ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΓΑΡΜΟΓΩΝ
ΤΜΗΜΑ ΜΗΧΑΝΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ Τ.Ε.

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΑΣΦΑΛΕΙΑ ΥΠΟΛΟΓΙΣΤΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΣΕ ΔΙΚΤΥΑ SMART GRID

ΟΝΟΜΑΤΕΠΩΝΥΜΟ ΣΠΟΥΔΑΣΤΩΝ: Βασιλείου Λάμπρος
Πέππας Θεμιστοκλής

ΕΠΟΠΤΕΥΩΝ ΚΑΘΗΓΗΤΗΣ: Απόστολος Φούρναρης

ΠΑΤΡΑ – 2014

ΠΡΟΛΟΓΟΣ

Σύμφωνα με τις επιταγές για ένα αξιόπιστο, προσαρμοστικό και οικονομικό δίκτυο ενέργειας, η παγκόσμια κοινότητα ενεργειακών συστημάτων προσανατολίζεται στην ενσωμάτωση τεχνολογιών πληροφορικής και δικτύων στο υπάρχον ενεργειακό πλέγμα ώστε να ελέγχεται, παράγεται, διανέμεται και καταναλώνεται καλύτερα η ηλεκτρική ενέργεια. Στόχος είναι το δίκτυο ηλεκτρικής ενέργειας να λειτουργεί σε πραγματικό χρόνο σαν ένα μεγάλο πληροφοριακό σύστημα όπου η ηλεκτρική ενέργεια θα είναι βασικό αγαθό. Όμως, όπως όλα τα πληροφοριακά συστήματα έτσι και το έξυπνο αυτό δίκτυο ενέργειας είναι ευάλωτο σε επιθέσεις πληροφοριακών συστημάτων (hacking, cyber attacks) με τεράστια συμφέροντα να διακυβεύονται τόσο σε τοπικό όσο και σε εθνικό, πολυεθνικό επίπεδο σε περίπτωση δικτυακής εισβολής. Η πτυχιακή εργασία στοχεύει στη μελέτη του έξυπνου δικτύου (smart grid) και των κενών ασφάλειας που υπάρχουν στα πληροφοριακά συστήματα που το απαρτίζουν με στόχο τον χαρακτηρισμό του «έξυπνου» δικτύου ενέργειας από πλευράς ασφάλειας. Το έξυπνο δίκτυο Smart Grid είναι στην ουσία ο αντικαταστάτης του υπάρχον απαρχαιωμένου δικτύου ηλεκτρικής ενέργειας. Τα ευεργετικά χαρακτηριστικά του έξυπνου δικτύου συμβάλλουν στην καλύτερη αξιοποίηση της ηλεκτρικής ενέργειας τόσο στην πλευρά της παραγωγής όσο και στην πλευρά της κατανάλωσης.

Ωστόσο, η χρήση νέων τεχνολογιών και ειδικά αυτών που έχουν άμεση σχέση με το διαδίκτυο, ενδεχομένως να εισάγουν νέες απειλές και κακόβουλες πράξεις στην ασφάλεια του έξυπνου δικτύου. Οι επιτιθέμενοι (hackers ,spammers κτλ), αν υπάρχουν κενά ασφάλειας, ίσως το εκμεταλλευτούν και καταφέρουν να υποκλέψουν απόρρητες πληροφορίες ή ακόμα και να διακόψουν την παροχή ρεύματος και άλλων απαραίτητων υπηρεσιών. Άρα όπως είναι λογικό τα ζητήματα ασφάλειας στο έξυπνο δίκτυο παίζουν πρωταρχικό ρόλο, και με αυτά θα ασχοληθούμε στην πτυχιακή μας εργασία.

ΠΕΡΙΛΗΨΗ

Στην παρούσα πτυχιακή εργασία θα αναφερθούμε στην ασφάλεια των υπολογιστικών συστημάτων στο έξυπνο δίκτυο ηλεκτρικής ενέργειας. Τα πρώτα δύο κεφάλαια είναι εισαγωγικά στην πτυχιακή μας εργασία και έχουν σκοπό να μυήσουν τον αναγνώστη στο έξυπνο δίκτυο και στην ασφάλειά του. Στα κεφάλαια τρία έως και εφτά αναφερόμαστε σε ένα συστατικό ή χαρακτηριστικό του έξυπνου δικτύου και αφού το περιγράψουμε συνοπτικά παρουσιάζουμε τους πιθανούς κινδύνους καθώς και τρόπους αντιμετώπισης του. Κλείνοντας την πτυχιακή μας εργασία αναφερόμαστε στους τρόπους αντιμετώπισης των κινδύνων του έξυπνου δικτύου καθώς και στα συμπεράσματά μας.

