχνά δαπανηρό και απαιτεί σημαντική τεχνική προσπάθεια. Οι εφαρμογές Logistics για παράδειγμα, αυτή τη στιγμή επικεντρώνονται στην προσέγγιση εντοπισμού (δηλ. τη θέση του τελευταίου σημείου ανάγνωσης) και είναι περιορισμένοι σε τέτοιες εφαρμογές εφοδιασμού όπου οι πληροφορίες είναι απαραίτητες και ουσιαστικής σημασίας, όπως για παράδειγμα η θερμοκρασία που πρέπει να ελέγχεται κατά τη μεταφορά εμβολίων. Οι προάγγελοι της επικοινωνίας σε αντικείμενα καθημερινής χρήσης έχουν κάνει ήδη την εμφάνισή τους, ιδιαίτερα σε σχέση με το RFID, για παράδειγμα, η επικοινωνία μικρής εμβέλειας όπως η χρήση έξυπνων κλειδιών- καρτών από τις πόρτες των δωματίων ενός ξενοδοχείου ή αντίστοιχα εισιτήρια για σκι που επικοινωνούν με τα lift. Περισσότερο φουτουριστικά σενάρια περιλαμβάνουν ένα έξυπνο τραπέζι παιγνιόχαρτων, όπου η πορεία του παιχνιδιού βιντεοσκοπείται χρησιμοποιώντας τραπουλόχαρτα εξοπλισμένα με RFID. Παρόλα αυτά όλες αυτές οι εφαρμογές εξακολουθούν να περιλαμβάνουν ειδικά συστήματα σε τοπική ανάπτυξη, επομένως δεν μιλάμε για ένα «Διαδίκτυο» με την έννοια ενός ανοικτού, επεκτάσιμου και τυποποιημένου συστήματος.

# Μέρος Α: Τρόπος Διαχείρισης του Internet of Things (IoT)

## Α1. Ένα Πλαίσιο Γνωστικής Διαχείρισης για την Ενδυνάμωση του IoT

Το πλαίσιο γνωστικής διαχείρισης για την ενδυνάμωση του IoT, έχει την ικανότητα να προσαρμόζει δυναμικά τη συμπεριφορά του μέσω μίας δυνατότητας αυτοδιαχείρισης (self- Management), λαμβάνοντας υπόψιν πληροφορίες και γνώση- που προέρχονται από την εκμάθηση των μηχανών- σχετικές με την υπόθεση (π.χ. εσωτερική κατάσταση και κατάσταση του εξωτερικού περιβάλλοντος), καθώς επίσης και πολιτικές (π.χ. καθορισμός στόχων, περιορισμοί, κανόνες κλπ). Οι γνωστικές τεχνολογίες συνιστούν μια μοναδική και αποτελεσματική προσέγγιση για την αντιμετώπιση της τεχνολογικής ετερογένειας του IoT και την επίγνωση της κατάστασης, της αξιοπιστίας και της αποτελεσματικότητας.

Το πρότυπο «7 τρισεκατομμύρια συσκευές για 7 δις ανθρώπους» όπως περιγράφεται στο IEEE Vehicular Technology Magazine (Uusitalo, 2006) υποδηλώνει ότι η διαχείριση της ποσότητας των αντικειμένων που θα αποτελέσουν μέρος του Internet of Things (IoT) απαιτεί κατάλληλη αρχιτεκτονική και τεχνολογικά θεμέλια. Διαδικτυακά συνδεμένοι αισθητήρες, ενεργοποιητές και άλλοι τύποι έξυπνων συσκευών και αντικειμένων χρειάζονται μια κατάλληλη υποδομή επικοινωνίας μεταξύ τους.

Την ίδια στιγμή, η έλλειψη όσον αφορά τη λειτουργικότητα διαχείρισης ξεπερνάει την τεχνολογική ετερογένεια και την πολυπλοκότητα των διάχυτων δικτύων, και δημιουργεί την ανάγκη για τον καθορισμό αναγκαίων μηχανισμών για την καλύτερη κατανόηση της κατάστασης. Τέτοιοι μηχανισμοί θα πρέπει να παρέχουν υψηλή αξιοπιστία μέσω της δυνατότητας να χρησιμοποιούν ετερογενή αντικείμενα με συμπληρωματικό τρόπο για αξιόπιστη παροχή υπηρεσιών.

Επιπλέον, η ενεργειακή αποδοτικότητα πρέπει να είναι δυνατή μέσω της επιλογής των πλέον αποδοτικών και κατάλληλων αντικειμένων από το σύνολο των ετερογενών αντικειμένων. Ο μεγάλος αριθμός αντικειμένων και συσκευών τα οποία πρέπει να αντιμετωπιστούν και η ποικιλία των τεχνολογιών δικτύωσης και επικοινωνίας, καθώς και τα διοικητικά όρια που πρέπει να υποστηριχθούν απαιτούν διαφορετική προσέγγιση όσον αφορά το management του IoT. Η ιδέα είναι να καταστεί δυνατή η απρόσκοπτη και διαλειτουργική σύνδεση μεταξύ ετερογενών συσκευών και συστημάτων, να αποκρύπτεται η πολυπλοκότητά τους προς τους χρήστες/ ενδιαφερόμενους, παρέχοντας παράλληλα εξελιγμένες υπηρεσίες (Weiser, 1991).

Το κεφάλαιο αυτό παρουσιάζει ένα πλαίσιο γνωστικής διαχείρισης με στόχο την υπέρβαση αυτής της τεχνολογικής ετερογένειας και πολυπλοκότητας. Αυτό το πλαίσιο περιλαμβάνει τις δυνατότητες του να επιλέγεται δυναμικά η συμπεριφορά στοιχείων του IoT (ελεγχόμενη ρύθμιση παραμέτρων του συστήματος), μέσω της λειτουργικότητας της αυτοδιαχείρισης, λαμβάνοντας υπόψη τις πληροφορίες και τις γνώσεις (που λαμβάνονται μέσω της μηχανικής μάθησης) σχετικά με το περιβάλλον λειτουργίας (π.χ. εσωτερική κατάσταση και κατάσταση του περιβάλλοντος), καθώς και πολιτικές (καθορισμός στόχων, περιορισμών, κανόνων κ.λπ.).

Το πλαίσιο περιλαμβάνει τρία βασικά επίπεδα δυνατοτήτων: το Εικονικό Αντικείμενο (VO), το Σύνθετο Εικονικό Αντικείμενο (CVO) και το Επίπεδο Χρηστών / Ενδιαφερομένων και Υπηρεσιών, τα οποία είναι επαναχρησιμοποιήσιμα για την υλοποίηση ποικίλων εφαρμογών, όπως ζωντανή υποβοηθούμενη διαβίωση, έξυπνο γραφείο, έξυπνες μεταφορές, διαχείριση αλυσίδας εφοδιασμού (iCore, 2018). Σε κάθε επίπεδο υπάρχει διαστρωμάτωση, η οποία διαθέτει μηχανισμούς για την εγγραφή, την αναζήτηση και την ανακάλυψη οντοτήτων και τη σύνθεση των υπηρεσιών. Οι γνωστικές οντότητες σε όλα τα επίπεδα παρέχουν τα μέσα αυτοδιαχείρισης (self-management), όπως παραμετροποίηση, θεραπεία, βελτιστοποίηση, προστασία. Από την άποψη αυτή, είναι σε θέση να αντιλαμβάνονται και να αιτιολογούν το πλαίσιο / κατάσταση τους (π.χ. με βάση το φιλτράρισμα συμβάντων, την αναγνώριση προτύπων κλπ) και να λαμβάνουν σχετικές αποφάσεις που βασίζονται στη γνώση (μέσω συναφών αλγορίθμων βελτιστοποίησης και μηχανικής μάθησης).

Τα εικονικά αντικείμενα (VO) στοχεύουν κατά κύριο λόγο στην αφαίρεση της τεχνολογικής ετερογένειας. Τα VO είναι εικονικές αναπαραστάσεις αντικειμένων πραγματικού κόσμου. (π.χ., αισθητήρες, ενεργοποιητές, συσκευές, κ.λπ.). Ένα Σύνθετο Εικονικό Αντικείμενο (CVO) είναι ένας γνωστικός συνδυασμός σημασιολογικά διαλειτουργικών VO το οποίο παρέχει υπηρεσίες σύμφωνα με τις προοπτικές των χρηστών/ ενδιαφερομένων και τις απαιτήσεις της εφαρμογής. Τα αντικείμενα που σχετίζονται με τους χρήστες/ ενδιαφερόμενα μέρη, μεταφέρουν τις αντίστοιχες απαιτήσεις.

Τέτοιες οντότητες είναι ικανές να ανιχνεύουν τις προθέσεις και τη συμπεριφορά χρηστών / ομάδων χρηστών, υπονοώντας και τελικά ενεργώντας εξ ονόματος των χρηστών. Από την άποψη αυτή, υπάρχει αδιάλειπτη υποστήριξη προς τους χρήστες, η οποία ευθυγραμμίζεται πλήρως με τις απαιτήσεις τους (οι μαθησιακές δυνατότητες

των γνωστικών οντοτήτων αυτού του επιπέδου εφαρμόζονται για την απόκτηση γνώσεων σχετικά με τις προτιμήσεις των χρηστών / ενδιαφερομένων κ.λπ.).

Επιπρόσθετα, το πλαίσιο αυτό περιλαμβάνει τρεις βασικές λειτουργίες, τη *Δυναμική Δημιουργία ενός CVO*, τη *Δημιουργία βασιζόμενη στη Γνώση ενός CVO* και την *Αυτοθεραπεία ενός CVO*. Η πρώτη ενέργεια αντιστοιχεί στη δημιουργία ενός CVO από το μηδέν, προκειμένου να παρασχεθεί η ζητούμενη υπηρεσία στους χρήστες. Η δεύτερη λειτουργία επιτρέπει την επαναχρησιμοποίηση ενός ήδη υπάρχοντος CVO. Η λειτουργία αυτοθεραπείας είναι υπεύθυνη για την εύρεση του βέλτιστου εναλλακτικού αντικειμένου, όταν ένα αντικείμενο πραγματικού κόσμου (RWO) δεν είναι προσβάσιμο και μέσω του εικονικού αντικειμένου (VO) του να διατηρήσει τη λειτουργικότητα του CVO.

### A1.1. Επισκόπηση συναφών μελετών σχετικά με το πλαίσιο Διαχείρισης του IoT

Η έννοια της εικονικής απεικόνισης συσκευών / αντικειμένων στο πεδίο του IoT αποτελεί βασικό ζήτημα στην πλειονότητα του Ίντερνετ του μέλλοντος, των έργων του IoT και των ερευνητικών πρωτοβουλιών. Οι Giusto, Iera, Morabito, Atzori και Blefari Melazzi, (Giusto, D., Iera, A., Morabito, G., Atzori, L., Blefari Melazzi, N., 2010) εισάγουν την έννοια του ευέλικτου ψηφιακού στοιχείου (VDI), που είναι ένα πακέτο πληροφοριών για υπηρεσίες, ανθρώπους και φυσικά αντικείμενα, ανεξάρτητα από τη δομή ή τη γεωγραφική θέση του στοιχείου. Ταυτόχρονα, μία μελέτη περίπτωσης πάνω στα διάχυτα εργαστήρια υπολογιστών και επικοινωνιών (Castellani, A.P., Bui, N., Casari, P., Rossi, M., Shelby, Z., Zorzi, M., 2010) στοχεύει στη δημιουργία μιας ανοικτής, επιχειρησιακής αρχιτεκτονικής που θα αντιμετωπίζει τα προβλήματα κλιμάκωσης για μεγάλο αριθμό παγκοσμίως διανεμημένων ασύρματων δικτύων αισθητήρων και ενεργοποιητών (SENSEI, 2018). Επιπλέον, στη μελέτη «Το Σημασιολογικό Middleware για Δικτυωμένα Ενσωματωμένα Συστήματα που εφαρμόζονται στο IoT» (Kostelnik, P., Sarnovsky, M., Furdik, K., 2011) περιγράφεται μια πλατφόρμα, η οποία μεταξύ άλλων έχει ως στόχο να μετατρέψει κάθε συσκευή σε μια διαδικτυακή υπηρεσία με σημασιολογική ανάλυση. Η πλατφόρμα διαθέτει μια αρχιτεκτονική με βάση τα ανοικτά πρωτόκολλα και το μεσαίο λογισμικό, με στόχο να μετασχηματίσει κάθε υποσύστημα ή συσκευή σε διαδικτυακή υπηρεσία με σημασιολογική ανάλυση.

Οι εικονικές αναπαραστάσεις των αντικειμένων του πραγματικού κόσμου (RWOs) εξετάζονται επίσης στο «ARTEMIS SOFIA project» (ARTEMIS SOFIA project, 2018) με στόχο

να καταστούν οι "πληροφορίες" του φυσικού κόσμου διαθέσιμες για έξυπνες υπηρεσίες - συνδέοντας τον φυσικό κόσμο με τον κόσμο της πληροφορίας. Το Smart-M3 (Franchi, A., Di Stefano, L., Tullio, S.C., 2010), που αποτελεί βασική συνιστώσα της πλατφόρμας Ανοικτής Καινοτομίας, στοχεύει στην παροχή της βάσης για τη λύση της πλατφόρμας διαλειτουργικότητας και της ανταλλαγής πληροφοριών μεταξύ τομέων. Το Smart-M3 καθιστά δυνατή τη συμπύκνωση και την ενσωμάτωση πληροφοριών μεταξύ όλων των εφαρμογών και τομέων που κυμαίνονται από διαφορετικούς ενσωματωμένους τομείς στον Παγκόσμιο Ιστό. Η έννοια του "ucode", ενός αναγνωριστικού αριθμού που αποδίδεται σε απτά "φυσικά αντικείμενα" και "χώρους" είναι ένα από τα εργασιακά θέματα του Ιαπωνικού Πανεπιστημιακού Κέντρου Αναγνώρισης (Center, 2018). Αυτή η έννοια των "ucodes" μπορεί επίσης να εφαρμοστεί για περιεχόμενο και πληροφορίες που δεν υπάρχουν στον πραγματικό κόσμο και για πιο αφηρημένες έννοιες.

Μια από τις πιο πρόσφατες μελέτες που σχετίζονται με τις εικονικές αναπαραστάσεις συσκευών / αντικειμένων είναι η έννοια του "Διαδικτύου των πραγμάτων" που συζητήθηκε στο ¨Αρχιτεκτονική του Διαδικτύου των πραγμάτων (IoT) (Guinard, D., Trifa, V., Mattern, F., Wilde, E., 2010), όπου ο στόχος είναι να ενσωματωθούν τα δεδομένα, οι λειτουργίες και η λειτουργικότητα στον Παγκόσμιο Ιστό, αντί να εκτίθενται αυτά μέσω κατακόρυφων σχεδίων συστημάτων. Συγκεκριμένα, προτείνεται ότι η εκμετάλλευση των τεχνολογιών του διαδικτύου είναι μια κατάλληλη λύση για την κατασκευή εφαρμογών πάνω από τις υπηρεσίες που προσφέρουν τα έξυπνα πράγματα.

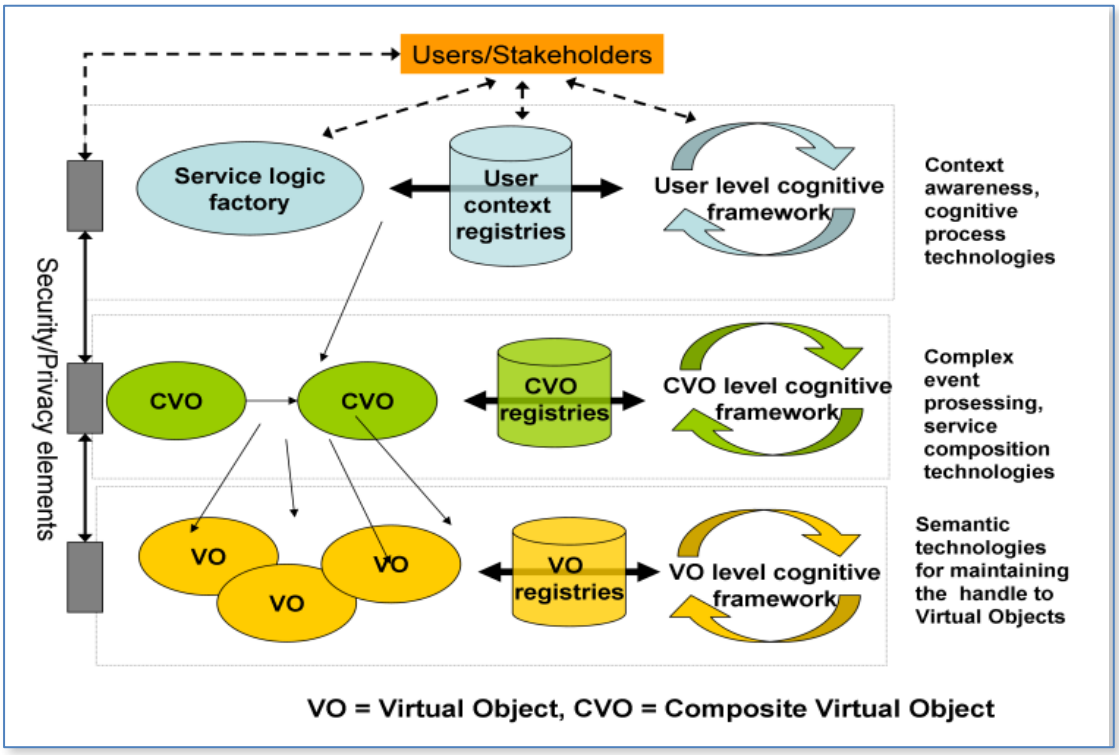
Όσον αφορά την έρευνα σχετικά με τη σημασιολογία VO και CVOs, διάφορες έρευνες αντιμετωπίζουν επίσης το ζήτημα ως μέσο διαλειτουργικότητας. Ένα παράδειγμα εργασίας είναι η «Ενεργοποίηση της άμεσης σύνδεσης μεταξύ ετερογενών» (De Poorter, E., Moerman, I., Demeester, P., 2011) η οποία αποσκοπεί στη διερεύνηση ενοποιημένων ιδεών, μεθόδων και υποδομών λογισμικού που διευκολύνουν την αποτελεσματική ανάπτυξη εφαρμογών που καλύπτουν και ενσωματώνουν το Διαδίκτυο και τον ενσωματωμένο κόσμο. Το πλαίσιο που παρουσιάζεται σε αυτό το έργο στοχεύει σε μια ποικιλία τομέων εφαρμογής και προηγμένων επιχειρηματικών διαδικασιών, ενώ παράλληλα είναι αγνωστικός στον τομέα εφαρμογής στον οποίο θα εφαρμοστεί, επιτρέποντας την επαναχρησιμοποίηση της τεχνολογίας και την ανταλλαγή πληροφοριών μεταξύ τομέων. Η ιδέα VO εισάγεται ως μια δυναμική εικονική αναπαράσταση πραγματικών κόσμων / ψηφιακών αντικειμένων. Επιπλέον,

εισάγεται η έννοια του CVO, ως συλλογή πληροφοριών και υπηρεσιών από μερικές ψηφιακές εικόνες του κόσμου και των VO τους. Η ιδέα της CVO οδηγεί σε έξυπνες υπηρεσίες, ικανοποιώντας τις απαιτήσεις (και από κρυμμένους ενδιαφερόμενους), ενώ οι λεπτομέρειες και η πολυπλοκότητα αποκρύπτονται από τους τελικούς χρήστες. Το προτεινόμενο πλαίσιο περιλαμβάνει γνωστικούς μηχανισμούς που επιτρέπουν τη δυναμική δημιουργία, την επίκληση, την ανάπτυξη, την αυτο-διαμόρφωση, την αυτοδιαχείριση των VO, CVOs και υπηρεσιών.

### A1.2. Πλαίσιο γνωστικής διαχείρισης για το IoT

Το πλαίσιο γνωστικής διαχείρισης για το IoT αποτελείται από το στρώμα των εικονικών αντικειμένων (VO), το στρώμα των σύνθετων εικονικών αντικειμένων (CVOs) και τα επίπεδα χρηστών/ ενδιαφερομένων, όπως έχουν ήδη παρουσιαστεί. Τα προαναφερθέντα επίπεδα του πλαισίου γνωστικής διαχείρισης του IoT απεικονίζονται στην Εικόνα 1.

*Εικόνα 1: Επίπεδα του πλαισίου της Γνωστικής Διαχείρισης (Πηγή: https://cordis.europa.eu/project/rcn/100873_en.html)*




Αυτό το πλαίσιο, επιτρέπει τη διαχείριση (management) διαφόρων αντικειμένων και τις λειτουργίες και τις υπηρεσίες που παρέχουν αυτά τα αντικείμενα. Έτσι, θα καταστεί

δυνατή η υλοποίηση ενός ευρύτερου οικοσυστήματος IoT το οποίο μπορεί να αξιοποιηθεί από πολλούς διαφορετικούς τύπους χρηστών και ενδιαφερομένων (σε διαφορετικούς τομείς εφαρμογής και χρήσης). Ενώ τα φυσικά αντικείμενα (RWOs) μπορεί να ανήκουν (ελέγχονται) από συγκεκριμένο ενδιαφερόμενο, τα εικονικά αντικείμενα (VO) (δηλαδή οι αντλήσεις πραγματικού κόσμου ή ψηφιακών αντικειμένων) μπορούν να ανήκουν (ελέγχονται) από συγκεκριμένους φορείς παροχής υπηρεσιών. Με τη σειρά του, τα CVOs μπορεί να ανήκουν (ελεγχόμενα) από έναν άλλο πάροχο που προσθέτει αξία συνδυάζοντας διαφορετικούς VO και παρέχοντας αυτούς τους συνδυασμούς στους χρήστες. Αυτή η ιεραρχική δομή οδηγεί σε ένα πολύπλοκο οικοσύστημα, το οποίο ανοίγει νέες ευκαιρίες για διάφορους ενδιαφερόμενους. Επιπλέον, το πλαίσιο της Γνωστικής Διαχείρισης θα εξασφαλίσει ότι η πολυπλοκότητα αυτού του οικοσυστήματος θα καλυφθεί καλά από τους διάφορους παράγοντες και ενδιαφερόμενους (Galis & Gavras, 2013).

a) <u>Επίπεδο εικονικών αντικειμένων (VO)</u>

Ο κόσμος του Διαδικτύου των πραγμάτων (IoT) χαρακτηρίζεται από δύο κύρια χαρακτηριστικά: (i) σημαντικό αριθμό αντικειμένων που εμπίπτουν στο πεδίο εφαρμογής οποιασδήποτε εφαρμογής IoT και (ii) εγγενώς αναξιόπιστη φύση τέτοιων αντικειμένων. Σκοπός των VO είναι η αποτελεσματική αντιμετώπιση τέτοιων ζητημάτων και η απόκρυψη της πολυπλοκότητας της υποδομής του IoT. Τα VO είναι εικονικές αναπαραστάσεις ROW και / ή ψηφιακών αντικειμένων που μπορούν να βελτιώσουν το IoT, οπότε τα πραγματικά αντικείμενα γίνονται ουσιαστικά "πάντα ανοιχτά"(always “on”). Ένα VO μπορεί να δημιουργηθεί δυναμικά και να καταστραφεί, μπορεί να αποτελείται από πληροφορίες, υπηρεσίες και είναι ένα δυναμικό αντικείμενο, καθώς πρέπει να αντιπροσωπεύει δυναμικά μεταβαλλόμενα πραγματικά αντικείμενα (RWOs).

Οι γνωστικοί μηχανισμοί στο επίπεδο VO επιτρέπουν την αυτοδιαχείριση και την αυτο-διαμόρφωση των RWOs. Επιπλέον, η εισαγωγή γνωστικών μηχανισμών θα οδηγήσει στη γνώση σχετικά με το πώς αντιδρούν τα RWO σε συγκεκριμένες καταστάσεις. Έτσι, η λειτουργία και ο έλεγχος αυτών των αντικειμένων θα γίνουν πιο αποτελεσματικά.

Το επίπεδο VO περιλαμβάνει μηχανισμούς που παρέχουν επίγνωση σχετικά με την παρουσία και τη συνάφεια των φυσικών αντικειμένων. Μια πλήρης γνώση για τα φυσικά αντικείμενα θα είναι απαραίτητη για να διατηρηθεί η σχέση μεταξύ των VO

και των πραγματικών αντικειμένων που αντιπροσωπεύουν. Αυτή η γνώση χρησιμοποιείται για να έχει μια σταθερή διαχείριση (την άντληση VO) στα καλύτερα κατάλληλα φυσικά αντικείμενα για να διατηρεί τη συσχέτισή τους, ανεξάρτητα από την κινητικότητά τους ή την αποτυχία ορισμένων συνδέσεων μεταξύ τους κ.λπ. Με άλλα λόγια, το επίπεδο VO περιλαμβάνει μηχανισμούς για την παρακολούθηση της κατάστασης / δυνατοτήτων των φυσικών αντικειμένων και τον έλεγχο των διαφόρων δεσμών με φυσικά αντικείμενα ώστε να διασφαλιστεί ότι τα VO είναι ανθεκτικά, ακόμη και όταν τα σχετικά φυσικά αντικείμενα ενδέχεται προσωρινά να μην είναι διαθέσιμα.

Μια άλλη σημαντική πτυχή αυτού του επιπέδου είναι η βελτιστοποίηση από την άποψη των πόρων. Σε αυτή την κατεύθυνση, η ενέργεια διαδραματίζει σημαντικό ρόλο στις μελλοντικές εφαρμογές του IoT. α φυσικά αντικείμενα έχουν ποικίλες πηγές ενέργειας - μερικές από αυτές λειτουργούν με μπαταρία και μερικές τροφοδοτούνται από το δίκτυο. Έχει νόημα ότι τα VO που αντιπροσωπεύουν συσκευές IoT με υψηλή παροχή ενέργειας θα μπορούσαν να αναλάβουν τα καθήκοντα σε σχέση με τα VO που έχουν χαμηλότερη παροχή ενέργειας. Στην πραγματικότητα, κατά τη διαδικασία σχηματισμού ενός CVO, τα VO θα πρέπει να επιλεγούν προσεκτικά για να αποκτήσουν το καλύτερο συνολικά προφίλ πόρων (κυρίως ενέργειας αλλά και άλλων πόρων που εξετάζονται επίσης). Ωστόσο, παράλληλα με τη βελτιστοποίηση των πόρων, θα πρέπει να ληφθεί μέριμνα και για την αξιοπιστία των VO και, συνεπώς, των CVOs. Για παράδειγμα, περισσότεροι VO θα μπορούσαν να μειώσουν την αξιοπιστία ενός CVO. Αυτό είναι κρίσιμο για ορισμένες εφαρμογές όπως η υγεία, οι οποίες απαιτούν μεγαλύτερη αξιοπιστία.

b) <u>Επίπεδο σύνθετων εικονικών αντικειμένων (CVO)</u>

Ένα CVO είναι μια γνωστική συσσωμάτωση σημασιολογικά διαλειτουργικών VO που καθιστούν τις υπηρεσίες σύμφωνα με τις προοπτικές του χρήστη / ενδιαφερομένων και τις απαιτήσεις εφαρμογής / υπηρεσιών. Οι γνωστικοί μηχανισμοί αξιοποιούντια για να επιτρέψουν την επαναχρησιμοποίηση των υφιστάμενων VO και CVOs από διάφορες εφαρμογές, ενδεχομένως και έξω από το πλαίσιο για το οποίο είχαν αρχικά αναπτυχθεί. Με αυτή την έννοια, το επίπεδο CVO περιλαμβάνει λειτουργίες που επιτρέπουν την εύρεση του βέλτιστου δυνατού τρόπου παράδοσης της εφαρμογής / υπηρεσίας, λαμβάνοντας υπόψη: (i) τις απαιτήσεις που προέρχονται από το επίπεδο χρήστη, (ii) τις δυνατότητες που προσφέρουν οι VO και (iii) τις υπάρχουσες λειτουργίες των CVOs. Ένα CVO είναι υπεύθυνο για την παροχή της ζητούμενης υπηρεσίας, κατά

τρόπο που είναι ο πλέον κατάλληλος σε σχέση με το προφίλ και την κατάσταση του χρήστη.

Αποτελεί μία από τις αρμοδιότητες του CVO να διασφαλιστεί η διαθεσιμότητα, η απόδοση και η αξιοπιστία της εφαρμογής και, ως εκ τούτου, των συστατικών υπηρεσιών. Από αυτή την άποψη, το CVO θα είναι υπεύθυνο για την επιλογή των καλύτερων VO (και ενδεχομένως άλλων CVOs), την ενορχήστρωση της λειτουργίας τους, το χειρισμό βλαβών και τελικά την απελευθέρωση των VO. Η επιλογή θα βασίζεται στην καταλληλότητα του VO / CVO, π.χ. όσον αφορά τη συνάφεια με την εφαρμογή, την κατάσταση και το προφίλ πληροφοριών και γνώσεων, καθώς και την κατάστασή τους, π.χ. όσον αφορά τον υπολογισμό, την αποθήκευση, τη μετάδοση και τους ενεργειακούς πόρους. Κάθε CVO θα διαθέτει επίσης τις δικές του (τοπικές) δυνατότητες γνωστικής λειτουργίας. Αυτά προέρχονται από την εκμάθηση της ύπαρξης εικονικού αντικειμένου, της συμπεριφοράς και των δυνατοτήτων καθώς και των παραμέτρων παρακολούθησης και εκμάθησης που σχετίζονται με τη λειτουργία σύνθετου εικονικού αντικειμένου. Αυτό θα χρησιμοποιηθεί για τη βελτιστοποίηση της λειτουργικότητας CVO και τη διαχείριση των περιεχομένων VO κατά τη διάρκεια του κύκλου ζωής CVO.

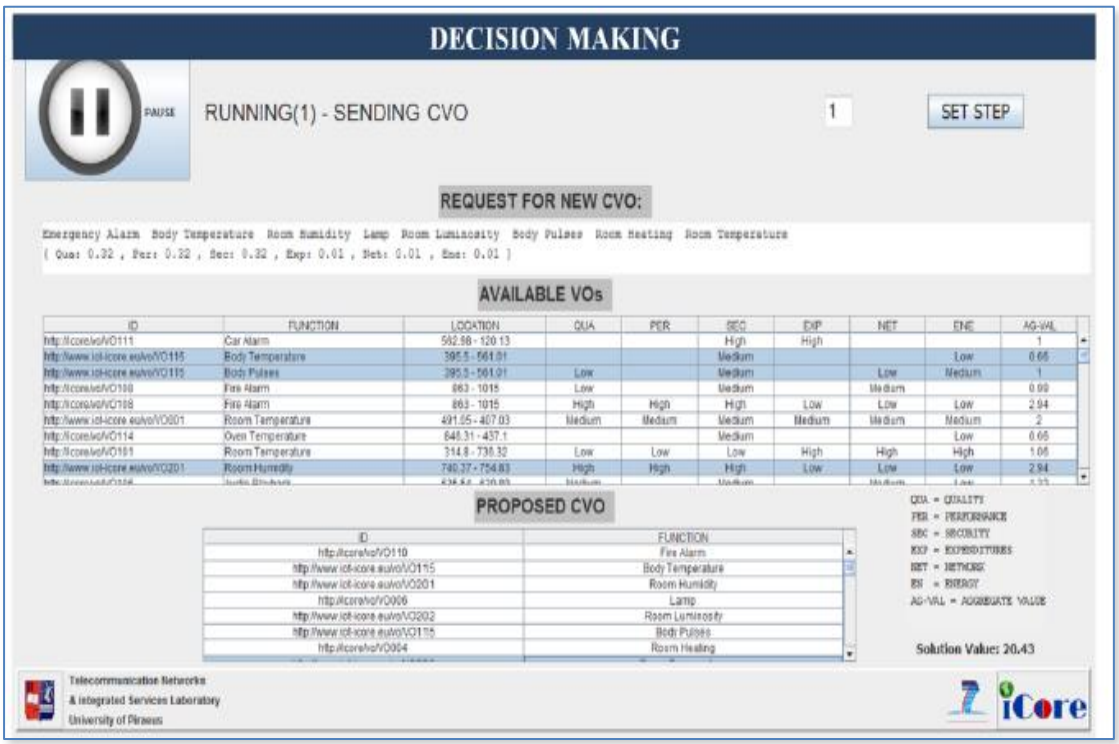
Δύο βασικοί μηχανισμοί του επιπέδου CVO που αναφέρονται στη συνέχεια είναι ο Μηχανισμός αντιστοίχισης αιτημάτων και καταστάσεων (Εικόνα 2) και ο Μηχανισμός λήψης αποφάσεων (Εικόνα 3) (Kelaidonis, D., Somov, A., Foteinos, V., Poulios, G., Stavroulaki, V., Vlacheas, P., Demestichas, P., Baranov, A., Rahim Biswas, A., Giaffreda, R., 2012).

*Εικόνα 2: Μηχανισμός αντιστοίχισης αιτημάτων και καταστάσεων (Πηγή: https://cordis.europa.eu/project/rcn/100873_en.html)*


Ο στόχος του μηχανισμού αντιστοίχισης αιτήσεων και καταστάσεων είναι να εντοπίζονται αιτήματα παρελθόντων υπηρεσιών που ταιριάζουν αρκετά με τα σημερινά και τις καταστάσεις κατά τις οποίες εκδόθηκαν, έτσι ώστε το έργο της σύνθεσης VO από το μηδέν να μπορεί να αποφευχθεί υπό ορισμένες συνθήκες. Προκειμένου να γίνει σύγκριση μεταξύ παρελθουσών και σημερινών καταστάσεων και

αιτημάτων, εντοπίστηκαν παράμετροι που τις περιγράφουν. Οι παράμετροι αιτήματος αποτελούνται από το σύνολο των αιτηθέντων λειτουργιών και πολιτικών. Οι παράμετροι κατάστασης συνίστανται από την ώρα της ημέρας κατά την οποία έγινε η αίτηση, την περιοχή ενδιαφέροντος και τα διαθέσιμα VO εκείνη τη στιγμή. Προκειμένου να ενισχυθεί η διαδικασία φιλτραρίσματος, οι απαιτούμενες λειτουργίες μπορούν να συνδυαστούν με προσεγγιστικές λειτουργίες, π.χ. μια λειτουργία λήψης βίντεο μπορεί να ικανοποιήσει μια απαίτηση για μια λειτουργία λήψης εικόνων. Το αποτέλεσμα αυτού του μηχανισμού είναι η αύξηση της απόδοσης (κυρίως από την άποψη του χρόνου), καθώς η διαδικασία δημιουργίας CVO από την αρχή είναι πιο περίπλοκη. Επιπλέον, η επαναχρησιμοποίηση των πόρων εισάγεται στο σύστημα.

*Εικόνα 3: Μηχανισμός λήψης αποφάσεων (Πηγή: https://cordis.europa.eu/project/rcn/100873_en.html)*




Ο μηχανισμός λήψης αποφάσεων ενεργοποιείται από τον μηχανισμό αντιστοίχισης αιτήσεων και καταστάσεων. Σκοπός του είναι να βρει τη βέλτιστη σύνθεση των VO που να ικανοποιεί τις απαιτούμενες λειτουργίες και πολιτικές. Λαμβάνει ως είσοδο ένα σύνολο διαθέσιμων VO, ένα σύνολο λειτουργιών για κάθε VO, ένα σύνολο χαρακτηριστικών για αυτά τα VO και, τέλος, τις ζητούμενες πολιτικές. Το αποτέλεσμα της διαδικασίας λήψης αποφάσεων είναι η δημιουργία και ενεργοποίηση ενός νέου

CVO. Η περιγραφή του νεοεμφανιζόμενου CVO καταγράφεται στο μητρώο CVO προκειμένου να είναι διαθέσιμο για μελλοντικές αιτήσεις.

c) Επίπεδο χρηστών/ ενδιαφερομένων και εξυπηρέτησης(User/Stakeholder and Service)

Από την οπτική των χρηστών / εφαρμογών, τρεις έννοιες, δηλαδή το IoT, η πανταχού παρούσα υπολογιστική και η περιβαλλοντική ευφυΐα, αποσκοπούν στην παροχή έξυπνων υπηρεσιών στους χρήστες (Schonwalder, J., Fouquet, M., Rodosek, G., Hochstatter, I., 2009). Ένα μέρος της ευφυΐας βασίζεται στην ευαισθητοποίηση της κατάστασης, π.χ. στην παροχή υπηρεσιών ανάλογα με τις ανάγκες που υπάρχουν στον τόπο, στον χρόνο και στη συνολική κατάσταση. Επίσης, σε κοινωνικό επίπεδο, η ευφυΐα απαιτεί επίσης να λαμβάνονται υπόψη οι ανάγκες διαφόρων χρηστών και ενδιαφερομένων. Οι ενδιαφερόμενοι μπορούν να είναι οι ιδιοκτήτες των αντικειμένων και των μέσων επικοινωνίας.

Οι διάφοροι ενδιαφερόμενοι που αποτελούν μέρος του σημερινού Διαδικτύου και θα αποτελέσουν μέρος του Μελλοντικού Διαδικτύου, έχουν ενδιαφέροντα που μπορεί να είναι αντικρουόμενα μεταξύ τους καθώς επίσης και τα δικά τους κριτήρια σχετικά με τον τρόπο με τον οποίο θα μπορούσαν να χρησιμοποιηθούν τα αντικείμενα αυτά και να έχουν πρόσβαση σε αυτά. Επομένως, μια βασική πρόκληση που πρέπει να αντιμετωπιστεί περιλαμβάνει τη διαχείριση της ποικιλίας των πληροφοριών, με σεβασμό της ακεραιότητας των επιχειρήσεων, των αναγκών και των δικαιωμάτων των χρηστών και των διαφόρων ενδιαφερομένων.

Στο παρόν στάδιο, οι αλληλεπιδράσεις μεταξύ χρηστών / ενδιαφερομένων και RWOs ή "πράγματα", είναι κυρίως χειροκίνητα. Η χρήση αυτών των RWO απαιτεί κανονική χειροκίνητη παρέμβαση του χρήστη. Ο χρήστης θα χρειαστεί πληροφορίες σχετικά με τον τρόπο χρήσης ενός "αντικειμένου" και πώς μπορούν να συνδυαστούν αυτά τα αντικείμενα για χρήση. Αυτό το επίπεδο παρέχει τους πραγματικούς μηχανισμούς επιπέδου χρήστη / υπηρεσιών που βρίσκονται πάνω από τα (C) VO και παρέχει τα μέσα για την αξιοποίηση των ψηφιακών αναπαραστάσεων των RWOs για τη δημιουργία εφαρμογών IoT πιο γνωστικών και ευαισθητοποιημένων ως προς την πρόθεση του τελικού χρήστη (Galis & Gavras, 2013).

Το επίπεδο χρήστη / ενδιαφερομένου και υπηρεσίας περιλαμβάνει μηχανισμούς για τον εντοπισμό των απαιτήσεων που προέρχονται από διαφορετικούς τύπους χρηστών, τις εξαρτήσεις που προκαλούν, από μόνοι τους και σε μεγάλες ομάδες χρηστών, καθώς

και σε ολόκληρο τον χώρο και τον χρόνο. Οι αλλαγές των καταστάσεων των χρηστών και των συσκευών, μεμονωμένα ή συλλογικά σε ολόκληρο τον πληθυσμό, τον χρόνο και το χώρο του χρήστη, συχνά παρουσιάζουν ορισμένα πρότυπα, έτσι η συμπεριφορά των χρηστών και μέρος των προθέσεων των χρηστών θα μπορούσαν να προκύψουν από αυτό. Επιπλέον, αυτό το επίπεδο περιλαμβάνει μηχανισμούς για την κατάλληλη (αυτοματοποιημένη) ανάλυση των απαιτήσεων εφαρμογής / υπηρεσίας για τη δημιουργία της κατάλληλης λογικής υπηρεσίας και των περιγραφών που επιτρέπουν λογική εξυπηρέτηση για τη δημιουργία παραδειγμάτων εφαρμογών και λειτουργιών ενεργοποίησης εφαρμογών στο επίπεδο CVO.

## A1.3. Εφαρμογή πλαισίου

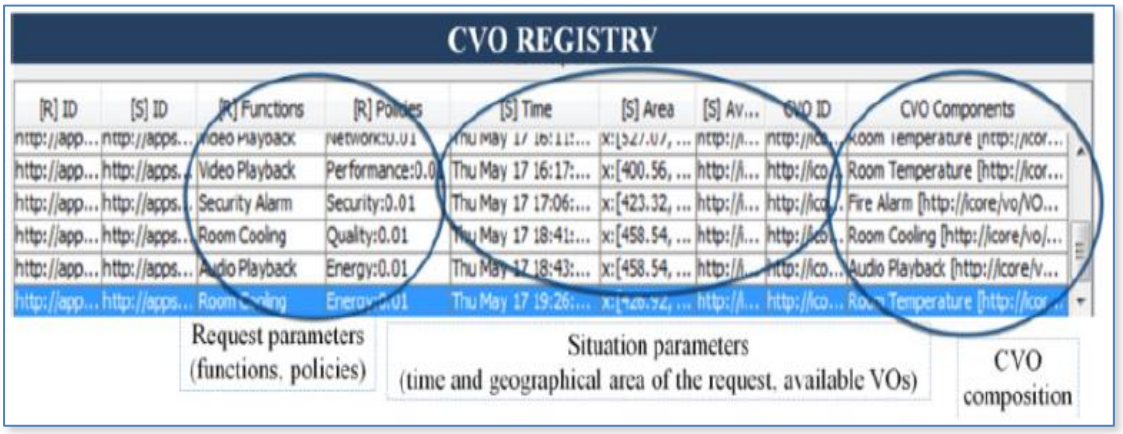
### A1.3.1 Λειτουργία

Ένα πρωτότυπο του πλαισίου της Γνωστικής Διαχείρισης που έχει περιγραφεί ανωτέρω, έχει εφαρμοστεί. Η τρέχουσα αντίστοιχη εφαρμογή περιλαμβάνει, εκτός από τα εξαρτήματα λογισμικού για τα διάφορα λειτουργικά στοιχεία που παρουσιάστηκαν στην προηγουμένως, έναν αριθμό πραγματικών αισθητήρων και ενεργοποιητών. Αυτή η υπό-ενότητα παρέχει μια υψηλού επιπέδου οπτική του εφαρμοσμένου πλαισίου και παρουσιάζει τρεις βασικές λειτουργίες που αυτό διαθέτει, δηλαδή η δυναμική δημιουργία CVO, η εκδοχή CVO βασισμένη στη γνώση και η αυτοθεραπεία ενός CVO (Galis & Gavras, 2013).

a) Δυναμική δημιουργία ενός CVO

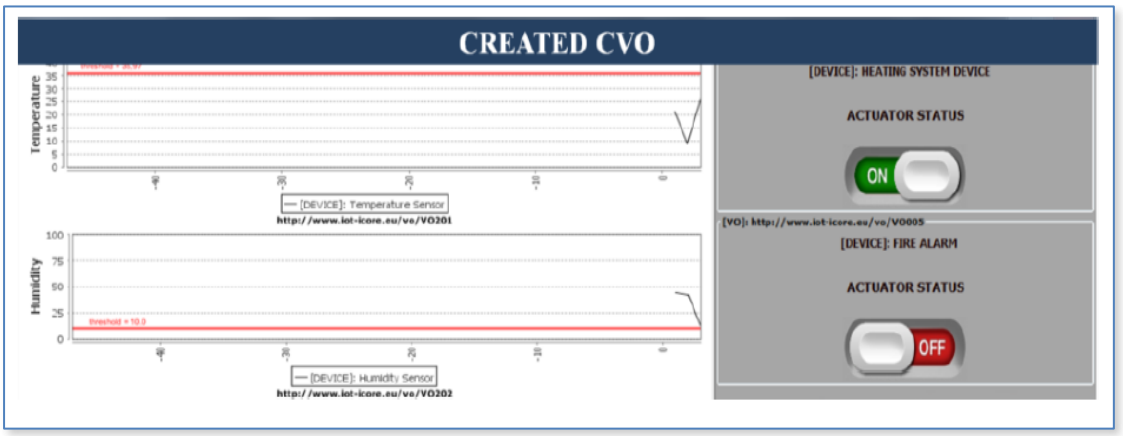
Ένας χρήστης ζητά μια υπηρεσία και δηλώνει τη σημασία των χαρακτηριστικών υπηρεσίας / λειτουργίας, που χαρακτηρίζονται ως πολιτικές, οι οποίες πρέπει να τηρούνται από το σύστημα. Αυτό το αίτημα καταγράφεται μέσω Διεπαφής Χρήστη σε επίπεδο Υπηρεσίας και επεξεργάζεται, προκειμένου να εξαχθούν οι απαιτούμενες λειτουργίες και οι καθορισμένες πολιτικές. Οι πληροφορίες αυτές εμπλουτίζονται με τις παραμέτρους της κατάστασης (περιοχή ενδιαφέροντος, ώρα αιτήματος) και διαβιβάζονται στον μηχανισμό αντιστοίχισης αιτήσεων και καταστάσεων. Επιπλέον, οι μηχανισμοί μάθησης παρέχουν πληροφορίες σχετικά με τις προτιμήσεις των χρηστών. Ο μηχανισμός αντιστοίχισης αιτήσεων και καταστάσεων αναζητά στο μητρώο CVO, ένα ήδη υπάρχον CVO που μπορεί να ικανοποιήσει το αίτημα (Εικόνα 4).

*Εικόνα 4: Μητρώο CVO (Πηγή: The IEEE International Conference on Internet of Things)*




Εάν η επαναχρησιμοποίηση μιας CVO δεν είναι δυνατή, τότε προωθεί τις σχετικές πληροφορίες στην απόφαση λήψης αποφάσεων, προκειμένου να δημιουργήσει τη βέλτιστη σύνθεση των VO, σύμφωνα με τις απαιτούμενες λειτουργίες και πολιτικές. Για το σκοπό αυτό, οι πληροφορίες σχετικά με τις διαθέσιμες λειτουργίες VO και τις παρεχόμενες λειτουργίες (περιγραφές VO) ανακτώνται από το μητρώο των VO. Μόλις δημιουργηθεί μια CVO, το αίτημα, η σχετική κατάσταση και η σύνθεση CVO καταγράφονται στο μητρώο CVO, προκειμένου να διασφαλιστεί ότι εάν μια παρόμοια συμφραζόμενη κατάσταση εμφανιστεί και πάλι, η λύση μπορεί να ανακτηθεί άμεσα. Τέλος, το CVO που δημιουργείται παρέχει την ζητούμενη υπηρεσία για χρήση (Εικόνα 5).

*Εικόνα 5: CVO που δημιουργήθηκε (Πηγή: The IEEE International Conference on Internet of Things)*




b) Εκδοχή CVO βασισμένη στη γνώση

Αυτή η διαδικασία επιτρέπει την επαναχρησιμοποίηση ενός ήδη υπάρχοντος CVO. Τα βήματα της προηγούμενης λειτουργίας επαναλαμβάνονται μέχρι να ληφθεί το αίτημα

από το στοιχείο αντιστοίχισης αιτήματος και κατάστασης. Σε αυτό το σημείο, το αίτημα υπηρεσίας και οι πληροφορίες κατάστασης μπορούν να συγκριθούν με τα αρχεία στο μητρώο CVO για επαρκή αντιστοιχία. Τα προηγούμενα αρχεία που αντιστοιχούν σε στοιχεία CVO (VO) με λειτουργίες που δεν είναι διαθέσιμες στην τρέχουσα κατάσταση (είτε ακριβώς είτε κατά προσέγγιση) φιλτράρονται, καθώς σίγουρα δεν μπορούν να εκπληρώσουν τους στόχους υπηρεσίας. Τα υπόλοιπα αρχεία επαναξιολογούνται και κατατάσσονται βάσει μιας μέτρησης ομοιότητας ως προς την ικανοποίηση και το αρχείο με την υψηλότερη κατάταξη εξετάζεται σε σχέση με το κατώτατο όριο ομοιότητας (Galis & Gavras, 2013). Το ποσοστό ικανοποίησης εξαρτάται από το ποσό των συνολικών αιτούμενων λειτουργιών που είναι διαθέσιμες καθώς και από τους συσχετισμούς τους και υπολογίζεται ως βαθμός (π.χ. άθροισμα) αυτών των συσχετισμών μεταξύ του συνόλου των αιτούμενων και των απαιτούμενων λειτουργιών CVO.

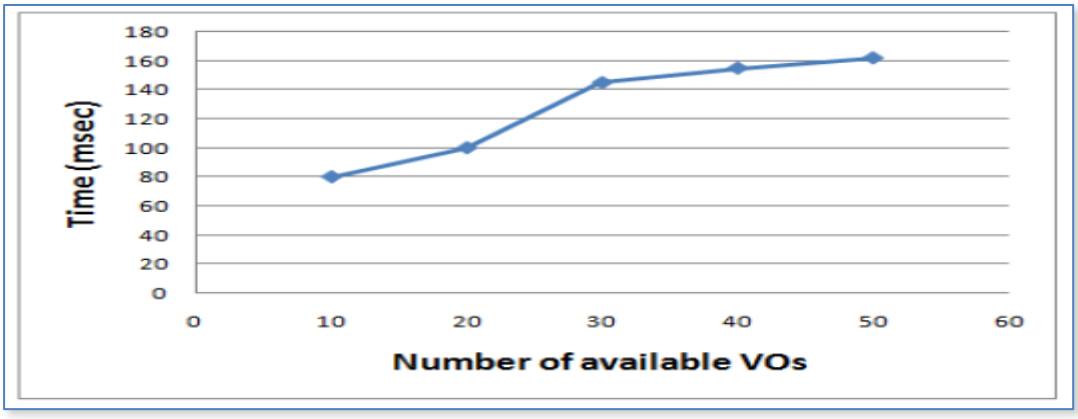
Εκτός από τις λειτουργίες, για τον υπολογισμό της συνολικής μετρικής ομοιότητας λαμβάνονται επίσης υπόψη και οι υπόλοιπες από τις παραμέτρους της κατάστασης και του αιτήματος. Εάν η συνολική μετρική ομοιότητα για υπάρχον CVO ισούται με ή υπερβαίνει ένα συγκεκριμένο όριο, τότε αυτό το υφιστάμενο CVO μπορεί να θεωρηθεί κατάλληλο για νέο-εκδοθέν αίτημα. Με αυτό τον τρόπο, τα στοιχεία επιπέδου CVO μπορούν να εφαρμόσουν γνωστές λύσεις ως απάντηση σε μια αίτηση υπηρεσίας, μειώνοντας έτσι τον χρόνο που απαιτείται για το χειρισμό των αιτημάτων από το επίπεδο της Υπηρεσίας.

c) Αυτοθεραπεία ενός CVO

Η διαδικασία αυτοΐασης επιτρέπει την ανίχνευση ενός προβλήματος στη λειτουργία ενός χρησιμοποιημένου RWO και του αντίστοιχου VO και τη δυναμική αναδιάταξη του αντίστοιχου CVO για να ξεπεραστεί το πρόβλημα. Αυτή η διαδικασία ενεργοποιείται όταν εντοπιστεί μια βλάβη ενός VO εξαιτίας της έλλειψης προσέγγισης του RWO (π.χ. λόγω απώλειας συνδεσιμότητας του VO με το RWO, αποτυχίες υλικού RWO κ.λπ.). Ένα αίτημα ανασυγκρότησης εκδίδεται από το στοιχείο αίτησης και αντιστοίχισης κατάστασης στο στοιχείο λήψης αποφάσεων. Το στοιχείο λήψης απόφασης επιλέγει τότε το πιο κατάλληλο VO (και συνεπώς RWO) για την αντικατάσταση του προβληματικού VO. Πληροφορίες σχετικά με την ανασυγκρότηση του CVO αποθηκεύονται στο μητρώο CVO.