Θα ξεκινήσουμε παρουσιάζοντας στο εισαγωγικό κεφάλαιο (1^{ο}) τα θέματα ασφάλειας που παρουσιάζονται στο έξυπνο δίκτυο. Επίσης, θα αναφερθούμε διεξοδικά στις ερευνητικές τάσεις για να αποκτήσουμε εικόνα για την πρόοδο που σημειώνεται. Στο επόμενο κεφάλαιο (2^{ο}) θα αναφερθούμε στο έξυπνο δίκτυο και θα παρουσιάσουμε όσο ποιο αναλυτικά γίνεται τα θέματα που άπτονται στους κινδύνους που υφίσταται καθώς και τρόπους αντιμετώπισής τους. Συνεχίζοντας στο επόμενο κεφάλαιο (3^{ο}) θα παρουσιάσουμε τα προβλήματα ασφάλειας καθώς τους τρόπους αντιμετώπισης τους όσον αφορά τους έξυπνους μετρητές και τον τελικό καταναλωτή. Στο σημείο αυτό πρέπει να αναφέρουμε ότι οι έξυπνοι μετρητές είναι βασικό και αναπόσπαστο συστατικό των έξυπνων δικτύων.

Τα επόμενα δύο κεφάλαια (4^{ο} και 5^{ο}) παρουσιάζουν θέματα ασφάλειας που άπτονται της αυτοματοποιημένης διανομής και μεταφοράς ηλεκτρικού φορτίου. Τα κεφάλαια αυτά αναφέρονται στα συστατικά του ηλεκτρικού δικτύου που εμπλέκονται στην μεταφορά και διανομή της ηλεκτρικής ενέργειας, από τον παραγωγό στον καταναλωτή του ηλεκτρικού δικτύου. Το επόμενο κεφάλαιο (6^{ο}) αναφέρεται στην κατανεμημένη παραγωγή ηλεκτρικής ενέργειας. Αυτό το κεφάλαιο όπως και το επόμενο (7^{ο}) εστιάζουν σε κινδύνους που αντιμετωπίζουν η παραγωγή ηλεκτρικής ενέργειας και η εφοδιαστική αλυσίδα του έξυπνου δικτύου. Το προ-τελευταίο κεφάλαιο (8^{ο}) παρουσιάζει συνολικά τρόπους αντιμετώπισης των κινδύνων στο έξυπνο δίκτυο (στην ολότητά του). Στο τελευταίο κεφάλαιο (9^{ο}) της πτυχιακής μας εργασίας παρουσιάζουμε τα συμπεράσματά της έρευνας που πραγματοποιήσαμε.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΠΙΝΑΚΑΣ ΕΙΚΟΝΩΝ

ΠΙΝΑΚΑΣ ΠΙΝΑΚΩΝ

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

COTS: Commercial Off The Shelf

SCADA: Supervisory Control And Data Acquisition

PCS: Process Control Systems

HDVC: High Voltage Direct Current

AC: Asynchronous Current

DC: Direct Current

ENTSO: European Network of Transmission System Operators

ACER: Agency for the Cooperation of Energy Regulators

DSO: Distribution System Operator

TSO: Transmission System Operator

NSO: Network System Operator

AMI: Advanced Metering Infrastructure

MDM: Metering Data Management

CIRT: Computer Incident Response Team

BCP: Business Continuity Plan

HAN: Home Area Network

BAN: Business Area Network

IAN: Industrial Area Network

NAN: Neighbor Area Network

WAN: Wide Area Network

MitM: Man in the Middle

DSL: Digital Subscriber Line

GPRS: General Packet Radio Service

MPLS: Multi Protocol Label Switching

PLC: Power Line Carrier

IP: Internet Protocol

SMCG: Smart Meter Co-ordination Group

LMS: Local Metrological Network

FAN: Field Area Network

LAN: Local Area Network

BAN: Building Area Network

HVAC: Heating, Ventilation, and Air Conditioning

NISTIR: National Institute of Standards and Technology

NISTIR: National Institute of Standards and Technology Internal Report

DoS: Denial Of Service

DDOS: Distributed Denial of Service

RTC: Real Time Clock

PPM: Parts Per Million

PKI: Public Key Infrastructure

DAS: Distribution Automation Systems

SPID: Strategic Power Infrastructure Defense

HES: Head-End System

DMZ: De Militarized Zone

ENISA: European Network & Information Security Agency

1. ΕΙΣΑΓΩΓΗ

Η σημερινή δομή του ηλεκτρικού δικτύου είναι παρωχημένη τόσο από την πλευρά της υποδομής όσο και των υπηρεσιών που παρέχει. Γι' αυτό το λόγο γίνεται σταδιακά η εισαγωγή σε λειτουργία του έξυπνου δικτύου (Smart Grid). Το έξυπνο δίκτυο είναι μια αναβαθμισμένη έκδοση του υπάρχοντος απαρχαιωμένου δικτύου ηλεκτρικής ενέργειας. Παρέχει πολλές νέες λειτουργίες που μπορούν να ανταποκριθούν στις νέες απαιτήσεις των χρηστών του. Αυτή η αναβάθμιση του ηλεκτρικού δικτύου μπορεί να δημιουργήσει καινούργια προβλήματα ασφάλειας στο σύστημα. Με αυτά τα ζητήματα ασφάλειας θα ασχοληθούμε στην παρούσα πτυχιακή εργασία.

Το έξυπνο δίκτυο ηλεκτρικής ενέργειας είναι η σύγκλιση της τεχνολογίας των πληροφοριών, των επικοινωνιών και της μηχανικής του υπάρχοντος ηλεκτρικού δικτύου για να παράσχουν ένα πιο ισχυρό, αποτελεσματικό και ευέλικτο σύστημα. Η ιδέα πίσω από το έξυπνο δίκτυο προσδιορίζει την προσθήκη της αμφίδρομης επικοινωνίας και των πληροφοριών στο δίκτυο ηλεκτρικής ενέργειας για την διευκόλυνση παροχής στους καταναλωτές μετρήσεων σε πραγματικών χρόνο, την δυνατότητα απομακρυσμένου ελέγχου των οικιακών συσκευών μέσω έξυπνων μετρητών, και την διευκόλυνση της ευρείας χρήσης των προγραμμάτων ανταπόκρισης στη ζήτηση. Η ανταπόκριση στην ζήτηση γίνεται δυνατή από ένα βοηθητικό πρόγραμμα για τον έλεγχο των φορτίων των καταναλωτών, προκειμένου να μειωθεί το συνολικό φορτίο του συστήματος. Αυτές οι τεχνολογίες θα μετατρέψουν το δίκτυο ηλεκτρικής ενέργειας σε ένα αμφίδρομο σύστημα ενέργειας στο οποίο οι πελάτες θα μπορούν να παρέχουν καθώς και να λαμβάνουν ηλεκτρικό ρεύμα από το ηλεκτρικό δίκτυο, μετατρέποντας έτσι το πλέγμα σε ένα κατανεμημένο σύστημα παραγωγής ηλεκτρικής ενέργειας.

Η ασφάλεια είναι ζωτικής σημασίας για σημαντικές υποδομές όπως ηλεκτρικό δίκτυο. Είναι γνωστό ότι οι παραβιάσεις της ασφάλειας των συστημάτων πληροφορικής στο δίκτυο ηλεκτρικής ενέργειας μπορεί να έχουν καταστροφικά αποτελέσματα και η πιθανότητα των εν λόγω παραβάσεων αυξάνεται, καθώς το δίκτυο ηλεκτρικής ενέργειας όλο και περισσότερο στηρίζεται σε πολύπλοκα διασυνδεδεμένα δίκτυα υπολογιστών. Αυτό θα αποτελέσει σημαντική πρόκληση για το σχεδιασμό του συστήματος ασφαλείας στο έξυπνο δίκτυο. Κανείς από τους υπάρχοντες μηχανισμούς πιστοποίησης δεν πληροί τις απαιτήσεις ενός έξυπνου δικτύου, καθώς και οι υπάρχουσες λύσεις ταυτοποίησης βασίζονται σχεδόν αποκλειστικά σε εμπορικές λύσεις (COTS) ή απλά βασίζονται στην υποδομή ασφαλείας του διαδικτύου. Ωστόσο, οι γνωστές μέθοδοι για την εξασφάλιση δικτύων ηλεκτρονικών υπολογιστών ή του διαδικτύου μπορεί να μην είναι επαρκείς λόγω έλλειψης των απαραίτητων ασφαλών μηχανισμών ή να είναι επιρρεπείς σε επιθέσεις Denial of Services (DoS).Οι επιθέσεις άρνησης εξυπηρέτησης (DoS) είναι οι επιθέσεις εναντίον ενός υπολογιστή ή μιας παρεχόμενης υπηρεσίας, οι οποίες έχουν ως σκοπό να καταστήσουν τον υπολογιστή ή την υπηρεσία ανίκανη να δεχτεί άλλες συνδέσεις και έτσι να μην μπορεί να εξυπηρετήσει άλλους πιθανούς πελάτες.

1.1. ΚΙΝΔΥΝΟΙ ΑΣΦΑΛΕΙΑΣ

Το έξυπνο δίκτυο πρόκειται να εισάγει καινούργια λειτουργικότητα στο υπάρχον σύστημα ηλεκτρικής ενέργειας, ωστόσο θα εισάγει αρκετούς κινδύνους ασφάλειας στο σύστημα. Βασιζόμαστε στο ηλεκτρικό δίκτυο για ηλεκτρικό ρεύμα και αυτή μας η εξάρτηση κάνει το ηλεκτρικό δίκτυο ένα κρίσιμο κεφάλαιο για την καθημερινότητά. Οποιαδήποτε διαταραχή στην διανομή ηλεκτρικής ενέργειας θα έχει μεγάλο κοινωνικό αντίκτυπο. Η ασφάλεια του ηλεκτρικού δικτύου είναι ένα σημαντικό θέμα. Το έξυπνο δίκτυο θα εισάγει αρκετούς νέους κινδύνους ασφάλειας που θα σχετίζονται με τις απαιτήσεις για επικοινωνία, τον αυτοματισμό των συστημάτων, τις νέες τεχνολογίες και την συγκέντρωση δεδομένων.