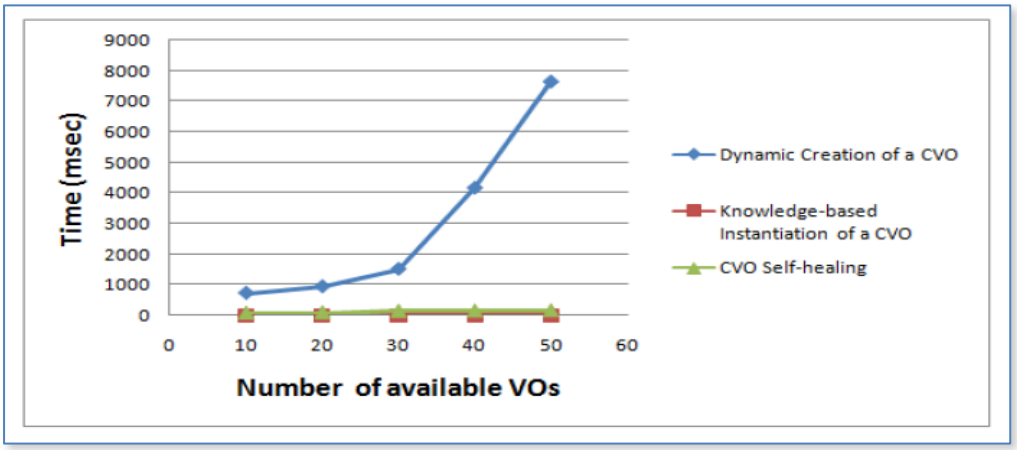
Προκειμένου να επιτευχθούν αποτελέσματα σχετικά με την αποτελεσματικότητα και την επεκτασιμότητα αυτού του πλαισίου, πραγματοποιήθηκαν διάφορα πειράματα για διαφορετικό αριθμό διαθέσιμων VO στην περιοχή ενδιαφέροντος. Η Εικόνα 6 παρουσιάζει τον χρόνο που απαιτείται για τον μηχανισμό λήψης αποφάσεων για να βρεθεί η βέλτιστη σύνθεση των VO, καθώς αυξάνεται ο αριθμός των διαθέσιμων VO. Όπως μπορεί να παρατηρηθεί, ενώ αυτή τη φορά αυξάνεται καθώς ο αριθμός των VO αυξάνεται, παρόλα αυτά παραμένει κάτω από ένα δευτερόλεπτο. Ο αλγόριθμος ILOG CPLEX OPTIMIZER (CPLEX) χρησιμοποιήθηκε για την αξιολόγηση αυτού του μηχανισμού.

*Εικόνα 6: Χρόνος εκτέλεσης μηχανισμού λήψης αποφάσεων (Πηγή: The IEEE International Conference on Internet of Things)*




Η Εικόνα 7 απεικονίζει τους χρόνους εκτέλεσης για όλες τις λειτουργίες. Όπως αναμένεται, η Δυναμική Δημιουργία ενός CVO επηρεάζεται κυρίως από την αύξηση των διαθέσιμων VO. Συγκεκριμένα χρειάζονται πάνω από 700msec για 10 VOs, ενώ το ποσό αυτό αυξάνεται σε πάνω από 7000msec για 50 VOs. Η εξοικονόμηση χρόνου είναι εμφανής στην περίπτωση της εκδοχή του CVO βασισμένου στη γνώση, όπου η ζητούμενη υπηρεσία μπορεί να προσφερθεί σε λίγα μόνο msec (λόγω της λειτουργίας μόνο του μηχανισμού αντιστοίχισης αιτήσεων και καταστάσεων). Επιπλέον, επιτυγχάνεται εξοικονόμηση χρόνου στην περίπτωση της Αυτοθεραπείας ενός CVO. Αυτή η λειτουργία αντικαθιστά μόνο το VO που δεν μπορεί να λειτουργήσει σωστά και εκμεταλλεύεται τα υπόλοιπα. Επομένως, απαιτείται ελάχιστος χρόνος, σε σύγκριση με τη δημιουργία του CVO από το μηδέν (Galis & Gavras, 2013).

*Εικόνα 7: Χρόνος εκτέλεσης των λειτουργιών πλαισίου γνωστικής διαχείρισης (Πηγή: The IEEE International Conference on Internet of Things)*




### A1.3.2 Παράδειγμα υποβοηθούμενης διαβίωσης

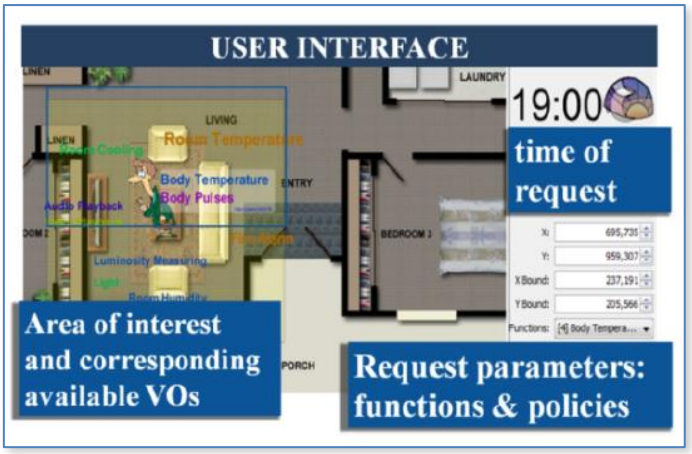
Αυτή η υποενότητα παρουσιάζει ένα ενδεικτικό παράδειγμα του τρόπου με τον οποίο οι τρεις λειτουργίες του προτεινόμενου πλαισίου μπορούν να εφαρμοστούν σε ένα σενάριο υποβοηθούμενης διαβίωσης. Το σενάριο περιλαμβάνει δύο διαφορετικούς (επιχειρηματικούς) τομείς. (α) ένα έξυπνο σπίτι όπου ζει μια ηλικιωμένη γυναίκα (κ. Σοφία) που επέλεξε μια υποβοηθούμενη διαβίωση και (β) ένα ιατρικό κέντρο όπου οι γιατροί παρακολουθούν από απόσταση την περιβαλλοντική κατάσταση και την κατάσταση της υγείας της κ. Σοφίας χρησιμοποιώντας τα έξυπνα αντικείμενα που υπάρχουν στο έξυπνο σπίτι. Στην έξυπνη κατοικία έχει εγκατασταθεί ένα σύνολο RWO, που αποτελείται από αισθητήρες (αισθητήρες θερμοκρασίας, αισθητήρες υγρασίας, αισθητήρα φωτεινότητας) που συνδέονται με πλατφόρμα Waspmote (Libelium, 2018) και ενεργοποιητές (δηλαδή ανεμιστήρα, λυχνία LED, και μια λάμπα) που συνδέονται με μια πλατφόρμα Arduino (Arduino, 2018).

Αρχικά, ένας γιατρός μέσω κατάλληλου περιβάλλοντος χρήστη (Εικόνα 8) παρέχει ένα σύνολο εφαρμογών / απαιτούμενων λειτουργιών και πολιτικών εφαρμογής / υπηρεσιών (π.χ. ενεργειακή απόδοση). Στο επίπεδο υπηρεσίας, το σύνολο των παραμέτρων αιτήματος και κατάστασης εξάγεται και διαβιβάζεται στον μηχανισμό αντιστοίχισης αιτήματος και κατάστασης, ο οποίος με τη σειρά του αναζητά στο μητρώο CVO ένα CVO που είχε δημιουργηθεί προηγουμένως και θα μπορούσε να ικανοποιήσει την αιτούμενη εφαρμογή / υπηρεσία. Αρχικά δεν έχει βρεθεί η κατάλληλη CVO και οι παρασχεθείσες παράμετροι αποστέλλονται στη διαδικασία λήψης αποφάσεων, η οποία θα επιλέξει τα καταλληλότερα VO για να ικανοποιήσει τις απαιτήσεις και τις πολιτικές με τον καλύτερο δυνατό τρόπο και θα ενεργοποιήσει τη

δημιουργία ενός νέου CVO. Το νεοδημιουργημένο CVO καταχωρείται στο μητρώο CVO μαζί με τις παραμέτρους της κατάστασης, σύμφωνα με τις οποίες ζητήθηκε για μελλοντική αναφορά από το μηχανισμό αντιστοίχισης αιτήματος και κατάστασης.

Ο γιατρός ή μέλος του ιατρικού προσωπικού μπορεί να χρησιμοποιήσει το δυναμικά δημιουργημένο CVO για να παρακολουθήσει την ιατρική κατάσταση της κ. Σοφίας. Μπορούν να παρασχεθούν αναφορές σχετικά με τη λειτουργία του CVO και να αποθηκευτούν στο μητρώο CVO για μελλοντική χρήση. Κάποια στιγμή αργότερα, ένας άλλος γιατρός εκδίδει παρόμοιο αίτημα για παρακολούθηση της κ. Σοφίας. Το αίτημα αυτό μαζί με τα αιτήματα και τις παραμέτρους που προέρχονται από αυτό διαβιβάζονται στο μηχανισμό αντιστοίχισης αιτήματος και κατάστασης. Αυτή τη φορά, υπάρχει ήδη ένα CVO που μπορεί να ικανοποιήσει τις απαιτήσεις εφαρμογής / υπηρεσίας στο μητρώο CVO. Επομένως, η αντιστοίχιση Αίτησης και Κατάστασης προχωρά με την άμεση εκδοχή του, χωρίς να χρειάζεται να ενεργοποιηθεί ο μηχανισμός λήψης αποφάσεων. Κατά τη διάρκεια της εκτέλεσης του CVO, ένας από τους χρησιμοποιούμενους αισθητήρες φωτεινότητας αποτυγχάνει. Αυτό εντοπίζεται από το εφαρμοσμένο CVO και ενεργοποιείται ο μηχανισμός λήψης αποφάσεων ώστε να βρεθούν εναλλακτικές συσκευές αισθητήρων φωτεινότητας που θα μπορούσαν να αξιοποιηθούν (μέσω των αντίστοιχων VO) προκειμένου να αντικατασταθούν στο συνολικό CVO, διασφαλίζοντας έτσι τη συνέχεια της παροχής υπηρεσιών. Το CVO έχει επαναρυθμιστεί κατάλληλα.

*Εικόνα 8: Γραφικό περιβάλλον διεπαφής χρήστη (Πηγή: The IEEE International Conference on Internet of Things)*



## Α2. Μοντέλα επικοινωνίας

Μια σημαντική παράμετρος η οποία πρέπει να διερευνηθεί και να αναπτυχθεί είναι τα μοντέλα επικοινωνίας μεταξύ των συσκευών του IoT. Η διερεύνηση του τρόπου με τον οποίο οι συσκευές του IoT συνδέονται και επικοινωνούν σε σχέση με τα τεχνικά μοντέλα επικοινωνίας, είναι ιδιαίτερης σημασίας στο τρόπο διαχείρισης του IoT. Τον Μάρτιο του 2015, το Συμβούλιο Αρχιτεκτονικής του Διαδικτύου (Internet Architecture Board, IAB) κυκλοφόρησε ένα κατευθυντήριο αρχιτεκτονικό έγγραφο για τη δικτύωση των έξυπνων αντικειμένων, που περιγράφει ένα πλαίσιο τεσσάρων κοινών μοντέλων επικοινωνίας το οποίο χρησιμοποιείται από συσκευές IoT.

Τα μοντέλα αυτά επικοινωνίας είναι το μοντέλο Device-to -Device, το Μοντέλο Device-to-Cloud, το Μοντέλο Device-to-Gateway και το Μοντέλο Back-End Data-Sharing (Tschofenig, 2018) τα οποία και αναπτύσσονται ακολούθως.

### Α2.1. Μοντέλο Device-to -Device

Το μοντέλο επικοινωνίας Device-to-Device αντιπροσωπεύει δύο ή περισσότερες συσκευές που συνδέονται άμεσα και επικοινωνούν μεταξύ τους. Η επικοινωνία είναι άμεση μεταξύ των συσκευών και δεν παρεμβάλλεται ενδιάμεσος server εφαρμογών. Οι συσκευές αυτές επικοινωνούν μέσω πολλών τύπων δικτύων, συμπεριλαμβανομένων των δικτύων IP ή το Internet. Ωστόσο αυτές οι συσκευές δύνανται να χρησιμοποιούν πρωτόκολλα όπως Bluetooth, 40 Z-Wave, 41 ή ZigBee42 για τη καθιέρωση device-to-device επικοινωνίας (Εικόνα 9).

*Εικόνα 9: Παράδειγμα μοντέλου επικοινωνίας Device-to-Device*


Το μοντέλο αυτό επιτρέπει τις συσκευές που συμμορφώνονται με ένα συγκεκριμένο πρωτόκολλο επικοινωνίας να επικοινωνούν και να ανταλλάσσουν μηνύματα για να επιτευχθεί η λειτουργία τους. Το Device-to-Device μοντέλο χρησιμοποιείται ευρέως σε εφαρμογές όπως τα συστήματα οικιακού αυτοματισμού, που συνήθως χρησιμοποιούν μικρά πακέτα δεδομένων πληροφοριών για την επικοινωνία μεταξύ συσκευών με χαμηλό ρυθμό μετάδοσης δεδομένων. Οικιακές IoT συσκευές όπως διακόπτες φωτισμού, κλειδαριές,

λαμπτήρες κλπ συνήθως στέλνουν μικρές ποσότητες πληροφοριών μεταξύ τους. Αυτές οι συσκευές έχουν συχνά άμεση σχέση μεταξύ τους και έχουν συνήθως ενσωματωμένη ασφάλεια, όμως χρησιμοποιούν και μοντέλα δεδομένων για συγκεκριμένες συσκευές που απαιτούν επιπλέον προσπάθειες ανάπτυξης από κατασκευαστικής πλευράς. Αυτό μεταφράζεται στη δημιουργία της ανάγκης, από κατασκευαστικής πλευράς, να γίνει μία περεταίρω αναπτυξιακή προσπάθεια για την υλοποίηση συσκευών με χρήση των τυποποιημένων μορφών δεδομένων.

Από την οπτική γωνία των χρηστών όταν χρησιμοποιείται το πρωτόκολλο επικοινωνίας του μοντέλου Device-to-Device, παρατηρείται συχνά μη συμβατότητα συσκευών, γεγονός που αναγκάζει το χρήστη να επιλέξει μια οικογένεια συσκευών που να χρησιμοποιεί το ίδιο πρωτόκολλο. Παραδείγματος χάριν, η οικογένεια των συσκευών που χρησιμοποιεί το πρωτόκολλο Z-Wave δεν είναι συμβατή με την οικογένεια συσκευών που χρησιμοποιεί το πρωτόκολλο ZigBee. Παρόλο που αυτές οι ασυμβατότητες περιορίζουν τις επιλογές των χρηστών, σε συσκευές που να χρησιμοποιούν ένα συγκεκριμένο πρωτόκολλο, οι χρήστες επωφελούνται από το γεγονός ότι τα προϊόντα μιας συγκεκριμένης οικογένειας τείνουν να επικοινωνούν καλύτερα μεταξύ τους (Duffy Marsan, 2018).

### A.2.2. Μοντέλο Device-to-Cloud

Στο μοντέλο επικοινωνίας Device-to-Cloud, η IoT συσκευή συνδέεται απευθείας σε μια διαδικτυακή υπηρεσία cloud όπως ένας πάροχος υπηρεσιών εφαρμογής, ώστε να ανταλλάσσει δεδομένα και να διαχειρίζεται την κίνηση μηνυμάτων. Αυτή η προσέγγιση συχνά εκμεταλλεύεται υπάρχοντες μηχανισμούς επικοινωνίας όπως η παραδοσιακή ενσύρματη Ethernet ή Wi-Fi συνδέσεις για να εγκαταστήσει μια σύνδεση μεταξύ της συσκευής και του δικτύου IP, το οποίο τελικά συνδέεται με την υπηρεσία cloud. Η Εικόνα 10 απεικονίζει ένα διάγραμμα μοντέλου επικοινωνίας Device-to-Cloud.

*Εικόνα 10: Παράδειγμα μοντέλου επικοινωνίας Device-to-Cloud*

Αυτό το επικοινωνιακό μοντέλο χρησιμοποιείται από κάποιες γνωστές συσκευές IoT, όπως το Learning Thermostat της Nest Labs και η SmartTV της Samsung. Στην περίπτωση του Learning Thermostat της Nest, η συσκευή μεταδίδει δεδομένα σε μια cloud βάση δεδομένων όπου τα δεδομένα μπορούν να χρησιμοποιηθούν για να αναλύουν την κατανάλωση οικιακής ενέργειας. Ή σύνδεση αυτή με το cloud δίνει τη δυνατότητα στον χρήστη να αποκτήσει εξ αποστάσεως πρόσβαση στον θερμοστάτη του μέσω ενός smartphone ή μέσω του ιστού (web). Υποστηρίζει επίσης αναβαθμίσεις λογισμικού για τον θερμοστάτη. Παρομοίως με την τεχνολογία SmartTV της Samsung, η τηλεόραση χρησιμοποιεί μια διαδικτυακή σύνδεση για να μεταδίδει πληροφορίες προβολών του χρήστη στη Samsung για ανάλυση και να ενεργοποιεί τις διαδραστικές λειτουργίες αναγνώρισης ομιλίας που διαθέτει η τηλεόραση. Σε αυτές τις περιπτώσεις, το μοντέλο Device-to-Cloud προσθέτει αξία στον χρήστη επεκτείνοντας τις δυνατότητες της συσκευής πέρα από τα εγγενή της χαρακτηριστικά (Samsung Privacy Policy--SmartTV Supplement, 2018).

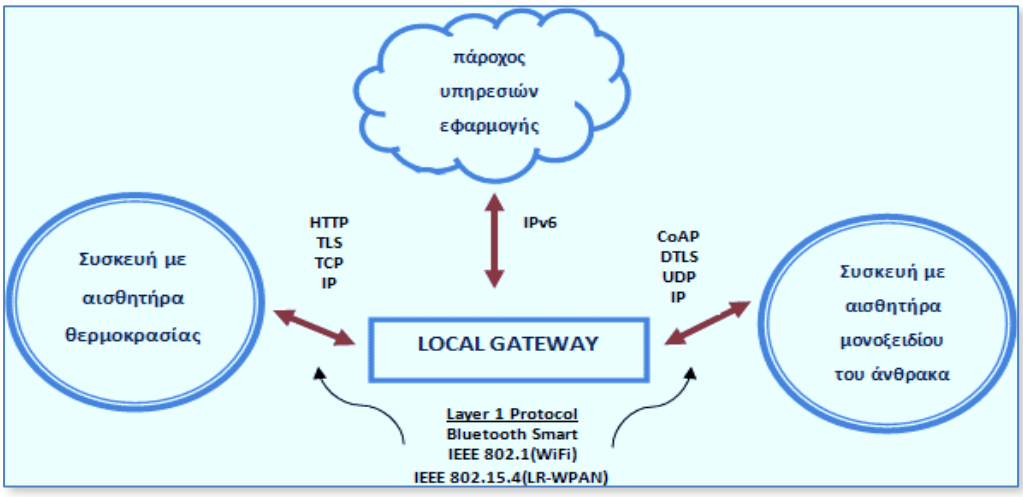
Ακόμη όμως και στο μοντέλο επικοινωνίας Device-to-Cloud, υπάρχουν προκλήσεις όσον αφορά τη διαλειτουργικότητα όταν γίνεται προσπάθεια ενοποίησης συσκευών με διαφορετικά κατασκευαστικά χαρακτηριστικά. Συνήθως, η συσκευή και η υπηρεσία cloud παρέχονται από τον ίδιο προμηθευτή, όμως εάν χρησιμοποιούνται πρωτόκολλα δεδομένων βιομηχανικής ιδιοκτησίας μεταξύ της συσκευής και της υπηρεσίας cloud, τότε ο ιδιοκτήτης ή ο χρήστης της συσκευής ενδεχομένως να δεσμεύεται από συγκεκριμένη υπηρεσία cloud, περιορίζοντας ή αποτρέποντας τη χρήση εναλλακτικών πάροχων υπηρεσιών. Το πιο γνωστό παράδειγμα αυτής της περίπτωσης είναι αυτό της Apple και του Icloud. Αυτό αναφέρεται κοινώς ως «κλείδωμα προμηθευτών» (vendor lock-in), ένας όρος που περικλείει άλλες όψεις της σχέσης με τον πάροχο όπως η ιδιοκτησία και η πρόσβαση στα δεδομένα. Ταυτόχρονα, οι χρήστες μπορούν να είναι σίγουροι ότι συσκευές που είναι σχεδιασμένες για τη συγκεκριμένη πλατφόρμα μπορούν να ενσωματωθούν (Christos Stergiou, Kostas E. Psannis, Byung-Gyu Kim, Brij Gupta, 2016).

### A.2.3. Μοντέλο Device-to-Gateway

Στο μοντέλο Device-to-Gateway, ή αλλιώς Device-to-application-layer-Gateway (ALG), η συσκευή IoT συνδέεται μέσω μιας υπηρεσίας ALG ως αγωγός για να επιτευχθεί μια σύνδεση με την υπηρεσία cloud. Με πιο απλά λόγια, αυτό σημαίνει ότι το μοντέλο Device-to-Gateaway διαθέτει λογισμικό εφαρμογής, το οποίο δρα ως διαμεσολαβητής μεταξύ της συσκευής και της υπηρεσίας cloud και παρέχει ασφάλεια και άλλες λειτουργίες όπως

δεδομένα ή μετάφραση πρωτοκόλλων. Η εικόνα που ακολουθεί απεικονίζει το μοντέλο Device-to-Gateway.

*Εικόνα 11: Παράδειγμα μοντέλου επικοινωνίας Device-to-Gateway*




Αρκετές μορφές του μοντέλου αυτού βρίσκονται στις καταναλωτικές συσκευές. Σε πολλές περιπτώσεις, οι συσκευές που χρησιμοποιούν αυτό το μοντέλο επικοινωνίας είναι τα smartphones, τα οποία «τρέχουν» εφαρμογές για να επικοινωνήσουν με τις IoT συσκευές και να μεταφέρουν δεδομένα σε μια υπηρεσία cloud. Αυτό είναι συχνά το μοντέλο που χρησιμοποιείται σε δημοφιλή είδη ευρείας κατανάλωσης, όπως τα personal fitness trackers. Αυτές οι συσκευές δεν έχουν την ικανότητα να συνδεθούν απευθείας σε μια υπηρεσία cloud, έτσι συχνά βασίζονται σε εφαρμογές των smartphones οι οποίες λειτουργούν ως μεσάζοντες για να συνδεθεί η συσκευή εκγύμνασης στο cloud.

Μια άλλη μορφή του μοντέλου επικοινωνίας Device-to-Gateway είναι η ανάδυση των συσκευών “Hub” σε εφαρμογές οικιακού αυτοματισμού. Τα “Hub” είναι συσκευές που λειτουργούν ως Local Gateway μεταξύ των μεμονωμένων IoT συσκευών και μιας υπηρεσίας cloud, αλλά μπορούν επίσης να γεφυρώσουν το χάσμα της διαλειτουργικότητας μεταξύ των IoT συσκευών. Για παράδειγμα, το Hub SmartThings είναι μια αυτόνομη συσκευή Gateway που έχει εγκατεστημένους Z-Wave και Zigbee πομποδέκτες για να μπορεί να επικοινωνεί και με τις δύο οικογένειες των συσκευών. Στη συνέχεια, συνδέεται με την υπηρεσία cloud Smart Things, επιτρέποντας στο χρήστη να αποκτήσει πρόσβαση στις συσκευές χρησιμοποιώντας μόνο μία εφαρμογή smartphone και μια σύνδεση στο Internet.

Αυτό το μοντέλο επικοινωνίας χρησιμοποιείται σιγά σιγά για την ενσωμάτωση νέων έξυπνων συσκευών σε ένα ήδη υπάρχων σύστημα με συσκευές που δεν είναι διαλειτουργικές. Ένα μειονέκτημα αυτής της προσέγγισης είναι ότι η συνεχής και απαραίτητη ανάπτυξη του

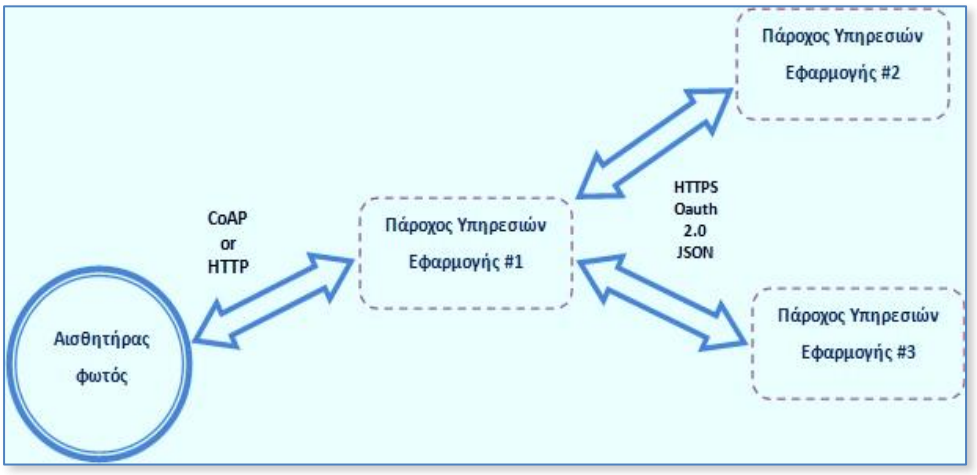
συστήματος και του λογισμικού εφαρμογών το κάνει πολύπλοκο και με μεγάλο κόστος (How It Works, 2018).

### A.2.4. Μοντέλο Back-End Data-Sharing

Το μοντέλο Back-End Data-Sharing αναφέρεται σε μια αρχιτεκτονική επικοινωνίας η οποία επιτρέπει στους χρήστες να εξάγουν και να αναλύουν τα δεδομένα του έξυπνου αντικειμένου από μια υπηρεσία cloud, σε συνδυασμό με δεδομένα από άλλες πηγές. Αυτή η προσέγγιση είναι μια επέκταση του μοντέλου επικοινωνίας Device-to-Cloud, η οποία επιτρέπει στις συσκευές IoT να ανεβάζουν τα δεδομένα μόνο για έναν πάροχο υπηρεσιών εφαρμογής. Η Back-End Data-Sharing αρχιτεκτονική επιτρέπει τα δεδομένα που συλλέγονται από μια IoT συσκευή να συγκεντρώνονται και να αναλύονται.

Παραδείγματος χάριν, ένας εταιρικός χρήστης ο οποίος είναι υπεύθυνος για ένα συγκρότημα γραφείων ενδιαφέρεται να συγκεντρώσει και να αναλύσει τα δεδομένα κατανάλωσης ενέργειας που παράγονται από όλους τους αισθητήρες IoT και τα Internet-enabled συστήματα που βρίσκονται στις εγκαταστάσεις της εταιρείας. Συχνά στο μοτέλο Device-to-Cloud, τα δεδομένα κάθε αισθητήρα ή συστήματος IoT αποθηκεύονται σε μια stand-alone βάση δεδομένων. Το μοντέλο Back-End Data-Sharingθα επιτρέψει στην εταιρεία να έχει εύκολη πρόσβαση και ανάλυση των δεδομένων που παράγονται από όλο το φάσμα των συσκευών στο κτίριο. Επίσης, αυτό το είδος της αρχιτεκτονικής διευκολύνει την ανάγκη για φορητότητα των δεδομένων. Η Back-End Data-Sharing αρχιτεκτονική επιτρέπει στους χρήστες να μετακινούν τα δεδομένα τους όταν εναλλάσσουν IoT συσκευές, χωρίς να δημιουργείται κάποιο πρόβλημα. Η Εικόνα 12 απεικονίζει το μοντέλο Back-End Data-Sharing.

*Εικόνα 12: Παράδειγμα μοντέλου επικοινωνίας Back-End Data-Sharing*



Η αρχιτεκτονική του μοντέλου αυτού είναι μια προσέγγιση για την επίτευξη της διαλειτουργικότητας μεταξύ αυτών των back-end συστημάτων. Όμως αυτό το μοντέλο είναι τόσο αποτελεσματικό όσο τα υποκείμενα σχέδια του IoT συστήματος. Οι Back-End Data-Sharing αρχιτεκτονικές δεν μπορούν να ξεπεράσουν πλήρως τα κλειστά σχέδια του IoT συστήματος (Ravindra P. Nitin S.Wagh, 2018).

Συνοψίζοντας θα λέγαμε ότι τα τέσσερα βασικά μοντέλα επικοινωνίας επιδεικνύουν τις υποκείμενες στρατηγικές σχεδιασμού που χρησιμοποιούνται για να επιτρέψουν στις συσκευές IoT να επικοινωνήσουν. Εκτός από ορισμένες τεχνικές παραμέτρους, η χρήση αυτών των μοντέλων επηρεάζεται σε μεγάλο βαθμό από την «κλειστή» φύση των δικτυωμένων IoT συσκευών. Στην περίπτωση του μοντέλου device-to-gateway, το κύριο χαρακτηριστικό του είναι η ικανότητά του να ξεπεράσει τους περιορισμούς που υπάρχουν στη συνδεσιμότητα των IoT συσκευών. Αυτό σημαίνει ότι η διαλειτουργικότητα των συσκευών και τα ανοικτά πρότυπα αποτελούν βασικούς παράγοντες στο σχεδιασμό και την ανάπτυξη των συστημάτων IoT.

Η συνολική αξία της συσκευής ενισχύεται όταν επιτρέπεται στο χρήστη καλύτερη πρόσβαση σε μια συσκευή IoT και τα δεδομένα της. Για παράδειγμα, σε τρία από τα τέσσερα μοντέλα επικοινωνίας, οι συσκευές συνδέονται με τις υπηρεσίες ανάλυσης δεδομένων σε ένα περιβάλλον cloud. Με τη δημιουργία αγωγών επικοινωνίας δεδομένων στο cloud, οι χρήστες και οι πάροχοι υπηρεσιών μπορούν να χρησιμοποιούν ευκολότερα το σύνολο των δεδομένων, μεγάλη ανάλυση δεδομένων, οπτικοποίηση δεδομένων και τεχνολογίες πρόβλεψης analytics.

## Α.3. Η ασφάλεια στον τομέα του IoT

Το IoT εισάγει μια νέα εποχή. Το Διαδίκτυο διαδραματίζει σημαντικό ρόλο στον ψηφιακό μετασχηματισμό όλων των βιομηχανιών. Η τεχνολογική καινοτομία δημιουργεί τεράστιους αριθμούς συνδέσεων, βελτιώνει σημαντικά την αποδοτικότητα και καθιστά τη ζωή των ανθρώπων πιο βολική. Η αγορά του IoT πρόκειται να αναπτυχθεί περεταίρω τα επόμενα χρόνια (Instituto National de Ciberseguridad, red.es, Huawei, 2017).

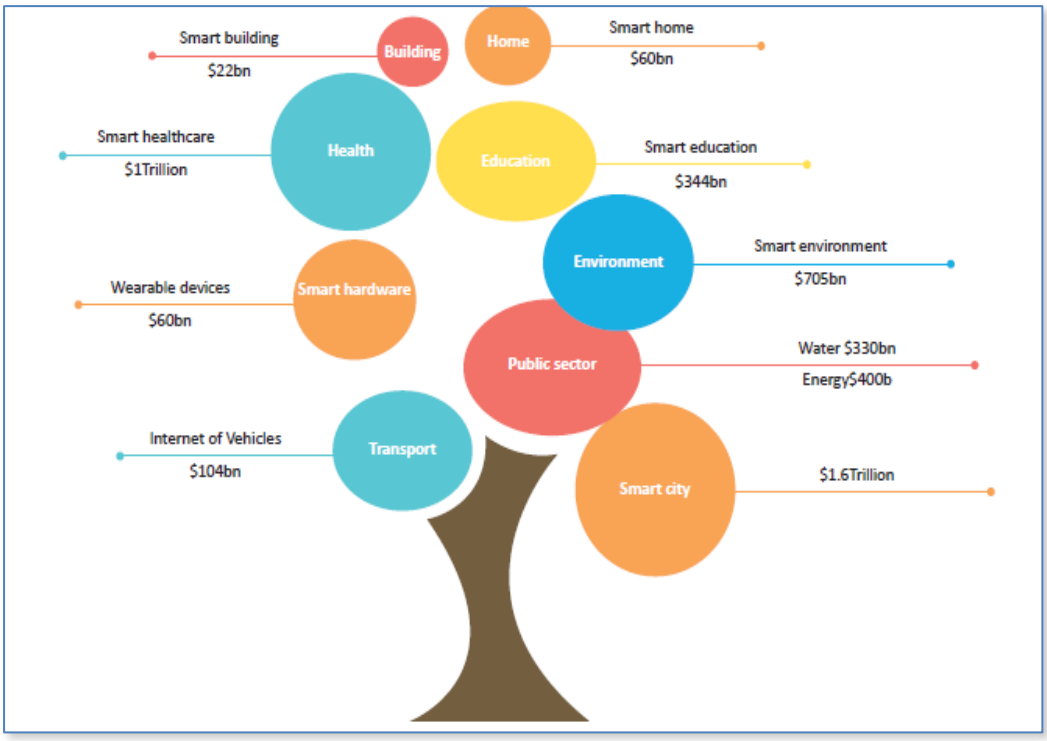
Το IoT οδηγεί τον ψηφιακό μετασχηματισμό σε όλες τις βιομηχανίες. Οι εταιρείες, οι κυβερνήσεις, οι οργανισμοί και οι κοινότητες σε ολόκληρο τον κόσμο προσπαθούν να ερευνήσουν και να επενδύσουν στο IoT και να συλλέξουν, να αναλύσουν και να

χρησιμοποιήσουν τα δεδομένα που αυτό δημιουργεί. Αυτό θα διευκολύνει την ταχεία ανάπτυξη όλων των βιομηχανιών.

Το IoT θα αποτελέσει μέρος της ζωής μας, όπως έχει ήδη αποτελέσει το Διαδίκτυο. Το έξυπνο σπίτι, η έξυπνη εκπαίδευση, η έξυπνη υγειονομική περίθαλψη, οι φορητές συσκευές, το Διαδίκτυο των οχημάτων (IoV) και άλλες βιομηχανίες κάνουν ευρεία χρήση του IoT. Με τα πάντα συνδεδεμένα μεταξύ τους, τα άτομα και η κοινωνία στο σύνολό της θα ωφεληθούν πάρα πολύ.

Η τεράστια δημοτικότητα των κινητών συσκευών, καθώς και η προκύπτουσα σειρά από πλατφόρμες και υπηρεσίες που έχουν αναπτυχθεί γύρω τους, ωθούν την ταχεία ανάπτυξη της αγοράς IoT. Η Gartner, Inc. προβλέπει ότι οι συνδεδεμένες συσκευές παγκοσμίως θα φθάσουν τα 20,8 δισεκατομμύρια μέχρι το 2020. Πρόκειται για ένα σύνθετο ετήσιο ρυθμό ανάπτυξης (CAGR) 34% (Instituto National de Ciberseguridad, red.es, Huawei, 2017). Η Εικόνα 13 δείχνει μια πρόβλεψη της αγοράς του IoT ανά εφαρμογή.

*Εικόνα 13: Πρόβλεψη αγοράς IoT ανά εφαρμογή (Πηγή: Ovum, GSMA, Gartner)*




## Α.3.1. Απειλές και προκλήσεις για την ασφάλεια του Διαδικτύου

Στις 21 Οκτωβρίου 2016, καταγράφηκε στις ΗΠΑ, η μεγαλύτερη επίθεση DDoS, αναγκάζοντας περισσότερους από 100 γνωστούς ιστότοπους, συμπεριλαμβανομένου του Amazon, να βρίσκονται εκτός σύνδεσης για αρκετές ώρες. Η επισκεψιμότητα της επίθεσης έφθασε πάνω

από 1 Tbit / s. Αυτή η επίθεση δεν είχε καμία σχέση με τις κοινές επιθέσεις DDoS που ξεκινούν από συσκευές πληροφορικής (όπως υπολογιστές και διακομιστές). Ξεκίνησε από κάμερες IP (IPCs), οικιακούς δρομολογητές, ψηφιακές συσκευές εγγραφής βίντεο και άλλες μικροσυσκευές που είχαν μολυνθεί από το κακόβουλο λογισμικό Mirai και προκάλεσε σοβαρές δυσλειτουργίες.

Στις 23 Δεκεμβρίου 2015, η ουκρανική διανομή ηλεκτρικού ρεύματος επηρεάστηκε από μια επίθεση που διέκοψε την ισχύ σε μεγάλο αριθμό χρηστών για αρκετές ώρες. Οι χάκερ χρησιμοποίησαν το BlackEnergy για να αποκτήσουν πρόσβαση στο σύστημα διαχείρισης της διανομής ενέργειας και στη συνέχεια μπόρεσαν να εκδώσουν εντολές διακοπής, να διαγράψουν και να αντικαταστήσουν τα δεδομένα του συστήματος και να εκτελέσουν λειτουργίες απενεργοποίησης.

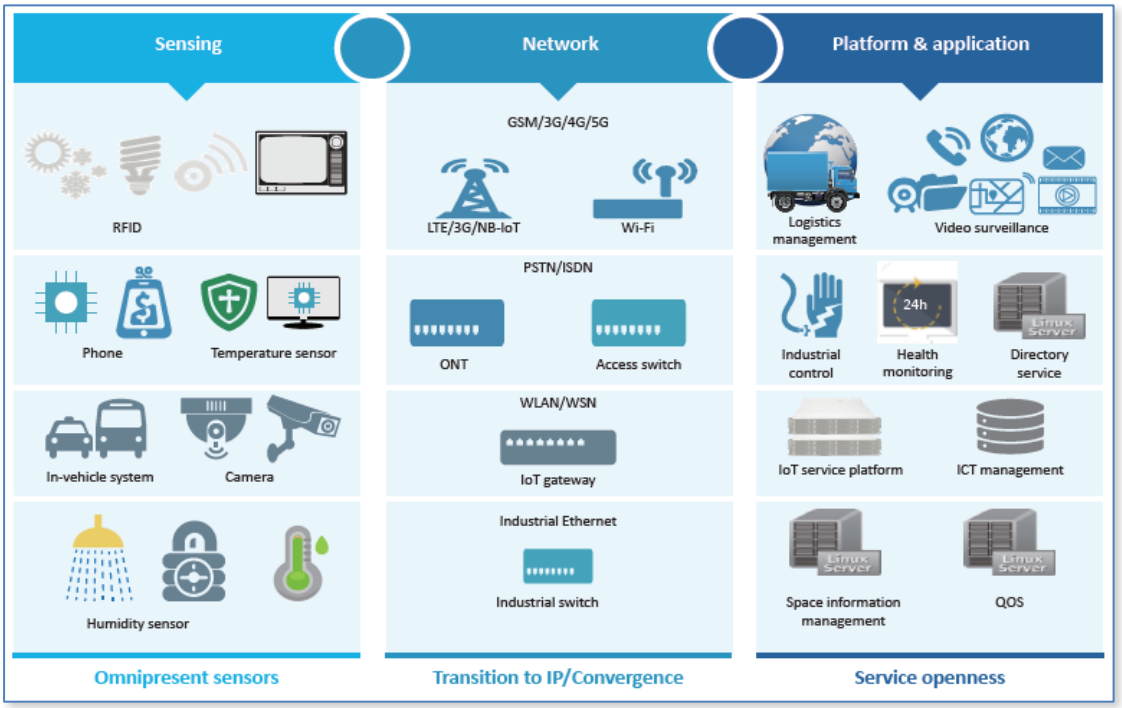
Τον Ιούλιο του 2015, το περιοδικό Wired αποκάλυψε ότι οι χάκερ ήταν σε θέση να διαταράξουν εξ αποστάσεως την οδήγηση των οχημάτων Jeep Cherokee. Η Fiat Chrysler Automobiles NV, μητρική εταιρεία του Jeep, έλαβε μέτρα ασφαλείας σε επίπεδο δικτύου για να αποτρέψει αυτό το είδος απομακρυσμένης χειραγώγησης. Επίσης, απέσυρε περίπου 1,4 εκατομμύρια αυτοκίνητα και φορτηγά εξοπλισμένα με ευαίσθητα ραδιόφωνα στις ΗΠΑ.

Η αλήθεια είναι ότι οι απειλές για την ασφάλεια δεν τελειώνουν ποτέ. Τα παραδοσιακά δίκτυα εξακολουθούν να αντιμετωπίζουν πολλά ζητήματα ασφάλειας ακόμη και με τη λήψη πολλών πληροφοριακών μέτρων ασφαλείας. Αυτή η πρόκληση δεν μπορεί να αποφευχθεί στην εποχή του IoT. Σε μια έρευνα Forrester (Instituto National de Ciberseguridad, red.es, Huawei, 2017) σε οργανισμούς σε όλο τον κόσμο, το 47% των βιομηχανικών οργανώσεων που χρησιμοποιούν ή σκοπεύουν να χρησιμοποιήσουν το IoT είχαν προηγουμένως βιώσει παραβιάσεις ασφαλείας στις βιομηχανικές τους εφαρμογές. Περαιτέρω έρευνα δείχνει ότι:

- το 27% των συστημάτων ελέγχου εκτίθενται ή μολύνονται.
- Το 80% του εξοπλισμού χρησιμοποιεί έναν απλό κωδικό πρόσβασης.
- Το 70% της επικοινωνίας δεν είναι κρυπτογραφημένο.
- Το 90% των αναβαθμίσεων του υλικολογισμικού δεν ελέγχουν τις υπογραφές. Πολλές συσκευές δεν αναβαθμίζονται ή δεν μπορούν να αναβαθμίσουν.

Η αυξανόμενη χρήση του IoT ενισχύει την παραγωγικότητα και διευκολύνει τη ζωή των ανθρώπων, αλλά επιφέρει εκτεταμένες απειλές για την ασφάλεια. Απειλές ασφαλείας προκύπτουν από τρία στρώματα (όπως φαίνεται στην Εικόνα 14).

*Εικόνα 14: Τρία στρώματα του IoT και τα χαρακτηριστικά τους (Πηγή: Building a Trusted and Managed IoT World)*




Οι πανταχού παρόντες αισθητήρες προκαλούν μη αξιόπιστα τελικά σημεία IoT.

- Τα εξωτερικά τελικά σημεία δεν είναι διαχειρίσιμα και είναι επιρρεπή σε φυσική επίθεση, αλλοίωση και πλαστογράφηση.
- Οι οδηγοί συσκευών μπορεί να είναι αναξιόπιστοι και να διαχέονται και να ελέγχονται εύκολα.
- Οι ενημερώσεις κώδικα δεν είναι άμεσα διαθέσιμες για τα λειτουργικά συστήματα (OS) ή τα τρωτά σημεία του λογισμικού.
- Λαμβάνοντας υπόψη το κόστος, οι πόροι και οι υπολογιστικές δυνατότητες των τελικών σημείων είναι περιορισμένες. Τα παραδοσιακά μέσα προστασίας και οι τεχνολογίες ασφάλειας, όπως το λογισμικό προστασίας από ιούς, ενδέχεται να μην είναι εφαρμόσιμα.

Η μετάβαση του στρώματος δικτύου σε IP και σύγκλιση προκαλεί απειλές.

- Τα ελαττώματα στα ασύρματα πρωτόκολλα, όπως η έλλειψη αποτελεσματικού ελέγχου ταυτότητας, μπορεί να οδηγήσουν σε διαρροή στην πλευρά πρόσβασης.
- Οι ιδιωτικές βιομηχανικές εφαρμογές και τα πρωτόκολλα δεν μπορούν να αναγνωριστούν από συσκευές ασφαλείας και μπορούν εύκολα να αξιοποιηθούν χωρίς έγκαιρη ανίχνευση.

- Η μη κρυπτογραφημένη διαδικασία επικοινωνίας είναι επιρρεπής στις επιθέσεις manin-the-middle (MITM), όπως η αεροπειρατεία, η επανάληψη, η παραβίαση και η υποκλοπή.
- Τα δίκτυα που βασίζονται σε IP είναι ευάλωτα στις επιθέσεις και την εισβολή που βασίζονται στο Διαδίκτυο.

Το άνοιγμα της υπηρεσίας σε επίπεδο πλατφόρμας και εφαρμογής συνεπάγεται νέες απειλές για την ασφάλεια.

- Οι συσκευές που διαχειρίζονται σε επίπεδο πλατφόρμας είναι πολυάριθμες και διαδεδομένες, καθιστώντας δύσκολη την αναβάθμιση και διαχείριση της ασφάλειας τέτοιων συσκευών.
- Τα νέα πρωτόκολλα επικοινωνίας ενδέχεται να φέρουν ζητήματα ασφάλειας και ευπάθειες στο επίπεδο εφαρμογής, όπως οι παραμορφωμένες επιθέσεις πακέτων και οι επιθέσεις πλημμύρας.
- Τα ευπάθειες των νέων πλατφορμών και των ανοικτών API ανοίγουν πόρτες σε νέους κινδύνους.
- Η μη εξουσιοδοτημένη πρόσβαση οδηγεί σε διαρροή δεδομένων, όπως διαρροή διαπιστευτηρίων πιστοποίησης.
- Διάφορες εφαρμογές διάφορων δικτύων και κέντρων δεδομένων προκαλούν υψηλούς κινδύνους από επιθέσεις DDoS.
- Διάφορες εφαρμογές IoT μπορεί να είναι αναξιόπιστες.

Επιπλέον, οι συσκευές, τα δίκτυα και οι εφαρμογές του IoT μπορούν να ανήκουν σε διάφορους προμηθευτές. Ως εκ τούτου, ένας μόνο προμηθευτής δύσκολα μπορεί να δει σχεδόν ολόκληρη την επιφάνεια επίθεσης, πόσο μάλλον να εκτελέσει ολοκληρωμένη άμυνα της ασφάλειας.

Το απόρρητο είναι μία από τις μεγαλύτερες νομικές προκλήσεις για το IoT.

Το IoT σημαίνει ότι ένας μεγάλος αριθμός συνδεδεμένων συσκευών θα δημιουργήσει, θα στείλει και θα λάβει μεγάλους όγκους δεδομένων που συνδέονται με άτομα, με αποτέλεσμα την μόνιμη παρακολούθηση των δραστηριοτήτων των ανθρώπων μέσω πολλών διαφορετικών συσκευών. Η παρακολούθηση αυτή μπορεί να εγείρει διάφορες απαιτήσεις σχετικά με την προστασία της ιδιωτικής ζωής και την προστασία των προσωπικών δεδομένων. Αυτές οι ανησυχίες δεν είναι τίποτε νέο – οποιαδήποτε σχετική τεχνολογική αλλαγή έχει προκαλέσει ανησυχίες σχετικά με την ιδιωτικότητα. Είναι σωστό να ανησυχούμε

για την προστασία της ιδιωτικής ζωής, δεδομένου ότι το Διαδίκτυο των πραγμάτων περιλαμβάνει περισσότερες συσκευές και δεδομένα και συνεπώς μεγαλύτερες προκλήσεις.

### Α.3.2. Απαιτήσεις Βιομηχανίας για Ασφάλεια IoT

Η ασφάλεια του Διαδικτύου είναι συγκεκριμένη ανά κλάδο (όπως φαίνεται στην Εικόνα 15) και μπορεί να ποικίλει ως προς τις μορφές και τις απαιτήσεις με τις επιχειρηματικές ιδιότητες, τα αντικείμενα υπηρεσίας, τα όργανα διοίκησης και τους τρόπους εργασίας σε διαφορετικές βιομηχανίες.

- Βιομηχανία και ενέργεια: Διαδικτυακή ασφάλεια των βιομηχανικών συστημάτων ελέγχου και έξυπνα δίκτυα, όπως η ασφάλεια της έξυπνης υπολογιστικής υπηρεσίας (ICS) και τον έλεγχο εποπτείας και την απόκτηση δεδομένων (SCADA). Μια επίθεση σε ένα βιομηχανικό σύστημα ελέγχου μπορεί να «ρίξει» το σύνολο του συστήματος, ενδεχομένως να σταματήσει την παραγωγή και να οδηγήσει σε διακοπή λειτουργίας.
- Κινητικότητα: Προστασία των έξυπνων οχημάτων. Ασφάλεια και προστασία των μη επανδρωμένων οχημάτων. Προστασία δορυφορικών συστημάτων επικοινωνίας. Οι επιθέσεις ενδέχεται να προκαλέσουν σοβαρά τροχαία ατυχήματα και να θέσουν σε κίνδυνο τη ζωή των ανθρώπων.

*Εικόνα 15: IoT κλάδοι (Πηγή: Building a Trusted and Managed IoT World)*


- Φροντίδα υγείας: Προστασία συνδεδεμένων ιατρικών συσκευών. Κρυπτογράφηση για ιατρική και φαρμακευτική έρευνα. Ασφαλής και πανταχού παρούσα αποθήκευση ιατρικών δεδομένων. Ένα πιθανό σενάριο όπου τίθεται σε κίνδυνο η ζωή είναι όταν ένας χάκερ αποκτά τον έλεγχο του ασύρματου εμφυτεύσιμου απινιδωτή καρδιοανατάκτη (ICD) μέσα σε έναν ασθενή.

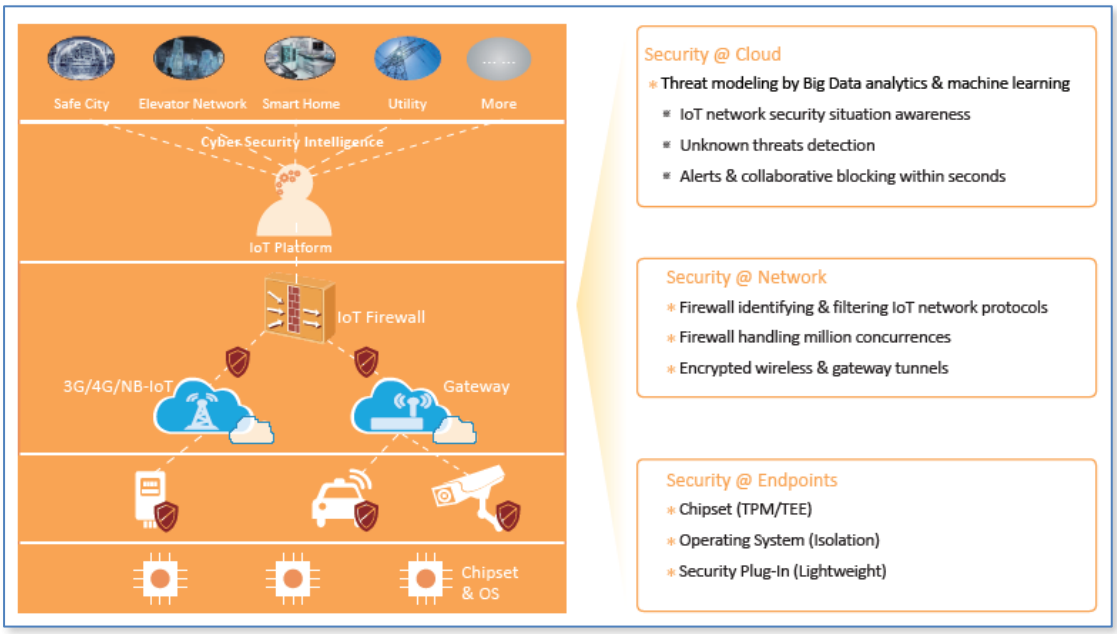
- ❖ Έξυπνη πόλη: Ασφαλής μετάδοση και αποθήκευση πληροφοριών που συλλέγονται από τεράστιους αριθμούς αισθητήρων. Εάν διακυβευτεί ένα σύστημα ελέγχου που χρησιμοποιείται στη σιδηροδρομική μεταφορά, ενδέχεται να προκύψει εσφαλμένος προγραμματισμός ή εκτροχιασμός.
- ❖ Οικονομία: Προστασία της πληρωμής μέσω κινητού τηλεφώνου από πλαστογράφηση. Τα άτομα και οι επιχειρήσεις θα υποστούν αναπόφευκτα ζημιά σε περίπτωση εκμετάλλευσης.