Η ραχοκοκαλιά του έξυπνου δικτύου θα είναι το ίδιο του το ηλεκτρικό δίκτυο. Αυτό το δίκτυο θα συνδέει τα διαφορετικά εξαρτήματα του έξυπνου δικτύου και θα επιτρέπει την αμφίδρομη επικοινωνία μεταξύ τους. Η διασύνδεση των εξαρτημάτων θα εισάγει κινδύνους στο σύστημα, αλλά αυτή η διασύνδεση είναι αναγκαία για να υλοποιηθούν οι κύριες λειτουργικότητες του έξυπνου δικτύου. Η διασύνδεση των διαφορετικών εξαρτημάτων θα αυξήσει την πολυπλοκότητα του ηλεκτρικού δικτύου, η οποία στην συνέχεια θα αυξήσει τον αριθμό των ευκαιριών για νέους κινδύνους στην ασφάλεια. Επίσης, θα αυξηθεί ο αριθμός των σημείων εισόδου από τα οποία μπορεί κανείς να αποκτήσει πρόσβαση στο ηλεκτρικό δίκτυο, όταν έχουν διασυνδεθεί όλα τα εξαρτήματα του έξυπνου δικτύου.

Το έξυπνο δίκτυο θα χρησιμοποιήσει τα δεδομένα που μεταδίδονται από το δίκτυο ηλεκτρικής ενέργειας και λογισμικό για να διατηρήσει αυτόματα το σύστημα ενέργειας. Το να βασιστεί κάποιος στο δίκτυο ηλεκτρικής ενέργειας για την μεταφορά πληροφοριών του συστήματος εισάγει κινδύνους για την ασφάλεια. Ορισμένα από τα εξαρτήματα απαιτούν δεδομένα σε πραγματικό χρόνο και οποιαδήποτε καθυστέρηση ή απώλεια δεδομένων μπορεί να έχει δυσμενείς επιπτώσεις στο δίκτυο ηλεκτρικής ενέργειας. Το λογισμικό που θα διαχειρίζεται την κατάσταση του συστήματος βρίσκεται επίσης σε κίνδυνο για κακόβουλο κώδικα που μπορεί να αλλάξει τη λειτουργικότητά του. Μια διαταραχή στις επικοινωνίες ή στο λογισμικό διαχείρισης κατάστασης μπορεί να οδηγήσει σε απώλεια της ενέργειας ή σε τραυματισμό ή απώλεια ζωής σε ακραίες περιπτώσεις.

Η δικτύωση των διαφορετικών εξαρτημάτων του συστήματος ηλεκτρικής ενέργειας θα απαιτήσει διαφορετικές τεχνολογίες να μπορέσουν να αλληλεπιδράσουν μεταξύ τους. Αυτή η αλληλεπίδραση μεταξύ των διαφορετικών τεχνολογιών θα εισάγει νέους κινδύνους για την ασφάλεια. Το έξυπνο δίκτυο θα πρέπει να μπορεί να υποστηρίξει παλιομοδίτικα συστήματα (legacy systems). Τα συστήματα αυτού του τύπου, στην πλειονότητα των περιπτώσεων, δεν υλοποιούν τα καινούργια χαρακτηριστικά ασφάλειας που έχουν τα μοντέρνα συστήματα, και όπως πολύ καλά γνωρίζουμε ένα σύστημα είναι τόσο ασφαλές όσο ο ποιο αδύναμος κρίκος του. Επιπλέον, οι καινούργιες τεχνολογίες που χρησιμοποιούνται στο έξυπνο δίκτυο μπορούν να έχουν ευπάθειες στην ασφάλεια που κάποιος θα μπορεί να εκμεταλλευθεί.

Το έξυπνο δίκτυο θα συλλέγει πολλά περισσότερα δεδομένα από ότι κάνει το υπάρχον σύστημα ηλεκτρικής ενέργειας. Εκτιμάται ότι θα υπάρξει μια μεγάλη αύξηση του μεγέθους δεδομένων που πρόκειται να διακινηθεί και να χρησιμοποιηθεί. Η αύξηση στην συλλογή δεδομένων μπορεί πιθανότατα να δημιουργήσει κινδύνους για την ασφάλεια. Επίσης, το έξυπνο δίκτυο θα συλλέγει νέους τύπους δεδομένων που δεν καταγράφονται στο παλιό σύστημα, πράγμα το οποίο επίσης μπορεί να δημιουργήσει κινδύνους για την ασφάλεια [1].

1.2. ΣΤΟΧΟΙ ΑΣΦΑΛΕΙΑΣ

Οι στόχοι για την ασφάλεια που πρέπει να τεθούν για το έξυπνο δίκτυο είναι διαφορετικοί από ότι ισχύει σχεδόν στους περισσότερους βιομηχανικούς κλάδους. Είναι σημαντικό να τονίσουμε ότι κάθε μέτρο για την ασφάλεια που εφαρμόζεται στο έξυπνο δίκτυο δεν πρέπει να εμποδίζει την διαθεσιμότητα ή την ασφάλειά του. Ένα παράδειγμα αυτού θα μπορούσε να είναι το κλείδωμα μετά από επανειλημμένες αποτυχημένες προσπάθειες εισαγωγής κωδικού πρόσβασης. Το σύστημα ενέργειας θα πρέπει να είναι πάντα διαθέσιμο. Συνεπώς, το κλείδωμα του συστήματος κατά την διάρκεια μιας έκτακτης κατάστασης θα μπορούσε να προκαλέσει προβλήματα ασφάλειας. Οι στόχοι ασφάλειας που πρέπει να αξιολογούνται στο έξυπνο δίκτυο είναι η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα. Στις περισσότερες βιομηχανίες η εμπιστευτικότητα και η ακεραιότητα έχουν υψηλότερη προτεραιότητα από την διαθεσιμότητα. Στο σύστημα ηλεκτρικής ενέργειας πρέπει να είναι πάντα διαθέσιμο το ηλεκτρικό ρεύμα, συνεπώς αυτός είναι ο σημαντικότερος στόχος για την ασφάλεια. Η ακεραιότητα είναι ο αμέσως επόμενος σημαντικός στόχος για την ασφάλεια και ακολουθεί η εμπιστευτικότητα.

Η διαθεσιμότητα είναι ο ποιο σημαντικός στόχος για την ασφάλεια. Κατά επέκταση ο σημαντικότερος στόχος για την ασφάλεια στα περισσότερα εξαρτήματα του συστήματος

ηλεκτρικής ενέργειας είναι επίσης η διαθεσιμότητα. Τα κρίσιμα συστήματα πραγματικού χρόνου στο έξυπνο δίκτυο έχουν κατ' εκτίμηση το μέγιστο καθυστέρηση 4 χιλιοστά του δευτερολέπτου. Αυτά τα συστήματα παρακολουθούν συνεχώς την κατάσταση του ηλεκτρικού δικτύου και μια διαταραχή στις επικοινωνίες μπορεί να προκαλέσει ενεργειακές απώλειες. Στον πίνακα 1 απαριθμούνται οι μέγιστες κατ' εκτίμηση απαιτήσεις για καθυστερήσεις.

Μέγιστη Καθυστέρηση	Τύπος Επικοινωνίας
Μικρότερη από 4 ms	Προστατευτική μετεγκατάσταση
Υπό-δευτερόλεπτα	Παρακολούθηση για την επίγνωση της κατάστασης ευρείας περιοχής
Δευτερόλεπτα	Εποπτικός έλεγχος και απόκτηση δεδομένων (SCADA) για τους υποσταθμούς και τους τροφοδότες
Λεπτά	Παρακολούθηση μη κρίσιμων εξαρτημάτων και πληροφορίες τιμολόγησης της αγοράς
Ώρες	Ανάγνωση μετρητών και πληροφορίες τιμολόγησης μεγαλύτερου χρονικού διαστήματος
Ημέρες / Εβδομάδες / Μήνες	Συγκέντρωση δεδομένων χρήσης για μεγάλο χρονικό διάστημα

Πίνακας 1, Κατ' εκτίμηση απαιτήσεις για μέγιστη καθυστέρηση στις επικοινωνίες [1]

Η ακεραιότητα είναι ο αμέσως επόμενος σημαντικός στόχος για την ασφάλεια στο έξυπνο δίκτυο. Το έξυπνο δίκτυο χρησιμοποιεί δεδομένα που συλλέγονται από διάφορους αισθητήρες και πράκτορες. Αυτά τα δεδομένα χρησιμοποιούνται για την παρακολούθηση της τρέχουσας κατάστασης του συστήματος ηλεκτρικής ενέργειας. Η ακεραιότητα αυτών των δεδομένων είναι πάρα πολύ σημαντική. Η μη εξουσιοδοτημένη τροποποίηση αυτών των δεδομένων ή η εισαγωγή δεδομένων από άγνωστες πηγές μπορεί να δημιουργήσει αποτυχίες ή καταστροφές στο σύστημα ηλεκτρικής ενέργειας. Το ηλεκτρικό ρεύμα στο ηλεκτρικό δίκτυο δεν πρέπει μόνο να είναι πάντα διαθέσιμο, αλλά θα πρέπει να έχει και ποιότητα. Η ποιότητα της ηλεκτρικής ενέργειας θα εξαρτάται από την ποιότητα της εκτίμησης για την τρέχουσα κατάσταση του συστήματος ηλεκτρικής ενέργειας. Η ποιότητα για την εκτίμηση της κατάστασης θα βασίζεται σε πολλούς παράγοντες, αλλά η ακεραιότητα των δεδομένων που εισάγονται είναι πολύ σημαντική.