Η ασφάλεια του IoT δεν αφορά μόνο την επιχειρηματική επιτυχία, αλλά και την εθνική οικονομία και το βιοπορισμό των ανθρώπων. Η οικοδόμηση ενός περιβάλλοντος ασφάλειας του IoT είναι επομένως επείγουσα απαίτηση.

### Α.3.3. Πολυλειτουργικό σύστημα ασφαλείας από άκρο σε άκρο για IoT

Με το IoT υπάρχουν πανταχού παρούσες απειλές ασφάλειας, από πλατφόρμες συστημάτων έως αισθητήρες. Η αγορά του IoT είναι πολυαναμενόμενη αλλά γεμάτη προκλήσεις. Οποιοσδήποτε κίνδυνος σε ένα μόνο σημείο μπορεί να θέσει σε κίνδυνο ολόκληρο το δίκτυο και τα συστήματα πυρήνα. Επομένως, η ασφάλεια πρέπει να λαμβάνεται υπόψη από την αρχή του σχεδιασμού του Διαδικτύου και πρέπει να δημιουργηθεί ένα πολυστρωματικό σύστημα ασφαλείας από άκρο σε άκρο (όπως φαίνεται στην Εικόνα 16).

*Εικόνα 16: Πολυεπίπεδη αρχιτεκτονική ασφαλείας για το IoT (Πηγή: Building a Trusted and Managed IoT World)*

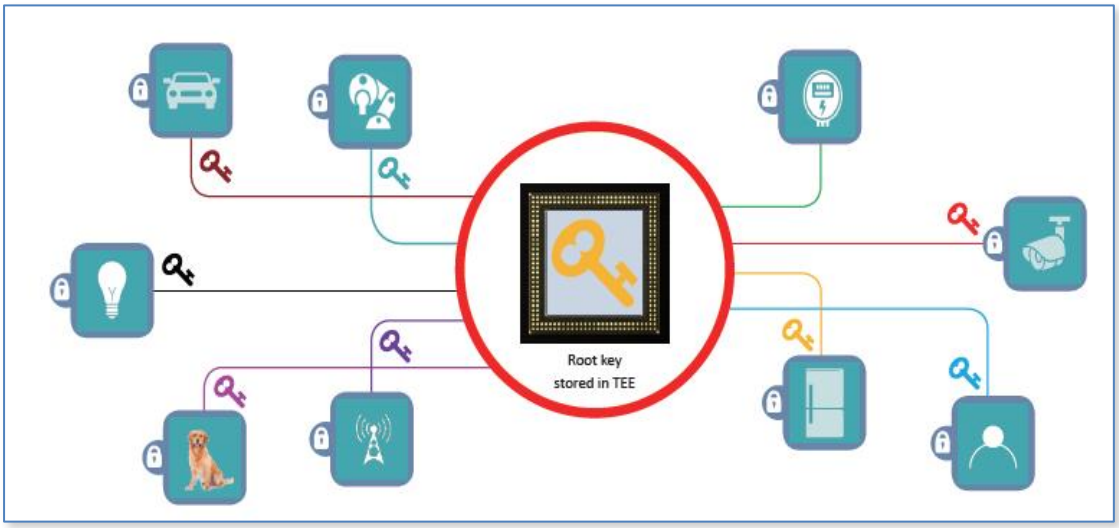


Η ασφάλεια του Διαδικτύου εκδηλώνεται σε τσιπ, συσκευές και λειτουργικά συστήματα, δίκτυα, πλατφόρμες διαχείρισης, εφαρμογές και λειτουργία της επιχείρησης. Οι τεχνικές και τα μέτρα ασφαλείας μπορούν να αναλυθούν από κάθε στρώμα. Εκτός από την προστασία ασφαλείας σε κάθε στρώμα, αναπτύσσεται ένα ολοκληρωμένο σύστημα άμυνας από άκρο σε άκρο με βάση την αλληλεξάρτηση της συσκευής, του σωλήνα και του cloud. Σε αυτό το σύστημα, η επίγνωση της κατάστασης ασφάλειας του όλο το IoT έχει ιδιαίτερη σημασία.

### A.3.3.1. Ασφάλεια τσιπ και λειτουργικό σύστημα

Ασφαλή τσίπ προτιμώνται σε συσκευές IoT που έχουν υψηλές απαιτήσεις ασφαλείας. Οι προμηθευτές τσιπ παρέχουν ισχυρή κρυπτογράφηση και απομόνωση σε επίπεδο hardware χρησιμοποιώντας διαφορετικές τεχνικές (όπως φαίνεται στην Εικόνα 17), όπως το Trusted Execution Environment (TEE) και η Trusted Platform Module (TPM), έτσι ώστε να αποθηκεύονται σημαντικά κλειδιά στο αξιόπιστο τσιπ για την αποφυγή διάρευσης δεδομένων. Επιπλέον, υποστηρίζεται ασφαλής εκκίνηση και ελέγχονται οι υπογραφές κατά τη διάρκεια της εκκίνησης και αναβάθμισης του λογισμικού και του υλικολογισμικού για να διασφαλιστεί η ακεραιότητα των δεδομένων (Instituto National de Ciberseguridad, red.es, Huawei, 2017). Το IoT απαιτεί οικονομικά αποδοτικές, ενεργειακά αποδοτικές και καθολικές τεχνικές ασφαλείας σε τσιπ.

*Εικόνα 17: Ασφάλεια chip TEE (Πηγή: Building a Trusted and Managed IoT World)*




Το λειτουργικό σύστημα είναι ένα απαραίτητο στοιχείο μιας ολοκληρωμένης λύσης ασφάλειας. Στους κοινούς ελαφρούς μηχανισμούς προγραμματισμού OS του IoT, η ενοποιημένη μνήμη διαμοιράζεται ανεξάρτητα από τη λειτουργία του χρήστη ή του πυρήνα.

Οι εφαρμογές και ο πυρήνας εκτελούνται όλα σε προνομιακή λειτουργία. Αυτό δημιουργεί πολλές αβεβαιότητες και απειλές ασφάλειας για τις υπηρεσίες συστημάτων.

Εάν εφαρμοστεί ο μηχανισμός απομόνωσης του ελαφρού ασφαλούς λειτουργικού συστήματος, ο τρόπος λειτουργίας χρήστη θα απομονωθεί από τη λειτουργία του πυρήνα και οι εφαρμογές θα απομονωθούν η μία από την άλλη. Η προστασία μνήμης και οι μεμονωμένοι μηχανισμοί προγραμματισμού για τον πυρήνα θα υποστηριχθούν για να βελτιώσουν σημαντικά την αξιοπιστία και την ασφάλεια του συστήματος.

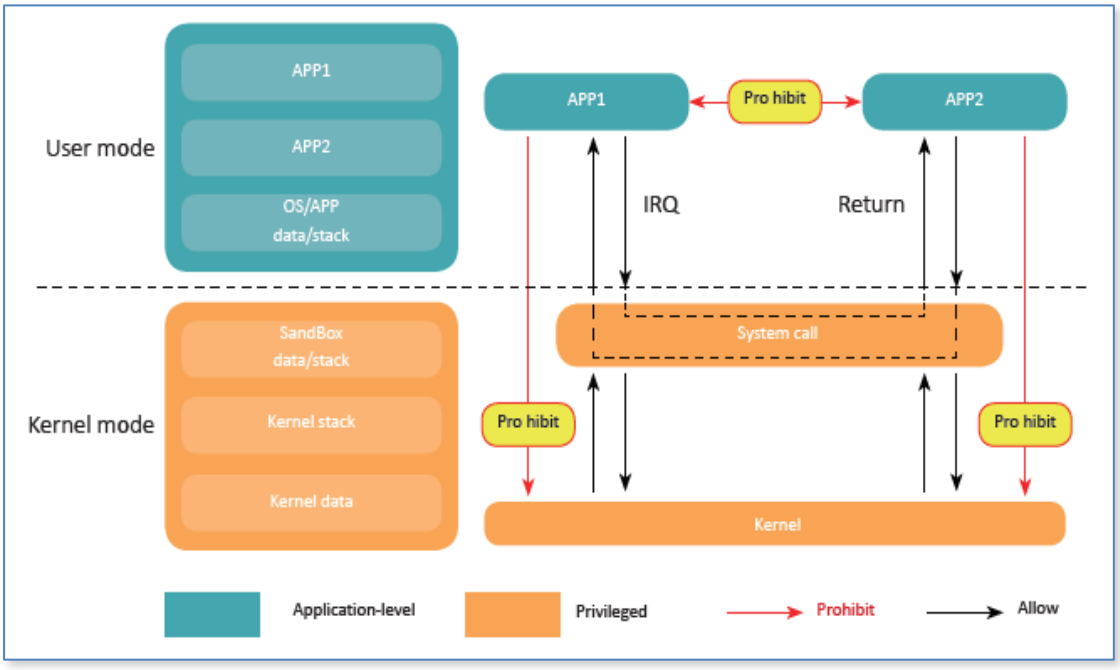
Το ασφαλές λειτουργικό σύστημα επανασχεδιάζει και διαχειρίζεται τη μνήμη για να διαιρέσει το χώρο για τον πυρήνα και τις εφαρμογές, χρησιμοποιεί τον μηχανισμό syscall για να διαχωρίσει τα δικαιώματα σε πυρήνα και λειτουργία χρήστη και σε εικονικές μηχανές (VMs) προκειμένου να προστατεύσει τα δικαιώματα διαφορετικών εφαρμογών και να παρέχει στους χρήστες δυνατότητα ρύθμισης προστασίας διεπαφών που βασίζονται στη μνήμη, στη μονάδα προστασίας μνήμης (MPU) ή στη μονάδα διαχείρισης μνήμης (MMU). Τα μέτρα προστασίας ασφαλείας (όπως φαίνεται στην Εικόνα 18) περιλαμβάνουν:

- Σχεδιασμός σωστής διάταξης μνήμης
- Διαχωρισμός λειτουργίας πυρήνα και λειτουργία χρήστη
- Απομόνωση διεργασιών για εφαρμογές
- Διεπαφή προστασίας μνήμης

Η ασφαλής περιοχή που δημιουργείται από τον ελαφρύ μηχανισμό απομόνωσης υπερασπίζεται το λειτουργικό σύστημα. Μια εφαρμογή μπορεί να δημιουργήσει μια ανεξάρτητη ασφαλή ζώνη βασισμένη στην ασφαλή περιοχή χρησιμοποιώντας την MPU. Κύρια χαρακτηριστικά του ελαφρού μηχανισμού απομόνωσης που δημιουργείται από το ασφαλές λειτουργικό σύστημα είναι τα εξής:

- Έλεγχος πρόσβασης: Τα sandboxes είναι απομονωμένα το ένα από το άλλο, έχουν ρυθμιστεί κανάλια πρόσβασης ασφαλείας και εκτελείται αποτελεσματική διαχείριση και έλεγχος για την αποτροπή μη εξουσιοδοτημένης πρόσβασης χρησιμοποιώντας κακόβουλο κώδικα.
- Ασφάλεια πυρήνα: Τοποθέτηση των βάσεων για την προστασία της ασφάλειας της αναβάθμισης του υλικολογισμικού (firmware μέσω του αέρα ή FOTA), αποθήκευσης ασφαλείας, διαχείριση κλειδιών, κρυπτογράφηση και αποκρυπτογράφηση, και αναγνωριστικό συσκευής.

*Εικόνα 18: Μηχανισμός ασφάλειας λειτουργικού συστήματος (Πηγή: Building a Trusted and Managed IoT World)*




Το ασφαλές λειτουργικό σύστημα μπορεί να παρέχει λειτουργίες όπως πιστοποίηση ταυτότητας, ασφαλή αναβάθμιση υλικολογισμικού, έλεγχο πρόσβασης στο Internet, κρυπτογράφηση και αποκρυπτογράφηση και διαχείριση κλειδιών.

### A.3.3.2. Ασφάλεια τελικού σημείου

Τα τελικά σημεία του IoT περιλαμβάνουν αισθητήρες πρόσβασης και συσκευές, οι οποίοι μπορούν να συλλέγουν δεδομένα και να έχουν πρόσβαση σε δίκτυα για την αναφορά δεδομένων. Τα χαρακτηριστικά τέτοιων τελικών σημείων είναι: η χαμηλή κατανάλωση ενέργειας, το χαμηλό κόστος, αδύναμη υπολογιστική και αποθηκευτική δυνατότητα, είναι φυσικώς προσβάσιμοι, έχουν μεγάλο κύκλο ζωής, έχουν πολύπλοκες διεπαφές και πρωτόκολλα κ.λπ.

Η παραδοσιακή αρχιτεκτονική ασφάλειας δεν μπορεί πλέον να ικανοποιεί αυτά τα χαρακτηριστικά. Απαιτείται μια νέα αρχιτεκτονική ασφαλείας για την εξασφάλιση της ασφάλειας του τελικού σημείου του IoT (όπως φαίνεται στην Εικόνα 19 ).

*Εικόνα 19: Μέτρα ασφαλείας τελικού σημείου (Πηγή: Building a Trusted and Managed IoT World)*


- Φυσική ασφάλεια: Νερό, σκόνη, σοκ και ηλεκτρομαγνητική απόφραξη στο περιβάλλον του IoT.
- Ασφάλεια πρόσβασης: Οι πλαστές συσκευές πρέπει να αποτρέπονται από την πρόσβαση στο δίκτυο και τα τελικά σημεία του IoT πρέπει να προστατεύονται από το να καταστούν ζόμπι σε επιθέσεις DDoS. Οι ελαφρές και εύκολες στην υλοποίηση εφαρμογές ασφαλείας και προσθήκες βοηθούν στην ανάλυση των ανωμαλιών του τελικού σημείου και στην κρυπτογράφηση των δεδομένων επικοινωνίας για την προστασία των τελικών σημείων από το να χρησιμοποιηθούν ως μέσα για την επίθεση κρίσιμων κόμβων δικτύου. Επιπλέον, απαιτούνται επίσης νέες τεχνολογίες, όπως ο ελαφρύς υποχρεωτικός μηχανισμός επαλήθευσης ταυτότητας, η κατανεμημένη πιστοποίηση ταυτότητας και η αλυσίδα μπλοκ.
- Ασφάλεια περιβάλλοντος: Ο μηχανισμός ασφαλείας σε επίπεδο πυρήνα που παρέχεται από το ελαφρύ, σε πραγματικό χρόνο και ενσωματωμένο λειτουργικό σύστημα προστατεύει το περιβάλλον. Η υπογραφή λογισμικού υποστηρίζεται για ασφαλή κωδικό υπηρεσίας εκκίνησης, έτσι ώστε να μπορούν να φορτωθούν μόνο έγκυρα και άθικτα πακέτα λογισμικού. Η λίστα επιτρεπόμενης πρόσβασης υποστηρίζεται για την αποτροπή κακόβουλου κώδικα και μη εξουσιοδοτημένης πρόσβασης.
- Ασφάλεια δεδομένων υπηρεσίας: Διαρροή δεδομένων, πρόληψη αντιγραφής και απομόνωση δεδομένων χρησιμοποιούνται για την ασφάλεια τοπικών δεδομένων.
- Ενιαία διαχείριση: Παρέχει διαχείριση ασφάλειας κατά τη διάρκεια ολόκληρου του κύκλου ζωής, συμπεριλαμβανομένης της ενεργοποίησης της συσκευής, ταυτοποίηση ταυτότητας, ασφαλής αποθήκευση, ασφαλής εκκίνηση, έλεγχος ακεραιότητας, αναβάθμιση λογισμικού και παροπλισμός συσκευών.

Το υλικό και το λογισμικό πρέπει να λαμβάνονται πλήρως υπόψη για την ασφάλεια των τελικών σημείων του IoT, συμπεριλαμβανομένης της ασφάλειας σε επίπεδο τσιπ, της ασφάλειας του OS και της σκλήρυνσης της ασφάλειας των τελικών σημείων που λειτουργούν με λειτουργικά συστήματα. Τα τελικά σημεία που είναι αξιόπιστα και διαχειριζόμενα αποτελούν τη βασική απαίτηση για την ασφάλεια του IoT, διότι το IoT δεν μπορεί να αναπτυχθεί ευρέως σε αναξιόπιστη βάση. Ως εκ τούτου, οι προμηθευτές πρέπει να επιλέξουν προσεκτικά τις τεχνικές ασφαλείας για να φιλοξενήσουν εξελιγμένα τελικά σημεία IoT βασισμένα στην ευαισθησία των δεδομένων, το επίπεδο πληροφοριών των τελικών σημείων και τα χαρακτηριστικά των διαφορετικών αρχιτεκτονικών δικτύων. Για παράδειγμα, οι προμηθευτές θα μπορούσαν να χρησιμοποιήσουν νέες τεχνικές ασφαλείας, όπως η ελαφριά κρυπτογράφηση ασφαλείας και η κατανεμημένη πιστοποίηση, για να εξισορροπήσουν την ασφάλεια, την κατανάλωση πόρων και το κόστος.

### Α.3.3.3. Ασφάλεια επιπέδου δικτύου

Το IoT επιφέρει την ανάγκη τα δίκτυα να υποστηρίζουν διάφορες υπηρεσίες, να μεταφέρουν μεγάλους όγκους κίνησης και να χρησιμοποιούν διαφορετικές ενσύρματες και ασύρματες τεχνικές. Οι ενσύρματες τεχνικές περιλαμβάνουν Ethernet, RS232, RS485 και PLC, ενώ οι ασύρματες τεχνικές περιλαμβάνουν GPRS, LTE, ZigBee, Z-Wave, Bluetooth και Wi-Fi. Οι περισσότεροι από τους παραδοσιακούς μηχανισμούς ασφαλείας εξακολουθούν να εφαρμόζονται στον κόσμο του IoT. Για παράδειγμα, μπορούν να χρησιμοποιηθούν οι ακόλουθοι μηχανισμοί: Απομόνωση ζώνης ασφαλείας δικτύου, έλεγχος ταυτότητας σε συσκευές που προσπαθούν να έχουν πρόσβαση σε δίκτυα, αυτόματη προστασία χρησιμοποιώντας τείχη προστασίας, αντι-DDoS, πρόληψη επίθεσης μέσω εφαρμογής και ιστού και ασφαλή μετάδοση σε σχέδια ελέγχου και χρήσης χρησιμοποιώντας IPsec.

Η ασφάλεια του δικτύου του IoT επικεντρώνεται σε δύο πτυχές: την ασφάλεια των νέων τεχνολογιών επικοινωνίας IoT (όπως NB-IoT και 5G) και τους μηχανισμούς ασφαλείας για πολλά πρωτόκολλα ιδιοκτησίας και βιομηχανικά δίκτυα ελέγχου (Instituto National de Ciberseguridad, red.es, Huawei, 2017).

Τα NB-IoT και 5G εγείρουν τις ακόλουθες απαιτήσεις ασφαλείας:

- Ενιαίος και κατανεμημένος έλεγχος ταυτότητας των τελικών σημείων IoT που χαρακτηρίζεται από υψηλή συνοχή και αποκέντρωση
- Προσαρμογή στο λογισμικό NFV, αυτόματη ανάπτυξη και δυναμικό προγραμματισμό

- ❖ Κρυπτογράφηση από άκρο σε άκρο και νέους ελαφρύς αλγόριθμους κρυπτογράφησης σε ένα ανοιχτό περιβάλλον
- ❖ Ανίχνευση σταυρωτής στρώσης στις επιθέσεις που ξεκίνησαν χρησιμοποιώντας συσκευές διαφορετικών προμηθευτών και συνεργασία πολλών λειτουργιών ασφαλείας

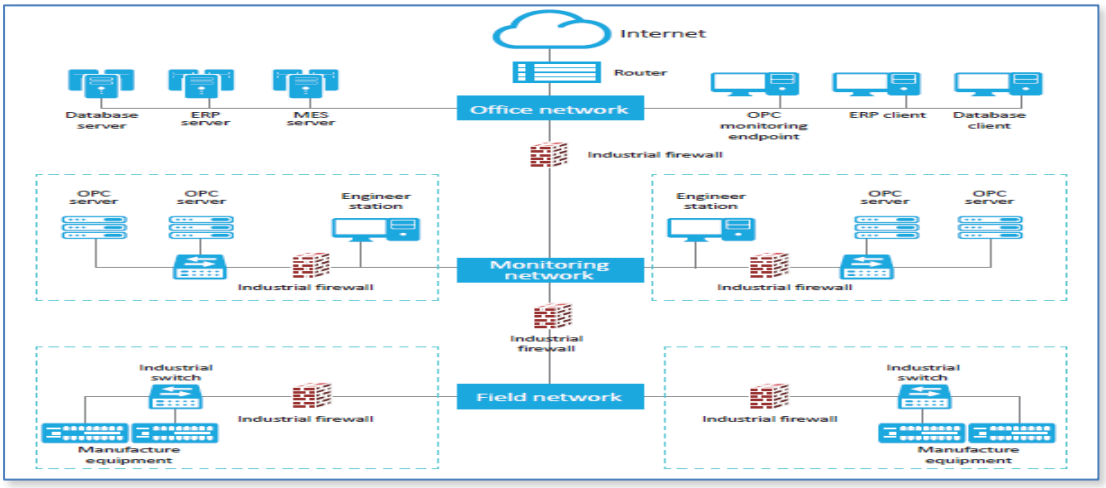
Το IoT πρέπει να κάνει πλήρη χρήση των χαρακτηριστικών μεταφοράς φυσικών επιπέδων των ασύρματων κινητών επικοινωνιών και να εφαρμόσει τεχνολογίες ασφάλειας για έλεγχο ταυτότητας, κρυπτογράφηση και ασφαλή μετάδοση, για να εξασφαλίσει την ποιότητα της μετάδοσης, να αποτρέψει την υποκλοπή σε άγνωστες τοποθεσίες και να αυξήσει τη δυσκολία στην εκτόξευση επιθέσεων MITM. Όσον αφορά τις διεπαφές αέρα, τα τελικά σημεία και τα δίκτυα πιστοποιούνται αμοιβαία σύμφωνα με τα ασύρματα πρότυπα, έτσι ώστε μόνο τα εξουσιοδοτημένα τελικά σημεία να έχουν πρόσβαση σε έγκυρα δίκτυα. Ασφαλή κανάλια δημιουργούνται μεταξύ τελικών σημείων και δικτύων για κρυπτογράφηση και προστασία ακεραιότητας για την αποφυγή διαρροής δεδομένων, παραβίασης και υποκλοπής.

Τα τελικά σημεία του IoT χρησιμοποιούν μεγάλο αριθμό αποκλειστικών διεπαφών (συμπεριλαμβανομένων των KNX, ModBus και CANBus), τα οποία συνδέονται με βιομηχανικά δίκτυα ελέγχου. Τα περισσότερα από αυτά τα σημεία και τα δίκτυα είναι σχεδιασμένα να λειτουργούν σε απομονωμένα περιβάλλοντα και ως εκ τούτου περιλαμβάνουν φτωχούς μηχανισμούς ασφαλείας. Νέα ζητήματα ασφάλειας προκύπτουν όταν αυτά τα τελικά σημεία και τα δίκτυα εισάγονται στο IoT. Για την αντιμετώπιση αυτών των ζητημάτων, τα τείχη προστασίας IoT (όπως φαίνεται στην Εικόνα 20), οι πύλες ασφαλείας και άλλες συσκευές πρέπει να είναι σε θέση:

- ❖ Εφαρμόζουν ανάλυση σε βάθος και αυτόματου φιλτράρισμα για βιομηχανικά πρωτόκολλα και εφαρμογές από διαφορετικές βιομηχανίες.
- ❖ Υποστηρίζουν κρυπτογράφηση για συσκευές πρόσβασης.
- ❖ Υποστηρίζουν φιλτράρισμα με βάση τα whitelist, συμπεριλαμβανομένου του αυτοπροσδιορισμένου φιλτραρίσματος πρωτοκόλλου.
- ❖ Υποστηρίζει αυτόματα τις επιθέσεις DDoS που χαρακτηρίζονται από την εξάντληση των πόρων των συσκευών και τις επιθέσεις επισκεψιμότητας εφαρμογών πολλών βιομηχανιών.

Τα προϊόντα ασφάλειας δικτύων πρέπει επίσης να παρέχουν προστασία από ιούς και προηγμένες απειλές (APT) για το IoT.

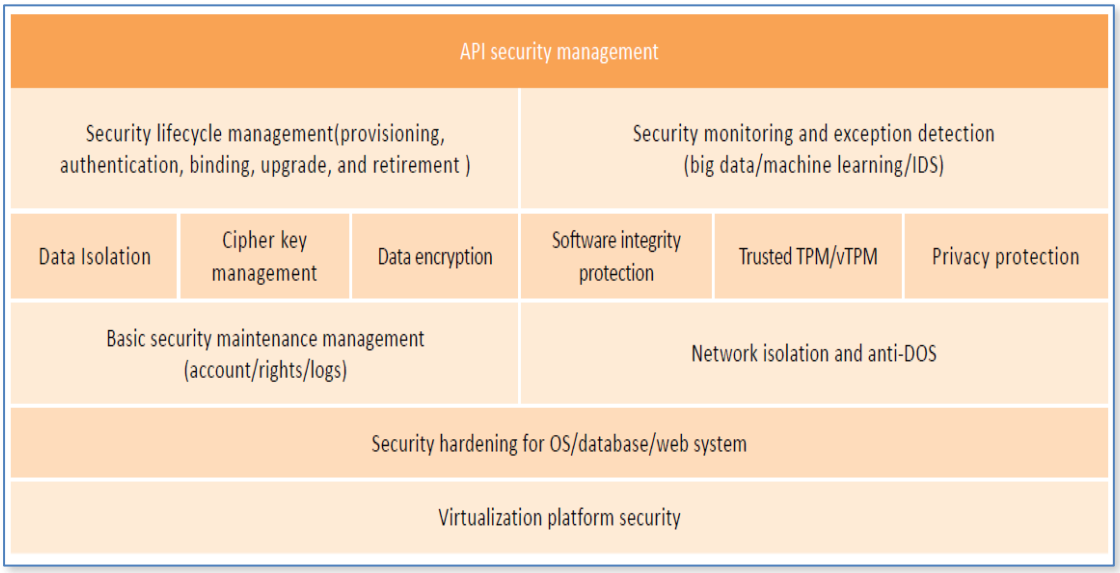
*Εικόνα 20: Εφαρμογή βιομηχανικών τειχών προστασίας (Πηγή: Building a Trusted and Managed IoT World)*




### A.3.3.4. Ασφάλεια πλατφόρμας και εφαρμογών

Η πλατφόρμα διαχείρισης IoT διαχειρίζεται κυρίως μεγάλο αριθμό τελικών σημείων, δεδομένων, λειτουργιών και ασφάλειας του IoT. Όπως φαίνεται στην Εικόνα 21, ο πιο κρίσιμος παράγοντας ασφάλειας σε όλους τους τύπους διαχείρισης είναι τα προσωπικά δεδομένα. Αυτό οφείλεται στο γεγονός ότι ένα μεγάλο μέρος των προσωπικών δεδομένων των χρηστών μπορεί να μεταδοθεί από διεσπαρμένα τελικά σημεία σε μια IoT cloud πλατφόρμα ή πλατφόρμα επεξεργασίας. Ως εκ τούτου, πρέπει να παρέχεται επαρκής προστασία για τα προσωπικά δεδομένα σύμφωνα με τις απαιτήσεις που ορίζονται στους νόμους περί προστασίας της ιδιωτικής ζωής των τοπικών χωρών και περιφερειών.

*Εικόνα 21: Ασφάλεια IoT πλατφόρμας (Πηγή: Building a Trusted and Managed IoT World)*



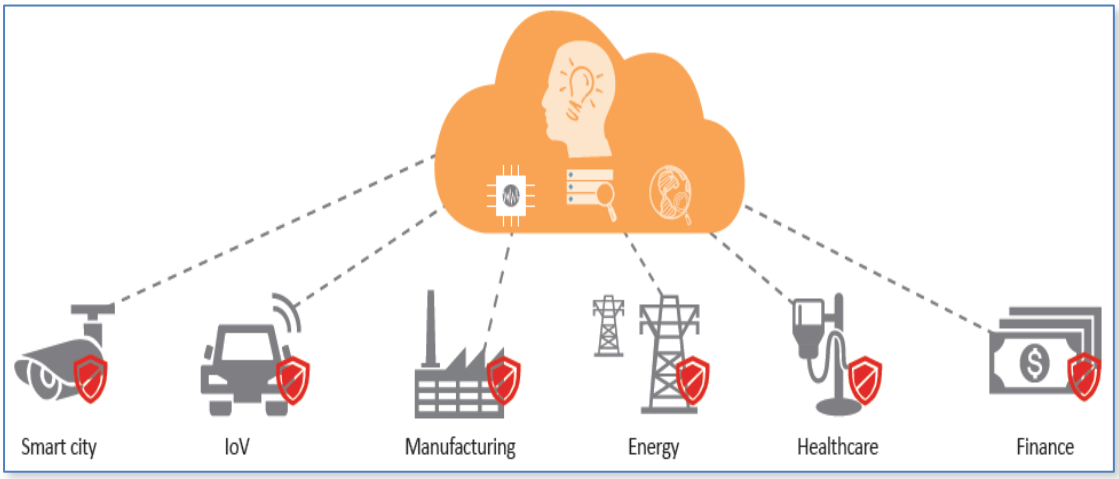
Επιπλέον, μια ποικιλία κατακόρυφων εφαρμογών, όπως το έξυπνο σπίτι, το IoV και η έξυπνη μέτρηση, πρέπει να έχουν πρόσβαση στην πλατφόρμα IoT. Πρέπει να παρέχονται μηχανισμοί απομόνωσης ασφαλείας για την αποθήκευση δεδομένων, επειδή οι απαιτήσεις ασφάλειας των δεδομένων ενδέχεται να διαφέρουν ανάλογα με τις εφαρμογές. Επιπλέον, πρέπει να διασφαλίζεται η εμπιστευτικότητα και η ακεραιότητα των δεδομένων κατά τη μετάδοσή τους. Οι ευαίσθητες πληροφορίες, όπως τα δεδομένα βίντεο, πρέπει να κρυπτογραφούνται για αποθήκευση στο cloud και τα δεδομένα πρέπει να διαγράφονται μετά τη λήξη της απαιτούμενης περιόδου διατήρησης δεδομένων προσωπικού χαρακτήρα.

Πρέπει επίσης να εξεταστεί η ασφάλεια των IoT εφαρμογών. Για την πρόσβαση στο cloud πρέπει να εφαρμοστεί υποχρεωτικός έλεγχος ταυτότητας και έλεγχος πρόσβασης. Πιθανά θέματα ευπάθειας των εφαρμογών δεν θα πρέπει να εκθέτουν τα δεδομένα των εφαρμογών κατά τη μετάδοσή τους. Πρέπει να παρέχεται αποτελεσματική κρυπτογράφηση και απομόνωση για την αποθήκευση δεδομένων σε Η / Υ και κινητά τελικά σημεία.

### A.3.3.5. Επίγνωση της κατάστασης ασφάλειας

Το σύστημα IoT, το οποίο αποτελείται από συσκευές, δίκτυα, πλατφόρμες και εφαρμογές, απαιτεί όχι μόνο πολλαπλά μέτρα προστασίας της ασφάλειας σε κάθε στρώμα, αλλά και τις έξυπνες δυνατότητες ανάλυσης ασφάλειας μεγάλων δεδομένων για τη συνέργεια cloud συσκευών (όπως φαίνεται στην Εικόνα 22). Αυτό θα επιτρέψει στο IoT να επιτύχει ευαισθητοποίηση σε επίπεδο δικτύου, ευαισθητοποίηση σχετικά με την κατάσταση, οπτικοποίηση και άμυνα ασφαλείας, σε όλο το δίκτυο, που θα είναι το μέλλον της ασφάλειας του IoT.

*Εικόνα 22: Επίγνωση της κατάστασης ασφάλειας για τη συνέργεια cloud συσκευών (Πηγή: Building a Trusted and Managed IoT World)*



Η μεγάλη ποσότητα των τελικών σημείων του IoT τα καθιστά εύκολο στόχο για επιθέσεις, δημιουργώντας απειλές για την IoT πλατφόρμα- πυρήνα. Η πλατφόρμα analytics ασφάλειας μεγάλων δεδομένων παρακολουθεί και αναλύει την κυκλοφορία και τη συμπεριφορά των τελικών σημείων ενάντια στις βασικές γραμμές σε πραγματικό χρόνο για να εντοπίσει γρήγορα τα μολυσμένα τελικά σημεία. Η πλατφόρμα μπορεί στη συνέχεια να συντονίσει τις συσκευές ασφαλείας για να περιορίσει τη μόλυνση και να απομονώσει τα μολυσμένα τελικά σημεία σύμφωνα με τις καθορισμένες πολιτικές ασφαλείας. Αυτή η σειρά ενεργειών θα προστατεύσει την κεντρική πλατφόρμα και το σύστημα εξυπηρέτησης.

Επιπρόσθετα, η πλατφόρμα analytics ασφάλειας μεγάλων δεδομένων μπορεί να λειτουργήσει ως ενιαία πλατφόρμα παρακολούθησης και διαχείρισης ασφάλειας για ολόκληρο το δίκτυο IoT. Με την παρακολούθηση του δικτύου και τον προγραμματισμό όλων των συσκευών ασφαλείας, η πλατφόρμα μπορεί να αποτρέψει γνωστές και άγνωστες απειλές, ιδιαίτερα προχωρημένες και επίμονες απειλές (APTs), όπως οι επιθέσεις στο Ουκρανικό δίκτυο ηλεκτρικής ενέργειας. Με τη βιβλιοθήκη πληροφοριών για τις απειλές και την ευαισθητοποίηση σε επίπεδο δικτύου, η πλατφόρμα analytics ασφάλειας μεγάλων δεδομένων προβλέπει την τάση της ασφάλειας του IoT και εφαρμόζει αντίμετρα για την ενεργητική υπεράσπιση των απειλών.

### Α.3.4. Πρακτικές Ασφάλειας IoT

Τα ζητήματα ασφάλειας του IoT μπορούν να αντιμετωπιστούν ακολουθώντας γνωστές πρακτικές στον τομέα της ασφάλειας των τεχνολογιών πληροφορικής. Αυτό πρέπει να γίνεται σε κάθε στάδιο της διαδικασίας ανάπτυξης, από τα στάδια της έρευνας και του σχεδιασμού μέχρι την ανάπτυξη της αγοράς. Θα πρέπει επίσης να εξεταστεί η αξιολόγηση της ευπάθειας του υλικολογισμικού και η σκλήρυνση των συστημάτων και των επικοινωνιών.

Λόγω της ποικίλης χρήσης των συσκευών IoT σε εφαρμογές όπως επιχειρηματικά περιβάλλοντα, οικιακές συσκευές, βιομηχανικά συστήματα και υγειονομική περίθαλψη, οι ορθές πρακτικές θα πρέπει να εφαρμόζονται στην ορθή χρήση και διαμόρφωση στο τελικό σημείο.

Η εκτίμηση των κινδύνων, η ανάλυση απειλών και η ανάλυση αντικτύπου πιθανών επιθέσεων θα πρέπει να διεξάγονται κατά περίπτωση, έτσι ώστε να μπορούν να επιλέγονται κατάλληλες πρακτικές ασφαλείας για την επίτευξη της καλύτερης ισορροπίας κόστους, χρηστικότητας και ασφάλειας. Για παράδειγμα, μια συσκευή που σχεδιάζεται να λειτουργεί σε σενάρια υγειονομικής περίθαλψης πρέπει να εξετάζει πολλές περισσότερες παραμέτρους και να

εφαρμόζει αυστηρότερες πρακτικές ασφαλείας από ένα έξυπνο ρολόι (Instituto National de Ciberseguridad, red.es, Huawei, 2017).

Καθώς οι κατασκευαστές αναπτύσσουν συσκευές IoT, υπάρχουν εγγενείς τεχνικοί περιορισμοί χρόνου και αγοράς που επηρεάζουν τη διαλειτουργικότητα και το σχεδιασμό των συσκευών. Ορισμένες συσκευές περιορίζονται από τεχνικούς παράγοντες όπως περιορισμένους εσωτερικούς πόρους επεξεργασίας, μνήμη ή απαιτήσεις κατανάλωσης ενέργειας. Οι κατασκευαστές υπόκεινται σε πίεση για τη μείωση του κόστους μονάδας της συσκευής ελαχιστοποιώντας το κόστος σχεδιασμού εξαρτημάτων και προϊόντων. Ωστόσο, πρέπει επίσης να εξετάσουν τους κινδύνους των ζητημάτων ασφάλειας.

#### Α.3.4.1. Πρακτικές Ασφάλειας στον Σχεδιασμό

Όπως αναφέρθηκε προηγουμένως, πρέπει να δοθεί προσοχή σε όλα τα πιθανά στάδια του κύκλου ζωής της ανάπτυξης του IoT, από το σχεδιασμό και την υλοποίηση έως τη χρήση του πελάτη.

- Παροχή σχετικών κανονισμών αγοράς και νομοθετικών προθέσεων ασφάλειας και έρευνας σχετικά με το στοχευόμενο περιβάλλον.
- Αυτό το αρχικό στάδιο θα βοηθούσε να προσδιοριστεί η βιωσιμότητα και τα πράγματα που πρέπει να εξεταστούν στα επόμενα στάδια.

#### Α.3.4.2. Πρακτικές Ασφάλειας στην Τεχνολογική Ανάπτυξη

Αφού προσδιοριστούν οι συνθήκες και οι περιορισμοί που σχετίζονται με τη χρήση και το περιβάλλον λειτουργίας, πρέπει να ληφθεί υπόψη η ασφάλεια του υλικού και του λογισμικού.

- Υλικό (Hardware)

  Ανάλογα με τους περιορισμούς του τομέα και το επίπεδο κρισιμότητάς του, μπορούν να παρατηρηθούν οι ακόλουθες πρακτικές:

  - *Ασφάλεια εκκίνησης:* Παρέχετε μηχανισμούς για την προστασία της διαδικασίας εκκίνησης και των αξιόπιστων ενημερώσεων.
  - *Firmware, μνήμη και αποθήκευση:* Εξασφαλίστε την ασφαλή ενημέρωση του υλικολογισμικού και επιτρέψτε την κρυπτογραφική επαλήθευση. Επαληθεύστε τυχόν διαρροή πληροφοριών λόγω ενσωματωμένων κωδικών πρόσβασης. Χρησιμοποιήστε κρυπτογράφηση στα μέσα αποθήκευσης.

- *CPU και μικροελεγκτές*: Σε εξαιρετικά κρίσιμες περιπτώσεις χρήσης, θα ήταν επιθυμητό να υπάρχουν μηχανισμοί που να ανιχνεύουν επιθέσεις παραβίασης ή αντίστροφης μηχανικής για την αποφυγή χειραγώγησης.
- *Φυσική πρόσβαση:* Προστατεύστε ή απενεργοποιήστε διεπαφές όπως θύρες USB και JTAG. Σχεδιάστε αντίμετρα για δυσμενείς περιβαλλοντικές συνθήκες.
- *Στοιχεία δικτύου*: Χρησιμοποιήστε ασύρματες κάρτες, Bluetooth ή εξαρτήματα RF που συμμορφώνονται με τα τρέχοντα πρότυπα ασφαλείας.
- *Διαχείριση ενέργειας*: Έχετε έναν εφεδρικό μηχανισμό σε περίπτωση διακοπής.

❖ Λογισμικό (Software)

- *Λειτουργικό Σύστημα (OS):* Επιλέξτε ένα αποδεδειγμένο λειτουργικό σύστημα και εφαρμόστε όλα τα μέτρα σκλήρυνσης που συνιστώνται σε κάθε περίπτωση. Ακολουθήστε την αρχή του ελάχιστου προνομίου. Δώστε ιδιαίτερη προσοχή στα δικαιώματα και τις άδειες των χρηστών και ενεργοποιήστε την προστασία κατά των εκμεταλλεύσεων για λειτουργίες OS, όπως ASLR, NX μνήμη και sandboxing.
- *API και πλαίσιο ανάπτυξης:* Εάν παρέχεται, εξασφαλίστε την ασφάλεια χρήσης μέσω πολιτικών αξιολόγησης ευπάθειας και ενημέρωσης.
- *Ενημερώσεις*: Έχετε μια στρατηγική ενημερώσεων για το λειτουργικό σύστημα καθώς και το λογισμικό, ακόμη και στην περίπτωση λογισμικού άλλου κατασκευαστή.

### Α.3.4.3. Πρακτικές Ασφάλειας σε λειτουργικότητα και ανάπτυξη

❖ *Εγκατάσταση και διαμόρφωση*: Η παροχή ενός καλά σχεδιασμένου συνόλου διαδικασιών για την εγκατάσταση και διαμόρφωση με ασφαλή τρόπο. Υποχρέωση στους χρήστες να αλλάξουν τις προεπιλεγμένες ρυθμίσεις ασφαλείας, όπως τον προεπιλεγμένο κωδικό πρόσβασης.

❖ *Συνδεσιμότητα και υπηρεσίες:* Ταυτοποίηση των περιττών διαμορφώσεων δικτύου, όπως οι ανοιχτές θύρες. Υποχρεωτική κρυπτογράφηση σε όλους τους τύπους επικοινωνιών.

- *Κρυπτογράφηση*: Επιλογή μιας αποδεδειγμένης σουίτας κρυπτογράφησης ή επαλήθευση πιθανών αδυναμιών, όπως γεννήτριες ψευδό-τυχαίων αριθμών, εάν πρόκειται να χρησιμοποιηθεί ιδιόκτητη κρυπτογράφηση.
- *Προστασία προσωπικών δεδομένων*: Εξασφάλιση της προστασίας προσωπικών ή ευαίσθητων δεδομένων και ενεργοποίηση των μηχανισμών καταστροφής δεδομένων και κρυπτογραφημένου χώρου αποθήκευσης σε συσκευές και τελικά σημεία όπου μπορούν να αποθηκευτούν αυτά τα δεδομένα.
- *Έλεγχος ταυτότητας και εξουσιοδότηση:* Εάν είναι απαραίτητο, χρησιμοποίηση ασφαλών μηχανισμών για την αλληλεπίδραση και δημιουργία συνδέσεων με συσκευές και υπηρεσίες, όπως υπηρεσίες cloud.
- *Αντιμετώπιση προβλημάτων δημιουργίας αντιγράφων ασφαλείας και καταστροφών*: Σε ορισμένες περιπτώσεις, συνιστάται να παρέχονται διαδικασίες ασφαλείας για την εξασφάλιση της δημιουργίας αντιγράφων ασφαλείας και την πλήρη ανάκτηση δεδομένων και του λειτουργικού συστήματος σε περίπτωση καταστροφών. Η αποθήκευση αντιγράφων ασφαλείας πρέπει να είναι κρυπτογραφημένη.

#### Α.3.4.4. Πρακτικές Ασφάλειας κατά την επαλήθευση και τη δοκιμή

Μετά την κατασκευή ενός προϊόντος και την εφαρμογή των πρακτικών ασφάλειας, ο κύκλος θα πρέπει να συνεχιστεί και η αποτελεσματικότητά τους θα πρέπει να δοκιμαστεί. Τα σημεία ελέγχου πρέπει να περιλαμβάνουν:

- Επισκόπηση υλικού και δοκιμές για χειραγώγηση
- Ανάλυση κυκλοφορίας δικτύου
- Ανάλυση ασφαλείας διασύνδεσης
- Επαλήθευση της ταυτότητας και αδυναμίες στην προεπιλεγμένη διαμόρφωση
- Δοκιμή υπηρεσιών και δοκιμών εισόδου για έλεγχο της άμυνας κατά των επιθέσεων DoS και fuzzing
- Επαλήθευση των διαδικασιών δημιουργίας αντιγράφων ασφαλείας και ανάκτησης σε πραγματικά σενάρια
- Μηχανισμός ενημέρωσης και έλεγχος επαλήθευσης της ακεραιότητας για υλικολογισμικό και λογισμικό
- Συμμόρφωση με τους κανονισμούς στο περιβάλλον λειτουργίας

### Α.3.4.5. Πρακτικές Ασφάλειας για τη λειτουργία χρήστη και τη συντήρηση

Τα μέτρα που ελήφθησαν στα προηγούμενα στάδια θα καταστούν άχρηστα αν οποιοσδήποτε ή οτιδήποτε αλληλεπιδρά με τη συσκευή IoT αγνοεί τις βέλτιστες πρακτικές ασφαλείας. Πρέπει να ληφθούν υπόψη τα ακόλουθα σημεία:

- Εάν μια λειτουργία ή υπηρεσία που παρέχεται στη συσκευή δεν χρησιμοποιείται ή δεν είναι απαραίτητη, απενεργοποιήστε την.
- Κρατήστε τη συσκευή ενημερωμένη και σωστά ρυθμισμένη.
- Χρησιμοποιήστε ισχυρούς κωδικούς πρόσβασης και να τους αλλάζετε τακτικά.
- Όταν οι συσκευές IoT πρέπει να ενσωματωθούν σε άλλες υποδομές, πρέπει να αξιολογηθεί η συνδεσιμότητα του δικτύου και οι αλληλεπιδράσεις με το περιβάλλον. Στη συνέχεια, μπορεί να επιλεγεί η κατάλληλη θέση για τη συσκευή. Αποφύγετε ανεπιθύμητες παρεμβολές και έκθεση.
- Οι μη χρησιμοποιούμενες συσκευές IoT μπορούν να γίνουν ένα πιθανό και ανεξέλεγκτο πρόβλημα ασφαλείας. Παρακολουθήστε τις μη χρησιμοποιούμενες συσκευές IoT. Εναλλακτικά, διαγράψτε τα δεδομένα για συσκευές που πρόκειται να μη χρησιμοποιηθούν.

### Α.3.4.6. Πρακτικές προστασίας προσωπικών δεδομένων

Το απόρρητο μπορεί να προστατευθεί με πολλούς τρόπους, όπως τεχνολογικά μέσα. Ωστόσο, οι νόμοι και οι κανονισμοί παρέχουν το ελάχιστο υποχρεωτικό σύνολο απαιτήσεων.

Εντός της Ευρωπαϊκής Ένωσης, ο βασικός κανονισμός είναι ο νέος κανονισμός γενικής προστασίας δεδομένων (EU GDPR). Προτείνει την έννοια της «Ιδιωτικότητας από το σχεδιασμό» και απαιτεί αξιολόγηση της επίπτωσης της ιδιωτικής ζωής (Privacy Impact Assessment, PIA) για συγκεκριμένη επεξεργασία δεδομένων. Το PIA αποτελεί σημαντικό εργαλείο για την εκπλήρωση των υποχρεώσεων προστασίας δεδομένων. Όπως αναφέρεται στο GDPR, το PIA απαιτείται όταν ένα είδος επεξεργασίας είναι πιθανό να οδηγήσει σε υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.

Προκειμένου να διασφαλιστούν τα δικαιώματα και οι ελευθερίες των ατόμων, στο μέτρο του εύλογου περιθωρίου, η ομάδα εργασίας του άρθρου 29, η συμβουλευτική αρχή της Ευρωπαϊκής Ένωσης για την προστασία των δεδομένων, διατυπώνει ορισμένες συστάσεις όπως:

- Οι PIA πρέπει να εκτελούνται πριν αρχίσουν να εφαρμόζονται νέες IoT εφαρμογές.

- Κάθε ενδιαφερόμενος στο IoT πρέπει να εφαρμόζει τις αρχές της Προστασίας Προσωπικών Δεδομένων από το σχεδιασμό και την προκαθορισμένη Προστασία Προσωπικών Δεδομένων.
- Πολλοί εμπλεκόμενοι στο IoT χρειάζονται μόνο συγκεντρωτικά δεδομένα και δεν χρειάζονται τα ακατέργαστα δεδομένα που συλλέγονται από συσκευές IoT. Τα ενδιαφερόμενα μέρη πρέπει να διαγράψουν τα ακατέργαστα δεδομένα μόλις εξαχθούν τα δεδομένα που απαιτούνται για την επεξεργασία των δεδομένων τους.
- Οι κατασκευαστές συσκευών πρέπει να ενημερώνουν τους χρήστες σχετικά με τους τύπους δεδομένων που συλλέγονται από αισθητήρες και επεξεργάζονται περαιτέρω, τους τύπους δεδομένων που λαμβάνουν και τον τρόπο επεξεργασίας και συνδυασμού των δεδομένων.
- Οι κατασκευαστές συσκευών πρέπει να είναι σε θέση να επικοινωνούν με όλους τους εμπλεκόμενους φορείς αμέσως μόλις το υποκείμενο των δεδομένων αποσύρει τη συγκατάθεσή του ή αντιταχθεί στην επεξεργασία δεδομένων.
- Ομοίως με τη λειτουργία "μην ενοχλείτε" στα smartphone, οι συσκευές IoT πρέπει να προσφέρουν μια επιλογή "μην συλλέγετε" για να προγραμματίσουν ή να απενεργοποιήσουν γρήγορα τους αισθητήρες.
- Για να αποφευχθεί η παρακολούθηση τοποθεσίας, οι κατασκευαστές συσκευών θα πρέπει να περιορίζουν τα δακτυλικά αποτυπώματα της συσκευής απενεργοποιώντας ασύρματες διεπαφές όταν δεν χρησιμοποιούνται. Εναλλακτικά, θα πρέπει να χρησιμοποιούν τυχαία αναγνωριστικά στοιχεία (όπως τυχαίες διευθύνσεις MAC για να ανιχνεύσουν δίκτυα Wi-Fi) για να αποτρέψουν τη χρήση ενός σταθερού αναγνωριστικού να χρησιμοποιηθεί για την παρακολούθηση τοποθεσίας.
- Οι χρήστες έχουν δικαίωμα πρόσβασης στα προσωπικά τους δεδομένα. Θα πρέπει να τους παρέχονται εργαλεία που να τους επιτρέπουν να εξάγουν εύκολα τα δεδομένα τους σε δομημένη και κοινή μορφή. Επομένως, οι κατασκευαστές συσκευών θα πρέπει να παρέχουν φιλική προς το χρήστη διεπαφή για χρήστες που επιθυμούν να αποκτήσουν συγκεντρωτικά δεδομένα και ακατέργαστα δεδομένα που εξακολουθούν να αποθηκεύονται.
- Πρέπει να υπάρχει μια ρύθμιση για να γίνεται διάκριση μεταξύ διαφορετικών ατόμων που χρησιμοποιούν την ίδια συσκευή, ώστε να μην μπορούν να μάθουν για τις δραστηριότητες του άλλου.
- Οι προεπιλεγμένες ρυθμίσεις κοινωνικών εφαρμογών που βασίζονται σε συσκευές IoT θα πρέπει να ζητούν από τους χρήστες να εξετάζουν, να επεξεργάζονται και να

αποφασίζουν σχετικά με τις πληροφορίες που παράγονται από τις συσκευές τους πριν να δημοσιεύονται σε κοινωνικές πλατφόρμες.

- Οι πληροφορίες που δημοσιεύονται από συσκευές IoT στις πλατφόρμες κοινωνικών μέσων δεν θα πρέπει να γίνονται δημόσιες ή να αναπροσαρμόζονται από τις μηχανές αναζήτησης, από προεπιλογή.
- Η συγκατάθεση για τη χρήση μιας συνδεδεμένης συσκευής και για την επεξεργασία δεδομένων που προκύπτει πρέπει να γίνεται κατόπιν ενημέρωσης και να παρέχεται ελεύθερα. Οι χρήστες δεν θα πρέπει να τιμωρούνται οικονομικά ή έχουν υποβαθμισμένη πρόσβαση στις δυνατότητες στις συσκευές τους εάν αποφασίσουν να μην χρησιμοποιήσουν τη συσκευή ή μια συγκεκριμένη υπηρεσία.