Ο τελευταίος στόχος για την ασφάλεια είναι η εμπιστευτικότητα. Η απώλεια εμπιστευτικότητας στα δεδομένα στο έξυπνο δίκτυο έχει λιγότερο κίνδυνο είτε από την διαθεσιμότητα είτε από την ακεραιότητα. Στο έξυπνο δίκτυο υπάρχουν συγκεκριμένες περιοχές που η εμπιστευτικότητα είναι ποιο σημαντική. Η προστασία των πληροφοριών των πελατών, οι γενικές πληροφορίες της επιχείρησης και οι πληροφορίες της αγοράς ηλεκτρικής ενέργειας είναι μερικά παραδείγματα [1].

1.3. ΚΙΝΔΥΝΟΙ ΕΝΑΝΤΙΟΝ ΠΡΟΤΕΡΗΜΑΤΩΝ

Η ανάπτυξη του έξυπνου δικτύου δεν είναι σίγουρο το κατά πόσον θα κάνει το ηλεκτρικό δίκτυο ασφαλέστερο, ποιο αξιόπιστο ή ποιο προστατευμένο. Η ιστορία μας έχει διδάξει ότι η υιοθέτηση καινούργιων τεχνολογιών δεν μας πηγαίνει πάντα ένα βήμα μακρύτερα. Χαρακτηριστικό παράδειγμα είναι η πυρηνική ενέργεια που ενώ είναι καθαρότερη από τα ορυκτά καύσιμα έχουν συμβεί μείζονα και πολύνεκρα ατυχήματα λόγω προβλημάτων ασφάλειας. Για πολλά χρόνια η χρησιμοποίηση της πυρηνικής ενέργειας είχε μείνει στάσιμη λόγω αυτών των προβλημάτων ασφάλειας και παρά μόνο τα τελευταία χρόνια γίνονται βήματα προς τα εμπρός με την εμφάνιση ασφαλέστερων πυρηνικών σταθμών. Η σύγκριση του έξυπνου δικτύου όμως με την πυρηνική ενέργεια είναι ατυχής, γιατί το έξυπνο δίκτυο είναι κατά βάση μια συλλογή τεχνολογιών πολλές από τις οποίες λειτουργούν ανεξάρτητα η μία από την άλλη. Το έξυπνο δίκτυο αντιμετωπίζει τα δικά του προβλήματα ασφάλειας, που πολλές φορές είναι μοναδικά, τα οποία μπορεί να έχουν διαφορετικούς ενδιαφερόμενους ακόμα και διαφορετικά συμφέροντα των συμμετεχόντων που πρέπει να ληφθούν υπόψη.

Ωστόσο, όπως και το υπάρχων ηλεκτρικό δίκτυο αντιμετωπίζει θέματα επάρκειας και αλληλεξάρτησης, αντίστοιχα θέματα θα αντιμετωπίσει και θα επιλύσει επιτυχώς και το έξυπνο δίκτυο. Αυτό που πρέπει να ληφθεί υπόψη κατά το σχεδιασμό και την υλοποίηση του έξυπνου δικτύου είναι το που πρέπει να ενσωματωθούν η επάρκεια, η ανθεκτικότητα ακόμα και η αυτό-επάρκεια μέσα στο υπάρχον ηλεκτρικό δίκτυο. Αυτή η ενσωμάτωση πρέπει να γίνει με τέτοιο τρόπο ώστε να διατηρηθούν οι οικονομίες κλίμακας που παρέχει ένα ανεξάρτητο δίκτυο. Εάν αυτή η ενσωμάτωση γίνει με λανθασμένο τρόπο αυτό θα σημαίνει ότι έχει δημιουργηθεί ένα δίκτυο το οποίο είναι λιγότερο αξιόπιστο και επιρρεπές σε επικαλυπτόμενες διακοπές ρεύματος. Από την άλλη εάν η ενσωμάτωση είναι επιτυχημένη τότε αυτό σημαίνει ότι έχει δημιουργηθεί ένα δίκτυο που αυξάνει την αξιοπιστία, μειώνει τα κόστη και κάνει εύκολη τη δημιουργία καινοτομιών. Τόσο η ποιότητα όσο και η ασφάλεια θα πρέπει να ενσωματωθούν σε κάθε διεργασία και να θεωρηθούν με σωστό τρόπο από την αρχή. Αυτό περιλαμβάνει τους προμηθευτές των προϊόντων, τους ολοκληρωτές συστημάτων και υπηρεσιών καθώς και τους τελικούς χρήστες. Παρόλο που ο καθένας έχει έναν ρόλο στο δίκτυο που πρέπει να επιτελέσει, αυτό που δεν πρέπει να παραγνωρίζει με κανένα τρόπο είναι τόσο η ασφάλεια όσο και η ποιότητα.

Και αυτό μας οδηγεί στην ερώτηση για τον έλεγχο και στην ανάθεση εργασιών σε εξωτερικές εταιρείες[1]. Συχνά πολλές εταιρείες κοινής ωφέλειας[2] ρωτούν τι πρέπει να αγοράσουν για να είναι ασφαλείς και σύμφωνες με τα πρότυπα ασφάλειας. Μια τυπική απάντηση ενός ειδικού σε θέματα ασφάλειας είναι ότι η ασφάλεια είναι μια διαδικασία και όχι ένα προϊόν. Ένας άλλος θα μπορούσε να προσθέσει ότι η ασφάλεια δεν μπορεί να είναι μια υπηρεσία που παρέχεται από έναν εργολάβο. Στην περίπτωση του έξυπνου δικτύου τα μέρη που το απαρτίζουν είναι υπεύθυνα για την ασφάλεια του. Σε κάποιες περιπτώσεις η ευθύνη για την ασφάλεια του έξυπνου δικτύου διαχέεται σε όλα τα διασυνδεδεμένα μέρη του, από τις εταιρείες που παράγουν ηλεκτρικό ρεύμα, σε αυτές που το μεταφέρουν και το διανείμουν και στους τελικούς καταναλωτές. Σε καθένα από αυτά τα μέρη υπάρχει η υποχρέωση να παρέχουν την απαραίτητη ασφάλεια και να εξασφαλίζουν συμμόρφωση με τους κανονισμούς. Αυτό βέβαια δεν σημαίνει ότι άλλα μέρη, εξωτερικά ως προς το έξυπνο δίκτυο, δεν μπορούν να παρέχουν υπηρεσίες παρακολούθησης της λειτουργίας του, εγκατάστασης αναβαθμίσεων, ακόμα και υπηρεσίες εγκατάστασης πολιτικών ασφάλειας και δημιουργίας διαδικασιών ασφάλειας.

Οποιεσδήποτε εξαρτήσεις δημιουργούνται είτε από χρήση υπηρεσιών από κάποιον εργολάβο είτε από την εξάρτηση σε κανονισμούς ή πρότυπα απαιτούν σταθερή και αδιάλειπτη επαγρύπνηση του αντίστοιχου μέρους του έξυπνου δικτύου. Η κύρια ευθύνη ενός εργολάβου είναι να ικανοποιήσει τους όρους του συμβολαίου που έχει υπογράψει. Η αντιμετώπιση απειλών ασφάλειας είναι συνήθως μέσα στις υποχρεώσεις του εργολάβου, αλλά σπάνια είναι δική του ευθύνη από την στιγμή που έχει εκπληρώσει τους όρους του συμβολαίου. Σημαντικό σημείο στην σχέση εργολάβου με αυτόν που του έχει αναθέσει το έργο για την ασφάλεια είναι ο ξεκάθαρος καθορισμός των μετρικών για την συμμόρφωση και υλοποίηση του συμβολαίου, τα οποία όμως ταιριάζουν στους κινδύνους ασφάλειας που αντιμετωπίζει ο οργανισμός. Επιπλέον, πρέπει να παρέχεται και η απαιτούμενη ευελιξία έτσι ώστε να μπορούν να αλλάζουν τα μετρικά ασφάλειας και οι υποχρεώσεις του εργολάβου με βάση τις μελλοντικές αλλαγές που μπορεί να προκύψουν στα ζητήματα ασφάλειας. Με βάση τα παραπάνω θα μπορούσε κάποιος να αναθέσει λειτουργίες ασφάλειας σε έναν εργολάβο, αλλά η ανάθεση του ρίσκου σε κάποιον άλλο εκτός οργανισμού είναι ένα άλλο ζήτημα. Εάν στο έξυπνο δίκτυο βρίσκουν πεδίο εφαρμογής πολιτικές ασφάλισης έναντι κινδύνων θα μπορούσε να αποζημιωθεί ο οργανισμός εάν ο εργολάβος δεν κάνει σωστά την δουλειά του. Ωστόσο, δεν θα μπορούσε ο οργανισμός να ανακτήσει την εμπιστοσύνη των πελατών ή να διορθώσει τις παραβιάσεις συμμόρφωσης με τους κανονισμούς [17].

[1]Για συντομία θα αναφερόμαστε σε αυτές ως εργολάβους.

[2]Μπορεί να είναι είτε δημόσιες είτε ιδιωτικές (αυτή η σημείωση ισχύει για το σύνολο του κειμένου).