## Α.4. Διαχείριση κινδύνου στο IoT

Οι προειδοποιήσεις σχετικά με τους κινδύνους του Ίντερνετ των πραγμάτων (IoT) είναι εύκολο να βρεθούν. Αυτές οι προειδοποιήσεις παρερμηνεύουν τη φύση του κινδύνου και πώς η καινοτομία καθιστά την τεχνολογία ασφαλέστερη. Αυτή η νέα εφαρμογή τεχνολογίας ψηφιακών δικτύων έχει πολλές προκλήσεις για την πολιτική, από τη διαχείριση του ραδιοφάσματος, την ιδιωτική ζωή, τον εντοπισμό δεδομένων και την απασχόληση. Θα χρειαστούν χρόνια για να αναπτυχθούν τα πλαίσια πολιτικής για την ασφαλή μεγιστοποίηση των ωφελειών του IoT. Το παρόν κεφάλαιο εξετάζει τον κίνδυνο και το πώς τον μετράμε, ως τρόπο καθοδήγησης της ανάπτυξης πολιτικής.

Όλες οι νέες τεχνολογίες διατίθενται με κίνδυνο. Πόσο μεγάλος είναι ο κίνδυνος αποτελεί διαφορετικό ζήτημα. Ακόμα κι αν κάθε συσκευή IoT είναι ευάλωτη σε επίθεση, αυτό δεν μεταφράζεται σε τεράστιο νέο κίνδυνο. Πρέπει να εξακολουθήσουμε να ρωτάμε αν οι επιτιθέμενοι θα εκμεταλλευτούν κάθε ευπάθεια (απίθανο) και ποιες θα είναι οι συνέπειες της εκμετάλλευσης - και αυτές οι συνέπειες μπορεί να κυμαίνονται από φάρσα έως απειλητική για τη ζωή, αλλά σε λίγες μόνο περιπτώσεις υπάρχει πραγματικός κίνδυνος για την κοινωνία. Αυτό που πρέπει να εξετάσουμε είναι πόσο αυξάνεται ο κίνδυνος σε σύγκριση με τους κινδύνους στον κυβερνοχώρο που αντιμετωπίζουμε τώρα και πώς μπορούμε να διαχειριστούμε και να μειώσουμε τον κίνδυνο που απορρέει από τη χρήση νέων τεχνολογιών, όπως είναι η IoT, χωρίς υπερβολική αντίδραση με τρόπο που να βλάπτει την καινοτομία, την επιχειρηματικότητα και την οικονομική ανάπτυξη.

### Α.4.1. Πώς αξιολογείται ο κίνδυνος για το Διαδίκτυο των πραγμάτων

Οι άνθρωποι αποδέχονται και διαχειρίζονται τον κίνδυνο. Οι καταναλωτές και οι επιχειρήσεις λαμβάνουν αποφάσεις με βάση την ανοχή τους σε κινδύνους και τις εκτιμήσεις τους τόσο για τον κίνδυνο όσο και για την αξία που παρέχει η "επικίνδυνη" δραστηριότητα. Οι αντιλήψεις για τον κίνδυνο διαμορφώνονται από τις γνώσεις και τις υποθέσεις σχετικά με την ασφάλεια: ότι οι κατασκευαστές έχουν κάνει ασφαλή προϊόντα, ότι τα πρότυπα και οι κανονισμοί παρέχουν καθοδήγηση για την παραγωγή και τη χρήση και ότι τα δικαστήρια θα παράσχουν διορθωτικά μέτρα σε περίπτωση αποτυχίας της ασφάλειας.

Οι ανησυχίες σχετικά με το IoT και τον κίνδυνο αντανακλούν μια ευρύτερη αλλαγή στην κοινωνία. Αντί για την χρυσή χιλιετία της δεκαετίας του 1990, ζούμε σε έναν κόσμο που συχνά απεικονίζεται ως δυστοπικός. Αλλά με τα περισσότερα μέτρα - το προσδόκιμο ζωής, η αιτία θανάτου, η οικονομική ευημερία ή η συχνότητα βίαιου κινδύνου σύγκρουσης έχει μειωθεί σημαντικά για μεγάλο μέρος του παγκόσμιου πληθυσμού[2]. Είναι δύσκολο να υποστηριχτεί διαφορετικά όταν η κύρια αιτία θανάτου σε πολλές Χώρες, συμπεριλαμβανομένων των ΗΠΑ, είναι η παχυσαρκία.

Τα μέσα μαζικής ενημέρωσης διαμορφώνουν τη γνώση και τις στάσεις του κοινού και αυτό μπορεί να στρεβλώσει την αντίληψη του κινδύνου (Slovic, 1987). Το σημαντικό έργο στο θέμα αυτό είναι του Paul Slovic, "Η αντίληψη του κινδύνου", που δημοσιεύτηκε στο Science το 1987. Έγραψε:

> *«Ενώ οι τεχνολογικά εξελιγμένοι αναλυτές χρησιμοποιούν αξιολόγηση κινδύνου για την αξιολόγηση των κινδύνων. . . [διότι] η πλειοψηφία των εμπειριών των πολιτών με τους κινδύνους τείνει να προέρχεται από τα μέσα ενημέρωσης, τα οποία μάλλον περιγράφουν λεπτομερώς ατυχίες και απειλές. . . . Η κυρίαρχη αντίληψη για τους περισσότερους Αμερικανούς (και μία που αντιπαραθέτει έντονα τις απόψεις των περισσότερων επαγγελματιών εκτιμητών κινδύνου) είναι ότι αντιμετωπίζουν σήμερα περισσότερο κίνδυνο από ό, τι στο παρελθόν και ότι ο μελλοντικός κίνδυνος θα είναι ακόμη μεγαλύτερος από τον σημερινό.»*

Έχει γίνει μια συνήθης πρακτική στον κυβερνοχώρο για τους ερευνητές να ανακοινώνουν κάποια ευπάθεια ή απειλή και ότι αυτό πρέπει να ληφθεί από τα μέσα μαζικής ενημέρωσης.

[2] Αυτή η δήλωση απαιτεί μακρότερη συζήτηση από αυτή που δικαιολογείται για αυτή την εργασία, αλλά το βάρος των στοιχείων από οντότητες όπως η Παγκόσμια Οργάνωση Υγείας και τα διάφορα ακαδημαϊκά ιδρύματα που εντοπίζουν τις συγκρούσεις την υποστηρίζει.

Είναι ελεύθερη η δημοσιότητα, αλλά αυτή η πρακτική μπορεί να διαστρεβλώσει την κατανόησή μας για τον κίνδυνο και να την υπερβάλει λαμβάνοντας μια μεμονωμένη περίπτωση έξω από το πλαίσιο. Αυτό που μετράει είναι μια εκτίμηση των πραγματικών συνεπειών. Για το IoT, ενώ χρησιμοποιούνται δισεκατομμύρια συσκευές IoT, δεν αποδίδεται ούτε ένας θάνατος. Αυτό μπορεί να αλλάξει καθώς η χρήση συσκευών IoT διευρύνεται και οι λειτουργίες που εκτελούνται από συσκευές IoT γίνονται πιο εξελιγμένες. Προς το παρόν, η απουσία ή ο κίνδυνος πρέπει να αποτελέσει το υπόβαθρο για οποιαδήποτε προσέγγιση των διαφόρων παραμέτρων στο IoT (Lewis, 2016).

Τα αυτοκίνητα είναι ένα καλό παράδειγμα του τρόπου με τον οποίο το IoT θα αλλάξει τον κίνδυνο. Τα αυτοκίνητα συντρίβονται συστηματικά από λάθος του χειριστή. Ορισμένα ατυχήματα προκαλούνται από την αποτυχία του εξοπλισμού ή, λιγότερο συχνά, από ελαττώματα στο σχεδιασμό ή την κατασκευή. Κανείς δεν θέλει να εμπλακεί σε αυτοκινητιστικό δυστύχημα και αναμένουμε από τους κατασκευαστές να λάβουν μέτρα για τη μείωση του κινδύνου.

Πολλοί ερευνητές έχουν δείξει ότι είναι δυνατό να «χακάρουν» τα αυτοκίνητα και ότι οι ευπάθειες που έχουν ανακαλύψει θα μπορούσαν να χρησιμοποιηθούν υποθετικά για να προκαλέσουν συντριβή. Τα ακραία σενάρια είναι ότι ένας χάκερ θα μπορούσε να αναλάβει τα συστήματα φρεναρίσματος και επιτάχυνσης ή θα μπορούσε να σβήσει τον κινητήρα του αυτοκινήτου ενώ κινείται με μεγάλη ταχύτητα. Αυτά τα παραδείγματα υπονοούν, αλλά δεν είναι καθοριστικά. Το πρώτο ερώτημα θα ήταν αν ο αριθμός των ατυχημάτων που προκλήθηκαν από την πειρατεία ήταν μεγαλύτερος από τον αριθμό των συγκρούσεων που αποφεύγονται από τα «έξυπνα» αυτοκίνητα. Αν το IoT εμποδίζει περισσότερα ατυχήματα από αυτά που μπορεί να προκαλέσουν οι χάκερς, υπάρχει καθαρό κέρδος για την κοινωνία. Δεδομένου ότι σχεδόν όλα τα ατυχήματα στο αυτοκίνητο περιλαμβάνουν σφάλμα χειριστή, μια υπόθεση εργασίας είναι ότι τα ημιαυτόνομα αυτοκίνητα είναι πιθανό να μειώσουν το σφάλμα του χειριστή και να μειώσουν τον αριθμό των τροχαίων ατυχημάτων και το καθαρό όφελος για την κοινωνία υπερτερεί του κινδύνου.

Ο κίνδυνος θα μειωθεί καθώς η καινοτομία μειώνει την πιθανότητα ή τις συνέπειες της πειρατείας ενός αυτοκινήτου ή μιας άλλης συσκευής IoT. Αυτού του είδους η καινοτομία είναι πιθανό να είναι εξελικτική, με διαδοχικά μοντέλα αυτοκινήτων πιο ασφαλή από τα προηγούμενα. Η διαφορά μεταξύ της ασφάλειας ενός αυτοκινήτου που χτίστηκε πριν από 20 χρόνια και ενός κατασκευασμένου σήμερα είναι σημαντική και μπορούμε να αναμένουμε την ίδια εξελικτική διαδικασία για τα συνδεδεμένα αυτοκίνητα και τις συσκευές IoT. Μπορούμε να επιταχύνουμε αυτήν την καινοτομία μέσω της κανονιστικών διατάξεων, αλλά

η αυξημένη νομοθεσία έρχεται επίσης με τον κίνδυνο ότι πρέπει να ληφθεί υπόψη σε οποιαδήποτε απόφαση. Ο κανονισμός αλλάζει τις επιχειρηματικές αποφάσεις και τις επενδύσεις. Συνήθως, αυτό είναι για το καλύτερο, αλλά μια κακώς σχεδιασμένη ή περιττή ρύθμιση μπορεί να επιβάλει ένα κόστος στις κοινωνίες το οποίο μειώνει άσκοπα τις ευκαιρίες και την ανάπτυξη.

Το παράδειγμα του αυτοκινήτου μας βοηθά επίσης να σκεφτούμε πώς να διαχειριστούμε τον κίνδυνο του IoT. Ενώ τα αυτοκίνητα περιέχουν τώρα πολλούς μικρούς υπολογιστές, μερικοί από τους οποίους είναι ευάλωτοι σε hacking, υπάρχουν μόνο μερικά συστήματα που προκαλούν μεγάλη ανησυχία. Η πρόσβαση σε αυτές τις κρίσιμες λειτουργίες που ελέγχουν τη λειτουργία του αυτοκινήτου δημιουργεί κίνδυνο. Η πρόσβαση σε ένα ενσωματωμένο σύστημα ψυχαγωγίας (το οποίο είναι πιθανό να συνδεθεί ασύρματα στο Internet) δημιουργεί κίνδυνο μόνο εάν το σύστημα ψυχαγωγίας συνδέεται επίσης με μια κρίσιμη λειτουργία. Το χακάρισμα ενός αυτοκινήτου αυξάνει μόνο τον κίνδυνο, εάν μπορούν να χειριστούν κρίσιμες λειτουργίες. Ο τρόπος με τον οποίο ένα αυτοκίνητο έχει σχεδιαστεί για να λειτουργεί σε περίπτωση βλάβης του υπολογιστή, επίσης, καθορίζει τον κίνδυνο, αυτοκίνητα που μπορούν να συνεχίσουν να λειτουργούν με υποβαθμισμένα IoT συστήματα είναι ασφαλέστερα.

Τα ημιαυτόνομα αυτοκίνητα που αυτοματοποιούν τις λειτουργίες όπως η αποφυγή σύγκρουσης και η διατήρηση των λωρίδων θα κάνουν τα αυτοκίνητα ακόμα ασφαλέστερα. Ταυτόχρονα, τα ημιαυτόνομα αυτοκίνητα που συνδέονται με το Διαδίκτυο έρχονται με αυξημένη ευπάθεια, και αυτά τα τρωτά σημεία μπορούν να μεταφραστούν σε κάποια αύξηση του κινδύνου. Το πρόβλημα της δημόσιας πολιτικής είναι να ρωτήσουμε πώς μειώνουμε το κοινωνικό κόστος των κακών αποτελεσμάτων χρησιμοποιώντας μέτρα που δεν επιφέρουν κόστος στην καινοτομία ή στις εύλογες ελευθερίες. Τα "εργαλεία" για τη μείωση του κινδύνου είναι η νομοθεσία, οι βελτιώσεις των προϊόντων και οι αγωγές.

Οι κατασκευαστές ζυγίζουν τον κίνδυνο των αγωγών και του κόστους ευθύνης, καθώς και τη ζημιά στο εμπορικό σήμα (που θα μπορούσε να είναι σημαντική) αν ένα αυτοκίνητο αποδειχθεί ότι είναι επικίνδυνο επειδή είναι ευάλωτο σε πειρατεία. Η απόφασή τους εξαρτάται επίσης από τις ρυθμιστικές αρχές και την ικανότητά τους να δημιουργούν πρότυπα για ασφαλή αυτοκίνητα IoT. Μέσα από ένα συνδυασμό ρυθμιστικών κινήτρων και δυνάμεων της αγοράς (συμπεριλαμβανομένης της ευθύνης), οι εταιρείες αυτοκινήτων έχουν κάνει τα αυτοκίνητα εξαιρετικά ασφαλέστερα. Το 1921, υπήρχαν 24 θάνατοι στις Ηνωμένες Πολιτείες για κάθε εκατομμύριο μίλια οδήγησης. Μέχρι το 2013, οι βελτιώσεις στον σχεδιασμό και την τεχνολογία σε συνδυασμό με τη νομοθεσία οδήγησαν στη μείωση των ατυχημάτων σε

ελαφρώς περισσότερο από ένα θανάσιμο ατύχημα ανά εκατομμύριο μίλια οδήγησης και ο αριθμός αυτός συνεχίζει να συρρικνώνεται (Fatality Analysis Reporting System (FARS), 2018).

Οι κοινωνίες μπορούν να εφαρμόσουν αυτά τα ίδια εργαλεία στο IoT. Το IoT δημιουργεί τρία είδη κινδύνου - μια συσκευή IoT μπορεί να παρουσιάσει δυσλειτουργία, θα μπορούσε να χακαριστεί, ή οι προσπάθειές μας για την προστασία της ιδιωτικής ζωής ή για την ενίσχυση της ασφάλειας των συσκευών IoT να δημιουργήσουν οικονομικές ζημιές που υπερτερούν της μείωσης του κινδύνου. Οι ασφαλιστικές εταιρείες υπολογίζουν τον κίνδυνο χρησιμοποιώντας αναλογιστικά δεδομένα, ιστορικά αρχεία που δείχνουν πόσο συχνά είναι πιθανό να συμβεί ένα συμβάν και τι είναι πιθανό να κοστίσει αυτό το συμβάν. Δεν διαθέτουμε αναλογιστικά δεδομένα για τα περισσότερα πράγματα στην ασφάλεια του κυβερνοχώρου, συμπεριλαμβανομένου του IoT. Αυτό καθιστά δύσκολη την ακριβή πρόβλεψη του κινδύνου, αλλά μπορούμε να καθορίσουμε τους παράγοντες που διαμορφώνουν την εξίσωση κινδύνου:

- Ευπάθεια: Η δυνατότητα ενός εισβολέα να αποκτήσει πρόσβαση και έλεγχο μιας υπολογιστικής συσκευής, να χειριστεί ή να εξαγάγει δεδομένα ή να ελέγξει ή να διακόψει τις υπηρεσίες. Οι περισσότεροι ερευνητές πιστεύουν ότι οι υπολογιστικές συσκευές που χρησιμοποιούνται στο Διαδίκτυο των πραγμάτων θα είναι ακόμη πιο ευάλωτες από τις τεχνολογίες του Διαδικτύου στις οποίες είμαστε συνηθισμένοι, δεδομένων των τεχνικών περιορισμών πολλών υπολογιστικών συσκευών IoT. Πολλές από αυτές τις συσκευές δεν θα έχουν την απαιτούμενη υπολογιστική ισχύ για να εκτελούν παραδοσιακές λειτουργίες ασφαλείας γνωστών επιτραπέζιων υπολογιστών και φορητών υπολογιστών, γεγονός που τους καθιστά εύκολους στόχους
- Πρόθεση: Απλά επειδή μια συσκευή IoT είναι ευάλωτη δεν σημαίνει ότι κάποιος θα την εκμεταλλευτεί για κακόβουλους σκοπούς. Ένας εισβολέας πρέπει να αποφασίσει να εκμεταλλευτεί μια ευπάθεια αφού υπολογίσει εάν η επίθεση θα προσφέρει πολιτικό, στρατιωτικό, οικονομικό ή κοινωνικό όφελος. Η πρόθεση μπορεί να αντικατοπτρίζει την απλή κακία, το έγκλημα, την κατασκοπεία, την τρομοκρατία, τον πόλεμο - όλα τα συνηθισμένα κίνητρα που παρατηρούνται στην ασφάλεια στον κυβερνοχώρο.
- Συνέπειες: Οι υπολογιστικές συσκευές είναι ευάλωτες και οι επιτιθέμενοι ενδέχεται να εκμεταλλευτούν αυτά τα τρωτά σημεία, αλλά το τελικό ερώτημα είναι, ε και; Υπάρχει ήδη υψηλό επίπεδο βίας, εγκληματικότητας και ατυχήματος στις κοινωνίες,

όμως οι κοινωνίες έχουν μια αξιοσημείωτη ικανότητα να απορροφήσουν τέτοια πράγματα. Οι περισσότερες από τις ευπάθειες που εντοπίζονται στις συσκευές του Διαδικτύου οδηγούν σε γεγονότα που θα μπορούσαν να χαρακτηριστούν ως φάρσες. Το μεγαλύτερο ερώτημα είναι εάν το IoT εισάγει συστημικές αδυναμίες που θα οδηγούσαν σε απώλεια ζωής ή σημαντική οικονομική ζημία.

Η Ευπάθεια, η πρόθεση και οι συνέπειες μας επιτρέπουν να εκτιμήσουμε την πιθανότητα ενός καταστροφικού συμβάντος IoT. Οι περισσότερες αναλύσεις επικεντρώθηκαν στην ευπάθεια του IoT, η οποία είναι εμφανώς υψηλή. Αυτή όμως δεν είναι η πιο σημαντική μεταβλητή για την πρόβλεψη του κινδύνου. Για να εκτιμήσουμε τον κίνδυνο που δημιουργείται από το συνδυασμό των ευάλωτων συσκευών, των κακόβουλων παραγόντων και των ενδεχομένως επιβλαβών συνεπειών, θα πρέπει να αναρωτηθούμε πόσο πιθανό είναι να δούμε κακόβουλη δράση για την εκμετάλλευση των τρωτών σημείων ώστε να προκληθούν επιζήμιες συνέπειες. Ένα από τα καθήκοντά μας στην αξιολόγηση του κινδύνου είναι να αναλύσουμε το πλήθος των συσκευών IoT σε εκείνους όπου η κρισιμότητα της λειτουργίας ή η επεκτασιμότητα της επίθεσης δημιουργεί πραγματικό κίνδυνο. Είναι αυτή η διασταύρωση κρίσιμης λειτουργίας και ευάλωτων συσκευών όπου ο κίνδυνος είναι μεγαλύτερος.

Ένα σημείο εκκίνησης είναι να υποθέσουμε ότι το IoT δεν θα είναι πιο ασφαλές από οποιαδήποτε άλλη τεχνολογία Διαδικτύου - και σε ορισμένες περιπτώσεις μπορεί να είναι ακόμη λιγότερο ασφαλές. Η εμπειρία των τελευταίων 20 ετών έχει δείξει πόσο δύσκολο είναι να γράψουμε ασφαλείς κώδικες. Η πολυπλοκότητα (ή η έλλειψη της) της συσκευής IoT δημιουργεί πρόσθετες ευπάθειες. Πολλές συσκευές IoT θα έχουν περιορισμένη δυνατότητα να ενημερώσουν το λογισμικό τους. Θα αντιμετωπίσουν δυσκολίες στη διαχείριση της αυθεντικότητας και της κρυπτογράφησης. Οι μεγαλύτερες, πιο εξελιγμένες συσκευές IoT θα είναι σε καλύτερη θέση να εκτελούν λειτουργίες ασφαλείας, αλλά αυτές οι επιλογές προσφέρονται με πρόσθετο κόστος και πολυπλοκότητα που μπορεί να μειώσει τη ζήτηση σε επίπεδο καταναλωτή. Περιορισμοί στην απόδοση της συσκευής θα περιορίσουν την ικανότητά μας να διασφαλίζουμε το IoT.

Πολλές συσκευές IoT είναι καταναλωτικά αγαθά. Τα σενάρια για την πρόκληση σημαντικών ζημιών από την πειρατεία καταναλωτικών συσκευών IoT καθίστανται ολοένα και πιο προβληματικές, καθώς αναζητούμε εύλογες καταστάσεις όπου τα συστήματα προστασίας των καταναλωτών παράγουν οτιδήποτε άλλο εκτός από τοπικό και προσωρινό αποτέλεσμα.

Για να πάρουμε μια ακραία περίπτωση, αν οι χάκερ μπορούσαν να καταλάβουν τον έλεγχο ενός κρίσιμου συστήματος αεροσκαφών, οδηγώντας σε σύγκρουση, το αποτέλεσμα θα ισοδυναμούσε με τρομοκρατική βομβιστική επίθεση. Αυτό προϋποθέτει, ωστόσο, ότι το πλήρωμα του αεροσκάφους δεν θα μπορούσε να ανακτήσει τον έλεγχο. Μια απλή προφύλαξη θα ήταν να διασφαλιστεί ότι το πλήρωμα είχε την ικανότητα να παρακάμπτει τα συστήματα IoT ή να επαναφέρει το σύστημα σε ορισμένες βασικές λειτουργικές ρυθμίσεις. Πολλές συσκευές που χρησιμοποιούμε τώρα, όπως τα αεροσκάφη, έχουν ήδη σχεδιαστεί για να αντιμετωπίσουν την αποτυχία των εξαρτημάτων και τα προγράμματα εκπαίδευσης πιλότων λαμβάνουν υπόψη την αποτυχία. Ομοίως, η ανάληψη ελέγχου ενός ανελκυστήρα θα απαιτούσε την αποτροπή των τριών ή τεσσάρων μηχανικών συστημάτων ασφαλείας που χρησιμοποιούνται από τους σύγχρονους ανελκυστήρες.

Η επαναληψιμότητα μιας επίθεσης IoT καθορίζει επίσης τον ψυχολογικό της αντίκτυπο. Οι αμυχές που φαίνεται να είναι επαναλαμβανόμενες και ασταμάτητες θα δημιουργήσουν φόβο και αβεβαιότητα, παρόμοιες με το φόβο και την αβεβαιότητα που έπληξαν τις Ηνωμένες Πολιτείες μετά τις 9/11 (Lewis, 2016), όταν δεν ήταν ξεκάθαρο αν οι επιθέσεις αυτοκτονίας ήταν οι εναρκτήριοι γύροι μιας μακράς εκστρατείας επιθέσεων. Η ικανότητα να προκαλέσει πτώση αεροπλάνου δημιουργεί τρομοκρατία, αλλά η αδυναμία πρόβλεψης του πότε και πόσο συχνά θα επαναληφθούν αυτά τα επεισόδια αυξάνουν εκείνο τον φόβο.

Οι περισσότεροι που υπολογίζουν την ευπάθεια του IoT υποθέτουν ότι ένα μόνο περιστατικό hacking μπορεί να αναπαραχθεί σε μαζική κλίμακα, αλλά στις περισσότερες περιπτώσεις, η πρόκληση δεν είναι να χακάρει ένα μόνο αυτοκίνητο ή ψυγείο, είναι να χακάρει αρκετές χιλιάδες σε καταστάσεις και συνθήκες που παράγουν μαζική επίδραση. Ο αριθμός των μεταβλητών που εμπλέκονται σε αυτό το είδος μαζικού συμβάντος υποδηλώνει ότι αυτό το είδος παραβίασης του IoT είναι πολύ απίθανο. Δεν θέλουμε να εξάγουμε συστηματική επίδραση από ένα παράδειγμα όπου οι χάκερ, υπό ιδανικές συνθήκες, μπορούν να προκαλέσουν δυσλειτουργία μιας μόνο συσκευής, σε κάποια μεγαλύτερη απειλή για την ασφάλεια. Το μέσο επίπεδο ασυμφωνίας και ακόμη και το χάος που οι σύγχρονες οικονομίες δέχονται σε καθημερινή βάση είναι υψηλό. Τα χτυπήματα του IoT θα πρέπει να υπερβούν αυτό το όριο ώστε να είναι αισθητά επικίνδυνα.

Οι περισσότερες συσκευές IoT δεν θα εκτελέσουν κρίσιμες λειτουργίες ούτε θα δημιουργήσουν ή θα αποθηκεύσουν κρίσιμα δεδομένα. Αυτό ισχύει ιδιαίτερα για τις συσκευές IoT των καταναλωτών. Αυτό σημαίνει ότι ακόμη και αν αυτές οι συσκευές των καταναλωτών έχουν προσβληθεί, το αποτέλεσμα είναι πολύ πιθανό να είναι μια απλή ενόχληση. Ένα έθνος με μεγαλύτερη έκθεσή του στις φάρσες δεν αντιμετωπίζει αυξημένο

κίνδυνο. Είναι συστημικό ρίσκο - η δυνατότητα δημιουργίας σημαντικών διαταραχών κάνοντας επίθεση σε ένα μόνο κρίσιμο κόμβο (όπως το FedWire, το ηλεκτρικό δίκτυο ή ένα πυρηνικό εργοστάσιο παραγωγής ηλεκτρικής ενέργειας) ή με ταυτόχρονη επίθεση μεγάλου αριθμού στόχων για να υπάρξει σημαντική επίδραση. Μια απλή προφύλαξη θα ήταν να διασφαλίσουμε ότι ορισμένα κρίσιμα συστήματα, τα οποία δεν συνδέονται πλέον με το Διαδίκτυο, παραμένουν αποσυνδεδεμένα μέχρι να μπορέσουμε να αξιολογήσουμε και να ελέγξουμε καλύτερα τον κίνδυνο.

### Α.4.2. Αυτονομία και Ρίσκο

Η απόφαση για το κατάλληλο επίπεδο αυτονομίας του IoT είναι ένα θεμελιώδες ζήτημα για την ασφάλεια. Η ισορροπία ανάμεσα στην αυτόνομη λειτουργία και τον ανθρώπινο έλεγχο διαμορφώνει ρίσκο στο IoT. Ένας εύκολος τρόπος για να γίνει αντιληπτό είναι να αναρωρηθούμε αν μια συσκευή IoT αντικαθιστά έναν άνθρωπο (όπως σε ένα αυτοκίνητο χωρίς οδηγό) ή βελτιώνει τον άνθρωπο (όπως ένα έξυπνο αυτοκίνητο που βοηθά τους οδηγούς αυτοματοποιώντας λειτουργίες όπως φρενάρισμα και αποφυγή σύγκρουσης). Ο τρόπος με τον οποίο οι αυτόνομες συσκευές IoT πρέπει να λειτουργούν συνεχίζει μια αντιπαράθεση που χρονολογείται από τις προηγούμενες συζητήσεις για τους υπολογιστές, όπου ορισμένοι επιστήμονες είδαν τους υπολογιστές να βελτιώνουν την ανθρώπινη απόδοση ενώ άλλοι τις είδαν ως αντικατάσταση των ανθρώπων (Markoff, 2015).

Πολλοί άνθρωποι έχουν ήδη αλληλεπιδράσει με αυτόνομη υπολογιστική συσκευή όταν παίζουν βιντεοπαιχνίδια. Ο "αντίπαλος" που παράγεται από υπολογιστή σε ένα βιντεοπαιχνίδι "ανιχνεύει" τις ενέργειές σας και λαμβάνει αποφάσεις σχετικά με τον τρόπο αντίδρασης. Αυτό γίνεται με ένα ισχυρό υπολογιστή που περιέχεται στο κιβώτιο παιχνιδιών που τρέχει λογισμικό και αναλαμβάνει δράση για να ανταποκριθεί στις κινήσεις σας, με βάση μερικά προ-ρυθμισμένα μενού επιλογών. Αυτό συμβαίνει σε χιλιοστά του δευτερολέπτου. Το αποτέλεσμα είναι μια ψευδαίσθηση ότι ο αντίπαλος σκέφτεται και αλληλεπιδρά με το περιβάλλον του. Ο πραγματικός κόσμος είναι πολύ πιο πολύπλοκος από το τεχνητό περιβάλλον παιχνιδιών, απαιτώντας πολλούς περισσότερους συντελεστές εισόδου και πολύ πιο πολύπλοκο προγραμματισμό, αλλά τα βιντεοπαιχνίδια δείχνουν τη δυνατότητα για αυτόνομες συσκευές και δημιουργούν ένα πρότυπο για την κατασκευή αυτόνομων συστημάτων. Είναι ενδιαφέρον να σημειωθεί ότι ένας από τους κορυφαίους κατασκευαστές τσιπ γραφικών για τα βιντεοπαιχνίδια, η Nvidia, έχει γίνει ένας σημαντικός προμηθευτής τσιπ για κινητά υπολογιστικά και αυτοδιαχειριζόμενα αυτοκίνητα.

Ο καθορισμός του βαθμού ανεξαρτησίας των συσκευών IoT είναι μια απόφαση σχετικά με τον κίνδυνο. Για να χρησιμοποιήσουμε το παράδειγμα του αυτοκινήτου, ένα αυτοκίνητο κυλάει στο δρόμο, οδηγώντας με αυτόματο πιλότο και ο οδηγός ασχολείται με την αποστολή μηνυμάτων. Σε περίπτωση έκτακτης ανάγκης απαιτείται ο οδηγός να πάρει ξαφνικά τον έλεγχο. Η εμπειρία των συστημάτων αυτόματου πιλότου στα αεροπλάνα υποδηλώνει ότι αυτή η απότομη μετάβαση από το μηχάνημα προς τον έλεγχο του ανθρώπου δημιουργεί ρίσκο- οι πιλότοι βασίζονται σε έναν υπολογιστή για να πετάξουν στο αεροπλάνο και στη συνέχεια πρέπει να πάρουν ξαφνικά αποφάσεις χωρίς επαρκή συνειδητοποίηση της κατάστασης (Konnikova, 2014). Επιπλέον, η εμπειρία από τους αυτόματους πιλότους δείχνει ότι ο κίνδυνος αυξάνεται με την πάροδο του χρόνου. Οι άνθρωποι συνηθίζουν τα αυτο-λειτουργούντα συστήματα και οι ικανότητές τους ως οδηγός (ή πιλότος) υποβαθμίζονται από αχρηστία. Ο οδηγός δεν χρειάζεται μόνο να αντιδρά γρήγορα, πρέπει να ξέρει τι να κάνει και να έχει εμπειρία να το κάνει.

Πόσος έλεγχος θα πρέπει να δοθεί στο αυτόνομο σύστημα εξαρτάται από τη περίσταση. Εάν η πιθανότητα απότομων, μη αναμενόμενων αλλαγών είναι υψηλή, οι αυτόνομες συσκευές ενδέχεται να μην ανταποκριθούν αποτελεσματικά. Στις περιπτώσεις όπου ο ανθρώπινος χειριστής έχει πρωταρχικό έλεγχο ή μπορεί να υπερισχύσει του ελέγχου της μηχανής, ο κίνδυνος μειώνεται σημαντικά. Με τα επανδρωμένα αεροσκάφη, για παράδειγμα, αν ένας πιλότος μπορεί να διορθώσει έγκαιρα τις επικίνδυνες ενέργειες αεροσκαφών, ελαχιστοποιείται ο κίνδυνος. Ο κίνδυνος μπορεί να αντιμετωπιστεί με τον περιορισμό των αυτόνομων λειτουργιών, την εξασφάλιση της εμπλοκής του ανθρώπινου χειριστή και με διερεύνηση ως προς το πού μπορεί να αφαιρεθεί με ασφάλεια ο χειρισμός των ανθρώπων από τον έλεγχο.

Αυτό υποδηλώνει ότι έως ότου μπορέσουμε να είμαστε πιο σίγουροι για την αξιοπιστία και ασφάλεια των συσκευών IoT, μπορεί να είναι σημαντικό να σχεδιάσουμε συστήματα που θα επιτρέπουν χειροκίνητο έλεγχο για συστήματα που παρέχουν ζωτικές υπηρεσίες ή που θα μπορούσαν να προκαλέσουν μαζική επίδραση. Η αντίρρηση ότι η παροχή στους καταναλωτές της εξουσίας για απεμπλοκή θα μειώσει τα οικονομικά οφέλη του IoT είναι αληθινή, αλλά για το σχετικά μικρό σύνολο συσκευών IoT που θα μπορούσαν να παράγουν μαζική επίδραση ή κρίσιμη λειτουργία, ο αυξημένος κίνδυνος το δικαιολογεί αυτό.

Υπάρχουν επίσης μακροχρόνιες και σοβαρές ανησυχίες για τον κίνδυνο ότι τα αυτόνομα συστήματα θα ξεπεράσουν, θα ανταγωνιστούν και θα αντικαταστήσουν τον άνθρωπο. Η πρόοδος προς αυτά τα συστήματα εξαρτάται από την ανάπτυξη της τεχνητής νοημοσύνης, όπου οι υπολογιστές σκέπτονται σαν άνθρωποι και δε λειτουργούν από ένα καθορισμένο

πρόγραμμα. Προς το παρόν, οι προκλήσεις ασφάλειας που δημιουργούνται από το IoT θα είναι πιο προφητικές: προστασία δεδομένων και πρόληψη μη εξουσιοδοτημένης πρόσβασης και ελέγχου.

### Α.4.3. Έλεγχος ταυτότητας και κρυπτογράφηση για τη διαχείριση κινδύνου στο IoT

Οι τεχνολογικές λύσεις για μεγαλύτερη ασφάλεια του IoT περιλαμβάνουν κρυπτογράφηση και ισχυρή πιστοποίηση ταυτότητας. Μεγαλύτερη χρήση κρυπτογράφησης και βελτιωμένες λειτουργίες επαλήθευσης θα μειώσει τον κίνδυνο για την ιδιωτική ζωή και την ασφάλεια σε όλες τις εφαρμογές του Διαδικτύου, αλλά η υιοθέτηση τόσο της κρυπτογράφησης όσο και της αυθεντικοποίησης έχουν προκαλέσει μέχρι στιγμής δύσκολες προκλήσεις όχι μόνο για το IoT αλλά για όλες τις δραστηριότητες στο Διαδίκτυο (Lewis, 2016).

Το IoT δεν αλλάζει το σημαντικότερο πρόβλημα που αντιμετωπίζουμε σήμερα στη προστασία του δικτύου και των δεδομένων- εξαγωγή δεδομένων που οδηγούν στην κλοπή πνευματικής ιδιοκτησίας, επιχειρηματικών εμπιστευτικών πληροφοριών και προσωπικών πληροφοριών. Η κλοπή δεδομένων είναι μικρότερο πρόβλημα για το IoT. Οι περισσότερες συσκευές IoT δεν αποθηκεύουν πνευματικά ή επιχειρηματικά εμπιστευτικά δεδομένα.

Οι συσκευές IoT θα δημιουργήσουν ροή νέων δεδομένων σχετιζόμενων με τη προσωπική συμπεριφορά. Η εισαγωγή των IoT τεχνολογιών αποτελεί μεταβατική στιγμή για την προστασία της ιδιωτικής ζωής. Οι Αμερικανοί εμπορεύονται την ιδιωτική ζωή για εκρηκτική ανάπτυξη στις υπηρεσίες Διαδικτύου. Οι Ευρωπαίοι έκαναν ένα διαφορετικό εμπόριο - διατήρησαν την ιδιωτική ζωή του 1980 και κέρδισαν μια οικονομία του Διαδικτύου το 1980 σε αντάλλαγμα. Οι Αμερικανοί καταναλωτές έχουν πολύ λίγο έλεγχο των προσωπικών τους δεδομένων σήμερα, πολύ λιγότερο από ό, τι πριν από την εμπορία του Διαδικτύου. Το επιχειρηματικό μοντέλο του Διαδικτύου είναι η εξαγωγή προσωπικών δεδομένων, η αντιστοίχιση με περισσότερα προσωπικά δεδομένα, η συγκέντρωσή τους και στη συνέχεια η χρήση τους για εμπορικούς σκοπούς. Οι καταναλωτές το αποδέχονται σε ένα σιωπηρό εμπόριο υπηρεσιών - το Διαδίκτυο άλλαξε τις προτιμήσεις και τη συμπεριφορά τους. Το IoT θα καταστήσει ευκολότερη τη δημιουργία, τη συλλογή και την αποθήκευση αυτών των προσωπικών δεδομένων.

Οι εταιρείες θα συλλέγουν δεδομένα από συσκευές IoT για τη βελτίωση των προϊόντων και των υπηρεσιών και τη δημιουργία επιπλέον εσόδων. Αν και το IoT θα δημιουργήσει νέα δεδομένα σε ποσότητα, μεγάλο μέρος αυτών των δεδομένων θα έχει συχνά μικρή αξία (πίεση ελαστικών ή η μέση θερμοκρασία σε ψυγείο, για παράδειγμα), αλλά ακόμη και

ασήμαντα δεδομένα μπορεί να είναι χρήσιμα όταν συγκεντρώνονται για αναλυτικούς σκοπούς ή σε σχέση με άλλα δεδομένα. Σε γενικές γραμμές, ωστόσο, τα περισσότερα δεδομένα IoT, ακόμη και όταν συγκεντρωθούν και συσχετιστούν, θα δημιουργήσουν μικρό κίνδυνο για την ιδιωτική ζωή ή την ασφάλεια.

Ο αδύναμος έλεγχος ταυτότητας αποτελεί σημαντικό πρόβλημα για την ασφάλεια στον κυβερνοχώρο και μέχρι στιγμής τόσο η συμπεριφορά των χρηστών όσο και οι υπάρχουσες τεχνολογίες σήμαιναν ότι δεν είναι εύκολο να διορθωθεί. Είναι εύκολο να παραβιαστούν ταυτότητες ή να ληφθούν παράνομα, διαπιστευτήρια που επιτρέπουν σε έναν εισβολέα να πάρει τον έλεγχο ενός δικτύου ή μιας συσκευής. Ο έλεγχος ταυτότητας προσδιορίζει εάν μια εντολή είναι νόμιμη ή όχι (γενικά αναφέρεται ως άδεια). Ο έλεγχος ταυτότητας στο διαδίκτυο είναι αδύναμος επειδή η επιθυμία για ευκολία και αξιοπιστία τόσο από τους καταναλωτές όσο και από τις εταιρείες έχει περιορίσει τη χρήση ισχυρών τεχνολογιών ελέγχου ταυτότητας. Οι άνθρωποι θέλουν γρήγορη πρόσβαση, όχι μια περίπλοκη διαδικασία. Αυτός είναι ο λόγος για τον οποίο εξακολουθούμε να χρησιμοποιούμε κωδικούς πρόσβασης, οι οποίοι σε πολλές περιπτώσεις μπορούν να "σπάσουν" σε δευτερόλεπτα. Οι ίδιες προτιμήσεις για ευκολία και αξιοπιστία θα ισχύουν και για συσκευές IoT.

Αυτό που δεν λειτουργεί για τους ανθρώπους δεν θα λειτουργήσει και για το IoT. Στο IoT, μια συσκευή θα λάβει κακόβουλο κώδικα που προσποιείται ότι είναι μια ενημερωμένη έκδοση ή μια τροποποίηση και την αποδέχεται σα να προέρχεται από μια νόμιμη ή αξιόπιστη πηγή. Ωστόσο, οι ισχυρές τεχνολογίες ελέγχου ταυτότητας δεν σχεδιάστηκαν για τους απλούς υπολογιστές με περιορισμένη μνήμη και ισχύ επεξεργασίας που θα χρησιμοποιούν πολλές συσκευές IoT. Οι πρώτες γενιές συσκευών του IoT θα συνεχίσουν να βασίζονται σε ξεπερασμένες τεχνολογίες ελέγχου ταυτότητας και έτσι θα είναι ευάλωτες.

Οι Αμερικανοί μπόρεσαν να αγοράσουν ισχυρά προϊόντα κρυπτογράφησης για περισσότερο από μια δεκαετία, αλλά λίγοι τα χρησιμοποιούν. Αυτοί που τα χρησιμοποιούν έχουν προβλήματα εφαρμογής και ορισμένα προϊόντα κρυπτογράφησης έχουν βασικά ελαττώματα τα οποία μπορούν εύκολα να γίνουν αντικείμενο εκμετάλευσης. Η κρυπτογράφηση λειτουργεί καλύτερα όταν παρέχεται κεντρικά από έναν πάροχο υπηρεσιών, όπως όταν η Apple ή το Gmail κρυπτογραφούν τα μηνύματά σας παρά από τη προσπάθεια του ατόμου να το κάνει μεμονωμένα.

Η κρυπτογράφηση αλλάζει το κείμενο, το οποίο μπορεί να διαβάσει κανείς, σε ένα πλήθος γραμμάτων και συμβόλων. Η ισχυρή κρυπτογράφηση απαιτεί πρόσθετους υπολογιστικούς πόρους (συχνά σε περιορισμένη προσφορά σε συσκευές IoT) και έναν τρόπο διαχείρισης των

κρυπτογραφικών κλειδιών που χρησιμοποιούνται για την κρυπτογράφηση και αποκρυπτογράφηση της κίνησης από και προς τις συσκευές IoT (το κλειδί μπορεί να είναι μια φράση ή ένα διακριτικό που μετατρέπει κρυπτογραφημένα μηνύματα σε απλό κείμενο και αντίστροφα). Τα προγράμματα κρυπτογράφησης είναι επίσης δύσκολο να γραφτούν. Το IoT θέτει ιδιαίτερες προκλήσεις στην κρυπτογράφηση, καθώς πολλές συσκευές θα είναι απλές, κινητές και θα βασίζονται στην ασύρματη συνδεσιμότητα (η οποία είναι πιο εύκολη στην παρακολούθηση). Αν το IoT ακολουθεί το πρότυπο του ανθρώπινου Διαδικτύου, οι άνθρωποι δεν θα καταβάλουν ιδιαίτερη προσπάθεια για να χρησιμοποιήσουν την κρυπτογράφηση και οι συσκευές δεν θα σχεδιαστούν για να είναι ασφαλείς.

Ορισμένες λειτουργίες του IoT (αλλά όχι όλες) θα απαιτούν την κρυπτογράφηση των δεδομένων και των εντολών για ασφάλεια. Οι συμβατικές λύσεις κρυπτογράφησης περιλαμβάνουν υποδομές δημόσιου κλειδιού (PKI) και ασφαλή επίπεδα μεταφοράς (όπως SSL ή TLS, που συχνά ορίζονται από το HTTPS). Το PKI είναι μια μέθοδος για την ασφαλή ανταλλαγή κλειδιών κρυπτογράφησης, μια μέθοδος διαχείρισης κλειδιών που επιτρέπει σε ξένους να ανταλλάσσουν κλειδιά για κωδικοποίηση και αποκωδικοποίηση. Μεγάλες βιομηχανικές συσκευές IoT μπορούν να χρησιμοποιούν υπάρχοντα προϊόντα κρυπτογράφησης, αλλά απλές συσκευές μπορεί να απαιτούν τη δημιουργία ελαφριάς κρυπτογράφησης που απαιτεί λιγότερη μνήμη και ισχύ επεξεργασίας.

Το SSL είναι μια ευρέως αναπτυγμένη τεχνολογία κρυπτογράφησης που χρησιμοποιείται για την προστασία των ιστοτόπων. Το SSL δεν είναι άτρωτο, αλλά παρέχει επαρκές επίπεδο ασφάλειας για πολλές καταναλωτικές και εμπορικές δραστηριότητες. Το TLS είναι μια βελτιωμένη έκδοση του SSL. Το SSL και το TLS μπορούν να παρέχουν ασφαλή έλεγχο ταυτότητας και οι τεχνολογίες ελέγχου ταυτότητας είναι πιθανό να βελτιωθούν ταχύτερα από την επερχόμενη κρυπτογράφηση IoT. Αυτό υποδηλώνει ότι μια καλή στρατηγική για τις απαιτήσεις IoT θα ήταν να επικεντρωθεί πρώτα στην ενίσχυση της αυθεντικότητας και της έγκρισης για το διαδίκτυο. Τα επόμενα χρόνια, νέες τεχνολογίες πιστοποίησης θα διατίθενται στην αγορά. Θα χρησιμοποιήσουν διάφορους συνδυασμούς έξυπνων τηλεφώνων, αναλύσεις δεδομένων που βασίζονται σε σύννεφο, μοντέλα συμπεριφοράς και βιομετρικά στοιχεία για την ασφαλή αναγνώριση αυτών των IoT συσκευών πρόσβασης και την επιδίωξη έκδοσης εντολών.

Η κρυπτογράφηση δεδομένων, η πρόσβαση και οι λειτουργίες ελέγχου αυξάνουν την ασφάλεια, αλλά αυξάνουν το κόστος. Η κρυπτογράφηση απαιτεί πρόσθετους υπολογιστικούς πόρους (συχνά σε περιορισμένη προσφορά σε συσκευές IoT). Απαιτεί επίσης "διαχείριση κλειδιών", έναν τρόπο διαχείρισης των κρυπτογραφικών κλειδιών που

χρησιμοποιούνται για την κρυπτογράφηση και την αποκρυπτογράφηση της κυκλοφορίας. Η διαχείριση των κλειδιών μπορεί να είναι δύσκολη και δαπανηρή, ειδικά όταν γίνεται σε κλίμακα. Η κρυπτογράφηση επί της πλατφόρμας μπορεί να είναι ελκυστική για τους σχεδιαστές συσκευών IoT, διότι προσθέτει κόστος και πολυπλοκότητα. Αυτό ισχύει ιδιαίτερα για τις συσκευές καταναλωτών, οι οποίες είναι πιο πιθανό να έχουν περιορισμένη υπολογιστική ισχύ και μνήμη. Οι βιομηχανικές εφαρμογές του IoT (οι οποίες θα είναι λιγότερες σε σχέση με τις συσκευές των καταναλωτών αλλά θα παράγουν περισσότερη αξία για την οικονομία) ενδέχεται να μην αντιμετωπίσουν το ίδιο περιορισμό, αφού θα είναι μεγάλα μηχανήματα. Η κρυπτογράφηση στην τελική συσκευή είναι ακατάλληλη και αναποτελεσματική. Η κρυπτογράφηση του IoT πιθανόν να απαιτεί την ανάπτυξη προγραμμάτων κρυπτογράφησης με λιγότερη υπολογιστική ένταση, αλλά θα απαιτηθεί περαιτέρω έρευνα και ανάπτυξη για την εύκολη και ασφαλή ανάπτυξη της κρυπτογράφησης του IoT. Αυτός είναι ένας τομέας όπου διαδικασίες τυποποίησης, ίσως υπό την ηγεσία του Εθνικού Ινστιτούτου Προτύπων και Τεχνολογίας (NIST), εάν είναι απαραίτητο, θα μπορούσαν να αναπτύξουν απαιτήσεις για συσκευές IoT κατάλληλες για τη λειτουργία και το κόστος τους.

Η κρυπτογράφηση IoT πιθανόν να απαιτεί την ανάπτυξη προγραμμάτων κρυπτογράφησης με λιγότερη υπολογιστική ένταση και το σχεδιασμό δικτύων IoT ώστε να εκτελούνται ορισμένες από τις εργασίες κρυπτογράφησης εκτός συσκευής, αλλά απαιτείται περαιτέρω έρευνα και ανάπτυξη για την εύκολη και ασφαλή ανάπτυξη της κρυπτογράφησης του IoT. Οι δυσκολίες κρυπτογράφησης δεδομένων και λειτουργιών θα αποτελέσουν εμπόδιο στην αγορά του IoT και μια γενική απαίτηση όλες οι συσκευές IoT να χρησιμοποιούν ισχυρή κρυπτογράφηση δεν θα έχει νόημα για όλες τις συσκευές και τις λειτουργίες IoT και πρέπει να λαμβάνεται υπόψη η αξία και η ευαισθησία των δεδομένων ή των λειτουργιών.

### Α.4.4. Διαχείριση του IoT κινδύνου

Το IoT είναι νέο, αλλά το ίδιο ισχύει και για το Διαδίκτυο. Το Διαδίκτυο εμπορευματοποιήθηκε μόλις πριν από 20 χρόνια. Λιγότερο από 40 εκατομμύρια άνθρωποι το χρησιμοποιούσαν τότε. Σήμερα υπάρχουν πάνω από 3 δισεκατομμύρια χρήστες Διαδικτύου και περισσότερες από 9 δισεκατομμύρια συνδεδεμένες συσκευές. Ένα πράγμα που έχουμε μάθει για το Διαδίκτυο τα τελευταία 20 χρόνια είναι ότι δημιουργεί τόσο οφέλη όσο και κινδύνους και ότι τα οφέλη αντισταθμίζουν τους κινδύνους. Το ίδιο μάθημα ισχύει για την ασφάλεια του Διαδικτύου των πραγμάτων.

Μεγάλο μέρος της συζήτησης για την ασφάλεια του IoT εστιάζεται στην ευπάθεια των συσκευών και στην ανάγκη να σκληρυνθούν οι συσκευές IoT. Υπάρχουν όρια στην αξία αυτής της στρατηγικής. Είναι πιο χρήσιμο να σκεφτόμαστε την ασφάλεια του IoT με διάφορους τρόπους και να εξετάζουμε το περιβάλλον απειλής, τον βαθμό αυτονομίας και την αρχιτεκτονική των IoT δικτύων ως βασικά στοιχεία κάθε στρατηγικής διαχείρισης των κινδύνων του IoT.

Το θέμα ευπάθειας δεν αποτελεί καλό προγνωστικό παράγοντα κινδύνου. Απλώς και μόνο επειδή οι συσκευές είναι ευάλωτες, δεν σημαίνει ότι θα έχουν πειραχτεί ή ότι ένα χακάρισμα θα έχει επιζήμιες συνέπειες. Μέχρι στιγμής, ο IoT κίνδυνος παραμένει σε μεγάλο βαθμό υποθετικός. Αυτό μπορεί να αλλάξει καθώς αυξάνεται ο αριθμός και το είδος των συσκευών IoT, αλλά πρέπει να σταθμιστεί η αύξηση του κινδύνου σε σχέση με την αύξηση της ασφάλειας και της αποδοτικότητας (Lewis, 2016).

Με το πρώτο Διαδίκτυο, υπήρξε ελάχιστη ή καθόλου αμφισβήτηση της ιδέας της ψηφιοποίησης των επιχειρηματικών πρακτικών ώστε να αποκομιστούν τα οφέλη από το χαμηλότερο κόστος και την καλύτερη απόδοση. Ωστόσο, οι δημόσιες αντιλήψεις για τον κίνδυνο μεταβάλλονται, με γνώμονα την άκρως δημοσιοποιημένη αναγνώριση του αριθμού και του εύρους των κακόβουλων επιθέσεων στον κυβερνοχώρο. Αυτές οι μεταβαλλόμενες αντιλήψεις δημιουργούν δυνάμεις που θα αναδιαμορφώσουν τις ιδιωτικές αποφάσεις και τη δημόσια πολιτική για το IoT.

#### Α.4.4.1. Επιχειρηματικές αποφάσεις και κυβερνητική δράση για τη διαχείριση κινδύνου του IoT

Όσον αφορά το IoT, μπορούμε να παραπλανηθούμε εάν υποθέσουμε ότι το IoT είναι ένας κοινός παρονομαστής που ισχύει εξίσου σε πολύ διαφορετικές βιομηχανίες και προϊόντα. Είναι ένας όρος "portmanteau", ένας απλός τρόπος για να περιγράψει κάποιος ένα πολύπλοκο ζήτημα, αλλά αυτή η απλότητα είναι κακός οδηγός για την πολιτική. Η διαχείριση των κινδύνων απαιτεί δράση σε πολλά επίπεδα από πολλούς διαφορετικούς παράγοντες, αλλά μερικές βασικές αρχές βασισμένες στα δεδομένα μπορούν να βοηθήσουν στη λήψη αποφάσεων. Οι κίνδυνοι που δημιουργούνται από τη χρήση συσκευών διαδικτύου μπορούν να αντιμετωπιστούν και να μειωθούν, αλλά αυτό θα απαιτήσει κάποιο συνδυασμό έρευνας, κανόνων και κινήτρων.

Τα ίδια προβλήματα που μας εμποδίζουν να καταστήσουμε ασφαλέστερο τον κυβερνοχώρο θα επιβραδύνουν επίσης την πρόοδο στην ασφάλεια του IoT: τεχνολογική αβεβαιότητα,

περιορισμένη διεθνής συνεργασία, έλλειψη κινήτρων για βελτίωση, περιορισμένη ρυθμιστική αρχή για την ασφάλεια, αδυναμία ηλεκτρονικής ταυτότητας και επιχειρηματικό μοντέλο Internet βασισμένο στην εκμετάλλευση των προσωπικών δεδομένων. Ταυτόχρονα, οι ίδιες προσεγγίσεις που χρησιμοποιούμε για να καταστήσουμε τον κυβερνοχώρο πιο ασφαλή μπορούν να χρησιμοποιηθούν για τη διαχείριση και τη μείωση των κινδύνων που δημιουργούνται από τη χρήση συσκευών IoT: έρευνα, κίνητρα και ρύθμιση.

Εάν οι κυβερνήσεις, οι εταιρείες και οι καταναλωτές προσεγγίσουν το IoT με τον τρόπο με τον οποίο προσεγγίζουν το αρχικό, ανθρώπινο Διαδίκτυο, αυτό θα περιλαμβάνει την επέκταση των κανόνων που έχουμε τώρα για την ευθύνη, την ιδιωτικότητα και το κόστος στο Διαδίκτυο των πραγμάτων και στη συνέχεια τον εντοπισμό των σημείων όπου το υπάρχον νομικό πλαίσιο είναι ανεπαρκές, οδηγώντας είτε σε νέους νόμους και κανονισμούς, είτε σε μια προσέγγιση «κοινού δικαίου» που επιτρέπει στα δικαστήρια να επιλύσουν την ευθύνη. Αυτή η διαδικασία "επέκτασης" έχει σημαντικές επιπτώσεις σε θέματα όπως προστασία της ιδιωτικής ζωής, ασφάλεια και ταυτότητα, καθώς ορισμένοι από τους ισχύοντες νόμους και πολιτικές που δημιουργήθηκαν για τον φυσικό κόσμο αποδείχθηκαν ανεπαρκείς για το ανθρώπινο Διαδίκτυο και απαιτούσαν την ανάπτυξη νέων νόμων και πολιτικών.

Πού και πώς θα χρησιμοποιηθεί μια συσκευή IoT θα είναι μια επιχειρηματική απόφαση που θα ισορροπήσει την καλύτερη επίδοση ενάντια στις αυξήσεις του κινδύνου και του κόστους. Μια καλή πολιτική μπορεί να βοηθήσει να γίνουν αυτές οι επιχειρηματικές αποφάσεις πιο εύκολες. Η πολιτική και ο νόμος μπορούν να διευκρινίσουν τον τρόπο με τον οποίο οι εταιρείες και οι καταναλωτές πρέπει να αντιμετωπίζουν τον κίνδυνο και την ευθύνη και πού πρέπει να επενδύσουν.

Μπορούμε να βελτιώσουμε τη λήψη αποφάσεων σχετικά με το IoT εάν χρησιμοποιήσουμε τρεις μετρήσεις για την αξιολόγηση του κινδύνου: την αξία των δεδομένων, την κρισιμότητα μιας λειτουργίας και την κλιμάκωση της αποτυχίας. Αυτά βοηθούν τους υπεύθυνους χάραξης πολιτικής, τους ρυθμιστές και τους νομοθέτες να εντοπίζουν τις περιπτώσεις στις οποίες η κυβερνητική παρέμβαση είναι απαραίτητη για την ασφάλεια του IoT και όπου δεν χρειάζονται τέτοιες ενέργειες. Η απενεργοποίηση του ψυγείου ή του κλιματισμού είναι ενοχλητική. Η απενεργοποίηση μιας μηχανής αεριωθουμένων κατά την πτήση θα ήταν απειλητική για τη ζωή. Οι συσκευές IoT που παρέχουν ευαίσθητες λειτουργίες απαιτούν υψηλότερο βαθμό ελέγχου και προσπάθειας για ασφάλεια. Το IoT δημιουργεί κίνδυνο όταν η λειτουργία που εκτελεί είναι ζωτικής σημασίας για τη ζωή και την ασφάλεια, όταν τα δεδομένα που παράγει είναι πραγματικά ευαίσθητα και όταν τα αποτελέσματα των παρεμβολών είναι επεκτάσιμα. Οι συσκευές που κάνουν αυτά τα πράγματα θα πρέπει να

τηρούνται σε υψηλότερα πρότυπα μέσω κυβερνητικής δράσης. Αυτές που δεν μπορούν να αφεθούν στις δυνάμεις της αγοράς και στη δικαστική δράση για να διορθωθούν.

Οι αποφάσεις σχετικά με την αυτονομία θα αποτελέσουν καθοριστικό παράγοντα για την ασφάλεια των συσκευών IoT. Εάν οι φυσικοί χειριστές μπορούν να παρεμβαίνουν σε μια λειτουργία IoT, αυτό θα μειώσει τον κίνδυνο. Αυτό μειώνει επίσης τα οφέλη, επομένως οι κοινωνίες θα πρέπει να αποφασίσουν πού και σε ποιο βαθμό η αυτονομία της συσκευής είναι αποδεκτή και πού να διατηρήσει μια ικανότητα για ανθρώπινη παρέμβαση. Χρησιμοποιώντας τις μετρήσεις της ευαισθησίας της λειτουργίας και της επεκτασιμότητας του αποτελέσματος, μπορούμε να προσδιορίσουμε ποιες συσκευές IoT απαιτούν όρια ή περιορισμούς στην αυτόνομη λειτουργία.

Η επεκτασιμότητα της αποτυχίας συμβάλλει στον προσδιορισμό του κινδύνου. Για να προχωρήσει πέρα από μια φάρσα ή κακούργημα, ένας χάκερ πρέπει να επιτύχει μαζική επίδραση. Αυτό σημαίνει ταυτόχρονα να χακάρει εκατοντάδες ή χιλιάδες συσκευές-μια απίθανη προοπτική-ή να βρεί μια συσκευή IoT που ελέγχει πο0λλές άλλες. Αυτές οι συσκευές "εντολής" χρειάζονται υψηλότερο βαθμό ελέγχου και προσοχής στην ασφάλεια, άλλες όχι. Ο αρμόδιος κυβερνητικός φορέας, θα πρέπει να λάβει μέτρα για να εντοπίσει μεμονωμένα σημεία αποτυχίας για την κρίσιμη υποδομή και στη συνέχεια να προσδιορίσει τις συνθήκες "τέλειας θύελλας" για το IoT, αυτές τις απίθανες περιστάσεις όπου κάποιος συνδυασμός αποτυχιών του IoT (είτε κακόβουλες είτε φυσικές) θα μπορούσε να έχει καταστροφικές συνέπειες. Οι επενδύσεις στην έρευνα σχετικά με τα ελαφριά συστήματα κρυπτογράφησης και επαλήθευσης ταυτότητας που είναι κατάλληλα για το IoT θα ενισχύσουν τις ενέργειες του ιδιωτικού τομέα για την παραγωγή προϊόντων λογισμικού για την ασφάλεια του IoT (Lewis, 2016).

Οι συσκευές IoT θα γίνουν πιο ασφαλείς με την πάροδο του χρόνου μέσω μιας διαδικασίας αυξητικής καινοτομίας, αλλά μπορούμε να επιταχύνουμε αυτή τη διαδικασία με την έρευνα, τους κανόνες και τα κίνητρα, ιδίως με την αύξηση της χρηματοδότησης της E & A για οικονομικά αποδοτικούς τρόπους για μεγαλύτερη ασφάλεια των συσκευών IoT. Ορισμένα κίνητρα θα είναι το αποτέλεσμα της επίλυσης διαφορών. Εάν οι συσκευές IoT αποτύχουν, οι ενάγοντες θα επιδιώξουν την αποκατάσταση και τα δικαστήρια θα αναθέσουν την ευθύνη. Ο προσεκτικά σχεδιασμένος κανονισμός που αποφεύγει την τεχνολογική συνταγογράφηση μπορεί να επιταχύνει τη βελτίωση και οι υπάρχουσες εντολές για την ασφάλεια των μεταφορών, της υγείας και των καταναλωτικών προϊόντων μπορούν να αναβαθμιστούν για να καλύψουν το ΊoT.

Είναι προς το δημόσιο συμφέρον να μειωθεί η συχνότητα των ατυχημάτων που μπορούν να προληφθούν και να μειωθεί ο κίνδυνος, αλλά αυτό δεν απαιτεί τέλεια ασφάλεια IoT. Η προληπτική δράση που βασίζεται σε ανεκδοτολογικές αποδείξεις ή υποθετικές καταστάσεις θα επιβραδύνει την εφευρετικότητα και θα εμποδίσει τις βελτιώσεις που απαιτούνται για την καλύτερη ασφάλεια. Δεν γνωρίζουμε ποιες διαδρομές θα πάρει η καινοτομία του IoT ή πώς θα το χρησιμοποιήσουν οι καταναλωτές, οπότε πρέπει να αφήσουμε περιθώρια για πειραματισμό και αειφορία. Τίποτα που χρησιμοποιούμε δεν έρχεται με τέλεια ασφάλεια. Καθώς οι τεχνολογίες ωριμάζουν, η καινοτομία, η ρύθμιση και οι δυνάμεις της αγοράς μειώνουν τον κίνδυνο, αλλά ο κίνδυνος εξακολουθεί να υφίσταται ακόμη και στις ώριμες τεχνολογίες και ζούμε με αυτό, εκτιμώντας ότι τα οφέλη που κερδίζουμε είναι μεγαλύτερα από την πιθανότητα κάτι κακό να συμβεί.

Αυτό είναι πολύ παρόμοιο με τις αποφάσεις που αντιμετωπίσαμε στο πρώτο Διαδίκτυο όταν εμπορευόταν: επιλέγουμε να αναπτύξουμε γρήγορα λιγότερο ασφαλή προϊόντα για να κερδίσουμε το οικονομικό τους πλεονέκτημα ή να επιβραδύνουμε την ανάπτυξη (και την καινοτομία) για να περιμένουμε την καλύτερη ασφάλεια. Στην περίπτωση του Διαδικτύου, η απόφαση ήταν να δεχτούμε τον κίνδυνο για να αποκομίσουμε τα οικονομικά οφέλη του Διαδικτύου. Αυτή ήταν η σωστή απόφαση και πρέπει να λάβουμε την ίδια απόφαση για το IoT.

Η εναλλακτική λύση θα ήταν να επιβληθούν απαιτήσεις ασφάλειας ή προστασίας προσωπικών δεδομένων για συσκευές IoT. Αυτό είναι πιο εύκολο να ειπωθεί από το να γίνει πράξη, εν μέρει επειδή ακόμη και αν μια συσκευή IoT γίνει πιο ασφαλής, θα εξακολουθεί να συνδέεται με μεγάλα ασύμμετρα δίκτυα. Η ασφάλεια του IoT αντιμετωπίζει τα ίδια προβλήματα με την ασφάλεια του κυβερνοχώρου γενικά. Η έκταση των τρωτών σημείων του λογισμικού είναι τέτοια που αν κάποιος θέλει να διεισδύσει και είναι επίμονος, πιθανότατα θα πετύχει.

Παρ 'όλα αυτά, ο καθένας χρησιμοποιεί ηλεκτρονικούς υπολογιστές και το Διαδίκτυο. Αυτό αντικατοπτρίζει τις αποφάσεις των διαχειριστών, των επενδυτών και των καταναλωτών σχετικά με τον κίνδυνο. Το IoT αυξάνει τον αριθμό των συσκευών που μπορούν να χακαριστούν, αλλά οι συνέπειες αυτού εξαρτώνται σε μεγάλο βαθμό από την κρισιμότητα της λειτουργίας, την επεκτασιμότητα και την ευαισθησία των δεδομένων.

Η εισαγωγή συσκευών IoT θα είναι σταδιακή και οι βελτιώσεις θα είναι αυξητικές. Αυτό σημαίνει ότι ο κίνδυνος θα είναι μεγαλύτερος για την πρώτη γενιά συσκευών IoT. Ο φόβος ότι έχουμε λίγα μόνο χρονικά διαστήματα για να διασφαλίσουμε ότι το IoT υιοθετείται κατά

τρόπο που να ελαχιστοποιεί τον κίνδυνο είναι άστοχος και οι προβλέψεις ότι θα υπάρξουν δισεκατομμύρια περισσότερες συσκευές IoT τα επόμενα χρόνια δημιουργούν μια εσφαλμένη αντίληψη. Η μέση ηλικία ενός αυτοκινήτου, για παράδειγμα, είναι 12 χρόνια. Τα ψυγεία τείνουν να αντικαθίστανται κάθε 15 χρόνια. Αυτό σημαίνει ότι 10 χρόνια από τώρα, περισσότερα από τα μισά αυτοκίνητα και τα ψυγεία θα είναι ακόμα "χαζά" και όχι σε αυξημένο κίνδυνο. Σημαίνει επίσης ότι οι άνθρωποι που αντικαθιστούν τα ψυγεία τους 10 χρόνια από τώρα θα αγοράζουν βελτιωμένες και πιο ασφαλείς εκδόσεις των πρώτων "έξυπνων" συσκευών απλώς και μόνο λόγω της εμπειρίας και της καινοτομίας.

Οι κρίσιμες υποδομές γενικά έχουν ακόμη μεγαλύτερους κύκλους «ανανέωσης», ιδίως για τα μεγάλα κεφαλαιουχικά αγαθά. Αυτός ο μακρύς κύκλος ανανέωσης καθιστά ελάχιστη την αύξηση του κινδύνου. Πρέπει να ασχοληθούμε με την επιτάχυνση της ταχείας και ευρείας υιοθέτησης του IoT - για παράδειγμα στα ευφυή δίκτυα - όπου ο ρυθμός υιοθεσίας υπερβαίνει το ρυθμό βελτίωσης.

### Α.4.4.2. Διαχείριση κινδύνου για την προστασία δεδομένων και την ιδιωτικότητα στο IoT

Η ασφάλεια του IoT και η ασφάλεια στον κυβερνοχώρο γενικά, θα ωφεληθούν από έναν επαναπροσανατολισμό στη σκέψη μας για την ιδιωτικότητα και την ασφάλεια στον κυβερνοχώρο. Μεγάλο μέρος της προσπάθειας των τελευταίων 20 ετών έχει επικεντρωθεί στα δίκτυα ασφαλείας από την εισβολή και τη μείωση των τρωτών σημείων. Χωρίς να φανεί υπερβολικά απαισιόδοξο, αυτές είναι αδιέξοδες ενέργειες. Οι αποφασισμένοι εισβολείς θα επιτύχουν συνήθως την πρόσβαση σε ένα δίκτυο, ιδιαίτερα εάν έχουν επαρκείς πόρους. Το λογισμικό έχει γίνει τόσο περίπλοκο, με πολλά προϊόντα που βασίζονται σε εκατομμύρια γραμμές κώδικα, όπου είναι αδύνατο να αποφευχθούν ή να βρεθούν όλα τα σφάλματα. Ο επαναπροσανατολισμός της προσέγγισής στην ασφάλεια του κυβερνοχώρου θα επιδιώξει να εξασφαλίσει δεδομένα και όχι δίκτυα και να εξασφαλίσει τη συνεχή λειτουργία κρίσιμων λειτουργιών ακόμη και σε υποβαθμισμένο περιβάλλον.

Η προστασία δεδομένων και η ιδιωτική ζωή παρουσιάζουν παρόμοιες επιλογές. Μια προσέγγιση ενιαίου μεγέθους για την ασφάλεια των δεδομένων που παράγονται από μια συσκευή IoT δημιουργεί περίεργα αποτελέσματα και περιττά εμπόδια. Για να χρησιμοποιήσουμε ένα παράδειγμα από έναν κατασκευαστή κινητήρων αεροσκαφών, οι μηχανές αεροσκαφών αναφέρουν τώρα αυτόματα στα κέντρα συντήρησης την κατάσταση τους. Ορισμένες αναφορές περιλαμβάνουν το όνομα του μηχανικού σε ένα κέντρο

συντήρησης. Οι κανόνες προστασίας δεδομένων που αναπτύσσονται για πληροφορίες προσωπικής ταυτοποίησης (PII) δεν λειτουργούν για το Iot. Απλά επειδή τα δεδομένα του IoT περιλαμβάνουν PII δεν το καθιστούν πολύτιμο ή ευαίσθητο. Οι κανόνες προστασίας προσωπικών δεδομένων που έχουν αναπτυχθεί για συναλλαγές στο διαδίκτυο απαιτούν προσαρμογή για έναν κόσμο IoT (Lewis, 2016).

Το IoT θα διευρύνει σημαντικά το ποσό των δεδομένων που μεταφέρονται και αποθηκεύονται στα εθνικά σύνορα, δημιουργώντας μια σειρά προκλήσεων για την προστασία της ιδιωτικής ζωής. Το Iot θα περιπλέξει μόνο τα ήδη πολύπλοκα προβλήματα του εντοπισμού των δεδομένων και των προσπαθειών για περιορισμό των ροών δεδομένων πέρα από τα σύνορα, αλλά (όπως συμβαίνει γενικά με αυτούς τους κανόνες) θα δημιουργήσουν εμπόδια για τους κατασκευαστές που εξυπηρετούν μια παγκόσμια αγορά. Τα περισσότερα από αυτά τα δεδομένα θα έχουν μικρή αξία και δεν επηρεάζουν την ιδιωτικότητα. Οι κανόνες για τον περιορισμό της χρήσης δεδομένων από συσκευές IoT πρέπει να λαμβάνουν υπόψη την αξία των πληροφοριών. Ένας Γερμανός κατασκευαστής αυτοκινήτων μπορεί να συλλέξει δεδομένα από ξένους πελάτες σχετικά με την πίεση των ελαστικών τους από οθόνες επί του οχήματος και να το μεταπωλήσει, αλλά η βλάβη στην ιδιωτική ζωή είναι ανύπαρκτη. Η αξία αυτών των δεδομένων IoT, ακόμη και όταν συγκεντρωθούν, θα είναι πολύ χαμηλή. Οι κανονισμοί και οι συμφωνίες θα πρέπει να αντικατοπτρίζουν αυτό το θέμα και να ταξινομούν τα δεδομένα IoT με βάση την αξία και την ευαισθησία της ιδιωτικής ζωής (π.χ. προσωπικά δεδομένα για την υγεία σε αντίθεση με τα δεδομένα συσκευών).

Η προστασία δεδομένων δημιουργεί αναπόφευκτες εντάσεις μεταξύ της δημόσιας πολιτικής και των επιχειρηματικών αποφάσεων. Η πρωταρχική ένταση είναι ο πειρασμός της δημόσιας πολιτικής να επιβάλλει γενικές λύσεις για την ασφάλεια ή την προστασία της ιδιωτικής ζωής που δεν αντικατοπτρίζουν την αξία ή την ευαισθησία της λειτουργίας ή των δεδομένων. Τα περισσότερα δεδομένα του IoT δεν χρειάζονται αυστηρές διασφαλίσεις ιδιωτικότητας. Το Iot θα απαιτεί βαθμιαία κλίμακα προστασίας και μέτρων ασφαλείας που αντικατοπτρίζουν τον πραγματικό βαθμό κινδύνου, που καθορίζεται όχι μόνο από την πιθανή ευπάθεια, αλλά και από την αξία και την ευαισθησία τόσο των δεδομένων όσο και των λειτουργιών.

Τα δεδομένα που δημιουργούνται από συσκευές IoT θα πρέπει να αναλυθούν για να προσδιοριστεί πού χρειάζονται επιπλέον προστασίες όπως η κρυπτογράφηση (δεδομένου ότι η κρυπτογράφηση αυξάνει το κόστος και την πολυπλοκότητα των συσκευών) και που τα δεδομένα δεν απαιτούν ειδική επεξεργασία. Το να υποστηρίζουμε ότι όλα τα δεδομένα έχουν την ίδια αξία είναι απαρχαιωμένο και ανακριβές. Η διαφοροποίηση μεταξύ

σημαντικών και μη σημαντικών δεδομένων (μεμονωμένων και συγκεντρωτικών) και ο προσδιορισμός κρισιμότητας (όπως η ασφάλεια ζωής ή οι δυνητικές οικονομικές απώλειες) προσδιορίζει ποια συστήματα ενδοεπικοινωνίας είναι σημαντικά. Εάν χρησιμοποιήσουμε αυτές τις μετρήσεις, διαπιστώνουμε ότι η διακύμανση του IoT κινδύνου αυξάνει το ρίσκο για την ασφάλεια και την προστασία της ιδιωτικής ζωής σε απαράδεκτα επίπεδα σε μικρό μόνο αριθμό περιπτώσεων.

# Μέρος Β: Η σημασία του Internet of Things (IoT) στη Διαχείριση Έργων (Project Management)

## Β.1. Εισαγωγή

Η Διαχείριση Έργων (Project Management - PM) είναι μία από τις σημαντικότερες κατευθύνσεις στην επιστήμη της Διοίκησης και ωφελεί τις επιχειρήσεις μέσω της πραγματικής και λειτουργικής διαχείρισης των διαφόρων αλλαγών. Αυτό το επιτυγχάνει μέσω της συστηματικής προσέγγισης της εκκίνησης, του σχεδιασμού, της εκτέλεσης, της παρακολούθησης και του ελέγχου, της πραγματοποίησης σεναρίων ελέγχων και αποδοχής, και της τελικής παράδοσης του προϊόντος ή της υπηρεσίας στον πελάτη.

Τα παραπάνω αφορούν τη διαχείριση διαφόρων τύπων έργων με διάφορους παράγοντες όσον αφορά τις αλλαγές που απαιτούνται και την αβεβαιότητα που μπορεί να προκύψει (Sawyer, L., 2018). Καθώς η τεχνολογία έχει γίνει πλέον αναπόσπαστο μέρος της ζωής μας, σε αυτή την ενότητα εξετάζουμε τη σημασία του Διαδικτύου των Πραγμάτων (IoT) και τις συνέργειες που μπορούν να προκύψουν στην υλοποίηση της Διαχείρισης Έργων σε οργανισμούς που είναι έργο-κεντρικοί.

Η ενότητα αυτή εξετάζει επίσης τις προκλήσεις, τα εμπόδια και τα οφέλη του IoT σε συνέργεια με τις βασικές κατευθύνσεις στη Διαχείριση Έργων. Σε αυτό το πλαίσιο εξετάζεται και ο ρόλος του πιο κρίσιμου παράγονται κάθε οργανισμού ή επιχείρησης, που είναι οι άνθρωποι. Συνεπώς, εξετάζεται ο νέος ρόλος και σκοπός ενός διαχειριστή έργου και πώς αυτός επηρεάζεται από τις καινοτόμες προσπάθειες και συνέργειες που αναφέρθηκαν παραπάνω με βάση το IoT.

Οι οργανισμοί και το ευρύτερο επιχειρησιακό περιβάλλον έχουν σημειώσει σημαντικές αλλαγές τις τελευταίες δεκαετίες. Οι οργανισμοί απλώνονται από τοπικές μικρομεσαίες επιχειρήσεις σε οργανισμούς που ασχολούνται με έργα σε παγκόσμιο επίπεδο. Η Πληροφορική (IT) συνέβαλε στη μετάβαση στην ψηφιοποίηση και τον τρόπο με τον οποίο οδηγεί τις εξελίξεις στις παγκόσμιες αγορές τη σημερινή εποχή.

Ωστόσο, η επέκταση της υλοποίησης ενός έργου πέρα από γεωγραφικά σύνορα, η εφαρμογή στις παγκόσμιες αγορές και η παράλληλη υλοποίηση πολλαπλών έργων, είναι βασική οδηγοί για την συνέργεια μεταξύ βασικών αρχών Διαχείρισης Έργων (PM) και των τεχνολογιών Internet of Things (IoT). Ο συνδυασμός αυτός καλείται να αντιμετωπίσει τη πολυπλοκότητα που προκύπτει στα παραπάνω σύνθετα έργα και να υποστηρίξει την υλοποίηση τους σε όλη τη διάρκεια του κύκλου ζωής τους.

Από την έναρξη του έργου έως την παράδοση του έργου, εξασφαλίζεται μια ομαλή μετάβαση στα επιμέρους στάδια του κύκλου ζωής του έργου, ενώ είναι στρατηγικά ευθυγραμμισμένη με τα οράματα και τους στόχους του οργανισμού. Παρόλο που κάθε οργανισμός αντιπροσωπεύει ένα μοναδικό περιβάλλον και μία κουλτούρα, οι αρχές της Διοίκησης Έργων και οι κατευθυντήριες γραμμές που εφαρμόζουν οι αντίστοιχες μεθοδολογίες είναι επίσης μοναδικά προσαρμοσμένες. Σε οποιαδήποτε μορφή, οι αρχές της Διοίκησης Έργων αντιπροσωπεύουν ένα κεντρικό εργαλείο για την δημιουργία νέων καινοτομιών σε έναν οργανισμό (Morris P. et al, 2010).

Ως εκ τούτου, με την στρατηγική ανάθεση των προσαρμοσμένων μεθόδων Διοίκησης Έργων σε έναν οργανισμό, οι προκλήσεις και τα εμπόδια που παρουσιάζονται σε όλη τη διάρκεια του κύκλου ζωής του έργου θα παρεμβαίνουν από την ομάδα του έργου και θα ρυθμίζονται σύμφωνα με το σχέδιο του έργου. Στην πραγματικότητα, η αποτελεσματική εφαρμογή των αρχών PM αποφέρει ποιοτικές βελτιώσεις στα αποτελέσματα των επιχειρήσεων (Somasundaram, S. & Badiru, A.B., 1992).

Η παγκοσμιοποίηση διαδραματίζει κρίσιμο ρόλο στην αύξηση της πολυπλοκότητας των έργων. Ωστόσο, η εξέλιξη των τεχνολογιών πληροφορικής και διαδικτύου παρέχει νέες λύσεις, εργαλεία και υποστήριξη για την εφαρμογή των βασικών μεθόδων Διοίκησης Έργων από τους διαχειριστές μέσα στα μεταβαλλόμενα περιβάλλοντα. Παραδοσιακά, η διαχείριση του έργου χρησιμοποιήθηκε πάντοτε και στη διαδικασία διαχείρισης του χειρισμού ενός έργου σε χρόνο που βασίστηκε σε ένα μόνο τόπο (Evaristo. R. & Van Fenema, 1999) και ασχολήθηκε κυρίως με τη διαδικασία των εισροών / εκροών (Gorton I. et al, 1997).

Επίσης παρέχει ένα εργαλείο ζωτικής σημασίας και σημαντικής συνεργασίας για τους διαχειριστές του έργου και τους διάφορους ενδιαφερόμενους, τις ομάδες και τους φορείς που απασχολούνται στο πεδίο του έργου και κατόπιν κατά την παράδοση ή λειτουργία του παραγόμενου αποτελέσματος. Σημειώνεται επίσης, ότι μια κρίσιμη πτυχή του μεγάλου ποσοστού επιτυχίας του PM στα έργα είναι η ικανότητά του να συλλέγει δεδομένα, να τα αναλύει, να παρακολουθεί και να τα ελέγχει και στη συνέχεια να τα μεταδίδει μέσω συνεργατών που απασχολούνται σε διάφορα έργα και σε διαφορετικές τοποθεσίες (Jonsson N. et al , 2001).

Σύμφωνα με την τελευταία έκθεση των Ηνωμένων Εθνών (ΟΗΕ), μια καινούργια εποχή με βάση το πρότυπο της πανταχού παρουσίας έχει εξαπλωθεί και οι άνθρωποι θα γίνουν μέλη μειονοτήτων όταν αντιληφθούν την παραγωγή δεδομένων. Οι αλλαγές που επιφέρει η

τεχνολογία της πληροφορικής θα επιβαρυνθούν από εκείνες που δημιουργούνται από τη δικτύωση των καθημερινών αντικειμένων που είναι γνωστά ως IoT (INFSO D.4 Networked Enterprise & RFID INFSO G.2 Micro & Nanosystems).

Σήμερα, η πληροφόρηση και ο μεγάλος όγκος δεδομένων αντιπροσωπεύουν ένα επακόλουθο στοιχείο που ανήκουν σε μια εταιρία και παρέχουν ένα ανταγωνιστικό πλεονέκτημα έναντι των ανταγωνιστών της και μέσα στις συνεχώς μεταβαλλόμενες αγορές. Αυτή η κρισιμότητα παρέχει νέα παραδείγματα για τη χρήση δεδομένων και πληροφοριών που συλλέγονται από συσκευές IoT, παρέχοντας συλλογή και ανάλυση δεδομένων σε πραγματικό χρόνο (Real-Time Data - RTD) (Ghimire S et al, 2015).

## Β.2. Σύγχρονες προκλήσεις

Το Internet of Things θα μπορούσε να υποστηρίξει όλους τους ενδιαφερόμενους κατά τη διάρκεια του κύκλου ζωής ενός έργου, την επίλυση διαφόρων τεχνικών και επικοινωνιακών προβλημάτων, και την αύξηση του επιπέδου συνεργασίας μεταξύ των μερών. Το IoT δημιουργεί ευκαιρίες και με τη συνεχή ανάπτυξη της πληροφορικής τα όρια δεν έχουν καθοριστεί, ωστόσο με όλες τις δυνατότητες που πρέπει να προσφέρει η τεχνολογία IoT πρέπει να είναι ηθικός ο τρόπος συλλογής πληροφοριών και η αποθήκευση των δεδομένων με ασφάλεια (Weinberg et al, 2015).

Το Internet of Things αντιπροσωπεύει μια ανατρεπτική τεχνολογία: η δομή της είναι εξελικτική με απεριόριστες δυνατότητες. Επιτρέπει τον πλήρη έλεγχο των συνδεδεμένων με το διαδίκτυο συσκευών και αποτελεί μέρος του δικτύου. Παρά τα προβλήματα σχετικά με τον τρόπο με τον οποίο πρέπει να συνδεθούν τα αντικείμενα, τα σημαντικά ζητήματα που σχετίζονται με το "γιατί και πότε" τα αντικείμενα πρέπει να συνδεθούν μέσω των τεχνολογιών IoT και "ποιες" νέες αξίες που μπορούν να φέρουν για να ενισχύσουν τις υπάρχουσες υπηρεσίες και διαδικασίες των επιστημών και του περιβάλλοντος (McKinsey Global Institute., 2013).

Η διαχείριση του έργου απλώς υιοθετώντας την τεχνολογία του Διαδικτύου δεν θα μεταφραστεί σε όφελος για την επιχείρηση εκτός εάν χρησιμοποιούνται οι τεχνολογίες. Η χρήση της τεχνολογίας IoT αναφέρεται στον βαθμό διάχυσης του IoT στον οργανισμό και στο βαθμό στον οποίο ο οργανισμός απασχολεί, χρησιμοποιεί ή εφαρμόζει την τεχνολογία στις λειτουργίες του (Liu Z. et al, 2016).

Παρά τη σημαντική έρευνα σχετικά με την υλοποίηση τεχνολογιών πληροφορικής με επίκεντρο τον οργανισμό, εξακολουθεί να παραμένει ζήτημα για τους οργανισμούς. Η εφαρμογή της πληροφορικής είναι σύνθετη, χρονοβόρα και δαπανηρή και κάθε οργανισμός είναι διαφορετικός σε σχέση με τις αντίστοιχες διαδικασίες, τους ανθρώπους και τις λειτουργίες τους (Motiwalla, F. L. & Thompson, J., 2009).

Έτσι, ο βαθμός στον οποίο οι αποδεκτές θεωρίες εφαρμογής μπορούν να είναι χρήσιμες σε έναν οργανισμό που υιοθετεί μια τεχνολογία είναι περιορισμένος. Η υλοποίηση των τεχνολογιών IoT μπορεί να προσεγγιστεί ακόμη περισσότερο και δεν είναι μόνο πρόκληση για τον οργανισμό που την υιοθετεί, αλλά μπορεί να θεωρηθεί επίσης απειλητική για τις αλλαγές που μπορεί να επιφέρει και τη βιωσιμότητα του οργανισμού.

Για τους οργανισμούς είναι σαφές ότι οι τεχνολογίες IoT είναι απαραίτητες όχι μόνο για να διευκολύνουν ολοένα και πιο σύνθετες αλυσίδες εφοδιασμού αλλά και προκειμένου να είναι σε θέση να απευθύνονται στους πελάτες. Ωστόσο, η εφαρμογή του IoT είναι ιδιαίτερα δύσκολη, καθώς δεν είναι μόνο ένα σύστημα πληροφορικής που υλοποιείται, αλλά μια ευημερούσα και αναπτυσσόμενη ομάδα έξυπνων τεχνολογιών που παράγουν ένα τεράστιο όγκο δεδομένων (big data).

Τα big data πρέπει να αναλυθούν για να προσδώσουν αξία στην επιχείρηση - μια έννοια που αναφέρεται ως το παράδοξο της παραγωγικότητας της τεχνολογίας (Liu Z. et al, 2016). Είναι επομένως ιδιαίτερα σημαντικό για τους οργανισμούς να έχουν σαφείς και επικεντρωμένες, ως προς την κατανόηση τους, στρατηγικές και σχέδια εφαρμογής του IoT όταν υιοθετούν αυτές τις τεχνολογίες.

Οι σημαντικές προκλήσεις που αντιμετωπίζουν σήμερα οι οργανισμοί που είναι αφοσιωμένοι στην κουλτούρα της Διαχείρισης Έργων είναι η συνεχώς αυξανόμενη πολυπλοκότητα των διαδικασιών που εμπλέκονται στην υλοποίηση του έργου, των αντικειμένων ή των υπηρεσιών. Ταυτόχρονα αυξάνεται η δυσκολία λήψης έγκυρων και αποτελεσματικών εργαλείων υποστήριξης που βοηθούν στη διαχείριση όλων των διαδικασιών που εμπλέκονται σε έργα. Συνεπώς, η συλλογή δεδομένων σε πραγματικό χρόνο θα μπορούσε να επηρεάσει την κρίσιμη διαδικασία λήψης αποφάσεων, διευκολύνοντας τον ρόλο του Project Manager.

Έτσι, είναι θεμελιώδους σημασίας η έρευνα και η αντιστοιχία με τις εξελισσόμενες τεχνολογίες στον τομέα του Ίντερνετ των πραγμάτων (IoT) μαζί με προσεγγίσεις διαχείρισης έργων για τη δημιουργία ενός μοναδικού συστήματος.

Η δυνατότητα συλλογής πληροφοριών πραγματικού χρόνου που παράγονται από πρακτικά "έξυπνα αντικείμενα" στον πραγματικό κόσμο, ανοίγει ανεξερεύνητα παραδείγματα για διάφορες εφαρμογές. Ωστόσο, απαιτεί μεγάλη προσπάθεια για τη δημιουργία μιας αποτελεσματικής διαδικασίας διαχείρισης τέτοιων πληροφοριών και χρήσιμων γνώσεων από τα πρωτογενή δεδομένα που επιστρέφουν οι αισθητήρες (Ghimire S et al, 2015).

Με την παραδοχή ότι οι άνθρωποι (εργαζόμενοι, ενδιαφερόμενοι, ή όλοι οι χρήστες της τεχνολογίας μέσα σε έναν οργανισμό) είναι οι βασικοί συντελεστές στις υλοποιήσεις των έργων (Motiwalla, F. L. & Thompson, J., 2009), πραγματοποιείται ήδη διεξοδική έρευνα με επίκεντρο τον χρήστη ή τον καταναλωτή. Καθίσταται ήδη εκ των προτέρων η αντίληψη για την συνύπαρξη των τεχνολογιών του Διαδικτύου στα πλαίσια της εφοδιαστικής αλυσίδας.

Σε γενικές γραμμές, η υιοθέτηση της τεχνολογίας και η αποδοχή από τους χρήστες δεν αποτελούν νέο θέμα και ως εκ τούτου εκτεταμένη έρευνα έχει αφιερωθεί στην ανάπτυξή της σε θεωρητικό και πρακτικό επίπεδο με επίκεντρο τους οργανισμούς που είναι προσηλωμένοι σε μία έργο-κεντρική φιλοσοφία. Ένα πλήρες φάσμα θεωριών έχει αναπτυχθεί για να εξηγήσει τον τρόπο αποδοχής της τεχνολογίας από τον χρήστη. Η τεχνολογία πλέον χρησιμοποιείται ευρέως για την πρόβλεψη της συμπεριφοράς των καταναλωτών σε διάφορους κλάδους και τεχνολογικά πλαίσια.

Ωστόσο, η εμπειρική έρευνα λείπει όταν πρόκειται για την καθαρή εξέταση της ανθρώπινης πλευράς και για την εκτίμηση των προοπτικών των χρηστών των τεχνολογιών IoT και είναι ακόμη λιγότερο εμφανής στα πλαίσια της εφοδιαστικής βιομηχανίας. Επιπλέον, και όπως αναμένεται από την επιχειρησιακή έρευνα, οι λίγες υπάρχουσες θεωρίες που εξηγούν την αποδοχή του IoT από τον καταναλωτή και των τεχνολογικών καινοτομιών γενικά, έχουν αναπτυχθεί μέσω ποσοτικών αναλύσεων.

Στην πραγματικότητα, υπάρχει έλλειψη ποιοτικών αναλύσεων (Gammelgaard B., 2004) και ποιοτικές προσεγγίσεις που η αξιολόγηση των αντιλήψεων των καταναλωτών σχετικά με τις τεχνολογίες του IoT είναι περιορισμένες. Οι υπάρχουσες θεωρίες μέχρι σήμερα έχουν αναπτυχθεί μέσω της δομημένης δοκιμής νέων μεταβλητών σε σχέση με προηγούμενες θεωρίες με στόχο την ενημέρωση ή την επέκτασή τους (Easterby-Smith et al, 2002).

Με άλλα λόγια, οι αντιλήψεις των καταναλωτών σχετικά με το IoT έχουν εξηγήσει καθαρά μέσω της δοκιμής μεθοδολογιών αιτίου-αποτελέσματος. Η έρευνα στον τομέα της δια βίου μάθησης, η εφοδιαστική και η επιχειρηματική έρευνα θα μπορούσαν να επωφεληθούν από μια ποιοτική ανάλυση των καταναλωτικών αντιλήψεων (Gammelgaard B., 2004). Επομένως

ένα επιπρόσθετο ερώτημα στην έρευνα μας είναι: *Ποιες είναι οι απαιτήσεις και οι συνέπειες της εφαρμογής του IoT σε ένα έργο-κεντρικό περιβάλλον;*

Σε αυτή την ενότητα της πτυχιακής θα προσπαθήσουμε να διερευνήσουμε τη σημασία της ενσωμάτωσης του IoT σε σενάρια υλοποίησης έργων. Επιπλέον, στοχεύει να επισημάνει τα προνόμια που προκύπτουν από την εν λόγω ολοκλήρωση. Σχετικές θεωρίες και αρχές του IoT και της ενσωμάτωσης της στη Διαχείριση έργων θα χρησιμοποιηθούν για την υποστήριξη και τεκμηρίωση αυτής της συνέργειας.

Η παραπάνω επισκόπηση των προκλήσεων στη συνέργεια της διαχείριση έργων και του IoT, και μέσα σε ένα γενικότερο πλαίσιο που θα ονομάζαμε Context-Aware Computing (Borgia, E., 2014), προκαλούν μεγάλο ενδιαφέρον για περαιτέρω διερεύνηση σχετικά με το παρόν και το μέλλον των δύο εννοιών, την εξέταση των διαφορετικών χαρακτηριστικών τους και πως θα επηρεάσουν την πιθανή εφαρμογή ενός συνδυαστικού μοντέλου.

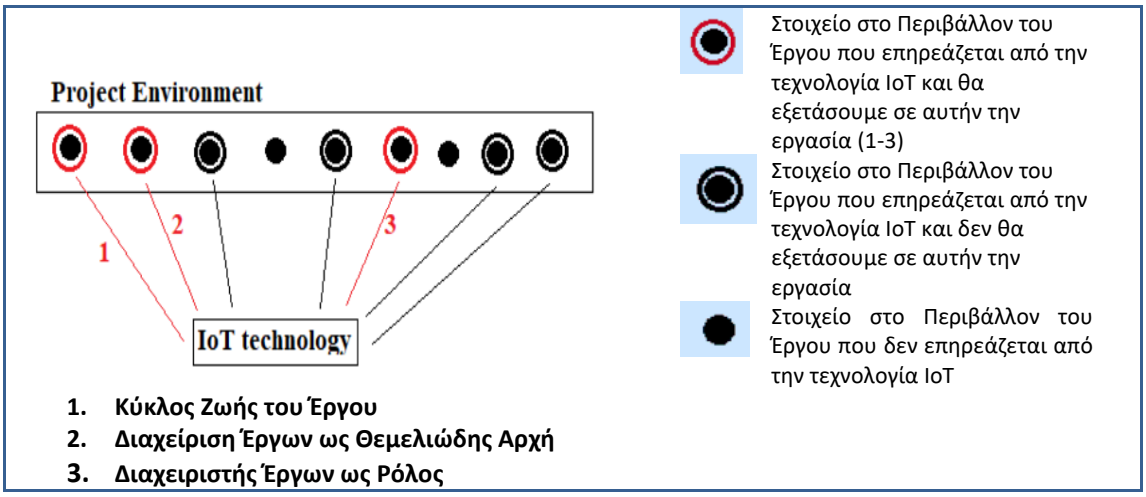
Είναι επίσης απαραίτητο να εξεταστεί πώς μια αλλαγή στην ενσωμάτωση των αρχών PM και IOT μπορεί να επηρεάσει την απόδοση των οργανισμών που έχουν έργο-κεντρική φιλοσοφία. Για το σκοπό αυτό, αναλύουμε περαιτέρω το παραπάνω ερευνητικό ερώτημα, θέτοντας τους ακόλουθους ερευνητικούς σκοπούς:

1) *Πώς το IoT θα υποστηρίξει τα Έργα στις δραστηριότητες ρουτίνας;*
2) *Πώς αλλάζουν οι βασικές αρχές Διαχείρισης Έργου λόγω της εφαρμογής του IoT;*
3) *Πώς θα διαμορφωθεί ο ρόλος των διαχειριστών έργων, από την τεχνολογία του IoT;*

Αντίστοιχα, οι παραπάνω στόχοι αποσκοπούν στην επισήμανση εξειδικευμένων γνώσεων σχετικά με την αντιστοίχιση μεταξύ της τεχνολογίας του IoT, και των στοιχείων του περιβάλλοντος ενός Έργου όπως: βασικές αρχές διοίκησης και ο ρόλος του διευθυντή έργων. Ειδικότερα, αυτή η αντιστοίχιση έχει ως στόχο να αποδείξει τη σημασία της νέας τεχνολογίας για τον κύκλο ζωής του έργου, επισημαίνοντας τις επιπτώσεις και τα πλεονεκτήματα της εφαρμογής της τεχνολογίας IoT (Borgia, E., 2014).

Ο δεύτερος σκοπός αυτής της αντιστοίχισης είναι να δοθεί καλύτερη κατανόηση των επιπτώσεων της εφαρμογής του IoT στις αρχές Διοίκησης και στο ρόλο του Διαχειριστή Έργων. Έτσι, τα παραπάνω ερευνητικά ερωτήματα προσπαθούν να περιορίσουν το επίκεντρο του ερευνητικού ζητήματος, ξεκινώντας από τα έργα γενικά για να ολοκληρώσουν τον προσδιορισμό των απαραίτητων χαρακτηριστικών των μελλοντικών Διευθυντών Έργου που καλούνται να χειριστούν την τεχνολογία του IoT στην καθημερινότητα τους.

*Εικόνα 23: Παράμετροι που θα εξεταστούν στη σημασία της εφαρμογής του IoT στη Διαχείριση Έργων*




## Β.3. Περιβάλλον Διαχείρισης Έργων

### Β.3.1. Ορισμός Έργου

Ο καθορισμός του όρου "Έργο" με ένα γενικευμένο τρόπο είναι θεμελιώδης για να εξασφαλιστεί μια βαθιά κατανόηση του θέματος. Ο Gaddis (1959) δημοσίευσε στο Business Review του Harvard τον ακόλουθο ορισμό: *«Ένα έργο είναι μια οργανωτική μονάδα αφιερωμένη στην επίτευξη ενός στόχου, γενικά την επιτυχή ολοκλήρωση ενός προϊόντος εγκαίρως, εντός προϋπολογισμού και σύμφωνα με προκαθορισμένες προδιαγραφές απόδοσης».*

Επιπλέον, το Διεθνές Ινστιτούτο PMI (2008) όρισε ως "έργο" μια προσωρινή προσπάθεια που αναλαμβάνει να δημιουργήσει ένα μοναδικό προϊόν, υπηρεσία ή αποτέλεσμα προοδευτικής επεξεργασίας. Κάθε χαρακτηριστικό είναι θεμελιώδες και απαραίτητο για την εγκαθίδρυση στο σωστό πλαίσιο.

Η έννοια του "προσωρινού" καθορίζει σιωπηρά ότι η προσπάθεια έχει καθορισμένο χρονικό διάστημα, με σωστή αρχή και συμπέρασμα. Η μοναδικότητα του αποτελέσματος εγγυάται από τη μη επαναληπτική διαδικασία που χρησιμοποιείται για να επιτευχθεί το παραγόμενο αποτέλεσμα. Ακόμη και με αναλογίες με άλλα έργα, το καθένα είναι μοναδικό στα χαρακτηριστικά και τις απαιτήσεις του. Όλα τα αποτελέσματα αποκτώνται λόγω προοδευτικής επεξεργασίας, που ορίζεται ως διαφορετικό είδος βημάτων.

Ο όρος "σχέδιο" λαμβάνει υπόψη διάφορες θεμελιώδεις πτυχές της επιχειρηματικής στρατηγικής και του επιχειρηματικού μοντέλου μιας επιχείρησης. Στην πραγματικότητα, το «έργο» ορίζεται κυρίως ως ένα εργαλείο που πρέπει να δημιουργηθεί για την επίτευξη στρατηγικών σχεδίων για την επιχείρηση. Το ίδιο το έργο αντιπροσωπεύει το σημείο ενδιαφέροντος των διαφόρων χαρακτηριστικών και απαιτήσεων:

- Οι ρόλοι στην ομάδα έργου
- Χρήση πόρων διαφόρων ειδών
- Περιορισμένος προϋπολογισμός
- Κύκλος ζωής
- Μέτρο απόδοσης
- Περιορισμένη διαθεσιμότητα χρόνου
- Πεδίο εφαρμογής και στόχος.

Μαζί με τη σημασία και τον αντίκτυπο στην επιχειρηματική στρατηγική της εταιρείας, ταυτόχρονα αποδίδεται, συνδυάζοντας όλα τα προηγούμενα στοιχεία, ένα ορισμένο επίπεδο ασάφειας που μειώνεται κατά την πρόοδο του έργου (Burke, 2014). Τα έργα αναπτύσσονται όλο και περισσότερο ως μέσο επίτευξης επιχειρηματικών στόχων, σε τέτοιο βαθμό ώστε η διαχείριση μέσω έργων να διαρθρώνεται ως κεντρική στρατηγική διαχείρισης. Μια στρατηγική που αντικατοπτρίζει την αμείλικτη αύξηση της πολυπλοκότητας την οποία οι επιχειρήσεις καλούνται να αντιμετωπίσουν (Smith, B. & Dodds, B., 1997).

Η διαχείριση των έργων έχει μεγάλη οικονομική σημασία και έχει σημειωθεί δραματική ανάπτυξη στις εργασίες του έργου σε διάφορους τομείς, βιομηχανίες και χώρες (Turner, R. et al, 2010). Τα έργα εξασφαλίζουν την επιτυχία σε περιόδους αλλαγής σε έναν οργανισμό. Ως εκ τούτου, μπορούν να θεωρηθούν απαραίτητα από την άποψη της δημιουργίας αξίας και οφέλους για έναν οργανισμό (Project Management Institute. , 2008).

Επιπλέον, "τα σχέδια έχουν σκοπό να φέρουν κάτι καινούριο στο αρχικό τους περιβάλλον, έτσι τα έργα είναι καινοτόμα και μπορούν να θεωρηθούν ως «επιχειρηματικές πράξεις» (Kuura, A. et al, 2014). Αν και η προσπάθεια μπορεί να είναι τουλάχιστον για μήνες ή δεκαετίες, το ίδιο το έργο έχει πάντα τις ίδιες κρίσιμες πέντε φάσεις που συνθέτουν τον "κύκλο ζωής του έργου".

Τα έργα έχουν έναν κύκλο ζωής στον οποίο οι δεξιότητες, τα εργαλεία και οι άνθρωποι πρέπει να χρησιμοποιήσουν αποτελεσματικά τους πόρους για να το ολοκληρώσουν (Jugdev, K., et al, 2013). Το PMI (2008) ορίζει τον «κύκλο ζωής του έργου» ως τη «συλλογή διαδοχικών

φάσεων έργου των οποίων το όνομα και ο αριθμός καθορίζονται από τις ανάγκες ελέγχου του οργανισμού» ή από τους οργανισμούς που εμπλέκονται στο έργο. Οι πέντε φάσεις που είναι συνήθεις σε κάθε έργο είναι:

1) η εκκίνηση
2) ο προγραμματισμός
3) η εκτέλεση
4) η παρακολούθηση και ο έλεγχος
5) το κλείσιμο.

*Εικόνα 24: Γραφική απεικόνιση του κύκλου ζωής του έργου (Anon, 2018)*


### Β.3.2. Έργο-κεντρικός προσανατολισμός των επιχειρήσεων και οργανισμών

Τα έργα έχουν γίνει ένας σημαντικός τρόπος για να δομηθεί η εργασία στους περισσότερους οργανισμούς και αποτελούν μία από τις πιο κρίσιμες οργανωτικές εξελίξεις (Burke, 2014). Ο όρος "έργο" παρουσιάζει τις σύγχρονες τάσεις στην αναδιοργάνωση των οργανισμών. Τόσο οι πολυεθνικές όσο και οι μικρο-μεσαίες επιχειρήσεις αναφέρονται στη λέξη για να περιγράψουν το επιχειρηματικό τους μοντέλο: έργα προσανατολισμένα ή έργα εντατικά ως προστιθέμενη αξία στις επιχειρήσεις τους (Söderlund, J., 2004).

Σύμφωνα με τους Gareis και Huemann (2000), οι οργανισμοί προσανατολισμένοι στο έργο βασίζονται κυρίως στην βασική αξία που παρέχεται από τις αρχές του PM, η οποία τελικά

αναπτύσσεται από τον ίδιο τον οργανισμό. Η σημασία της θεμελιώδης αρχής του PM για τον προσδιορισμό οργανισμών προσανατολισμένων σε μια έργο-κεντρική κουλτούρα δηλώνεται σαφώς από τους Turner και Keegan (2001), όταν ορίζουν την προσαρμογή των αναγκών και απαιτήσεων από τους πελάτες ως κύριο κινητήριο μοχλό της οργανωτικής δομής.

Από την άλλη πλευρά, λαμβάνοντας υπόψη τις απαιτήσεις των πελατών ως παράγοντα ενεργοποίησης μιας δομής προσανατολισμένης στις αρχές του PM, η ίδια η εταιρεία αποφασίζει να υιοθετήσει μια τέτοια στρατηγική επιλογή για το επιχειρηματικό της μοντέλο, στηρίζοντας την οργανωτική στρατηγική της Διοίκησης με βάση τα έργα (Huemann, 2014).

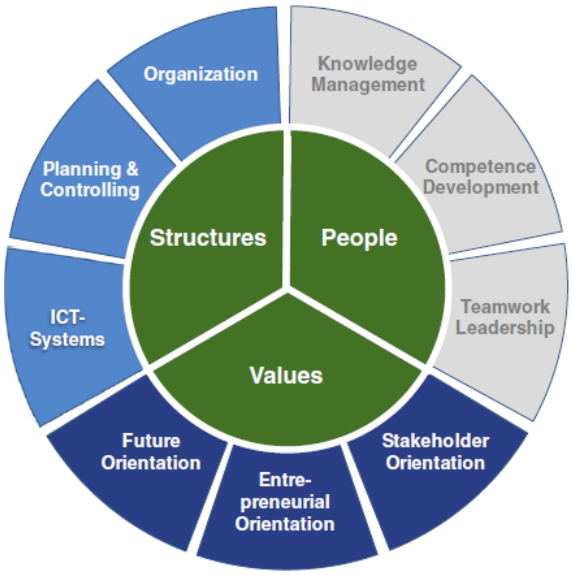
Επιπλέον, ο Hobday (2000) σχεδίασε ένα έργο-κεντρικό μοντέλο για οργανισμούς που βασίζεται στην καινοτόμο ώθηση και την έρευνα της καινοτομίας του σύνθετου συστήματος προϊόντων. Σύμφωνα με το Hobday (2000) η έργο-κεντρική επιχείρηση "*είναι σε θέση να αντιμετωπίσει τις αναδυόμενες προκλήσεις στην παραγωγή και ανταποκρίνεται με ευελιξία στις μεταβαλλόμενες ανάγκες των πελατών. Είναι επίσης αποτελεσματική στην ενσωμάτωση διαφορετικών τύπων γνώσης και δεξιοτήτων και στην αντιμετώπιση των κινδύνων του έργου και της διεύρυνσης του οράματος του οργανισμού*".

Τέτοιου είδους πλαίσια βασίζουν την επιχείρηση στην ιδιαιτερότητα των στόχων, των αποτελεσμάτων ή των επιτευγμάτων. Στην πραγματικότητα οι εξιδεικευμένες λύσεις προσφέρονται σε μεγάλους πελάτες λόγω ενός συγκεκριμένου, πολύπλοκου και οργανωμένου δικτύου προμηθευτών και συντονισμένων συμβάσεων. Την ίδια περίοδο, ο ακόλουθος ορισμός μίας έργο-κεντρικής επιχείρησης δόθηκε από τους Gareis και Huemann (2000):

'"Ένας έργο-κεντρικός οργανισμός είναι ένας οργανισμός, ο οποίος καθιερώνει τη 'Διοίκηση με βάση τα έργα' ως θεμελιώδη οργανωτική στρατηγική βάσει της οποίας:

- εφαρμόζει προσωρινές δομές για την εκτέλεση πολύπλοκων διαδικασιών
- διαχειρίζεται ένα χαρτοφυλάκιο με διαφορετικούς τύπους έργων
- έχει συγκεκριμένες μόνιμες δομές για να παρέχει ολοκληρωμένες λειτουργίες
- εφαρμόζει ένα «νέο μοντέλο διαχείρισης»
- έχει μια ξεκάθαρη κουλτούρα διαχείρισης έργου και
- αντιλαμβάνεται τον εαυτό του ως έργο-κεντρικό οργανισμό.

*Εικόνα 25: Μοντέλο ενός έργο-κεντρικού οργανισμού (Gemünden et al, 2017)*




Η διαχείριση του έργου, ως πολυεπιστημονική σύνθεση αρχών, διαδραματίζει κρίσιμο ρόλο στη διοίκηση ενός έργο-κεντρικού οργανισμού στον εικοστό πρώτο αιώνα. Τελικά, σήμερα είναι απαραίτητο να εγκαταλείψουμε τη θεωρία σχεδιασμού και ελέγχου και να δώσουμε έμφαση στη μάθηση σε πολύπλοκα κοινωνικά συστήματα στα οποία ο άνθρωπος είναι το επίκεντρο (Staadt, J. , 2012).

Οι ενδείξεις συζητήθηκαν επίσης από τον Jackson (2006) ο οποίος υποστηρίζει και πρότεινε έναν συνδυασμό διαφορετικών στοιχείων: συστήματα, μεθοδολογίες και μεθόδους. Με ιδιαίτερη έμφαση στην ανθρώπινη συνιστώσα, η ικανότητα δημιουργίας ενός σταθερού κύκλου μάθησης και ενός βρόχου αναγνωρίζεται ως μία από τις βασικές δυνατότητες διαχείρισης έργου που είναι ζωτικής σημασίας για την περαιτέρω ανάπτυξη μίας επιχείρησης (Staadt, J. , 2012).

### Β.3.3. Διοίκηση έργων ως θεμελιώδης αρχή

Η θεμελιώδης αρχή που μελετά, ερευνά και φροντίζει για την ενεργοποίηση των έργων ονομάζεται "Διαχείριση Έργων". Η διαχείριση του έργου ορίζεται στο PMBoK ως *"εφαρμογή γνώσεων, δεξιοτήτων, εργαλείων και τεχνικών για την προβολή δραστηριοτήτων για την κάλυψη των απαιτήσεων του έργου*" (PMI, 2008). Συνήθως, περιλαμβάνει:

- την κατανόηση των αναγκών των πελατών
- τον καθορισμό των αναγκών των ενδιαφερομένων

- τη δημιουργία ενός αποτελεσματικού καναλιού επικοινωνίας με τους ενδιαφερόμενους
- την εξισορρόπηση των ανταγωνιστικών περιορισμών του έργου όσον αφορά το εύρος, την ποιότητα, το χρονοδιάγραμμα, τον προϋπολογισμό, και τον κίνδυνο.

Η διαχείριση του έργου (PM) είναι μια καθιερωμένη επιστήμη που χαρακτηρίζεται από καθορισμένα όργανα των επαγγελματιών και κοινώς διαδεδομένες και αποδεκτές μεθοδολογίες που ορίζονται από διεθνείς μεθοδολογίες όπως PMBOK® και PRINCE2®.

Το ενδιαφέρον για το επιχειρηματικό μοντέλο των έργων και γενικότερα για τη διαχείριση έργων έχει αυξηθεί σημαντικά τις τελευταίες δεκαετίες. Η αρχή της διαχείρισης του έργου είναι διαδεδομένη σε αρκετές βιομηχανίες και σήμερα αποτελεί ένα διεπιστημονικό ερευνητικό ζήτημα με ευρύτερη δημοσιότητα (Pollack, J. & Adler, D., 2015). Επιπλέον, οι βιομηχανίες και οι επιχειρήσεις συνεχίζουν να εξελίσσονται γύρω από τις προσεγγίσεις διαχείρισης του έργου, ως ασφαλή δρόμο για την ανάπτυξη (Thomas. J. et al, 2004).

Αν και αναμφίβολα τόσο οι πρακτικές όσο και οι θεωρητικές πτυχές της διαχείρισης έργων (PM) έχουν αναπτυχθεί ραγδαία τα τελευταία χρόνια, κάποιοι ερευνητές έχουν καταστήσει σαφές ότι αυτό ήταν περιορισμένο και όχι συγκεκριμένο. Επιπλέον, έχει υπογραμμιστεί από άλλους ερευνητές ότι το πραγματικό παράδειγμα είναι να θεωρούνται τα έργα ως εργαλεία και η διαχείριση έργων ως ένα σύνολο μοντέλων και τεχνικών για τον σχεδιασμό και έλεγχο σύνθετων συστημάτων (Söderlund, J., 2004).

Μέσα στο PMBOK®, είναι επίσης δυνατό να βρεθούν οι διαφορετικές πτυχές που σχετίζονται με κάθε φάση του κύκλου ζωής του έργου. Ο αριθμός των φάσεων αλλάζει χρόνια με τα χρόνια λόγω της πολυπλοκότητας και της εξέλιξης του κλάδου, λαμβάνοντας επίσης υπόψη τις εξελισσόμενες ανάγκες των πελατών και των ενδιαφερομένων γενικότερα κατά τη διάρκεια ολόκληρης της διαδικασίας.

Οι διαδικασίες διαχείρισης ενός έργου συντονίζουν την αποτελεσματική ροή του έργου καθ 'όλη τη διάρκεια του κύκλου ζωής του, στηριζόμενοι σε μια καλή πρακτική των εργαλείων και των τεχνικών. Επιπλέον, οι Διευθυντές Έργου και η ομάδα θα καθορίσουν ποιες δεξιότητες και δυνατότητες ισχύουν για το έργο στο οποίο εργάζονται. Σύμφωνα με τον Οδηγό PMBOK® (PMI, 2013), οι διαδικασίες διαχείρισης του έργου ομαδοποιούνται σε πέντε κύριες ομάδες διεργασιών:

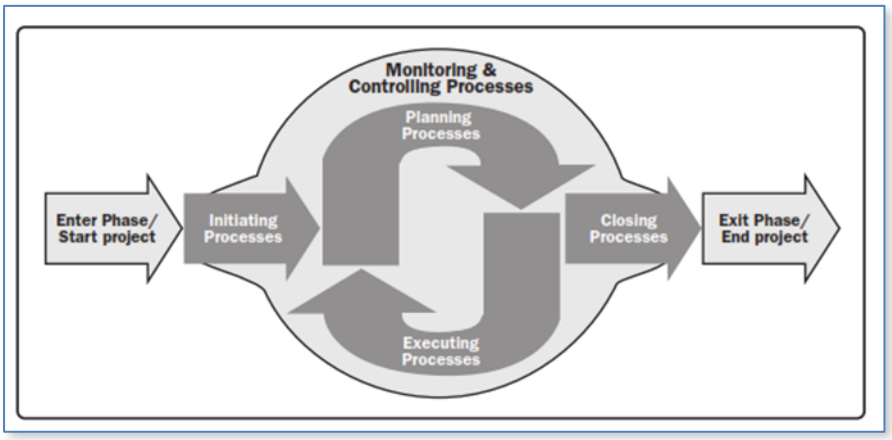
1. <u>Νέο έργο ή νέα φάση σε υφιστάμενο έργο</u>

2. Ομάδα Διαδικασιών Σχεδιασμού: Απαιτούμενες διαδικασίες για τον καθορισμό του πεδίου εφαρμογής του έργου, των τελικών του στόχων και του σχεδίου για την επίτευξη των στόχων του έργου.
3. Εκτέλεση ομάδας διεργασιών. Διαδικασίες που εκτελούνται για την εκτέλεση των εργασιών του έργου σύμφωνα με το σχέδιο και τις απαιτήσεις του έργου.
4. Ομάδα Διαδικασιών Παρακολούθησης και Ελέγχου: Διαδικασίες που παρακολουθούν, αναθεωρούν και εκτελούν διορθωτικές ή προληπτικές ενέργειες για τη βελτίωση της απόδοσης του έργου
5. Ομάδα διαδικασίας κλεισίματος: Οι διαδικασίες αυτές διασφαλίζουν ότι όλες οι εκκρεμείς δράσεις σε όλες τις ομάδες διεργασιών έχουν οριστικοποιηθεί προκειμένου να προχωρήσουν στο επίσημο έργο ή στο κλείσιμο φάσης.
6. Ομάδα διαδικασίας εκκίνησης: αυτές είναι διαδικασίες που απαιτούνται για την έγκριση της έναρξης ενός έργου.

Η αξία των ομάδων διεργασίας είναι ότι οι προαναφερόμενες ομάδες προσφέρουν έναν απλοποιημένο και εξιδανικευμένο τρόπο διαχείρισης του έργου που επιδιώκει να ελαχιστοποιήσει την παρερμηνεία και να καταστήσει ευκολότερη την κατανόηση της διαδικασίας.

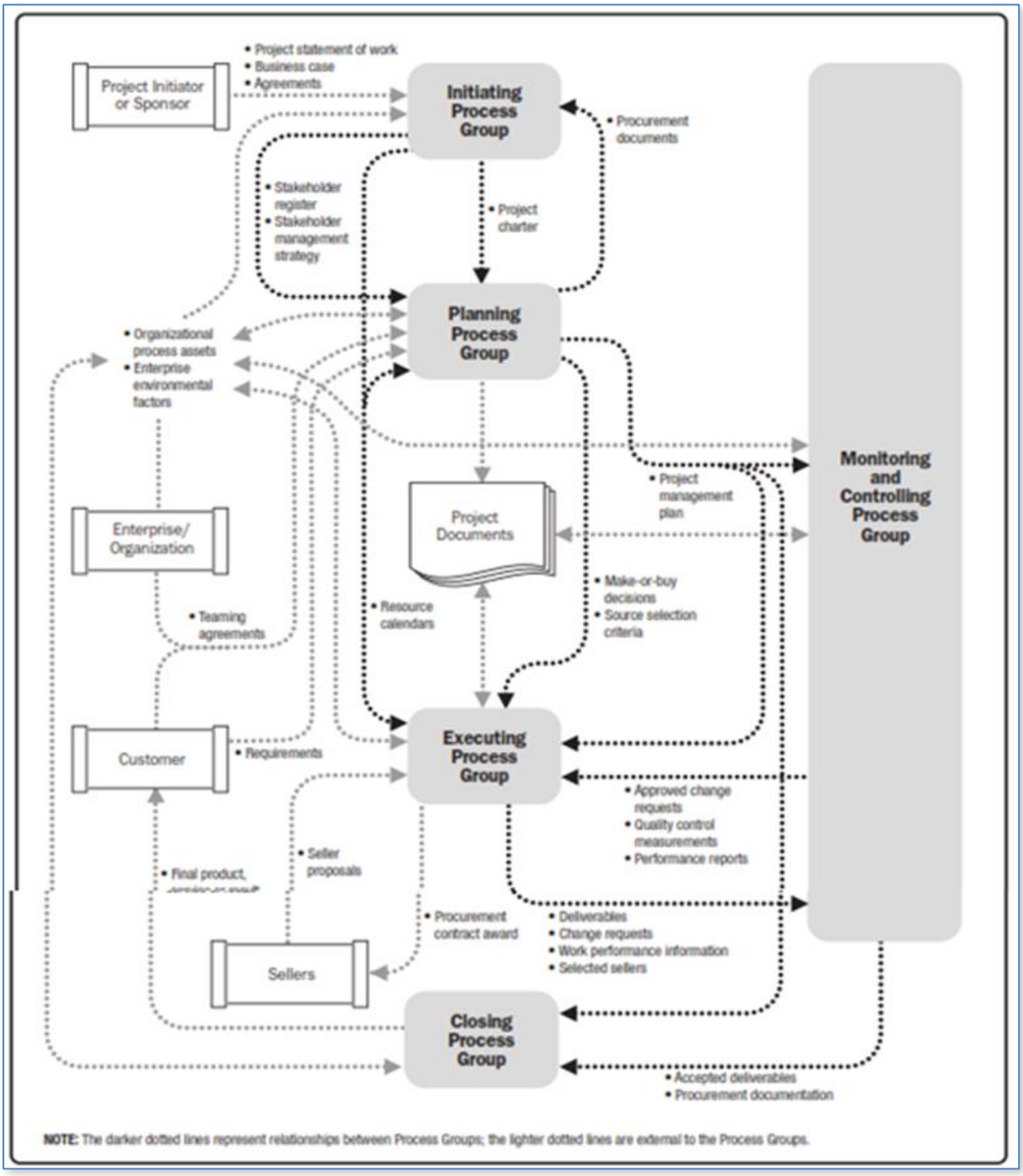
Όπως απεικονίζεται στην Εικόνα 24, η Ομάδα Διαχείρισης Παρακολούθησης και Ελέγχου εκτείνεται στην εκτέλεση των υπόλοιπων ομάδων διεργασίας.

*Εικόνα 26: Ομάδες Διαδικασιών Διαχείρισης Έργων (PMI, 2013)*




Οι πέντε ομάδες διεργασιών έχουν σαφείς εξαρτήσεις και τυπικά εκτελούνται με την ίδια σειρά σε κάθε έργο. Επομένως, η αλληλεπίδραση μεταξύ των ομάδων διεργασίας εξαρτάται από την παραγωγή που κάθε ομάδα παράγει καθώς η θέλησή τους θα επικαλύπτεται στις δραστηριότητές της (Εικόνα 27).

*Εικόνα 27: Διαδικασία αλληλεπίδρασης ομάδων σε ένα έργο ή φάση (PMI, 2013)*




Αυτό γίνεται διακριτό καθώς το έργο χωρίζεται σε πρόσθετα παραδοτέα έτσι ώστε η έξοδος μιας ομάδας διεργασιών (π.χ. το σχέδιο διαχείρισης έργου και τα έγγραφα έργου της ομάδας διαδικασίας προγραμματισμού) να ρίχνεται ως είσοδος στην επόμενη ομάδα διεργασιών (π.χ. την ομάδα διαδικασίας εκτέλεσης). Είναι πολύ σημαντικό να σημειωθεί ότι είναι ανεξάρτητες από τις περιοχές εφαρμογής ή την εστίαση της βιομηχανίας.

Όπως απεικονίζεται στην Εικόνα 27, κάθε ομάδα επεξεργασίας αξιοποιεί στη διαχείριση του έργου μια ομάδα συναφών δραστηριοτήτων οι οποίες συχνά επαναλαμβάνονται πριν από την ολοκλήρωση του έργου. Για παράδειγμα, μια τυπική διαδικασία P στη φάση σχεδιασμού συνδέεται με την Ομάδα Διαδικασιών Σχεδιασμού. Εάν η ίδια διαδικασία ενημερωθεί από άλλη διαδικασία E της Ομάδας διαδικασίας εκτέλεσης, τότε η διαδικασία P δεν θεωρείται μέρος της Ομάδας Διαδικασιών Εκτέλεσης αλλά εξακολουθεί να συνδέεται με την Ομάδα Διαδικασιών Σχεδιασμού.

Οι 47 διαδικασίες διαχείρισης έργων κατανέμονται μεταξύ των πέντε ομάδων διεργασιών. Η Ομάδα Διαδικασιών Εκκίνησης αποτελείται από δύο διαδικασίες. Η Ομάδα Διαδικασιών Σχεδιασμού καλύπτει 24 διαδικασίες και διεκπεραιώνει τη διεργασία Εκτέλεσης Διαδικασιών της Ομάδας 8. Η Ομάδα Διαδικασιών Παρακολούθησης και Ελέγχου αποτελείται από 11 διαδικασίες και την Ομάδα Διαδικασιών Κλεισίματος 2 διαδικασιών.

### Β.3.4. Μετατόπιση της θεωρίας στο περιβάλλον του έργου

Το επίκεντρο των παλιών προσεγγίσεων του PM ήταν η βελτιστοποίηση των διαδικασιών για να επιτευχθεί το καλύτερο δυνατό αποτέλεσμα (Pollack, J. & Adler, D., 2015). Αν και η τεχνική προσέγγιση εξακολουθεί να είναι σχετική, το σταθερό και αυξανόμενο ενδιαφέρον για τη διαχείριση έργων ως θεμελιώδη αρχή στην υλοποίηση έργων τις τελευταίες δεκαετίες, εξηγείται επαρκώς με την αύξηση της υιοθέτησης πιο ευέλικτων και σύγχρονων επιχειρησιακών μοντέλων μέσα σε διάφορες βιομηχανίες (Söderlund, J., 2004).

Αυτό το φαινόμενο, στην πραγματικότητα δεν είναι ιδιόμορφο σε ένα μόνο πεδίο, αλλά έχει τεκμηριωθεί από διάφορους ερευνητές που ασχολούνται με την επιχειρησιακή ανάπτυξη, και εταιρείες σε πολλούς εναλλακτικούς βιομηχανικούς τομείς. Συμπερασματικά, είναι γνωστό ότι για να καθοριστούν οι αλλαγές στον οργανισμό είναι θεμελιώδες και απαραίτητο να αποσταθεροποιηθούν οι υπάρχουσες δομές από τη βάση τους.

Η δομή πρέπει να αλλάξει σημαντικά για να επιτρέψει την καινοτομία, αλλά η διατήρηση επαρκούς σταθερότητας για τον οργανισμό είναι θεμελιώδους σημασίας για να αντιμετωπίσουν επιτυχώς τις μετατοπίσεις και τις διαδικασίες υλοποίησης. Για να φέρουν εις πέρας τωρινά και μελλοντικά έργα με αυξανόμενη πολυπλοκότητα, είναι απαραίτητο να δοθεί μεγαλύτερη έμφαση σε εκπαιδευτικά μοντέλα, στην καλλιεργημένη προσπάθεια δημιουργίας νέων τεχνικών.

Κρίσιμοι παράγοντες επιτυχίας ενός σύγχρονου οργανισμού/επιχείρησης στο σύγχρονο επιχειρηματικό περιβάλλον είναι οι (Thomas. J. et al, 2004):

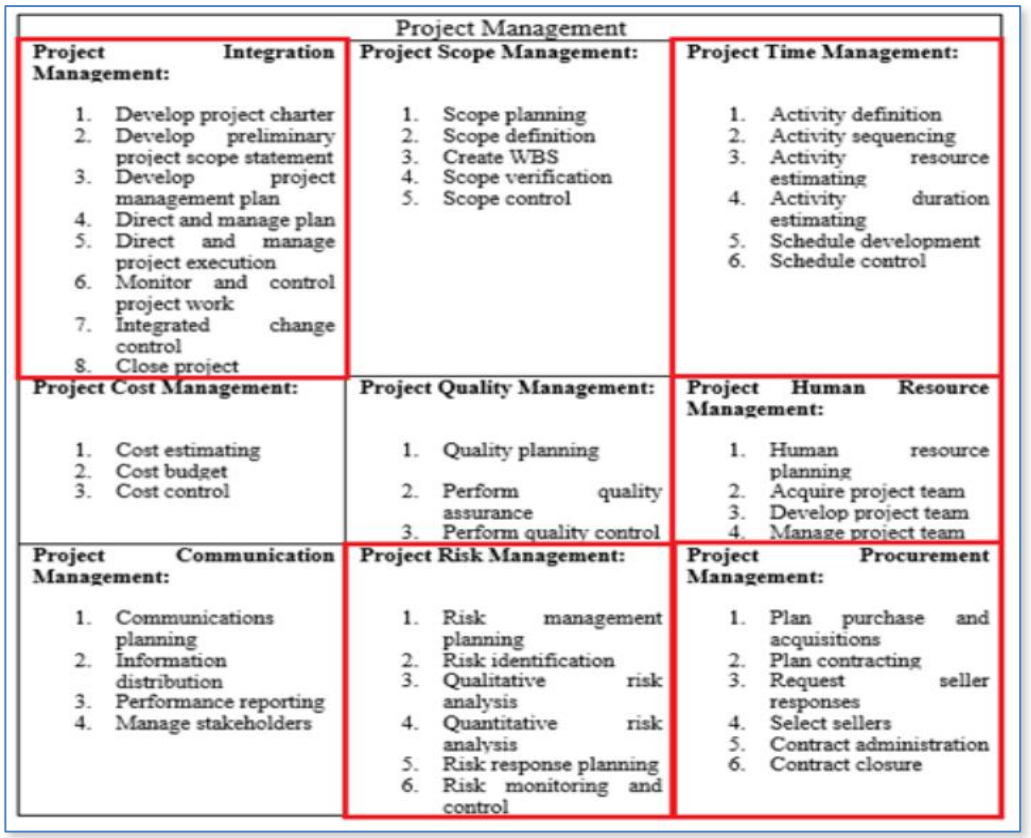
- η δημιουργική και κριτική σκέψη
- η αυτό-οργανωμένη δικτύωση
- η εικονική και διαπολιτισμική επικοινωνία
- η αντιμετώπιση της αβεβαιότητας και τα διάφορα πλαίσια αναφοράς
- η αύξηση της αυτογνωσίας και
- η ικανότητα οικοδόμησης και συμβολής σε ομάδες υψηλών επιδόσεων

Επιπλέον, τόσο η διοίκηση του έργου όσο και ο διαχειριστής του έργου πρέπει να λειτουργήσουν ως κύριοι παράγοντες ώθησης και οδηγοί στην επιτυχία της επιχείρησης, εξασφαλίζοντας μια συνεχή ανάπτυξη της επιχείρησης και μειώνοντας την αβεβαιότητα που χαρακτηρίζει την παγκόσμια αγορά.

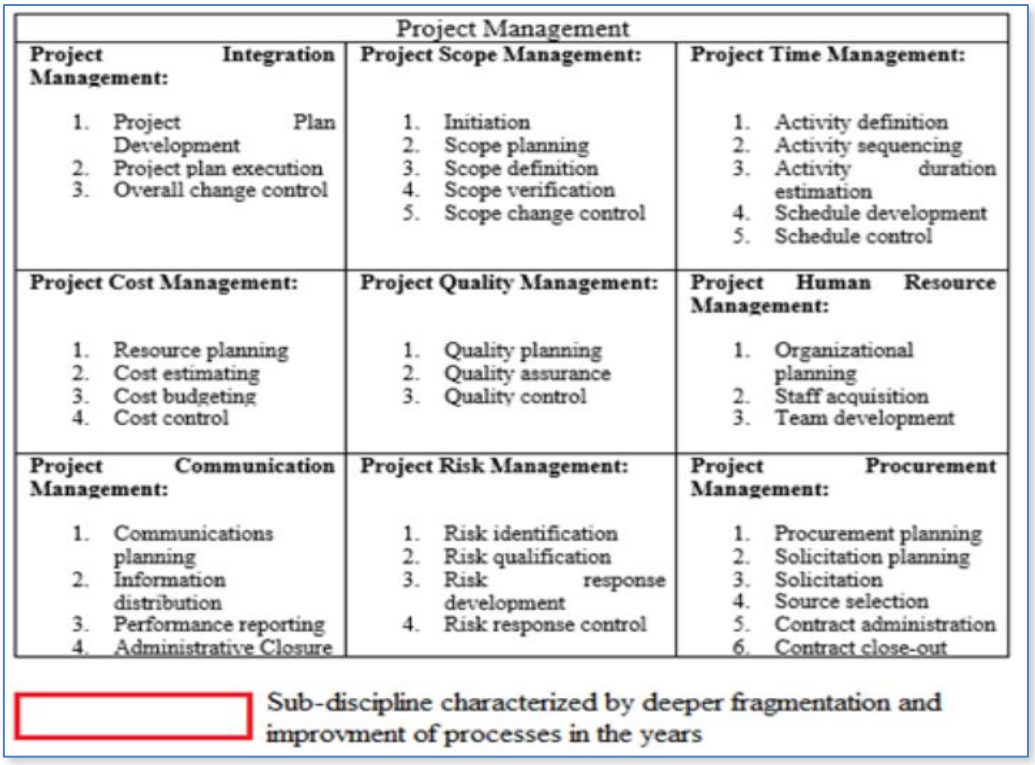
*Εικόνα 28: Διαφορετικές πτυχές των αρχών διαχείρισης έργων (Project Management Institute. , 2008)*

| Project Management | | |
|---|---|---|
| **Project Integration Management:**<br>1. Project Plan Development<br>2. Project plan execution<br>3. Overall change control | **Project Scope Management:**<br>1. Initiation<br>2. Scope planning<br>3. Scope definition<br>4. Scope verification<br>5. Scope change control | **Project Time Management:**<br>1. Activity definition<br>2. Activity sequencing<br>3. Activity duration estimation<br>4. Schedule development<br>5. Schedule control |
| **Project Cost Management:**<br>1. Resource planning<br>2. Cost estimating<br>3. Cost budgeting<br>4. Cost control | **Project Quality Management:**<br>1. Quality planning<br>2. Quality assurance<br>3. Quality control | **Project Human Resource Management:**<br>1. Organizational planning<br>2. Staff acquisition<br>3. Team development |
| **Project Communication Management:**<br>1. Communications planning<br>2. Information distribution<br>3. Performance reporting<br>4. Administrative Closure | **Project Risk Management:**<br>1. Risk identification<br>2. Risk qualification<br>3. Risk response development<br>4. Risk response control | **Project Procurement Management:**<br>1. Procurement planning<br>2. Solicitation planning<br>3. Solicitation<br>4. Source selection<br>5. Contract administration<br>6. Contract close-out |

*Εικόνα 29: Σύγκριση μεταξύ των πεδίων της διαχείρισης έργων από την 1η έκδοση PMBoK (PMI, 1996) έως την 6η έκδοση PMBoK (PMI, 2008)*



| Project Management | | |
|---|---|---|
| **Project Integration Management:**<br>1. Develop project charter<br>2. Develop preliminary project scope statement<br>3. Develop project management plan<br>4. Direct and manage plan<br>5. Direct and manage project execution<br>6. Monitor and control project work<br>7. Integrated change control<br>8. Close project | **Project Scope Management:**<br>1. Scope planning<br>2. Scope definition<br>3. Create WBS<br>4. Scope verification<br>5. Scope control | **Project Time Management:**<br>1. Activity definition<br>2. Activity sequencing<br>3. Activity resource estimating<br>4. Activity duration estimating<br>5. Schedule development<br>6. Schedule control |
| **Project Cost Management:**<br>1. Cost estimating<br>2. Cost budget<br>3. Cost control | **Project Quality Management:**<br>1. Quality planning<br>2. Perform quality assurance<br>3. Perform quality control | **Project Human Resource Management:**<br>1. Human resource planning<br>2. Acquire project team<br>3. Develop project team<br>4. Manage project team |
| **Project Communication Management:**<br>1. Communications planning<br>2. Information distribution<br>3. Performance reporting<br>4. Manage stakeholders | **Project Risk Management:**<br>1. Risk management planning<br>2. Risk identification<br>3. Qualitative risk analysis<br>4. Quantitative risk analysis<br>5. Risk response planning<br>6. Risk monitoring and control | **Project Procurement Management:**<br>1. Plan purchase and acquisitions<br>2. Plan contracting<br>3. Request seller responses<br>4. Select sellers<br>5. Contract administration<br>6. Contract closure |



| Project Management | | |
|---|---|---|
| **Project Integration Management:**<br>1. Project Plan Development<br>2. Project plan execution<br>3. Overall change control | **Project Scope Management:**<br>1. Initiation<br>2. Scope planning<br>3. Scope definition<br>4. Scope verification<br>5. Scope change control | **Project Time Management:**<br>1. Activity definition<br>2. Activity sequencing<br>3. Activity duration estimation<br>4. Schedule development<br>5. Schedule control |
| **Project Cost Management:**<br>1. Resource planning<br>2. Cost estimating<br>3. Cost budgeting<br>4. Cost control | **Project Quality Management:**<br>1. Quality planning<br>2. Quality assurance<br>3. Quality control | **Project Human Resource Management:**<br>1. Organizational planning<br>2. Staff acquisition<br>3. Team development |
| **Project Communication Management:**<br>1. Communications planning<br>2. Information distribution<br>3. Performance reporting<br>4. Administrative Closure | **Project Risk Management:**<br>1. Risk identification<br>2. Risk qualification<br>3. Risk response development<br>4. Risk response control | **Project Procurement Management:**<br>1. Procurement planning<br>2. Solicitation planning<br>3. Solicitation<br>4. Source selection<br>5. Contract administration<br>6. Contract close-out |

Sub-discipline characterized by deeper fragmentation and improvment of processes in the years

### Β.3.5. Πολυπλοκότητα του ρόλου του Διαχειριστή Έργων

Στο πραγματικό περιβάλλον του έργου, ο αντίκτυπος των νέων τεχνολογιών είναι βαθύς και ριζοσπαστικός. Για τους περισσότερους ενδιαφερόμενους υπάρχει η αντίληψη ότι συμβαίνουν σημαντικές αλλαγές, αλλά όλα είναι πολύ γρήγορα μέσα σε ένα σενάριο που χαρακτηρίζεται από πολυπλοκότητα και αβεβαιότητα (Smith, B. & Dodds, B., 1997). Αυτό είναι αποπροσανατολιστικό και δύσκολο για τους διευθυντικούς ρόλους.

Στην πραγματικότητα, οι διαχειριστές που αναλαμβάνουν έργα, ειδικά όταν το έργο απαιτεί δεξιότητες και προσεγγίσεις εκτός γνωστού τομέα, συχνά έχουν ανάγκη να αντιμετωπίσουν αλλαγές και προκλήσεις. Παρά τις δυσκολίες, όπου μια τέτοια αλλαγή μπορεί να ενσωματωθεί αποτελεσματικά στις διαδικασίες και τις μεθοδολογίες του έργου, η μάθηση μέσα στον οργανισμό εμπλουτίζεται σε μεγάλο βαθμό (Smith, B. & Dodds, B., 1997).

Η άνοδος των νέων τεχνολογιών και η αυξανόμενη πολυπλοκότητα του περιβάλλοντος υποχρεώνουν τις εταιρείες και τους επιχειρηματίες να αλλάξουν την προσέγγιση των επιχειρήσεων και της αγοράς. Η δυνατότητα να υπολογίζεται και να αναλύεται ο τεράστιος όγκος δεδομένων χάρη στα συνδεδεμένα αντικείμενα και ένα οικοσύστημα που χτίστηκε γύρω από έξυπνα αντικείμενα έγινε χρήσιμη για την πρόβλεψη καταστάσεων και διορθωτικών ενεργειών. Η ευελιξία και η γρήγορη ανταπόκριση στις εξωτερικές και ανεξέλεγκτες εισροές είναι μια απαραίτητη ικανότητα που απαιτείται για όλες τις οντότητες που εργάζονται μέσα στο περιβάλλον του έργου.

Λόγω της αλλαγής των εννοιών, η διαδικασία λήψης αποφάσεων απαιτείται από τους διαχειριστές των έργων όχι μόνο κατά τη φάση έναρξης και προγραμματισμού, αλλά είναι κρίσιμη επαναληπτική διαδικασία κατά τη διάρκεια ολόκληρου του κύκλου ζωής του έργου. Συνήθως, μέσα στη σύγχρονη αγορά που αλλάζει διαρκώς τους κανόνες και την εσωτερική δυναμική, οι διαχειριστές συμβάλλουν διαφορετικά στις επιχειρηματικές διαδικασίες και δραστηριότητες. Ιδιαίτερα, σε ένα έργο-κεντρικό οργανισμό που επικεντρώνεται στην ανάπτυξη σχετικών επιχειρηματικών μοντέλων, η κρισιμότητα σχετίζεται με τα ακόλουθα σημεία (Smith, B. & Dodds, B., 1997):

- ικανότητα επίτευξης επιχειρησιακών στόχων και λειτουργικών απαιτήσεων εντός ενός μείγματος εσωτερικών και εξωτερικών πόρων, που διαχειρίζεται ένα σύνολο παράλληλων έργων
- διαχείριση της αυξανόμενης πίεσης από γνωστούς και άγνωστους ανταγωνιστές, διεθνώς και από τις αναδυόμενες οικονομίες

- ❖ ενθάρρυνση καινοτόμων διαδικασιών και διαδικασιών δημιουργικότητας στα όρια του οργανισμού
- ❖ η συνεχής υιοθέτηση καινοτόμων συστημάτων και τεχνολογιών πληροφορικής για την αποτελεσματική και αποδοτική υποστήριξη του περιβάλλοντος έργου.

Οι σημαντικότερες προκλήσεις που αντιμετωπίζουν σήμερα οι υπεύθυνοι έργων δεν είναι μόνο η μετατόπιση των θεμελιωδών χαρακτηριστικών μέσα στο περιβάλλον που προσανατολίζεται στο έργο, αλλά και η αυξανόμενη πολυπλοκότητα των δραστηριοτήτων του κύκλου ζωής του έργου, ιδίως για να αναφέρουμε μερικά από αυτά:

- ❖ τις διαδικασίες και τα δίκτυα προμήθειας
- ❖ τις πιέσεις του κόστους
- ❖ τις αυξανόμενες προσδοκίες των χρηστών και των πελατών για ποιότητα
- ❖ γρήγορες απαντήσεις στις εισροές
- ❖ προσαρμοσμένες δραστηριότητες και διαδικασίες
- ❖ ασφάλεια των εργαζομένων και βοήθεια στη δημιουργία αναφορών.

Επιπλέον, η διαδικασία κατασκευής των περισσοτέρων έργο-κεντρικών επιχειρήσεων εξελίσσεται από την επιχείρηση με επίκεντρο την παραγωγή σε μια επιχειρηματική δραστηριότητα που εστιάζεται στον άνθρωπο. Στην πραγματικότητα, σήμερα επικεντρώνεται συνεχώς στους εργαζόμενους, τους προμηθευτές και τους πελάτες, ενισχύοντας τις σχέσεις και τις συνεργασίες μεταξύ του δικτύου που δημιουργήθηκε γύρω από το σενάριο ενός έργου. Παρόλη τη ταχύτητα των αλλαγών, οι διαχειριστές του έργου και οι ηγέτες των επιχειρήσεων πρέπει να γνωρίζουν τις καινοτομίες και η προληπτική στάση είναι πάντα πιο αναγκαία.

Δεν μπορούν να περιμένουν έως ότου οι νέες τεχνολογίες επηρεάσουν την υφή των εταιρειών για να προσδιορίσουν ποια είναι η αξία μιας επένδυσης. Επιπλέον, για να έχουμε μια σωστή ιδέα σχετικά με τις μελλοντικές τεχνολογίες, είναι απαραίτητη μια εκ των προτέρων μελέτη και ανάλυση, σχετικά με το οικονομικό δυναμικό και την ικανότητα να διαταράξει την πραγματική αγορά. Και οι δύο πτυχές σχετίζονται αυστηρά με μια μετατόπιση του ενδιαφέροντος μέσα στις βιομηχανίες για το τι αφορά η υιοθέτηση νέων τεχνολογιών και παράλληλα που εστιάζουν οι ικανότητες των διευθυντών έργων κατά τη διαχείριση μίας σύνθετης κατάστασης (Thomas. J. et al, 2004).

## B.4. IoT και Περιβάλλον Διαχείρισης Έργων

Παρά το γεγονός ότι οι ερευνητές και οι επαγγελματίες ανακαλύπτουν ακόμη τις δυνατότητες του IoT (Saariko T., et al, 2007), η τεχνολογία αποτελεί μια συγκεκριμένη ευκαιρία για μια εταιρία και, αν και όχι εξ ολοκλήρου, αναγνωρίζονται τα οφέλη από την εφαρμογή της στην κουλτούρα της εταιρείας. Το περιβάλλον του IoT χαρακτηρίζεται από αισθητήρες και ενεργοποιητές που σχετίζονται άμεσα με φυσικά αντικείμενα. Χρησιμοποιούνται για την αποκάλυψη διαφορετικών χαρακτηριστικών σχετικά με τους στόχους και η χρήση τους είναι απεριόριστη.

Τα δημιουργημένα δίκτυα ενισχύουν τους υπάρχοντες τεράστιους όγκους δεδομένων που ρέουν σε κεντρικούς εξυπηρετητές για περαιτέρω ανάλυση και συσχετισμούς. Το σύστημα, στο οποίο τα αντικείμενα μπορούν να αντιληφθούν και να επικοινωνήσουν με τον εαυτό τους και με το περιβάλλον, αποτελεί ένα κρίσιμο εργαλείο για την κατανόηση της πολυπλοκότητας και την επεξεργασία των γρήγορων απαντήσεων (Porter, M.E. & Heppelmann, J.E. , 2014). Τέτοιου είδους διαδραστικές εγκαταστάσεις, διαθέσιμες κατά απαίτηση, είναι κατάλληλες για την υποστήριξη επιχειρήσεων που είναι έργο-κεντρικές και, επιπλέον, για την ανάπτυξή τους.

Το IoT προσφέρει τη δυνατότητα να επηρεάσει διαφορετικές οικονομικές δραστηριότητες και βιομηχανίες, παρέχοντας μια σταθερή βάση για τα νέα επιχειρηματικά μοντέλα της αγοράς. Καθορισμένο ως ένα πανταχού παρόν δίκτυο, το IoT θα επηρεάσει επίσης τις έργο-κεντρικές εταιρείες που αντιπροσωπεύουν σήμερα το ευρύτερο τμήμα των εταιρειών. Η παρακάτω εικόνα παρουσιάζει τις έξι πιο σημαντικές επιδράσεις του IoT στις αρχές της διαχείρισης έργων.

*Εικόνα 30: 6 επιπτώσεις του IoT στην Διαχείριση Έργων*

Έτσι είναι λογικό να εξεταστεί ο αντίκτυπος της τεχνολογίας του IoT στις εταιρείες ως ριζική αλλαγή. Στην πραγματικότητα, η νέα αυτή εξέλιξη θα επηρεάσει όλες τις δραστηριότητες σε όλη την εταιρεία, επηρεάζοντας έτσι τις στρατηγικές αποφάσεις, τις επενδύσεις και την παραγωγικότητα *(Kortuem, G. et al, 2010)*.

Ένα καλό παράδειγμα βελτίωσης της αποτελεσματικότητας και της παραγωγικότητας είναι η περίπτωση της εταιρίας Stanley Black & Decker. Η εταιρεία αυτή εγκατέστησε ετικέτες RFID σε πολλά και σημαντικά κατασκευαστικά υλικά για τη συλλογή δεδομένων σε πραγματικό χρόνο. Αυτές οι πληροφορίες χρησιμοποιήθηκαν από τους εργαζόμενους, τους προϊσταμένους και τους διαχειριστές για να αποφασίσουν περαιτέρω βήματα των ενεργειών παραγωγής και διόρθωσης, εάν κρίνανε απαραίτητο.

Η χρήση της νέας τεχνολογίας προσέφερε τεράστια συμβολή στις υπηρεσίες των πελατών και στη διαχείριση των παραδόσεων (Fleisch E, 2018). Ένα άλλο παράδειγμα είναι η συνεργατική κατασκευή. Εκεί, οι τεχνολογίες Πληροφορικής/Επικοινωνιών (ICT) και η IoT υποστηρίζουν ένα βρόχο ανατροφοδοτήσεων χωρίς διαλείμματα μεταξύ κάθε τμήματος και των ρόλων που απασχολούνται στα έργα: σχεδιαστές προϊόντων, μηχανικοί, παραγωγή και εξυπηρέτηση πελατών.

Η αύξηση της πολυπλοκότητας των διαδικασιών και του τρόπου διαχείρισης των έργων στην πραγματική αγορά φέρνει στοιχεία αλυσιδωτών αλλαγών στο επιχειρησιακό περιβάλλον. Ο αριθμός των εμπλεκόμενων φορέων σε κάθε έργο αυξάνεται δραματικά, η ανταλλαγή πληροφοριών και επικοινωνίας είναι ζωτικής σημασίας για την επιτυχία του έργου και η αβεβαιότητα του περιβάλλοντος καθιστά τις προκλήσεις πολύ πιο δύσκολες και περίπλοκες για τη διαχείριση του. Είναι η κοινή σκέψη του καθενός ότι η διαχείριση έργων εμπλέκοντας διαφορετικές ομάδες, που βρίσκονται συχνά σε απομακρυσμένες τοποθεσίες, θα αντιμετωπίσει πολλές αποκλίσεις από το αρχικό σχέδιο του έργου (Atzori, L. et al, 2010).

Για τον παραπάνω λόγο, είναι σημαντικό να προσδιοριστούν οι καταστάσεις και οι συνθήκες που ενεργοποιούνται στις διάφορες φάσεις της εκτέλεσης του έργου και να παρέχεται έξυπνη υποστήριξη, βασισμένη στη στρατηγική διαχείριση και ανάλυση δεδομένων (Atzori et al., 2010). Επιπλέον, κρίσιμα επιχειρησιακά προβλήματα δεν επιλύονται με την εφαρμογή τεχνικών και λειτουργικών δεξιοτήτων, αλλά χρειάζεται να ληφθούν υπόψη οι πολυπλοκότητες των διαπροσωπικών διαδικασιών (Smith, B. & Dodds, B., 1997). Επιπλέον, θεωρώντας ένα έργο ως κοινό στόχο μεταξύ διαφόρων φορέων που καλούνται ενδιαφερόμενοι, ο συντονισμός μεταξύ όλων των μερών είναι θεμελιώδους σημασίας για την τελική επιτυχία της προσπάθειας.

Το IoT ενισχύει την ανάγκη σύναψης σχέσεων μεταξύ των εμπλεκομένων, σε μεγαλύτερη κλίμακα από οποιοδήποτε άλλο πληροφοριακό σύστημα, υποστηρίζοντας διαφορετικές διαπροσωπικές διαδικασίες. Η αυξημένη συνδεσιμότητα μεταξύ όλων των εμπλεκόμενων μερών και γενικά των ενδιαφερόμενων μερών θα πρέπει να επιτρέπει αποτελεσματικό και γρήγορο εντοπισμό των ζητημάτων. Μετά την αναγνώριση αυτών των ζητημάτων, το σύστημα υποστηρίζει τη διάγνωση και τις μελλοντικές διορθωτικές ενέργειες (Fleisch E, 2018). Αυτό το όφελος είναι ζωτικής σημασίας, και με έναν δομημένο συντονισμό του δικτύου IoT, τα συστήματα θα πρέπει να διαμορφώνονται και να συνεργάζονται με ελάχιστο αριθμό απαιτήσεων.

Συνδυασμένα, αυτά τα στοιχεία θα μπορούσαν να χρησιμοποιηθούν για την επίτευξη μεγαλύτερης αποτελεσματικότητας, αποδοτικότητας και ικανοποίησης (Fleisch E, 2018). Το IoT συμβάλλει στον προσδιορισμό της σημασίας των πληροφοριών που συλλέγονται, παρέχοντας μια λύση σε πραγματικό χρόνο και υποστηρίζοντας τη λήψη αποφάσεων σε πραγματικό χρόνο σε ένα ετερογενές, εξαιρετικά δυναμικό περιβάλλον (Atzori, L. et al, 2010).

### Β.4.1. Σημαντικότερες αλλαγές στη Διοίκηση Έργων

Η εμπορική εφαρμογή του IoT σίγουρα αυξάνεται έστω και με αργούς ρυθμούς, και θα αυξηθεί με μεγαλύτερη ταχύτητα μόλις ο χώρος του IoT φθάσει σε μεγαλύτερο βαθμό ωριμότητας. Για πολλές από αυτές τις συσκευές που θα συνδεθούν στο διαδίκτυο, θα ξεκινήσουν σχετικά έργα και θα ανατεθούν στους υπεύθυνους των έργων για να τα διεκπεραιώσουν με επιτυχία. Οι Υπεύθυνοι Έργων θα πρέπει να ξεπεράσουν τα νέα εμπόδια που θα προκαλέσει η επικράτηση του IoT. Επίσης, θα πρέπει να είναι περισσότερο αποτελεσματικοί για την αντιμετώπιση αυτών των έργων.

Οι άνθρωποι που θα έχουν την πρωτοπορία της εφαρμογής των IoT καινοτομιών, αυτή τη στιγμή είναι αρκετά νέοι στον χώρο του IoT. Οι Υπεύθυνοι Έργων συνήθως δεν έχουν πολυετή εμπειρία (αν υπάρχει) που να σχετίζεται ειδικά με τα προγράμματα IoT. Ωστόσο, η ζήτηση για εφαρμογή του IoT θα δημιουργήσει μια νέα κατεύθυνση για τους Υπεύθυνους Έργων που έχουν την πείρα και την εμπειρία να δουλεύουν με το IoT.

Υπάρχουν ουσιαστικά δύο τρόποι με τους οποίους το IoT θα επηρεάσει τη διαχείριση του έργου. Ο πρώτος τρόπος, όπως προαναφέρθηκε, είναι ότι θα προσφέρει μεγαλύτερη αποτελεσματικότητα στους Υπεύθυνους Έργων. Ο δεύτερος θα είναι νέοι προβληματισμοί για τους Υπεύθυνους Έργων που θα κληθούν να διαχειριστούν σχετικά με το IoT. Με την

ωρίμανση του IoT, ορισμένα από αυτά τα ζητήματα θα αυξηθούν σε εύρος και κλίμακα, ενώ ορισμένοι από αυτούς τους προβληματισμούς θα μπορούσαν αυτόματα να εξαλειφθούν καθώς επεκτείνεται η καινοτομία της τεχνολογίας. Επίσης, ο τρόπος με τον οποίο οι υπεύθυνοι έργων εργάζονται θα υποβληθεί σε σημαντική αλλαγή.

Η δυνατότητα μεγάλου όγκου δεδομένων θα οδηγήσει σε βελτιωμένες αναλύσεις

Οι υπεύθυνοι έργων θα επωφεληθούν από τον πολλαπλασιασμό των σημείων δεδομένων από τα οποία μπορούν να συλλέξουν πληροφορίες. Με την αύξηση των συνδεδεμένων συσκευών και την παραγωγή μεγάλου όγκου δεδομένων, τα έργα θα παρουσιάσουν αύξηση τόσο των ποιοτικών όσο και των ποσοτικών σχετικών δεδομένων από τα οποία θα ληφθούν αποφάσεις. Αυτά τα δεδομένα μπορούν στη συνέχεια να ενσωματωθούν σε ένα επιχειρησιακό σύστημα όπως μια πλατφόρμα προγραμματισμού επιχειρησιακών πόρων (Enterprise Resource Planning - ERP) ή ένα εργαλείο διαχείρισης έργου.

Οι έξυπνες εταιρείες θα χρησιμοποιήσουν αυτά τα δεδομένα με σύνεση για να λάβουν αποφάσεις με βάση την εμπειρική αξία των αποτελεσμάτων. Η αναφορά της προόδου και η ακρίβεια της εκτίμησης θα αυξηθούν από ευρύτερα, μετρήσιμα σημεία δεδομένων. Επιπλέον, καθώς το IoT ωριμάζει, τα δεδομένα που επιστρέφονται από τους αισθητήρες θα αυξήσουν εκουσίως την αξία για καταναλωτικές και εμπορικές εφαρμογές.

Αυτή η μακρόχρονη ροή δεδομένων θα παρέχει στις εταιρείες μια πλούσια σειρά από ποσοτικά στοιχεία που θα τους βοηθήσουν να μετρήσουν και να αξιολογήσουν όχι μόνο τα τρέχοντα μέτρα ποιότητας και απόδοσης, αλλά θα τους επιτρέψουν να προβλέψουν τις επιδόσεις στο μέλλον.

Η φάση των δοκιμών σε ένα έργο θα απαιτήσει μεγαλύτερο πλαίσιο πληροφοριών

Παρόλο που οι δοκιμές σε πιο παραδοσιακά έργα έχουν συμπεριλάβει ιδιαιτερότητες όπως οι προσομοιώσεις ακραίων καταστάσεων για να εξασφαλίσουν ότι οι πραγματικοί όγκοι επιχειρήσεων δεν θα αλλοιώσουν ένα σύστημα, το IoT θα απαιτήσει πολύ μεγαλύτερο βαθμό «δοκιμών υπό πλαίσιο». Για παράδειγμα, μπορεί κανείς να δει μια σειρά συσκευών με δυνατότητα IoT που μπορούν να δοκιμαστούν σε εργαστηριακό περιβάλλον υπό κανονικές συνθήκες. Αλλά όταν οι συσκευές αυτές τοποθετούνται στο πεδίο, οι συνθήκες μπορεί να είναι πολύ διαφορετικές από εκείνες που βρίσκονται σε εργαστηριακό περιβάλλον.

Αν ένας αισθητήρας ενσωματωμένος σε φάρο μπορεί εύκολα να περάσει από έλεγχο όταν δοκιμάζεται εντός ενός ελεγχόμενου περιβάλλοντος, τι συμβαίνει όταν ο συγκεκριμένος

φάρος βρίσκεται σε ένα άγονο βράχο (πχ στη Πολική Ζώνη), όπου οι συνθήκες είναι πιο κατάλληλες για ζώα της πολικής ζώνης παρά για ανθρώπους; Οι Υπεύθυνοι Έργων θα πρέπει να επανεξετάσουν τα σενάρια δοκιμών για να εξασφαλίσουν ότι επιτυγχάνουν τις κατάλληλες ρυθμίσεις στη πραγματική εφαρμογή.

Τα εργαλεία που χρησιμοποιούνται από τους Υπεύθυνους Έργων θα αλλάξουν

Για παράδειγμα, το Microsoft Project είναι από καιρό ένα αδιαμφισβήτητα απαραίτητο εργαλείο για τους Υπεύθυνους Έργων για το σχεδιασμό πόρων και το προγραμματισμό του έργου. Ανεξάρτητα από τη προτίμηση προς κάποιο εργαλείο διαχείρισης έργων, το IoT θα επιβάλλει σημαντικές αλλαγές σε εργαλεία όπως το Microsoft Project.

Δεδομένου ότι τα δεδομένα σε πραγματικό χρόνο διατίθενται στους Υπεύθυνους Έργων, η αυτοματοποίηση προηγουμένως δαπανηρών διοικητικών εργασιών θα αλλάξει τη δυναμική μεταξύ του Project Manager και των εργαλείων του / της. Η πορεία και η εμβέλεια αυτής της αλλαγής δεν είναι ακόμη πλήρως ξεκάθαρη, αλλά στους προσεχείς μήνες και χρόνια τα εργαλεία που χρησιμοποιούνται από τα μέλη του IoT θα εξελιχθούν καθώς αυξάνεται η διεισδυτικότητα του IoT.

Αλλαγές στο Συνεργατικό Πλαίσιο – κατάργηση διαχωριστικών γραμμών

Ακόμη και σε ένα μοντέλο Software as a Service (SaaS), όπου η υποδομή και το λογισμικό μπορεί να μην φιλοξενούνται εσωτερικά, εξακολουθεί να υπάρχει ανάγκη συνεργασίας μεταξύ του παρόχου και του πελάτη, καθώς πιθανόν θα απαιτηθούν σημεία ολοκλήρωσης και τροφοδοσίες συστήματος. Επίσης, τα τμήματα που λειτουργούν ανεξάρτητα μέσα στην ίδια την επιχείρηση θα πρέπει να αναδιοργανωθούν, καθώς το IoT φέρνει μαζί του την ανάγκη μεγαλύτερης συγχώνευσης μεταξύ των πολύ συχνά αντίθετων περιοχών της Πληροφορικής.

Με όλες τις διαδικασίες ενσωμάτωσης και υλοποίησης που απαιτούνται για ένα έργο IoT, τις πολλές συσκευές του και τα σημεία σύνδεσης των εσωτερικών συστημάτων τους, η συνεργασία δεν θα είναι απλώς προαιρετική αλλά ένα κρίσιμο στοιχείο για το έργο και την επιχειρησιακή επιτυχία.

Διευρύνεται ο ρόλος του Υπεύθυνου Έργων σε ειδικό του IoT

Ένα από τα εμπόδια που προκύπτουν από το χώρο του IoT είναι ότι θα χρειαστεί οι υπεύθυνοι έργων να κατευθύνουν τις εξελίξεις του IoT που θα προκύψουν αναπόφευκτα, ειδικά για τις μεγαλύτερες εταιρείες. Ως εκ τούτου, οι Υπεύθυνοι Έργων θα είναι στην πρώτη

γραμμή και θα πρέπει να μάθουν τα μέσα και τους στόχους της τεχνολογίας. Αυτό τους θέτει σε ισχυρή θέση να είναι υποστηρικτές και ειδικοί σε αυτό τον τομέα.

Οι υπεύθυνοι έργων, που ενδιαφέρονται έντονα και χρειάζονται ακριβή και μετρήσιμα στοιχεία, θα κατευθύνουν τις εξελίξεις στο νέο τοπίο του IoT. Η ικανότητά τους να αποκτούν δεδομένα πιο γρήγορα και να είναι πιο ακριβή σημαίνει ότι οι ρόλοι τους καθίστανται ολοένα και πιο σημαντικοί στη πορεία του χρόνου.

Και μέχρις ότου οι υπόλοιπες ομάδες να εξοικειωθούν με τα προγράμματα IoT, οι Διαχειριστές Έργων θα αποτελέσουν καθοδηγητική δύναμη για την κατανόηση των έργων IoT, των τελικών στόχων και της αποτελεσματικότητάς τους. Οι υπεύθυνοι έργων που είναι ευέλικτοι και ικανοί να προσαρμοστούν θα είναι πιθανό να οδηγήσουν την επόμενη γενιά έργων IoT.

Απαιτούνται νέα πρότυπα διαλειτουργικότητας και συμβατότητας

Ενώ το IoT έχει τη δυνατότητα να δημιουργήσει πληθώρα δεδομένων για χρήση από τις εταιρείες, εγείρει επίσης το ζήτημα της διαλειτουργικότητας. Όπως και με κάθε νέα τεχνολογία, η βιομηχανία IoT και οι κατασκευαστές συσκευών IoT δεν έχουν ακόμη καθορίσει σταθερά τα πρότυπα που είναι απαραίτητα για τη διασφάλιση της διαλειτουργικότητας και της συμβατότητας. Μέχρι να εδραιωθούν αυτά τα πρότυπα, θα αντιμετωπίζεται μια κατάσταση όπου τα δεδομένα που μετακινούνται από τα εργαλεία ανάλυσης ενός οργανισμού στα εργαλεία ενός άλλου θα είναι ακατανόητα.

Θέματα Ασφάλειας

Μία από τις μεγαλύτερες ανησυχίες που ανακύπτουν γύρω από το IoT είναι η ασφάλεια. Οι κυβερνοεπιθέσεις (πχ. η επίθεση Dyn DDoS) συχνά είναι αποτέλεσμα πολλών συσκευών με δυνατότητα IoT που υπονομεύονται κακόβουλα και μετατρέπονται σε botnets που πλημμυρίζουν και καταστρέφουν στόχους στο διαδίκτυο. Οι προβλέψεις δείχνουν ότι μεγαλύτερα κεφάλαια θα διατεθούν για την ασφάλεια στον κυβερνοχώρο.

Οι Υπεύθυνοι Έργων θα πρέπει να διασφαλίσουν ότι γίνονται οι κατάλληλες προβλέψεις για τη σταθεροποίηση της ασφάλειας οποιωνδήποτε συσκευών με δυνατότητα IoT σε έργα που υλοποιούνται. Θα πρέπει να εκτελεστούν πλήρεις έλεγχοι ασφαλείας για όλες τις ενεργοποιημένες συσκευές, ώστε να διασφαλιστεί τόσο η ασφάλεια όσο και η εμπιστοσύνη των ενδιαφερομένων μερών. Θα είναι ευθύνη των Υπεύθυνων Έργων να διασφαλίσουν ότι

αυτή η αυστηρότητα και η πειθαρχία θα εφαρμοστεί σε κάθε έργο του IoT, όχι ως δευτερεύουσα σκέψη, αλλά ως βασικό στοιχείο του σχεδιασμού.

Στις επόμενες ενότητες παρουσιάζουμε την εφαρμογή του IoT σε έργο-κεντρικές επιχειρήσεις και οργανισμούς, τις προκλήσεις και τα οφέλη, όπως και την επίπτωση στον ρόλο του Υπεύθυνου Έργου.

### Β.4.2. Έργο-κεντρικός οργανισμός και IoT

Οι εταιρείες πετρελαίου και φυσικού αερίου, οι εξορυκτικές βιομηχανίες ή οι επιχειρήσεις ενέργειας, οι οποίες ανήκουν σε κλάδους προσανατολισμένους στα έργα, θα ενισχυθούν δραστικά με την εφαρμογή του IoT. Στο συγκεκριμένο επιχειρηματικό περιβάλλον, πρέπει να αντιμετωπιστούν οι διάφορες προκλήσεις και να αντιμετωπιστούν μία σειρά από ζητήματα για να εξασφαλιστεί η εφαρμογή της τεχνολογίας IoT. Τόσο οι τεχνολογικές όσο και οι κοινωνικές πτυχές θα πρέπει να γίνουν κατανοητές πριν γίνει ευρεία η αποδοχή της εφαρμογής του IoT.

Λαμβάνοντας υπόψη μεγάλα έργα όπως η κατασκευή υπεράκτιων έργων, έργα εξόρυξης ή εκσκαφής, ο αριθμός των εργαζομένων και ο αριθμός των εταιριών που συμμετέχουν κατά τη διάρκεια του κύκλου ζωής των έργων είναι τεράστιος. Πολύ δύσκολα, θα συνδεθούν στο ίδιο πληροφοριακό σύστημα και θα έχουν πρόσβαση στα ίδια έγγραφα.

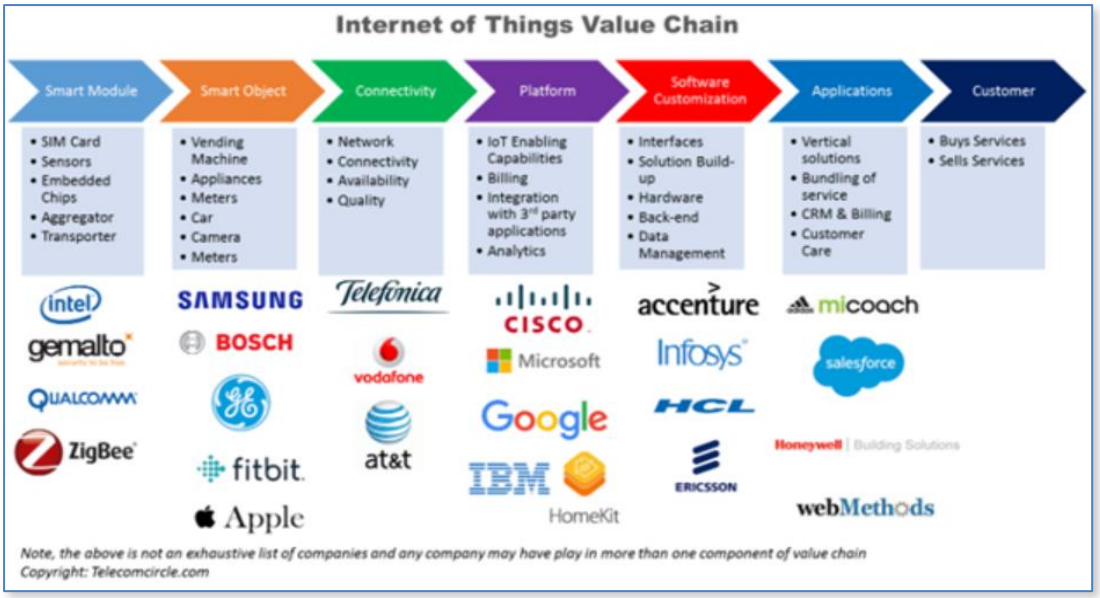
Κάθε μία από τις εμπλεκόμενες οντότητες θα χρησιμοποιήσει ένα κατάλληλο λογισμικό και προσωπικά έγγραφα που θα κοινοποιούνται μεταξύ των ομάδων σε περίπτωση ανάγκης, αλλά η συνεργασία θα σταματήσει σε αυτό το στάδιο. Είναι επίσης αναμενόμενο οι ομάδες να εργάζονται σε αρχεία που έχουν διαφορετική κατάληξη και ορισμένες φορές οι ενέργειες από κοινού είναι δύσκολες και ίσως όχι με πετυχημένη κατάληξη.

Επομένως, η διαλειτουργικότητα και η διασύνδεση αποτελούν το κεντρικό κρίσιμο σημείο για την υιοθέτηση του IoT σε έργο-κεντρικό περιβάλλον. Είναι σημαντικό, κατά τη φάση του σχεδιασμού και τη φάση της εγκατάστασης ή παραμετροποίησης, να εξασφαλιστεί υψηλό επίπεδο προσαρμογής μεταξύ των διαφόρων κόμβων του συστήματος, ενισχύοντας την αυτόνομη συμπεριφορά των διαφόρων μερών.

Οι μηχανές συνεχούς παρακολούθησης παρακολουθούν συνεχώς το περιβάλλον μέσω αισθητήρων και λαμβάνουν δυναμικά αποφάσεις και πραγματοποιούν συνεκτικές αλλαγές

σε πραγματικό χρόνο, δεδομένων των περιβαλλοντικών συνθηκών και των προτιμήσεων των καταναλωτών ή άλλων ενδιαφερομένων.

*Εικόνα 31: Αλυσίδα αξιών του IoT (πηγή: https://www.acgcc.com/wp-content/uploads/2017/10/Food-chai.png)*




Οι Porter και Heppelmann (2014) βλέπουν ένα εκθετικό κέρδος στην παραγωγικότητα και βελτιώσεις στις προσεγγίσεις διαχείρισης έργων και στις διαδικασίες αλυσίδας αξιών (Εικόνα 31). Η υλοποίηση του IoT σε ένα τέτοιο έργο-κεντρικό περιβάλλον θα αυξήσει την εγρήγορση και θα υποστηρίξει την ταχύτερη λήψη αποφάσεων από τους εμπλεκόμενους φορείς (Atzori, L. et al, 2010).

Σε γενικές γραμμές, η πρόσβαση σε μία περισσότερο περιεκτική πηγή δεδομένων και πληροφοριών θα μπορούσε να διευκολύνει τις μεγάλες αλλαγές και βελτιώσεις των επιπτώσεων σε κάθε φάση του κύκλου ζωής ενός έργου (Saariko T., et al, 2007). Η αύξηση της εγρήγορσης αποτελεί βασικό πλεονέκτημα του IoT για το σύγχρονο επιχειρηματικό μοντέλο μέσα σε έναν οργανισμό με έργο-κεντρικό προσανατολισμό, ωθεί τον Υπεύθυνο του Έργου να λαμβάνει πιο ενημερωμένες αποφάσεις.

Τα προβλήματα του IoT δεν σχετίζονται αποκλειστικά με την αλληλεπίδραση εντός του περιβάλλοντος και των ενδιαφερομένων. Οι πτυχές δικτύωσης είναι καθοριστικής σημασίας. Στην πραγματικότητα, όλα τα στοιχεία που συνθέτουν τη δομή του IoT σε ένα Έργο, όπως το RFID και τα ασύρματα αντικείμενα, απασχολούν λίγους πόρους από πλευράς υπολογιστικής ισχύος και ενεργειακής ικανότητας. Όλες οι πιθανές λύσεις πρέπει να λαμβάνουν υπόψη την

αποδοτικότητα των πόρων του συνόλου του συστήματος και την πιθανή κλιμάκωση των προβλημάτων (Ferreira Da Silva, F., & Oliveira & Sa, J., 2016).

### Β.4.3. Εφαρμογή του IoT σε Έργο-Κεντρικό Περιβάλλον

Τα σύγχρονα συστήματα πληροφορικής παρέχουν χρήσιμα μέσα για την επέκταση του διαδραστικού μαθησιακού περιβάλλοντος από απόσταση. Επιτρέπουν το διάλογο μεταξύ των μερών και την ενίσχυση της επικοινωνίας κάνοντας τη διαχείριση των έργο πιο ευέλικτη (Smith, B. & Dodds, B., 1997). Ειδικότερα, η τεχνολογία IoT θα αναβαθμίσει το διασυνδεδεμένο σύστημα.

Όλη η πτυχή επικοινωνίας που σχετίζεται με μια διαδικασία διαχείρισης έργου ενισχύεται από την ενημέρωση και την κοινή χρήση του νέου δικτύου σε πραγματικό χρόνο. Θα εξασφαλίσει απτά οφέλη σε όλο το επιχειρηματικό περιβάλλον, την κοινωνία, τα άτομα και το επιχειρηματικό μοντέλο γενικά, δημιουργώντας μια αποτελεσματική διαδικασία για την ανύψωση της διαδικασίας λήψης αποφάσεων σε ένα επίπεδο εγρήγορσης.

Πολλές εφαρμογές θα δημιουργηθούν χάρη στις απεριόριστες δυνατότητες υποστήριξης που μπορεί να παρέχει η ψηφιακή πλατφόρμα. Η ενίσχυση των μεθοδολογιών εκτέλεσης των έργων θα επηρεάσει την κοινωνική ζωή. Θα προσφέρει απτά οφέλη στη διαχείριση του περιβάλλοντος, στις κοινωνικές σχέσεις, τα άτομα και τις επιχειρήσεις με το προγραμματισμό και σχεδιασμό καινοτόμων υπηρεσιών και προϊόντων από διάφορους τομείς (Kortuem, G. et al, 2010).

Για παράδειγμα, η διαθεσιμότητα προς τον χρήστη διαδραστικών πολυμέσων και περιεχομένου ανά πάσα στιγμή είναι αυτός διαθέσιμος δημιουργεί σημαντικές αλλαγές στη διαδικασία μάθησης και τις προσεγγίσεις εκπαίδευσης που υιοθετούνται από τους οργανισμούς.

Ένας έργο-κεντρικός οργανισμός, έχοντας ευελιξία όσον αφορά τις λειτουργικές του διαδικασίες και μεθοδολογίες που συνδέονται άμεσα με το σύγχρονο πνεύμα της αγοράς, βρίσκεται στην πρώτη γραμμή εισαγωγής νέων θεωριών και εφαρμογής νέων τεχνολογιών. Επιπλέον, μια μεγάλη διαφορά που μπορεί να κάνει η τεχνολογία IoT είναι η δυνατότητα να εξασφαλίσει μια διαρκή διαδικασία μάθησης που προκύπτει με βάση μέρος των αποτελεσμάτων των δραστηριοτήτων του έργου.

Επιπλέον, επιτρέπει τη διαδραστική πρόσβαση στη βάση δεδομένων στο στάδιο όπου ξεκινούν νέα έργα. Έτσι, τα αποτελέσματα των έργων μπορούν να επιτευχθούν, να ληφθούν, να αναλυθούν και να χρησιμοποιηθούν ευρέως εντός του οργανισμού. Αυτό, με τη σειρά του, θα βοηθήσει τους οργανισμούς να βελτιώσουν την ανταπόκρισή τους στις μεταβαλλόμενες επιχειρηματικές ανάγκες.

### Β.4.4. Προκλήσεις εφαρμογής του IoT σε Έργο-Κεντρικό Περιβάλλον

Χαρακτηριστικό γνώρισμα των πρόσφατων μετατοπίσεων ή αλλαγών στον τρόπο υλοποίησης έργων είναι ο μεγάλος αριθμός φραγμών που προηγούνται της εγκατάστασης μίας νέας τεχνολογίας ή υπηρεσίας. Τα εμπόδια συνδέονται στενά με τη σημασία της εφαρμογής. Στην πραγματικότητα, οι βαθιές αλλαγές στην κουλτούρα της εταιρείας πρέπει να ξεπεράσουν αυστηρότερα εμπόδια από μια μικρή αλλαγή. Πράγματι ζητήματα που σχετίζονται με την εφαρμογή του IoT συνδέονται στενά με διάφορους τομείς: τον τεχνολογικό τομέα και τον τομέα της εταιρικής κουλτούρας.

Οι πιο σημαντικές προκλήσεις και φραγμοί στην εφαρμογή των τεχνολογιών IoT σε μια επιχείρηση είναι ο ρυθμός με τον οποίο υιοθετεί νέες τεχνολογίες. Η ανάγκη του IoT σχεδιάστηκε από τις ανάγκες των μεγάλων οργανισμών να βελτιώσουν τον τρόπο με τον οποίο συλλέγουν δεδομένα, διαχειρίζονται τις επιχειρηματικές τους διαδικασίες και παρακολουθούν τα προϊόντα τους.

Ωστόσο, καθώς οι καταναλωτές υιοθετούν αυτή την τεχνολογία με αργό ρυθμό, η περιορισμένη λειτουργικότητα της τεχνολογίας αποτελεί επίσης εμπόδιο στην υιοθέτησή της, για παράδειγμα οι τεχνολογίες που τοποθετούνται πάνω στο ανθρώπινο σώμα (wearables). Τα τεχνολογικά ζητήματα σχετίζονται με τον καθορισμό κοινών προτύπων για τις διάφορες τεχνολογίες που αποτελούν βασικά συστατικά του οικοσυστήματος του IoT. Κοινά πρότυπα για τα φυσικά και εικονικά μέρη πρέπει να επιλυθούν προκειμένου να επιτευχθεί ένα κοινό έδαφος για την κατασκευή της πλατφόρμας.

Η διαλειτουργικότητα είναι επίσης ένα τεράστιο πρόβλημα που πρέπει να ξεπεραστεί. Στην πραγματικότητα, διαφορετικές εταιρείες συνεργάζονται μέσα στο ίδιο οικοσύστημα για να δημιουργήσουν μια πιο σημαντική και πλήρη πλατφόρμα. Αυτό γιατί δεν εξασφαλίζεται η συμβατότητα των διαφόρων προτύπων που χρησιμοποιεί ο ενδιαφερόμενος και τα προβλήματα των διαφορετικών τύπων αρχείων είναι κοινά. Η ενίσχυση και επιτάχυνση με τα κατάλληλα υπολογιστικά εργαλεία υποστήριξης της επικοινωνίας σε ένα οργανισμό και η

αύξηση της ικανότητας ανταλλαγής δεδομένων με εσωτερικές και εξωτερικές ομάδες, σιωπηρά μια «αίσθηση εμπιστοσύνης» μεταξύ των ενεργά εμπλεκόμενων μερών είναι αναγκαία για την εφαρμογή και την απόλυτη χρήση των νέων τεχνολογιών.

Μια άλλη ιδιαίτερα εξεταζόμενη μεταβλητή εντός του IoT που αποτελεί σημαντικό εμπόδιο για την εφαρμογή είναι τα επίπεδα ασφαλείας των δεδομένων που συγκρατούνται στους αισθητήρες και τις ετικέτες RFID. Επίσης, σημειώνεται ότι σήμερα δεν τίθενται ζητήματα κανονισμών και προστασίας της ιδιωτικής ζωής στη φάση συλλογής δεδομένων του IoT.

Ένα άλλο εμπόδιο που αντιμετωπίζουν σήμερα οι οργανισμοί είναι το υψηλό κόστος της εφαρμογής του IoT στον οργανισμό και η δυνατότητα να χειριστεί όλα τα δεδομένα που συλλέγονται και αναλύονται στο χώρο αποθήκευσης που βρίσκεται στο cloud. Η υποδομή του οργανισμού μπορεί επίσης να λειτουργήσει ως εμπόδιο στην υλοποίηση και συνεπώς να αυξήσει το κόστος που συνδέεται με την τεχνολογία. Επιπλέον, η δομή της εταιρείας είναι ένας άλλος πιθανός μοχλός επιτυχούς ή αποτυχημένης υλοποίησης του IoT.

Στην πραγματικότητα, οι μικρές επιχειρήσεις δέχονται πιο εύκολα τις αλλαγές λόγω της ευελιξίας και της λιγότερο τυποποιημένης τους δομής. Στην περίπτωσή τους, η εφαρμογή νέων τεχνολογιών θα κρίνει τη βιωσιμότητα τους: στο εγγύς μέλλον, η εφαρμογή του IoT θα αποτελέσει το κατώτατο όριο για να παραμείνει μία μικρομεσαία επιχείρηση ενεργή στην αγορά, και όχι πλέον ως ένα εργαλείο για να αποκτήσει ανταγωνιστικό πλεονέκτημα έναντι των ανταγωνιστών. Οι παλαιότερες κατασκευαστικές εταιρείες είναι πραγματικά δομημένες και είναι κολλημένες στα παλιά τους πρότυπα. Η αποδοχή του οικοσυστήματος IoT θα άλλαζε ολόκληρη την αλυσίδα αξίας της εταιρείας.

Στις μεγάλες επιχειρήσεις, οι επενδύσεις που σχετίζονται με την υλοποίηση του IoT δεν επηρεάζουν μόνο σημαντικά τα οικονομικά μεγέθη αλλά και την οργανωτική δομή. Με μικρότερη προδιάθεση για κινδύνους και επιχειρηματικές ενέργειες, η κουλτούρα της "αξίας ή όχι" είναι βαθιά ριζωμένη στην εταιρεία.

Η ύπαρξη μιας αδύναμης ή ανεπτυγμένης υποδομής σε έναν οργανισμό επηρεάζει επίσης την εφαρμογή τεχνολογιών IoT με τέτοιο τρόπο ώστε οι τρέχουσες ροές εργασίας ή ροές διεργασιών που τίθενται σε κίνηση στην οργάνωση δεν είναι καλά καθορισμένες ή ενσωματωμένες, περιορίζοντας έτσι την τεχνολογία ώστε να λειτουργήσει επαρκώς.

Αναφορικά με προβλήματα που σχετίζονται με μια επιχείρηση με έργο-κεντρικό προσανατολισμό, είναι σημαντικό να επισημανθούν τα θέματα που σχετίζονται με την αποκάλυψη ευαίσθητων δεδομένων, τόσο εσωτερικά στην ομάδα του έργου ή σε τμήμα της

εταιρείας, όσο και εξωτερικά με όλο το περιβάλλον των εμπλεκόμενων φορέων. Είναι κρίσιμο να διασφαλιστεί ότι οι σωστές πληροφορίες θα μοιραστούν με τις κατάλληλες οντότητες για να διατηρηθεί μια τέλεια ισορροπία στο εσωτερικό του έργου όσον αφορά τους ρόλους και τους αριθμούς.

Στην πραγματικότητα, έχει φανεί ότι η διαγραφή δήθεν περιττών πληροφοριών επιδεινώνει τον κύκλο ζωής του έργου. Αυτό έχει ως συνέπεια μεγάλη απώλεια ελέγχου σχετικά με την κατάσταση της κάθε φάσης και τη διαδικασία λήψης αποφάσεων.

Συμπερασματικά, είναι σημαντικό να καταγράφονται διαφορετικές απόψεις σχετικά με την εφαρμογή και τη χρήση του IoT που δεν σχετίζονται αυστηρά και άμεσα με τα προηγούμενα θέματα. Η μελέτη των προβλημάτων που σχετίζονται με την εταιρική κουλτούρα και τη λήψη αποφάσεων δείχνει τη κρισιμότητα του να τονιστεί σε θεωρητικό και πρακτικό επίπεδο ότι η υλοποίηση του IoT είναι ζήτημα στρατηγικής αλλαγής μέσα στην εταιρεία.

Η υλοποίηση του συνδέεται με αποφάσεις βιωσιμότητας και αποφάσεις που θα επηρεάσουν τα μακροπρόθεσμα πλάνα της εταιρείας. Επιπλέον, η τεχνολογία όταν εφαρμοστεί σε έργο-κεντρικό περιβάλλον θα αλλάξει την ιδέα της "εμπειρίας", της μετατόπισης του δόγματος της προσωπικής εμπειρίας σε αυτό που ονομάζεται εμπειρία με βάση συλλεγμένη πληροφόρηση.

### B.4.5. Οφέλη εφαρμογής του IoT σε Έργο-Κεντρικό Περιβάλλον

Το πρωταρχικό πλεονέκτημα του IoT είναι η προστασία των πληροφοριακών στοιχείων με μεγάλη σημασία (assets) και η άμεση προσπέλαση των δεδομένων που λαμβάνονται από τις συσκευές για μια αποδοτική και αποτελεσματική ανάλυση. Αυτό ενεργεί για ορισμένους οργανισμούς ως ανταγωνιστικό πλεονέκτημα και ακόμη και ως βασική ικανότητα.

Οι τεχνολογίες IoT είναι σε θέση να επιφέρουν βελτιώσεις στις διαδικασίες και τις ροές εντός του οργανισμού. Εγγυώνται κέρδη στην παραγωγικότητα, μείωση του χρονοδιαγράμματος ολοκλήρωσης του έργου, εξασφάλιση ότι η μετάβαση μεταξύ των διαδικασιών θα είναι ομαλή και εξάλειψη οποιεσδήποτε ανεπιθύμητων διεργασιών εντός μίας ροής για να επιτευχθεί βελτιστοποιημένη ροή δεδομένων και εργασιών ενισχύοντας γενικά τις παραγωγικές διαδικασίες.

Η αναγνώριση των ζητημάτων την ώρα που εμφανίζονται είναι σημαντική για την αύξηση της αποτελεσματικότητας. Επιπλέον, η συλλογή δεδομένων σε πραγματικό χρόνο είναι

απαραίτητη για τον προγραμματισμό και την πρόβλεψη ενεργειών προκαταρκτικής συντήρησης.

Λόγω της χρήσης συμβατικών εργαλείων αποθήκευσης όπως συστήματα διακομιστή ή cloud, οι πληροφορίες λαμβάνουν υψηλότερο επίπεδο διαφάνειας, βελτιώνοντας τις διαδικασίες κοινής χρήσης. Το οικοσύστημα που δημιουργεί η τεχνολογία του IoT είναι θεμελιώδους σημασίας για την αξιοποίηση της αξίας των προϊόντων υπό διάφορες πτυχές. Έτσι, ο οργανισμός έχει τη δυνατότητα να παρέχει στους πελάτες μια καλύτερη εμπειρία, δηλαδή διαφανή, επιτρέποντάς τους να δουν οποιαδήποτε πληροφορία σχετική με τα σχέδιά τους ανά πάσα στιγμή.

Διαθέτοντας έξυπνες συσκευές συνδεδεμένες με το διαδίκτυο που επικοινωνούν και μεταδίδουν ανά πάσα στιγμή, ειδικά οι αισθητήρες, επιτρέπουν στις επιχειρήσεις να αποκτούν γνώσεις σε πραγματικό χρόνο και να ανταποκρίνονται στις ανάγκες πελατείας με ασφάλεια.

Λόγω της ανατροφοδότησης πληροφοριών σε πραγματικό χρόνο, οι επιχειρήσεις εστιάζουν επίσης στο δίκτυο υποστήριξης των απαραίτητων δραστηριοτήτων μετά τη χρήση, ξεκινώντας από την προβλεπτική συντήρηση, την αναβάθμιση των χαρακτηριστικών, τις ολοκληρωμένες υπηρεσίες και τις ολοκληρωμένες λύσεις. Η ανάλυση του σημαντικού αριθμού δεδομένων επηρεάζει και βελτιώνει την εμπειρία των πελατών με τα προϊόντα.

Αυτές οι δραστηριότητες δημιουργούν μια μετατόπιση μέσα στην επιχειρηματική μονάδα, μεταβαίνοντας από μια εταιρεία που βασίζεται σε προϊόν σε μια εταιρεία παροχής υπηρεσιών προϊόντων. Συμπερασματικά, οι συνεχείς ανατροφοδοτήσεις είναι χρήσιμες για τη διατήρηση της ανταγωνιστικότητας στην αγορά.

### B.4.6. Η επίδραση του IoT στο ρόλο του Υπεύθυνου Έργου

Ανεξάρτητα από το βαθμό στον οποίο η τεχνολογία προχωράει, είναι βέβαιο ότι το πιο ζωτικό συστατικό σε οποιαδήποτε πτυχή των έργων είναι οι άνθρωποι ως καταλύτες της προόδου και ως ο πιο κρίσιμος πόρος που παρουσιάζεται σε αυτόν τον κόσμο.

Ο ρόλος του διαχειριστή έργου γίνεται λιγότερο αυστηρός και πιο ευέλικτος στη γενική προσέγγιση του κύκλου ζωής του έργου. Λαμβάνοντας υπόψη ότι η εφαρμογή καινοτόμου τεχνολογίας είναι πάντα σημαντικό να εξεταστεί και να αναλογιστεί κανείς το ισοζύγιο

μεταξύ των πλεονεκτημάτων και των αρνητικών ζητημάτων κατά τη χρήση της. Ο ρόλος του διαχειριστή του έργου δεν αποτελεί εξαίρεση και το IoT επηρεάζει βαθιά αυτό τον ρόλο.

Η τεχνολογία είναι εκεί για να βοηθήσει τους ανθρώπους αντί να τους αντικαταστήσει, δηλώνοντας ότι με την πρόοδο της τεχνολογίας, ο ρόλος του διαχειριστή του έργου έχει επηρεαστεί ως επί το πλείστον θετικά. Οι κύριες διαδικασίες απλοποιούνται. Η επικοινωνία και η συνεργασία με τα ενδιαφερόμενα μέρη, και συγκεκριμένα με τα μέλη της ομάδας, ενισχύεται, βοηθώντας τους στα ευρήματά τους και τη λήψη αποφάσεων. Οι δυσλειτουργίες σχετικά με την ανταλλαγή πληροφοριών και δεδομένων είναι λιγότερο συχνές και η μεταφορά πληροφοριών είναι ευκολότερη και ταχύτερη.

Ο Υπεύθυνος Έργου έχει τη δυνατότητα να χρησιμοποιεί αξιόπιστα δεδομένα οπουδήποτε και αν είναι, κάτι που ενισχύει τη διαδικασία λήψης αποφάσεων. Οι αποφάσεις και οι σχετικές διαδικασίες ήταν πάντα μια χρονοβόρα οντότητα με ενσωματωμένη γραφειοκρατία, περιορισμούς στην ανάλυση και διαμόρφωση δεδομένων λόγω της έλλειψης πληροφοριών που παρουσιάστηκαν, οδηγώντας σε ανεπιτυχή συνεργασία και επικοινωνία μεταξύ των μερών.

Ωστόσο, η εφαρμογή των νέων τεχνολογιών θα εξαλείψει κάθε ασάφεια και θα επιτρέψει στον διαχειριστή του έργου να λειτουργήσει και να διατηρήσει τα επίπεδα παραγωγικότητάς του σε ιδιαίτερα αποτελεσματικές και αποδοτικές παραδόσεις έργων.

Είναι επίσης αξιοσημείωτο ότι οι πολυάριθμες πληροφορίες που είναι πάντα έτοιμες να χρησιμοποιηθούν δυσκολεύει το ρόλο του Υπεύθυνου Έργου και πρέπει να αντιμετωπιστούν με τον κατάλληλο τρόπο. Οι υπεύθυνοι έργων θα χάσουν τον μερικό έλεγχο των διαδικασιών του έργου λόγω της πρόσβασης στις πληροφορίες και από άλλα μέλη της ομάδας που θα συμμετέχουν στη λήψη αποφάσεων.

Ο μεγάλος όγκος δεδομένων που μπορεί να παρέχει το IoT στους διαχειριστές έργων ίσως να αποτελεί απειλή. Στην πραγματικότητα πάρα πολλές πληροφορίες θα μπορούσαν να επιβραδύνουν το έργο του Υπεύθυνου Έργου.

Η σπουδαιότητα των παραδοσιακών μεθοδολογιών και τεχνικών παραμένει ισχυρή και θα πρέπει να συνδυαστεί με την ύπαρξη κατάλληλων δεξιοτήτων ως προς τη χρήση προηγμένων και νέων εργαλείων εφαρμογής του IoT και του οικοσυστήματος πληροφορικής εν γένει. Δεξιότητες όπως η διαχείριση χρόνου, η επίλυση προβλημάτων, η ομαδικότητα κλπ εξακολουθούν να είναι ουσιώδεις και θεμελιώδεις για το ρόλο και πρέπει να επωφεληθούν από το νέο υπολογιστικό δίκτυο και οικοσύστημα του IoT.

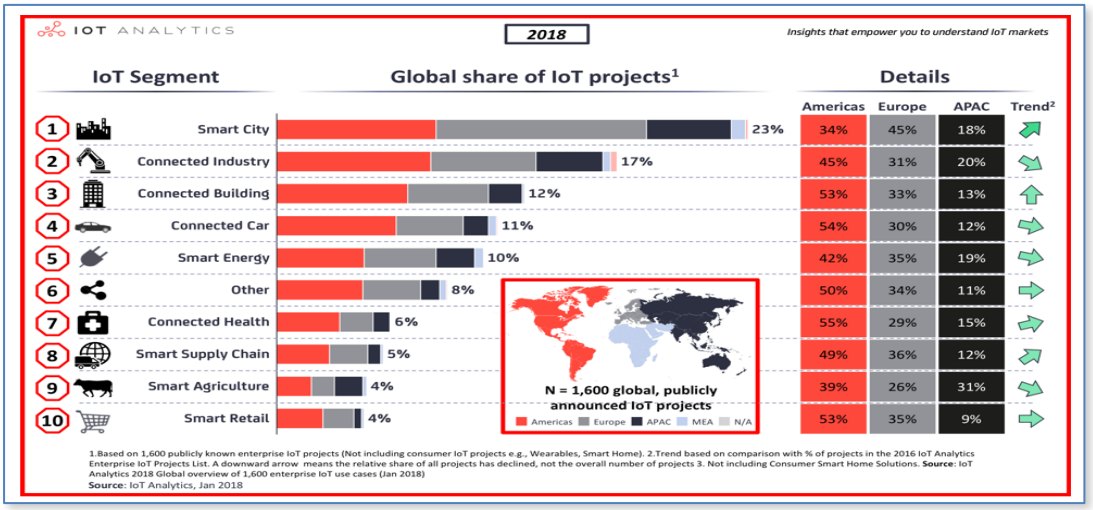
## B.5. Γενικές Εφαρμογές του IoT στο έργο-κεντρικό περιβάλλον

Το IoT μπορεί να εφαρμοστεί σε διάφορους τομείς και αντικείμενα και μπορεί να βοηθήσει στην επίλυση των καθημερινών προβλημάτων που αναφέραμε στις προηγούμενες ενότητες. Η ανακάλυψη των δυνατοτήτων του IoT και της τεχνολογίας αποτελεί μια συγκεκριμένη ευκαιρία για μια εταιρεία και, τα οφέλη της εφαρμογής στην κουλτούρα της εταιρείας αναγνωρίζονται.

Όπως αναφέρθηκε και σε προηγούμενες ενότητες, τα μεγάλα έργα μηχανικής είναι οι κύριοι δικαιούχοι της εφαρμογής του IoT. Για τον προηγούμενο λόγο είναι εύλογο να δηλωθεί ότι οι εταιρείες πετρελαίου και φυσικού αερίου, εξορυκτικές βιομηχανίες ή παραγωγής ενέργειας, οι οποίες είναι μεγάλες εταιρίες και έργο-κεντρικές, θα ενισχυθούν δραστικά μέσω της εφαρμογής της τεχνολογίας IoT. Η επίπτωση του IoT στο έργο-κεντρικό το περιβάλλον ορίζεται κυρίως από δύο δραστηριότητες: την παρακολούθηση και την αυτοματοποίηση των διαδικασιών.

Παρακολούθηση και έλεγχος Κτιρίων: Λόγω της λειτουργικότητας του IoT, η τοποθέτηση αισθητήρων στα τελικά έργα επιτρέπει τη συλλογή δεδομένων καθ 'όλη τη διάρκεια ζωής του κτιρίου. Με το χρόνο, τα κτίρια φθείρονται. Έτσι, οι αισθητήρες IoT επιτρέπουν την παρακολούθηση και αναφορά αυτών των αλλαγών στις ομάδες ανάπτυξης του έργου οι οποίες με τη σειρά τους φροντίζουν να διατηρήσουν την ποιότητα και τα πρότυπα του προϊόντος. Γενικά, η σημερινή τάση είναι η στροφή προς "έξυπνες" πόλεις και έξυπνη διαχείριση του περιβάλλοντος (Εικόνα 32). Οι έξυπνες πόλεις χαρακτηρίζονται από συνεχείς ενέργειες παρακολούθησης και ελέγχου.

*Εικόνα 32: Παγκόσμια κατανομή των έργων IoT (πηγή: https://iot-analytics.com/top-10-iot-segments-2018-real-iot-projects/)*



Το IoT μπορεί να σαρώσει αποτελεσματικά τη δομική κατάσταση των κτιρίων, των εγκαταστάσεων και των μνημείων. Μπορεί να ελέγχει και να αναλύει τις δονήσεις και να ανιχνεύει εξωτερικές απειλές για παράδειγμα. Η ρύπανση του θορύβου, τα φώτα των δρόμων και η διαχείριση αποβλήτων θα μπορούσαν επίσης να αντιμετωπιστούν με την τεχνολογία του IoT σε ένα αποτελεσματικό οικοσύστημα που δημιουργήθηκε μεταξύ διαφορετικών οντοτήτων.

Από περιβαλλοντική πλευρά, το IoT μπορεί να παρέχει κρίσιμα δεδομένα απαραίτητα για την πρόβλεψη και την ανίχνευση φυσικών καταστροφών και περιβαλλοντικών καταστροφών. Το πλαίσιο του IoT έχει την τάση να παρακολουθεί και να ιχνηλατεί τις εκπομπές χημικών ρύπων, δασικές πυρκαγιές και τις φυσικές προειδοποιήσεις.

Αυτοματοποίηση του IoT: Ο βιομηχανικός αυτοματισμός είναι επίσης ένας από τους διάφορους τομείς στους οποίους μπορεί να εφαρμοστεί το IoT. Η αυτοματοποίηση των διαδικασιών παραγωγής βελτιστοποιεί τη συνολική παραγωγική διαδικασία και τον κύκλο παραγωγής. Το IoT βοηθά επίσης στη διαχείριση αποθεμάτων, τη συντήρηση και επισκευή του μηχανήματος, καθώς και στη διαχείριση της υγείας του εργατικού δυναμικού.

Καθώς η υγεία αποτελεί προτεραιότητα για όλα τα άτομα, η εφαρμογή του IoT επιτρέπει την παρακολούθηση και τον εντοπισμό των προβλημάτων υγείας, παρακολουθώντας τα μοτίβα της καρδιακής συχνότητας, την αρτηριακή πίεση, τον παλμό, και άλλα. Αυτές οι πληροφορίες θα μεταφερθούν αυτόματα στους γιατρούς για ανάλυση. Αυτή η τεχνολογία θα είναι πολύ χρήσιμη για τα άτομα με ειδικές ανάγκες και τους ηλικιωμένους που διαμένουν μόνοι τους.

Επιπλέον, το Διαδίκτυο φέρνει πολλά επίπεδα πολυπλοκότητας. Το τελικό στάδιο της εξειδίκευσης είναι αυτό της "δημιουργίας εφαρμογών" που επιτρέπει τη δυνατότητα αυτοματισμού στους διάφορους αισθητήρες που εφαρμόζονται. Έχοντας αναφέρει αυτό, αυτό επίσης επιφέρει αλλαγές στον τρόπο ανάπτυξης των λογισμικών διαχείρισης έργων. Η ενσωμάτωση αισθητήρων IoT στο λογισμικό διαχείρισης έργων επιτρέπει τη δημιουργία ενός κεντρικού ταμπλό που διαχειρίζεται μια ολόκληρη επιχείρηση.

Αυτό το υψηλό επίπεδο αυτοματισμού ανοίγει ένα εντελώς νέο όραμα και ευκαιρία προς την υιοθέτηση της έννοιας διαχείρισης μίας "ενιαίας εφαρμογής λογισμικού". Εκτός αυτού, η εφαρμογή αισθητήρων IoT στα προγράμματα διαχείρισης έργων βοηθά στη μείωση των συνολικών αποβλήτων του έργου και συμβάλλει στη μείωση των κλοπών και τον καλύτερο έλεγχο στην κατανομή των πόρων.

Συμπερασματικά, ένα άλλο ακριβό λειτουργικό κόστος που προκύπτει σε ένα κατασκευαστικό έργο είναι η μεταφορά μηχανημάτων και εξοπλισμού απαραίτητα για την εκτέλεση των εργασιών. Με την εφαρμογή του IoT θα τοποθετούσαν τα RFID και τους αισθητήρες στα οχήματα, συλλέγοντας έτσι πληροφορίες για το πόσο χρόνο μετακινείται από τη μια θέση στην άλλη, λαμβάνοντας παράλληλα υπόψη τους πόρους που διατέθηκαν για τη μεταφορά. Επιτρέποντας τη δημιουργία ενός ζωντανού προϋπολογισμού από τη μεταφορά, το κόστος συντήρησης και τον εξοπλισμό λειτουργεί ως ανταγωνιστικό πλεονέκτημα κατά την υποβολή προσφορών έργου.

Ένα άλλο παράδειγμα που λαμβάνεται υπόψη είναι αυτό της ανάγνωσης των τύπων εξοπλισμού και οχημάτων και της ανάλυσης τους, έτσι ώστε τα χρονοδιαγράμματα συντήρησης να μπορούν να εφαρμοστούν στρατηγικά και να εξαλείψουν τυχόν καθυστερήσεις στον προγραμματισμό και την κινητοποίηση λόγω προβλημάτων συντήρησης των μηχανημάτων.

### B.5.1. Εφαρμογή της τεχνολογίας RFID στη διοίκηση κατασκευαστικών έργων

Η τεχνολογία αναγνώρισης ραδιοσυχνοτήτων (RFID) είναι ένας σημαντικός τεχνολογικός κλάδος του IoT που εφαρμόστηκε ευρέως σε διάφορους τομείς, όπως το λιανικό εμπόριο, οι ηλεκτρονικές συναλλαγές, η διαχείριση της εφοδιαστικής αλυσίδας, η επιστημονική έρευνα, η ασφάλεια και άλλοι. Έφερε σημαντικά οφέλη σε αυτούς τους τομείς μέσω της βελτίωσης της ορατότητας πληροφοριών σε πραγματικό χρόνο και ιχνηλασιμότητα (Lu W., et al, 2011).

Αυτή η δυνατότητα της συγκεκριμένης τεχνολογίας έρχεται να ταιριάξει στις αυξανόμενες απαιτήσεις για ταχύτητα και αποτελεσματικότητα εν όψει της ολοένα και μεγαλύτερης πολυπλοκότητας στη διοίκηση σύγχρονων κατασκευαστικών έργων. Στα έργα αυτά, υπάρχει η ανάγκη για ολοένα και ισχυρότερα πρότυπα διαχείρισης έργων κατασκευής (Construction Project Management - CPM). Τα κριτήρια επιτυχίας των παραδοσιακών μεθοδολογιών CPM έχουν διευρυνθεί έτσι ώστε μαζί με το κόστος, την ποιότητα, και το χρόνο (γνωστό ως τρίγωνο Διοίκησης Έργων) να συμπεριλάβουν επίσης την ασφάλεια και το περιβάλλον.

Αυτό απαιτεί από τους διαχειριστές του έργου να λάβουν καλύτερες αποφάσεις για βέλτιστη διαχείριση υλικών, εργασιών και μηχανημάτων με βάση τις διαθέσιμες πληροφορίες. Οι πληροφορίες αναγνωρίζονται ως ένα νέο στοιχείο για την επιτυχία του CPM. Η διαχείριση

ενός ιστού συσσωρευμένης πληροφορίας και γνώσης στην υποστήριξη μελλοντικών έργων ορίζουν νέες προκλήσεις για το σύγχρονο CPM.

Μεταξύ των πολλών προκλήσεων για τη διαχείριση των πληροφοριών στη Διοίκηση Κατασκευαστικών Έργων είναι η ιδιαίτερα έντονη ανάγκη για βελτίωση της πρόσβασης στη πληροφορία σε πραγματικό χρόνο και η ιχνηλασιμότητα της. Οι διαχειριστές έργων πρέπει να αποκτήσουν πληροφορίες σε πραγματικό χρόνο για τα υλικά, τους άνδρες και τα μηχανήματα, ώστε να προχωρήσουν γρήγορα σε προσαρμοσμένες αποφάσεις (Liu Z. et al, 2016).

### Β.5.1.1 Διαχείριση εφοδιαστικής αλυσίδας

Σε μια τυπική αλυσίδα εφοδιασμού υλικών, παραγγέλλονται δομικά υλικά και μεταφέρονται με φορτηγά ή πλοία από το εργοστάσιο σε διανομείς υλικών τους και, στη συνέχεια, στην αποθήκη της περιοχής. Σημαντικές πληροφορίες όπως ο κατασκευαστής, η ποσότητα, οι προδιαγραφές και άλλα πρέπει να είναι εύκολα διαθέσιμα στους υπεύθυνους για τη λήψη αποφάσεων, όπως το προφίλ πελατών για το τμήμα διοίκησης, οι οδηγοί φορτηγών στο δρόμο κλπ.

Οι πληροφορίες διαθέσιμες σε πραγματικό χρόνο είναι πιο σημαντικές όταν οι Just-In-Time (JIT) προσεγγίσεις στην εφοδιαστική αλυσίδα προσαρμόζονται για να αντιμετωπίσουν τα συμπαγή σημεία εργασιών που συνήθως εμφανίζονται σε υπό συμφόρηση αστικές περιοχές (Lu W., et al, 2011).

Για παράδειγμα, η κατασκευή ενός συγκεκριμένου θεμέλιου αξιοποιώντας μία JIT τεχνολογία επί τόπου χυτού απαιτεί πληροφορίες και συντονισμό σε πραγματικό χρόνο μεταξύ των εξωτερικών μπετονιέρων, των οδηγών φορτηγών για οδοστρώματα και των εργαζομένων στο χώρο, διαφορετικά το σκυρόδεμα θα μπορούσε να καθυστερήσει ή να φτάσει νωρίτερα προκαλώντας έτσι απώλεια. Στοιχεία χάλυβα ή προκατασκευασμένα εξαρτήματα (π.χ. συρματοπλέγματα, σύνθετα δοκάρια) θα πρέπει να μεταφέρονται εγκαίρως στις τοποθεσίες ή
η διαδικασία κατασκευής θα διακοπεί αν δεν υπάρχει αρκετός χώρος για να αποθηκευτούν αυτά τα στοιχεία.

Στην ιδανική περίπτωση, οι κατασκευαστές θα πρέπει να έχουν στη διάθεσή τους επίσης υλικά στοιχεία όπως το μέγεθος, τα βάρη, τις οδηγίες χειρισμού και τις μεθόδους

συναρμολόγησης. Σε αυτά τα σενάρια, είναι σε μεγάλο βαθμό επιθυμητή η πρόσβαση σε πληροφορίες και η ιχνηλασιμότητα τους σε πραγματικό χρόνο και η τεχνολογία RFID μπορεί να εφαρμοστεί για το σκοπό αυτό.

Οι πληροφορίες υλικού αποθηκεύονται σε ετικέτες RFID επικολλημένες στα υλικά. Παρόμοια με την πρακτική μεγάλων σούπερ μάρκετ στην Αμερική να επισημάνουν τα τρόφιμα και τα ποτά τους, αυτό έχει επίσης παρατηρηθεί στον κατασκευαστικό κλάδο για την επισήμανση μεγάλων δομικών στοιχείων. Αυτό που είναι πιο ενθαρρυντικό είναι ότι οι σημερινοί κατασκευαστές υλικών είναι ανοικτοί στην τεχνολογία RFID για την επισήμανση των προϊόντων τους. Επίσης οι τοποθεσίες των υλικών μπορούν να ανιχνευθούν αποτελεσματικά συνδυάζοντάς τα με το Παγκόσμιο Σύστημα εντοπισμού θέσης (GPS) και το Γεωγραφικό Σύστημα Πληροφοριών (GIS).

Από την άλλη πλευρά, τα ζητήματα είναι πολλά. Οι πληροφορίες που είναι προδιαγεγραμμένες για κατασκευαστικές χρήσεις (π.χ. συναρμολόγηση προκατασκευασμένων εξαρτημάτων) δεν έχουν ακόμη τυποποιηθεί. Το εύρος ανάγνωσης και η ακρίβεια της πληροφορίας γίνονται κρίσιμες, δεδομένου ότι τα κατασκευαστικά στοιχεία είναι συνήθως μεγάλα σε διαστάσεις. Η τιμή μονάδας χρέωσης για τις RFID επισημάνσεις (tags) πρέπει να μειωθεί πριν να μπορέσει να υιοθετηθεί μαζικά στην κατασκευαστική εφοδιαστική αλυσίδα.

Διαχείριση αποθεματικού

Η διαχείριση του υλικού στο αποθεματικό έχει ιδιαίτερη σημασία στα κατασκευαστικά έργα. Η σωστή ποσότητα υλικών στο απόθεμα μπορεί να διατηρήσει υγιή ταμειακή ροή για έναν ανάδοχο. Αυτό ισχύει ιδιαίτερα σήμερα καθώς οι εταιρείες τείνουν να αγοράζουν υλικά από την παγκόσμια αγορά ενώ υπάρχει επίσης το κόστος της αποθήκευσης και της φύλαξης τους στα εργοτάξια. Επιπλέον, μια καλή διαχείριση αποθεμάτων υλικών μπορεί να εξασφαλίσει την ομαλότητα των διαδικασιών κατασκευής.

Οι πληροφορίες αποθεματικού σε πραγματικό χρόνο μπορούν να διευκολύνουν περαιτέρω έναν άλλο γύρο διαδικασιών διαχείρισης υλικών, όπως η παραγγελία, μεταφορά, αποθήκευση και η χρήση. Παραδοσιακά, αυτά γίνονται χειροκίνητα μέσω της ανταλλαγής εγγράφων. Με τις προφανείς αδυναμίες τους, οι μέθοδοι της παραδοσιακή διαχείρισης αποθεμάτων αποδείχθηκε χαμηλής αποδοτικότητας και αποτελεσματικότητας. Η τεχνολογία RFID μπορεί να εφαρμοστεί για τη βελτίωση της διαχείρισης των αποθεμάτων δομικών υλικών.

Στην περιοχή αποθήκευσης μπορούν να εγκατασταθούν συσκευές αναγνώρισης RFID μεγάλης εμβέλειας ανακτώντας πληροφορίες υλικού που είναι ενσωματωμένες στις ετικέτες RFID που ενσωματώνονται στα υλικά. Όταν τα νεοαποκτηθέντα υλικά τοποθετούνται στην περιοχή, οι αναγνώστες διαβάζουν τις ετικέτες και ενημερώνουν τη βάση δεδομένων αποθεματικού αυτομάτως.

Όταν τα υλικά παραληφθούν για χρήση, το σύστημα εργάζεται με αντίστροφη μέθοδο, έτσι ώστε το απόθεμα αφαιρείται από τη βάση δεδομένων. Η τεχνολογία RFID μπορεί να βελτιώσει την παραγωγικότητα με την ανάγνωση όλων των πληροφοριών με μία μόνο κίνηση και την αυτόματη ενημέρωση. Είναι επίσης ευκολότερο για τους εργάτες οικοδομών να εντοπίσουν τα σωστά υλικά με την ανάγνωση των πληροφοριών που επισυνάπτονται στα υλικά.

Η έρευνα σε αυτή τη περιοχή εστιάζει στην ένωση της πληροφορίας που η διαχείριση της εφοδιαστικής αλυσίδας και η διαχείριση αποθεμάτων με RFID παράγουν. Αυτό θα βοηθήσει στην απρόσκοπτη εκτέλεση των δύο διαδικασιών. Η ολοκλήρωση θα πρέπει να ευθυγραμμιστεί περαιτέρω με άλλες ετερογενείς κατασκευαστικές διαδικασίες που εφαρμόζουν προσεγγίσεις Just-In-Time, ή ελάχιστης απαιτούμενης παραγωγής (lean production). Αυτό ακριβώς αντανακλά με το όραμα του "Internet of Things", όπου η πανταχού παρούσα τεχνολογία πληροφορικής και η αυτόματη αναγνώριση ταυτότητας μπορεί να επιτρέψει την ταυτοποίηση και αποθήκευση πληροφοριών σε οποιοδήποτε αντικείμενο και οπουδήποτε.

Διασφάλιση Ποιότητας

Η τεχνολογία RFID μπορεί να χρησιμοποιηθεί για τη βελτίωση της ποιότητας κατασκευής μέσω πολλών τρόπων. Για παράδειγμα, χρησιμοποιήθηκε από οργανισμούς λιμένων στο να υποδείξουν το βάθος των πασσάλων καθώς με τις προηγούμενες κατασκευαστικές πρακτικές οι πάσσαλοι δεν διεισδύουν στην καθορισμένη απόσταση. Σε αυτήν την περίπτωση, οι ετικέτες RFID μπορούν να φυτευτούν στα άκρα των πασσάλων και τα ραδιοσήματά τους να υποδείξουν το βάθος του εδάφους που οι πάσσαλοι έχουν εισχωρήσει στην πραγματικότητα.

Το RFID μπορεί επίσης να βοηθήσει στην αποφυγή απομίμησης των υλικών. Με ετικέτες RFID κάθε υλικό θα έχει έναν μοναδικό αύξοντα αριθμό από τον κατασκευαστή. Παρόμοια με την πρακτική στις βιβλιοθήκες για την τοποθέτηση ετικετών RFID σε βιβλία, αυτές οι ετικέτες μπορούν να τοποθετηθούν σε υλικά. Οι διαχειριστές έργων μπορούν ελέγξουν τα υλικά για

να διασφαλίσουν ότι παρέχονται τα υλικά που χρησιμοποιούνται από έναν εξειδικευμένο προμηθευτή και χρησιμοποιούνται κατάλληλα.

Μόλις τα υλικά χρησιμοποιηθούν, οι ενσωματωμένες πληροφορίες μπορούν να χρησιμοποιηθούν στο μέλλον να δείξουν «ξεχασμένα» περιουσιακά στοιχεία ή στη διαχείριση εγκαταστάσεων.

Η τοποθέτηση RFID σε τσιμεντόλιθους μπορεί να διευκολύνει τη δοκιμή ποιότητας, για παράδειγμα να δείξει τα συγκεκριμένα δείγματα δοκιμής. Το πλεονέκτημα της χρήσης RFID ετικετών έναντι της χρήσης των ετικετών χαρτιού είναι ότι οι πρώτες τοποθετούνται στο σκυρόδεμα και δεν αλλοιώνονται εκτός αν αφαιρεθούν. Ως εκ τούτου, αυτό εμποδίζει την αντικατάσταση των δοκών από σκυρόδεμα.

Διαχείριση αποβλήτων

Τα απόβλητα κατασκευής και κατεδαφίσεων (C & D) ορίζονται ως απόβλητα που προκύπτουν από δραστηριότητες κατασκευής, ανακαίνισης και κατεδάφισης. Κατά τις τελευταίες δεκαετίες, τα ζητήματα των αποβλήτων έχουν λάβει όλο και μεγαλύτερη προσοχή σε όλο τον κόσμο. Κανονικά, τα απόβλητα C & D θα πρέπει να παραδοθούν σε προκαθορισμένους χερσαίους χώρους. Οι έρευνες δείχνουν ότι η παράνομη απόρριψη αποβλήτων εξακολουθεί να είναι σοβαρό πρόβλημα που πρέπει να επιλυθεί.

Για παράδειγμα στο Χονγκ Κονγκ εφαρμόζεται ένα ειδικό σύστημα για την πρόληψη των παράνομων αποβλήτων. Συγκεκριμένα, το σύστημα καταγράφει τα φορτηγά που μεταφέρουν τα απόβλητα, διασφαλίζοντας ότι κάθε είδος αποβλήτων κατευθύνεται στην κατάλληλη εγκατάσταση για επαναχρησιμοποίηση, ανακύκλωση, ανάκτηση ή διάθεση. Παρόλα αυτά, η αποτελεσματικότητα δεν έχει φτάσει τα επιθυμητά επίπεδα. Και στην περίπτωση αυτή η τεχνολογία RFID μπορεί να συνδράμει.

Ένας RFID ανάγνωσης και εγγραφής δεδομένων εγκαθίσταται στην έξοδο του εργοταξίου. Πληροφορίες όπως η ώρα αναχώρησης, ο τύπος αποβλήτων, οι τοποθεσίες προορισμοί θα είναι γραμμένα στην ετικέτα RFID ως ένας πομπός τοποθετημένος στο φορτηγό. Με την άφιξη του φορτηγού στον καθορισμένο προορισμό, ένας άλλος αναγνώστης RFID θα διαβάσει τις πληροφορίες, θα τις συγκρίνει με τα αρχικά δεδομένα και θα εγκρίνει ή θα αρνηθεί την πρόσβαση.

Οι πληροφορίες στις ετικέτες RFID μπορούν να διαβαστούν και να γραφτούν αυτόματα χωρίς παρέμβαση του συμβαλλομένου ή των οδηγών φορτηγών. Έτσι η παράνομη ξεφόρτωση

αποβλήτων μπορεί να μειωθεί. Το σύστημα RFID μπορεί να συνδυαστεί με άλλα συστήματα, π.χ. χρέωσης με βάση τον όγκο αποβλήτων, ώστε να καταστεί πιο αποτελεσματική η διαχείριση αποβλήτων C & D.

### Β.5.1.2 Διοίκηση προσωπικού

Έλεγχος πρόσβασης και προσέλευσης στο χώρο εργασίας

Τα εργοτάξια έχουν ειδικές ανάγκες ελέγχου πρόσβασης. Ένα αποτελεσματικό σύστημα ελέγχου πρόσβασης μπορεί να κρατήσει το χώρο, το προσωπικό και τα περιουσιακά στοιχεία ασφαλή.

Αν συνδυαστεί με ένα σύστημα ελέγχου παρουσίας, μπορεί να παράσχει αρχείο χρόνου και παρουσίας ως βάση για περαιτέρω χρήσεις, όπως την κατανομή των εργασιών, τον υπολογισμό του μισθού και ούτω καθεξής. Οι τωρινές τεχνικές στον έλεγχος πρόσβασης και προσέλευσης στο χώρο εργασίας είναι χειροκίνητες και έχουν πολλά μειονεκτήματα. Για παράδειγμα, είναι χρονοβόρες (Lu W., et al, 2011).

Έχει ερευνηθεί ότι στα εργοτάξια μπορεί να υπάρξει συχνά μια μακρά σειρά αναμονής για είσοδο στο χώρο ειδικά μετά την ώρα του μεσημεριανού. Αν και σπάνια, υπάρχουν περιπτώσεις που οι εργάτες μπορεί να εξαπατήσουν το σύστημα ελέγχου προσέλευσης. Μερικές φορές, υπάρχουν διαφορές στους μισθούς όταν αυτοί υπολογίζονται βάσει του συνόλου των ωρών απασχόλησης και λαμβάνει τα στοιχεία από το σύστημα προσέλευσης. Το RFID μπορεί να εφαρμοστεί για να αναπτυχθεί πιο αποτελεσματικό και με μεγαλύτερη ακρίβεια σύστημα ελέγχου πρόσβασης και καταγραφής ωρών εργασίας.

Κάθε εργαζόμενος θα διαθέτει μια κάρτα RFID που θα μπορούσε να ενσωματωθεί σε μία υπάρχουσα κάρτα (π.χ. κάρτα μέσων μαζικής μεταφοράς) για την καταγραφή των αναγνωριστικών τους, φωτογραφιών, αρχών πρόσβασης και των εταιρειών όταν κάποιος απασχολείται σε περισσότερους του ενός υπεργολάβους. Ένας αναγνώστης στην είσοδο / έξοδο του εργοταξίου θα ανακτήσει τις πληροφορίες, θα τα συγκρίνει με τη βάση δεδομένων και θα εγκρίνει ή απορρίψει την πρόσβαση.

Το σύστημα θα καταγράφει αυτόματα τους χρόνους εισόδου και εξόδου και αυτές οι πληροφορίες θα χρησιμοποιηθούν για τον υπολογισμό των μισθών από το σύστημα μισθοδοσίας. Ενόψει πιθανής εξαπάτησης, αυτό το σύστημα RFID μπορεί να συνδυαστεί με βιομετρικές πληροφορίες, όπως δαχτυλικά αποτυπώματα, σάρωση ίριδας ή αναγνώριση

προσώπου. Αυτό το προτεινόμενο σύστημα δεν είναι καθόλου νέο σε άλλους τομείς, αλλά στον τομέα των κατασκευών δεν έχει ακόμη εισαχθεί ευρέως.

Διοίκηση προσωπικού – ασφάλεια στο χώρο εργασίας

Η ασφάλεια στο χώρο των κατασκευών αποτελεί βασικό ζήτημα στη σύγχρονη Διοίκηση Κατασκευαστικών Έργων. Το RFID μπορεί να εφαρμοστεί για τη βελτίωση των επιδόσεων ασφάλειας σε αυτό τον τομέα. Έρευνες έχουν δείξει ότι ένας σημαντικός λόγος των ατυχημάτων στο χώρο είναι ότι οι εργαζόμενοι δεν φορούν σωστά τα κράνη εργασίας τους, ιδιαίτερα σε ένα ζεστό ή υγρό περιβάλλον εργασίας όπως ένα εργοτάξιο. Προτείνεται η τοποθέτηση ετικετών RFID σε κράνη ασφαλείας, φθορίζον μπουφάν, μπότες ασφαλείας και ζώνη ασφαλείας.

Πληροφορίες σχετικά με την τοποθεσία των εργαζομένων σε πραγματικό χρόνο μέσα στο χώρο μπορούν να βοηθήσουν αρκετά στη διαχείριση της ασφάλειας. Για παράδειγμα, οι ισπανικές κατασκευαστικές εταιρείες FCC και ACCIONA εφαρμόζουν λύση παρακολούθησης των εργαζομένων για την ασφάλεια τους μέσα σε σήραγγες χρησιμοποιώντας το υπάρχον δίκτυο Wi-Fi ως υποδομή.

Χρησιμοποιώντας την τεχνολογία RFID, μπορεί να αναπτυχθεί ένα οικονομικά προσιτό σύστημα παρακολούθησης εργαζομένων για την παροχή πληροφοριών σε πραγματικό χρόνο, οι οποίες είναι κρίσιμες για την ασφάλεια (localization). Σαφώς, το παραπάνω πρέπει να λάβει υπόψη του ηθικά ζητήματα που πηγάζουν από την παρακολούθηση των εργαζομένων στο εργοτάξιο.

Μια άλλη σημαντική εφαρμογή είναι η υλοποίηση ενός συστήματος προφύλαξης και ασφάλειας με βάση τις δυνατότητες της τεχνολογίας RFID. Το σύστημα αυτό θα μπορούσε να ενημερώνει τους εργαζόμενους για πιθανούς κινδύνους στο χώρο χρησιμοποιώντας RFID παντού στο χώρο. Στην περίπτωση αυτή, ένα εργοτάξιο θα χωριστεί σε διαφορετικές ζώνες, με το καθένα να έχει διαφορετικό χρώμα (π.χ. κόκκινο, πράσινο και πορτοκαλί) για να υποδείξει τους πιθανούς κινδύνους.

Όλοι οι πιθανοί κίνδυνοι, όπως οι πυρκαγιές, οι ηλεκτρικοί και οι χημικοί κίνδυνοι, καταγράφονται σε ετικέτες RFID που είναι παντού στο χώρο. Συνδέοντας τις ετικέτες με έναν αναγνώστη RFID και ένα σύστημα συναγερμού, είναι δυνατό να δοθούν στους εργαζόμενους οδηγίες και προφυλάξεις σχετικά με τους πιθανούς κινδύνους.

### Β.5.1.3 Διοίκηση μηχανολογικού εξοπλισμού

Παρακολούθηση μηχανών και εργαλείων

Η αποτελεσματική διαχείριση μηχανών και εργαλείων δεν είναι μόνο η διαχείριση τους ως περιουσιακά στοιχεία, αλλά και η εξασφάλιση της ομαλότητας των προγραμματισμένων έργων. Η παρακολούθηση της χρήσης τους σε πραγματικό χρόνο καθίστανται πιο σημαντική όταν το εργοτάξιο είναι μεγάλο (π.χ. εκτέλεση εργασιών σε αστικό χώρο), επομένως και η τοποθέτηση μηχανών και εργαλείων γίνεται πιο κρίσιμη. Οι υπεύθυνοι του έργου μπορούν να μιλήσουν στους εργάτες χρησιμοποιώντας το κινητό τους τηλέφωνο αλλά δεν ισχύει το ίδιο στην παρακολούθηση των μηχανών. Η RFID τεχνολογία μπορεί να βοηθήσει στην περίπτωση αυτή (Lu W., et al, 2011).

Οι ετικέτες RFID μπορούν να αποθηκεύουν σε μία βάση δεδομένων το δανεισμό και την επιστροφή μηχανών και εργαλείων αποτρέποντας την απώλεια, την κακή τοποθέτηση ή τον διαρρήκτη. Αυτό μπορεί να ενισχυθεί περαιτέρω με τη σύνδεση της βάσης δεδομένων με το σύστημα καταγραφής του χρόνου εργασίας των εργαζομένων. Επιπλέον, η τεχνολογία RFID μπορεί να εφαρμοστεί για τον εντοπισμό μηχανών και εργαλείων (σε ένα ορισμένο μήκος κύματος και χωρίς επαφή με το αντικείμενο).

Λειτουργία μηχανολογικού εξοπλισμού

Ένα σύστημα ελέγχου της λειτουργίας των μηχανών μπορεί να αναπτυχθεί χρησιμοποιώντας την τεχνολογία RFID. Για την εκκίνηση του κινητήρα και τη λειτουργία βαρέων μηχανημάτων όπως γερανοί και εκσκαφείς, οι χειριστές πρέπει να σηκώσουν την κάρτα RFID τους μπροστά από έναν αναγνώστη RFID εγκατεστημένο στην αίθουσα χειρισμού μηχανής. Πρέπει να το κάνουν πάλι όταν φεύγουν ή σταματούν τα μηχανήματα.

Στην ιδανική περίπτωση, η άδεια χειρισμού πρέπει να ταυτίζεται με τις ικανότητες και τις εμπειρίες των εξουσιοδοτημένων προσώπων που μπορούν να αναγράφονται σε μια κάρτα RFID. Πληροφορίες όπως ο χειριστής και ο χρόνος λειτουργίας καταγράφονται και αποθηκεύονται σε ένα κεντρικό σύστημα. Αυτό επιτρέπει σε έναν υπεύθυνο του έργου να παρακολουθεί το ιστορικό χρήσης κάθε μηχανής και να υπολογίζει την απόσβεσή του. Αυτές οι πληροφορίες θα είναι επίσης πολύ χρήσιμες για την επιθεώρηση, τη συντήρηση ή τον υπολογισμό διαφόρων ποσοτήτων.

# Συμπεράσματα

Η παρούσα διατριβή έχει ως στόχο να ξεκινήσει μια συζήτηση και να τονίσει τη σημασία της ενσωμάτωσης του IoT στην καθημερινότητα του ανθρώπου, να εξετάσει τις παραμέτρους για την επιτυχή διαχείριση του Διαδικτύου των Πραγμάτων και να τονίσει τον αντίκτυπο της ενσωμάτωσης του IoT στη διαχείριση έργων και πιο συγκεκριμένα σε εταιρίες με έργο-κεντρικό προσανατολισμό, λαμβάνοντας υπόψη τόσο το εταιρικό όσο και το επιχειρηματικό μοντέλο.

Ξεκινάει παρουσιάζοντας τις βασικές έννοιες της Διαχείρισης Έργων και του Διαδικτύου των Πραγμάτων, στη συνέχεια αναπτύσσει τις βασικές παραμέτρους για την αποτελεσματική διαχείριση του IoT, όπως τα μοντέλα επικοινωνίας των συσκευών του IoT, η ασφάλεια και οι απαιτήσεις ασφαλείας στον τομέα του IoT και η Διαχείριση κινδύνου. Προχωράει περαιτέρω με τη διερεύνηση των επιπτώσεων στη διαχείριση έργων και τον αντίκτυπο στους ρόλους των υπεύθυνων έργων.

Η ενδελεχής εξέταση του τρόπου με τον οποίο μπορούμε να διαχειριστούμε το Διαδίκτυο των Πραγμάτων καταδεικνύει ότι το Διαδίκτυο των Πραγμάτων παρουσιάζει πληθώρα προνομίων για τους καταναλωτές, και έχει τη προοπτική να αλλάξει δομικά τον τρόπο με τον οποίο οι καταναλωτές αλληλεπιδρούν με την τεχνολογία. Στο μέλλον το IoT είναι πιθανόν να συγχωνεύσει τον εικονικό με τον πραγματικό κόσμο, με τρόπους τους οποίους σήμερα είναι πολύ δύσκολο να κατανοήσουμε.

Οι αποτελεσματικές αρχιτεκτονικές επικοινωνίας αποτελούν σημαντική κινητήρια δύναμη της αξίας που προσφέρεται στον τελικό χρήστη, ανοίγοντας δυνατότητες χρήσης των πληροφοριών με νέους τρόπους. Θα πρέπει να σημειωθεί, ωστόσο, ότι αυτά τα οφέλη έρχονται με συμβιβασμούς. Ιδιαίτερη προσοχή πρέπει να δοθεί στις οικονομικές επιβαρύνσεις που επιβάλλονται στους χρήστες όταν πρόκειται να συνδεθούν με τους πόρους του cloud, οι οποίες διαφέρουν από περιοχή σε περιοχή. Παρόλο που ο τελικός χρήστης έχει πολλά οφέλη από τα μοντέλα επικοινωνίας μεταξύ των συσκευών του IoT, θα πρέπει να αναφερθεί ότι τα αποτελεσματικά μοντέλα επικοινωνίας IoT ενισχύουν επίσης την τεχνολογική καινοτομία και την ευκαιρία για εμπορική ανάπτυξη.

Από την οπτική της ασφάλειας και της ιδιωτικότητας, η προβλεπόμενη διάχυτη εισαγωγή των αισθητήρων και των συσκευών στους ιδιωτικούς χώρους - όπως το σπίτι, το αυτοκίνητο, ακόμη και το ανθρώπινο σώμα μέσω των φορετών συσκευών IoT (wearables), θέτει συγκεκριμένες προκλήσεις. Καθώς τα πραγματικά αντικείμενα της καθημερινότητας μας

ολοένα και περισσότερο ανιχνεύουν και διαμοιράζουν δεδομένα που παρατηρούν σχετικά με εμάς, οι καταναλωτές πιθανότατα να εξακολουθούν να επιθυμούν ιδιωτικότητα.

Οι αρμόδιοι κανονιστικοί κυβερνητικοί φορείς θα συνεχίσουν να εφαρμόζουν νόμους, να εκπαιδεύουν τους καταναλωτές και τις επιχειρήσεις και να συνεργάζονται με τους συνηγόρους των καταναλωτών, τη βιομηχανία, τους ακαδημαϊκούς και άλλους εμπλεκόμενους φορείς του Διαδικτύου των πραγμάτων, προκειμένου να προωθηθεί η κατάλληλη προστασία της ασφάλειας και της ιδιωτικής ζωής, ενώ ταυτόχρονα πραγματοποιούνται προσπάθειες αυτορρύθμισης στον τομέα του IoT, σε συνδυασμό με την εφαρμογή της ασφάλειας των δεδομένων και την διεύρυνση της νομοθεσίας περί απορρήτου.

Καθώς η πλειοψηφία των χρηστών του Διαδικτύου είναι μηχανές και όχι άνθρωποι, η Διαχείριση κινδύνου (Risk Management) αποτελεί κρίσιμο και σημαντικό κομμάτι του τρόπου διαχείρισης του Διαδικτύου των Πραγμάτων. Οι συσκευές που απαρτίζουν το "Διαδίκτυο των πραγμάτων" (IoT) συνδέονται με το Διαδίκτυο, αναλαμβάνουν δράση και δημιουργούν τεράστια ποσά δεδομένων. Αυτές οι συσκευές θα εκτελούν προοδευτικά περισσότερες λειτουργίες, δημιουργώντας νέους κινδύνους για την ασφάλεια, αλλά χρειαζόμαστε περισσότερα για να αξιολογήσουμε τον κίνδυνο και να σχεδιάσουμε χρήσιμες πολιτικές.

Ένα αρχικό συμπέρασμα σχετικά με την ασφάλεια και τον κίνδυνο στο Διαδίκτυο των πραγμάτων είναι ότι οι δημοφιλείς απεικονίσεις υπερβάλλουν σημαντικά και διαστρεβλώνουν τον κίνδυνο.

- Το Διαδίκτυο των πραγμάτων δεν θα είναι πιο ασφαλές από το συμβατικό Διαδίκτυο και μπορεί να είναι πιο ευάλωτο, καθώς πολλές συσκευές IoT θα χρησιμοποιούν απλούς υπολογιστές με περιορισμένη λειτουργικότητα.
- Η αυξημένη ευπάθεια, ωστόσο, δεν σημαίνει αυξημένο κίνδυνο. Τα οφέλη του IoT υπερτερούν των δυνατοτήτων πρόκλησης βλάβης και ένας κίνδυνος που συνήθως δεν λαμβάνεται υπόψη είναι ότι τα πρόωρα ή υπερβολικά μέτρα για την ασφάλεια ή την ιδιωτική ζωή θα καταπνίξουν την οικονομική ανάπτυξη και την καινοτομία.
- Οι συσκευές IoT επιτρέπουν στους χάκερ να έχουν φυσικό αντίκτυπο. Οι ερευνητές έχουν επιδείξει πολλές ευπάθειες σε συσκευές IoT, αλλά οι συνέπειες αυτών των τρωτών σημείων χαρακτηρίζονται σε μεγάλο βαθμό ως κακόβουλες φάρσες. Μόνο συσκευές IoT που εκτελούν ευαίσθητες λειτουργίες ή όπου η διακοπή μπορεί να προκαλέσει μαζική επίδραση, αυξάνουν τον κίνδυνο. Αυτό σημαίνει ότι οι περισσότερες συσκευές IoT παρουσιάζουν μικρό κίνδυνο.

- Η κατάσταση της ιδιωτικής ζωής στο διαδίκτυο είναι τόσο επίφοβη, όπου είναι απίθανο ότι το IoT θα την επιδεινώσει.
- Τα ίδια προβλήματα που μας εμποδίζουν να καταστήσουμε ασφαλέστερο τον κυβερνοχώρο θα επιβραδύνουν την πρόοδο στην ασφάλεια του IoT: τεχνολογική αβεβαιότητα, περιορισμένη διεθνής συνεργασία, έλλειψη κινήτρων για βελτίωση, περιορισμένη ρυθμιστική εξουσία, αδυναμία ηλεκτρονικής ταυτότητας και επιχειρηματικό μοντέλο Internet βασισμένο στην εκμετάλλευση προσωπικών δεδομένων.
- Μπορούμε να επιταχύνουμε τη μείωση των κινδύνων με τις ίδιες προσεγγίσεις που χρησιμοποιούμε για τη γενική ασφάλεια στον κυβερνοχώρο: έρευνα, ευθύνη, διεθνή συνεργασία και ρύθμιση.
- Η αυτονομία θα είναι βασικός καθοριστικός παράγοντας για τον κίνδυνο στο Διαδίκτυο των Πραγμάτων. Ο περιορισμός της αυτονομίας της συσκευής ή η παροχή ενός τρόπου υπέρβασης της αυτονομίας μειώνει τον κίνδυνο. Τα πρότυπα IoT πρέπει να απαιτούν υψηλότερο βαθμό ανθρώπινης παρέμβασης και ελέγχου για ευαίσθητες λειτουργίες.
- Μια ασφαλής συσκευή που συνδέεται με ένα μη ασφαλές δίκτυο δεν συμβάλλει πολύ στη μείωση του κινδύνου. Δεδομένης της ασθενούς κατάστασης ασφάλειας στα περισσότερα δίκτυα, η μεγαλύτερη ασφάλεια του IoT απαιτεί καλύτερη χρήση κρυπτογράφησης, ισχυρού ελέγχου ταυτότητας και αυξημένης ανθεκτικότητας τόσο για συσκευές όσο και για δίκτυα.
- Μπορούμε να χρησιμοποιήσουμε τρεις μετρήσεις - την αξία των δεδομένων, την κρισιμότητα μιας λειτουργίας και την κλιμάκωση της αποτυχίας - να εκτιμήσουμε τον κίνδυνο του IoT. Οι συσκευές που δημιουργούν πολύτιμα δεδομένα, εκτελούν ζωτικής σημασίας λειτουργίες ή μπορούν να παράγουν μαζικά φαινόμενα πρέπει να τηρούνται σε υψηλότερα πρότυπα.
- Ο κίνδυνος είναι δυναμικός. Μειώνεται καθώς η τεχνολογία ωριμάζει και η εξοικείωση και η εμπειρία μεγαλώνουν. Καθώς κερδίζουμε εμπειρία στο IoT, ο κίνδυνος θα μειωθεί.

Όσον αφορά τη διαχείριση έργων και τη σημασία του IoT σε αυτήν, οι βιβλιογραφικές αναφορές και έρευνες δείχνουν ότι το έργο-κεντρικό περιβάλλον έχει μεγάλη υποστήριξη από την εφαρμογή της τεχνολογίας του IoT. Συγκεκριμένα, καθώς η τεχνολογία πληροφορικής εισάγεται με επιτυχία στη διαχείριση έργων, τα οφέλη είναι πολυάριθμα σε

πολλαπλά επίπεδα και επιπλέον το IoT θα επηρεάσει τα παραδοτέα των έργων και την ομαδική εργασία.

Σε μια καθημερινή χρήση, η νέα τεχνολογία θα αυξήσει την παραγωγικότητα και την αποδοτικότητα των διαδικασιών, μειώνοντας την σπατάλη πόρων, τόσο σε χρόνο όσο και σε χρήμα. Ο αντίκτυπος στον κύκλο ζωής του έργου είναι τεράστιος, στην πραγματικότητα όλες οι φάσεις επηρεάζονται από την τεχνολογία.

Ο κύριος οδηγός του αντίκτυπου είναι σίγουρα τα δεδομένα που συλλέγονται από έξυπνα αντικείμενα πάντα αξιόπιστα λόγω των προσεγγίσεων αποθήκευσης όπως το cloud ή server. Αυτή η προοπτική έχει ως αποτέλεσμα τη βελτιστοποίηση των διαδικασιών, την ενίσχυση της συνεργασίας και της επικοινωνίας λόγω της ταχύτερης ανταλλαγής δεδομένων και της υψηλότερης παραγωγικότητας όλων των μελών της ομάδας.

Η εφαρμογή του IoT δεν είναι εύκολη για μία εταιρεία. Στην πραγματικότητα έχουν τεκμηριωθεί τα τεχνολογικά και εταιρικά εμπόδια στις παραπάνω ενότητες. Ειδικότερα, τα τεχνολογικά ζητήματα συνδέονται εσωτερικά με την εταιρεία και εξωτερικά με το οικοσύστημα του IoT που πρέπει να δημιουργηθεί. Εσωτερικά, οι εγκαταστάσεις της εταιρείας πρέπει να είναι συμβατές και έτοιμες να στηρίξουν το οικοσύστημα.

Από την άλλη πλευρά, λόγω της έλλειψης κοινών προτύπων στον τομέα αυτό, στο εξωτερικό οικοσύστημα που δημιουργείται μεταξύ όλων των ενδιαφερομένων, πρέπει να βρεθεί ένα κοινό έδαφος για ό, τι αφορά την μορφή των αρχείων και τη διαλειτουργικότητα μεταξύ των διαφορετικών πλατφόρμων. Η εφαρμογή του οικοσυστήματος που δημιουργείται από το IoT για μία εταιρία είναι απαραίτητη από μακροοικονομική άποψη, προκειμένου να παραμείνει ανταγωνιστική στις αγορές της και να αυξήσει την ελκυστικότητα των πελατών.

Οι βασικές αρχές διαχείρισης έργου έχουν υποστεί σημαντική μεταβολή. Προηγουμένως, βασική αρχή της διαχείρισης έργου ήταν ο σχεδιασμός και η παρακολούθηση, επικεντρώνοντας αποκλειστικά στις σκληρές μεθοδολογίες (Pollack, J. & Adler, D., 2015). Τις τελευταίες δεκαετίες, οι ατομικές δεξιότητες γίνονται κυρίαρχες λόγω της αυξανόμενης πολυπλοκότητας του περιβάλλοντος έργου, η επικοινωνία είναι πλέον θεμελιώδης για τη διαχείριση των εμπλεκομένων και τη συνεργασία με εξωτερικά μέρη. Αυτό επιτρέπει τον συνδυασμό τυπικής και άτυπης αλληλεπίδρασης μεταξύ των μερών.

Σε αυτό το πλαίσιο, το IoT υποστηρίζει και ενισχύει και τις δύο πτυχές της διαχείρισης έργων. Στην πραγματικότητα, η απεριόριστη δυνατότητα συλλογής πληροφοριών από την υποδομή του IoT υποστηρίζει τον προγραμματισμό, τη κατάρτιση προϋπολογισμού και

παρακολούθηση, παρέχοντας πιο αξιόπιστες πληροφορίες για τη στήριξη αποφάσεων και δράσεων. Κατά τον ίδιο τρόπο, η επικοινωνία γίνεται ταχύτερη και ασφαλέστερη, η συμφόρηση απαλείφεται και τα δεδομένα διαβιβάζονται γρήγορα και με ασφάλεια μεταξύ των ενδιαφερομένων. Η λιγότερη ασάφεια και ο μικρότερος κίνδυνος θα αυξήσουν το ποσοστό επιτυχίας και την ικανότητα επίτευξης των παραδοτέων του έργου εντός περιορισμών.

Τα παραπάνω υπογραμμίστηκαν στις προηγούμενες ενότητες με τον τελικό σκοπό να καθοριστεί η μετατόπιση του επιχειρηματικού μοντέλου στο έργο-κεντρικό περιβάλλον που εφαρμόζει την τεχνολογία IoT από την παράδοση προϊόντων σε υπηρεσία. Οι νέες δυνατότητες θα επιφέρουν αλλαγές στις αρχές και τους ρόλους μέσα στο πλαίσιο της διαχείρισης έργων: θα είναι αναγκαίοι νέοι κανόνες και πολιτικές στο πλαίσιο του κύκλου ζωής του έργου για την αντιμετώπιση της περίπλοκης κατάστασης που θα προκύπτει από την ανταλλαγή δεδομένων μεταξύ των ενδιαφερομένων.

Οι διαχειριστές θα χρειαστεί να διαχειριστούν μια αυξανόμενη δέσμη δεξιοτήτων προκειμένου να χρησιμοποιήσουν αποτελεσματικά και επιτυχώς το μεγάλο όγκο δεδομένων που θα παρέχουν τα έξυπνα συνδεδεμένα στοιχεία. Χαρακτηριστικά που σχετίζονται με την τεχνολογία θα απλουστεύσουν το περιβάλλον που σχετίζεται με τα έργα, αλλά άλλες πτυχές του IoT θα αυξήσουν το επίπεδο πολυπλοκότητας, εισάγοντας νέα επίπεδα.

Το IoT ενισχύει όλους τους χαρακτηριστικούς ρόλους του έργου: οι τεχνικές δεξιότητες για τη στήριξη της διαδικασίας λήψης αποφάσεων θα υποστηρίζονται από την ποσότητα των δεδομένων που συλλέγονται από έξυπνα αντικείμενα και η επικοινωνία με τα ενδιαφερόμενα μέρη θα ενισχυθεί λόγω της διαφάνειας και της διευκόλυνσης της ανταλλαγής δεδομένων στο δημιουργούμενο οικοσύστημα. Όλα τα νέα χαρακτηριστικά θα διαμορφώσουν έναν πιο ευέλικτο ρόλο όσον αφορά τις προσεγγίσεις του κύκλου ζωής του έργου.

Η χρήση των δεδομένων από απομακρυσμένη πρόσβαση ισχυροποιεί τη διαδικασία λήψης αποφάσεων. Από την άλλη πλευρά ο έλεγχος της δυναμικής των έργων θα είναι δυσκολότερος. Στην πραγματικότητα ενδεχομένως να υπάρχει απώλεια του πλήρη ελέγχου από τον υπεύθυνο του έργου για το ίδιο το έργο και λανθασμένη ανάλυση των δεδομένων μπορεί να προκαλέσει ενδεχόμενη επιβράδυνση των εργασιών.

# Βιβλιογραφία


Anon. (2018, October). Ανάκτηση από https://project-management.com/top-5-project-management-phases/

Arduino. (2018, September). Ανάκτηση από Arduino: http://www.arduino.cc/

*ARTEMIS SOFIA project*. (2018, July). Ανάκτηση από http://www.sophia-project.eu/

Atzori, L. et al. (2010). The Internet of Things: A survey. *Computer Networks.*, 2787-2805.

B. N. Schilit and M. M. Theimer. (1994). Disseminating active map information to mobile. *Network,, vol. 8*(no. 5), σσ. 22–32.

Borgia, E. (2014). The Internet of Things vision: Key features, applications and open issues. . *Computer Communications. 54.*, 1-31.

Burke, R. &. (2014). *Project Management Leadership: Building Creative Teams.* John Wiley & Sons, 2nd edition.

Cardullo, M. (2003). *Genesis of the Versatile RFID Tag.* Ανάκτηση August 2018, από rfidjournal.com: www.rfidjournal.com/articles/pdf?392

Castellani, A.P., Bui, N., Casari, P., Rossi, M., Shelby, Z., Zorzi, M. (2010, March). Architecture and protocols for the Internet of Things: A case study. *Proc. Pervasive Computing and Communications Workshops (PERCOM Workshops)*, 678–683.

Center, U. I. (2018, July). Ανάκτηση από Ubiquitous ID Center: http://www.uidcenter.org/

Cho, C. S., & Gibson, G. E. (2001). Building project scope definition using project definition rating index. *Journal of Architectural Engineering*.

Christos Stergiou, Kostas E. Psannis, Byung-Gyu Kim, Brij Gupta. (2016). *Secure integration of IoT and Cloud Computing, Elsevier.* Future Generation Computer Systems.

*CMU SCS Coke Machine.* (2018, August). Ανάκτηση από cs.cmu.edu.: http://www.cs.cmu.edu/~coke/

D. Giusto, A. Iera, G. Morabito, and L. Atzori,. (2010.). *The Internet of Things.* New York, NY: Springer Science & Business Media.

De Poorter, E., Moerman, I., Demeester, P. (2011). Enabling direct connectivity between heterogeneous objects in the internet of things through a network service oriented architecture. *EURASIP Journal on Wireless Communications and Networking*, 61.

Duffy Marsan, C. (2018, August). *IAB Releases Guidelines for Internet-of-Things Developers.* Ανάκτηση από https://www.internetsociety.org/sites/default/files/Journal_11.1.pdf

Easterby-Smith et al. (2002). *Management Research: An Introduction.* 2nd edition. SAGE Publications. London. .

Evaristo. R. & Van Fenema, P. C. (1999). A typology of project management: emergence and evolution of new forms. . *International Journal of Project Management. 17 (5).*, 275-281.

Ferreira Da Silva, F., & Oliveira & Sa, J. (2016). Internet-of-Things: Strategic research agenda evolution. *Conference on Information Systems and Technologies (CISTI), 2016 11th Iberian .*

Fleisch E. (2018, October). *What is the internet of things – an economic perspective. Auto-ID labs white paper.* Ανάκτηση από http://www.im.ethz.ch/education/HS10/AUTOIDLABS-WP-BIZAPP-53.pdf

Franchi, A., Di Stefano, L., Tullio, S.C. (2010). Mobile Visual Search using Smart-M3. *Proc. IEEE Symposium on Computers and Communications (ISCC).*

Gaddis P.O. (1959). *The project manager.* Harvard Business Review.

Galis, A., & Gavras, A. (Επιμ.). (2013). A Cognitive Management Framework for Empowering the Internet of Things. *FIA 2013, LNCS 7858*, 187-199.

Gammelgaard B. (2004). Schools in logistics research. A methodological framework for analysis of the discipline. . *International Journal of Physical Distribution & Logistics Management. 34 (6).*, 479 – 491.

Gareis, R., Huemann, M.,. (2000). Project management competences in the project-oriented organisation. Στο J. S. Turner, *The Gower Handbook of Project Management* (σσ. 709-721). Gower, Aldershot.

Gemünden et al. (2017). The project-oriented organization and its contribution to innovation. . *International Journal of Project Management. 36. 147-160.* .

Ghimire S et al. (2015). IoT based situational awareness framework for real-time project management. *International Journal of Computer Integrated Manufacturing. 30(1)*, 74-83.

Giusto, D., Iera, A., Morabito, G., Atzori, L., Blefari Melazzi, N. (2010). CONVERGENCE: Extending the Media Concept to Include Representations of Real World Objects. *The Internet of Things*, 129–140.

Gorton I. et al. (1997). Collaborative tools and processes to support software engineering shift work. . *BT Technology Journal 15(3)*, 189-198.

Guinard, D., Trifa, V., Mattern, F., Wilde, E. (2010, December). From the Internet of Things to the Web of Things: Resource Oriented Architecture and Best Practices. *Architecting the Internet of Things.*

Hobday, M. (2000). The project-based organisation: an ideal form for managing complex products and systems. *Research Policy*, 29. 871–893.

Huemann, M. (2014). Managing the project-oriented organization. . Στο R. Turner, *Gower Handbook of Project Management* (σσ. 435–448). 5th. Edition. Surrey, England.

I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. (2002., Mar.). Wireless sensor. *Computer Networks networks: a survey, vol. 38*(no. 4), σσ. 393–422.

I. Toma, E. Simperl, and G. Hench. (2009.). A joint roadmap for semantic technologies and the internet of things. *Proceedings of the Third STI Roadmapping Workshop.*

iCore, F.-I.-2. p. (2018, September). *Internet Connected Objects for Reconfigurable Ecosystems.* Ανάκτηση από cordis.europa.eu: https://cordis.europa.eu/project/rcn/100873_en.html

Instituto National de Ciberseguridad, red.es, Huawei. (2017). *Building a Trusted and Managed IoT World.* Gobierno de España.

*internet_first_words.html.* (2018, August). Ανάκτηση από lk.cs.ucla.edu: https://www.lk.cs.ucla.edu/internet_first_words.html

J. P. Vasseur and A. Dunkels. (2008.). *IP for smart objects.* IPSO Alliance.

Jackson, M.C. (2006). Creative holism: a critical systems approach to complex problem situations. . *Systems Research and Behavioural Science*, 23 (5). 647-57.

Jonsson N. et al . (2001). Successful Management of Complex, Multinational R&D Projects. . *Proceedings of the thirty-fourth Hawai'I International Conference on Systems Sciences.* Hawai: IEEE Computer Society Press.

Jugdev, K., et al. (2013). An exploratory study of project success with tools, software and methods. *International Journal of Managing Projects in Business*, 6 (3), 534-551. .

Kelaidonis, D., Somov, A., Foteinos, V., Poulios, G., Stavroulaki, V., Vlacheas, P., Demestichas, P., Baranov, A., Rahim Biswas, A., Giaffreda, R. (2012). Virtualization and Cognitive Management of Real World Objects in the Internet of Things. *The IEEE International Conference on Internet of Things.* Besancon, France.

Konnikova, M. (2014, September 4). The Hazards of Going on Autopilot. *New Yorker*. Ανάκτηση November 2018, από http://www.newyorker.com/science/maria-konnikova/hazards-automation

Kortuem, G. et al. (2010). Smart Objects as Building Blocks for the Internet of things. . *IEEE Computer Society*, 44-51.

Kostelnik, P., Sarnovsky, M., Furdik, K. (2011, June). The Semantic Middleware for Networked Embedded Systems Applied in the Internet of Things and Services. *Proc. 2nd Workshop on Software Services (WoSS)*. Timisoara, Romania.

Kuura, A. et al. (2014). Entrepreneurship and projects: Linking segregated communities. *Scandinavian Journal of Management, 30, 214-230*.

L. Atzori, A. Iera, and G. Morabito. (2010., Oct.). The Internet of Things: A survey. *Computer, vol. 54*(no. 15), σσ. 2787–2805.

Lewis, J. A. (2016). *Managing Risk for the Internet of Things.* Center for strategic & International Studies, Washington DC. Ανάκτηση από www.csis.org

Libelium. (2018, September). Ανάκτηση από Waspmote: http://www.libelium.com/products/waspmote

Liu Z. et al. (2016). Supply chain technologies: Linking adoption, utilisation, and performance. *Journal of Supply Chain Management. 52 (4).*, 22-41.

Lu W., et al. (2011). Scenarios for applying RFID technology in construction project management. *Automation in Construction, vol. 20, issue 2*, 101-106.

M. L. HEILIG. (χ.χ.). Stereoscopic-television apparatus for individual use. *US2955156.*

M. Lamming and M. Flynn. (1994.). *Forget-me-not: Intimate computing in support of.* Proc FRIEND21.

M. Presser and A. Gluhak,. (2009.). The Internet of Things: Connecting the Real World with the. *EURESCOM mess@ ge–The Magazine for Telecom*.

M. Weiser. (χ.χ.). *The Computer for the 21st Century.* Ανάκτηση August 2018, από wiki.daimi.au.dk.: wiki.daimi.au.dk/pca/_files/weiser-orig.pdf

Mackenzie, K. D. (1991). *The Organizational Hologram: The Effective Management of Organizational Change.* Boston, MA: Kluwer Academic Publishers.

Markoff, J. (2015). *Machines of Loving Grace: The Quest for Common Ground between Humans and Robots.* New York: Ecco.

Massie, J. (1979). *Essentials of Management.* Englewood Cliffs: NJ: Prentice-Hall.

McKinsey Global Institute. (2013). *Disruptive technologies: Advanced that will transform life, business, and the global economy.* McKinsey & Company.

Morgan, G. (1993). *Imaginization: New Mindsets for Seeing, Organizing and Managing, Newbury Park and San Francisco.* CA: Sage Publications.

Morris P. et al. (2010). *The Oxford Handbook of Project Management. .* Oxford, UK: Oxford University Press.

Motiwalla, F. L. & Thompson, J. (2009). *Enterprise systems for management. Upper saddle River. .* NJ: Prentice Hall.

Nash, J. B. (1932). *Spectatoritis*.

*National Highway Traffic Safety Administration*. (2018, November). (National Highway Traffic Safety Administration) Ανάκτηση από fars.nhtsa.dot.gov: http://www-fars.nhtsa.dot.gov/Main/index.aspx

PMBOK Guide. (2000). *The Project Management.* ISBN: 1-880410-43-5: PMI Book Team.

Pollack, J. & Adler, D. (2015). Emergent trends and passing fads in project management research: a scientometric analysis of changes in the field. . *International Journal of Project Management. 33 (1), 236–248.* .

Porter, M.E. & Heppelmann, J.E. . (2014). How smart, connected products are transforming competition. . *Harvard Business Review*, 11-64.

Porter, M.E. & Heppelmann, J.E. . (2014). How smart, connected products are transforming competition. . *Harvard Business Review*, 11–64.

Project Management Institute. . (2008). *A guide to the Project Management Body of Knowledge: PMBOK guide.* Project Management Institute.

Ravindra P. Nitin S.Wagh. (2018, September). *www.ijaiem.org.* Ανάκτηση από ijaiem.org: http://www.ijaiem.org/Volume5Issue2/IJAIEM-2016-02-20-18.pdf

S. Sarma, D. L. Brock, and K. Ashton. (χ.χ.). *The Networked Physical World.*

S. Sarma, D. L. Brock, and K. Ashton. (χ.χ.). *The Networked Physical World.*

Saariko T., et al. (2007). The Internet of Things: Are you ready for what´s coming? *Business Horizons*, 667-676.

*Samsung Privacy Policy--SmartTV Supplement.* (2018, September). Ανάκτηση από samsung.com: http://www.samsung.com/sg/info/privacy/smarttv.html

Sawyer, L. (2018, October). *Benefits of Project Management Training.* Ανάκτηση από parallelprojecttraining.com.: http://www.parallelprojecttraining.com/our-approach/benefits-of-projectmanagement-training

Schonwalder, J., Fouquet, M., Rodosek, G., Hochstatter, I. (2009). Future Internet = content + services + management. *IEEE Communications Magazine, Vol 47*(7), σσ. 27–33.

SENSEI, F.-I.-2. p. (2018, September). *Integrating the Physical with the Digital World of the Network of the Future.* Ανάκτηση από cordis.europa.eu: https://cordis.europa.eu/project/rcn/85429_en.html

Slovic, P. (1987, April). Perception of Risk. *Science 236*(no. 4799).

*SmartThings*. (2018, September). Ανάκτηση από smartthings.com: http://www.smartthings.com/how-it-works

Smith, B. & Dodds, B. (1997). Developing managers in the project-oriented organization. *Journal of European Industrial Training. 21 (5). 165-170.*

Söderlund, J. (2004). Building theories of project management: past research, questions for the future. *International Journal of Project Management.*, 22. 183-191.

Somasundaram, S. & Badiru, A.B. (1992). Project management for successful implementation of continuous quality improvement. *International Journal of Project Management. 10 (2). 89–101.* .

Staadt, J. . (2012). Redesigning a project-oriented organization in a complex system – A soft systems methodology approach. . *International Journal of Managing Projects in Business. 5 (1). 51-66*.

Thomas. J. et al. (2004). Surfing on the edge of chaos – developing the master project manager. *PMI global conference 2004 – North America.* Conference proceedings. Newtown Square (PA): Project Management Institute.

Tschofenig, H. e. (2018, August). *Architectural Considerations in Smart Object Networking.* Ανάκτηση από rfc-editor.org: https://www.rfc-editor.org/rfc/rfc7452.txt

Turner, R. et al. (2010). *Perspectives on projects.* Routledge.

Turner, R.J., Keegan, A.,. (2001). Mechanisms of governance in the project-based organization: the role of the broker and steward. . *European Management Journal*, 254-267.

Uusitalo, M. (2006). Global Vision for the Future Wireless World from the WWRF. *Vehicular Technology Magazine, Vol 1*(No 2), σσ. 4–8.

Vogt, H. (2002,). Efficient Object Identification with Passive RFID Tags. *Pervasive Computing, vol. 2414*(no. 9), σσ. 98–113.

Weinberg et al. (2015). Internet of Things: Convenience vs privacy and security. . *Business Horizon. 58.*, 615-624.

Weiser, M. (1991, September). The Computer for the Twenty-First Century. *Scientific American*, σσ. 94-100.

Woodland, N. J. (χ.χ.). Wonders of Modern Technology: Barcodes Sweep the World.

Ζώης, Α.Κ.- Γαρουφάλης, Δ.Κ. (2008). *Οικονομικός Προγραμματισμός Επιχειρήσεων.* ΕΚΔ: Σύγχρονη Εκδοτική.