1.4. ΤΑΣΕΙΣ ΣΤΗΝ ΕΡΕΥΝΑ

Η ασφάλεια του έξυπνου δικτύου στο κυβερνοχώρο επικεντρώνεται συνήθως στα διαφορετικά εξαρτήματα του συστήματος ηλεκτρικής ενέργειας. Η πρώτη εργασία που σχετίζεται με το έξυπνο δίκτυο αφορά την ασφάλεια των Συστημάτων Ελέγχου Διεργασιών (PCS). Η πρόσφατη έρευνα επικεντρώνεται στα νέα εξαρτήματα του έξυπνου δικτύου και στις μεταξύ τους αλληλεπιδράσεις. Πρόοδος στην ασφάλεια του έξυπνου δικτύου έχει σημειωθεί στην προστασία των πληροφοριών των χρηστών, στους έξυπνους μετρητές, στην εκτίμηση της κατάστασης του συστήματος ηλεκτρικής ενέργειας, στην επικοινωνία των εξαρτημάτων και τέλος στην ανάλυση επιθέσεων στον κυβερνοχώρο.

Τα PCS έχουν χρησιμοποιηθεί με επιτυχία σε πολλούς βιομηχανικούς κλάδους με το πέρασμα των χρόνων. Ένα PCS είναι ένα αυτοματοποιημένο σύστημα που παρακολουθεί και ελέγχει μια διεργασία που χρησιμοποιεί υπολογιστές. Τα PCS λειτουργούν συνήθως ως απομονωμένα συστήματα που έχουν περιορισμένες ή και καθόλου εξωτερικές δικτυακές συνδέσεις. Τα PCS συνήθως χρησιμοποιούνται στις κατασκευές για να ελέγξουν κάποια πτυχή της παραγωγής. Τα PCS αλλάζουν όταν τρέχουν σε απομονωμένα περιβάλλοντα και όταν συνδέονται σε μεγαλύτερα δίκτυα. Αυτό εισάγει καινούργιους κινδύνους ασφάλειας, γιατί τα παραδοσιακά PCS είναι σχεδιασμένα με περιορισμένες δυνατότητες ασφάλειας. Από την στιγμή που τα PCS λειτουργούσαν σε απομονωμένα περιβάλλοντα, η ασφάλεια στον κυβερνοχώρο δεν ήταν σημαντικό θέμα.

Το έξυπνο δίκτυο θα συλλέγει πολλά περισσότερα δεδομένα χρηστών καθώς και νέους τύπους πληροφοριών. Τα νέα αυτά δεδομένα σε συνδυασμό με την διασύνδεση τους στο έξυπνο δίκτυο εγείρουν ανησυχίες σχετικά με την προστασία της ιδιωτικής ζωής των χρηστών. Υπάρχουν νόμοι και περιορισμοί για την προστασία της ιδιωτικής ζωής των χρηστών. Οι νόμοι αυτοί θα πρέπει να επεκταθούν για να προστατέψουν και τους χρήστες του έξυπνου δικτύου. Οι νέοι τύποι δεδομένων θα πρέπει να αναλυθούν και να ταυτοποιηθούν, έτσι ώστε να μπορέσουν να εντοπιστούν τα προβλήματα ασφάλειας και να γίνουν κατάλληλα βήματα για την διασφάλιση του απόρρητου των χρηστών.

Οι έξυπνοι μετρητές είναι η ψηφιακή έκδοση των σημερινών μετρητών ηλεκτρικής ενέργειας. Οι έξυπνοι μετρητές θα εγκατασταθούν στην τοποθεσία του πελάτη και θα χρησιμοποιούνται για να λαμβάνονται ηλεκτρικές μετρήσεις, οι οποίες ονομάζονται καταγραφές. Οι έξυπνοι μετρητές θα συνδέονται στο έξυπνο δίκτυο και περιοδικά θα του στέλνουν τις καταγραφές. Αυτές οι καταγραφές θα χρησιμοποιούνται για την εκτίμηση της κατάστασης ηλεκτρικής ενέργειας καθώς και για σκοπούς χρέωσης. Υπάρχουν μερικές προκλήσεις σχετικά με την ασφάλεια στους έξυπνους μετρητές που κυμαίνονται από επεμβάσεις στην λειτουργικότητα της συσκευής μέχρι και σε θέματα επικοινωνίας του έξυπνου μετρητή και του προμηθευτή ηλεκτρικής ενέργειας.

Τα PCS στο έξυπνο δίκτυο πρέπει να μοντελοποιήσουν την τρέχουσα κατάσταση του συστήματος ηλεκτρικής ενέργειας. Καθένα από τα μοντέλα που θα μπορούσε να χρησιμοποιηθεί ενέχει αρκετούς κινδύνους για την ασφάλεια. Τα μοντέλα εκτίμησης της κατάστασης είναι μέρος των PCS, αλλά εξετάζονται ξεχωριστά γιατί έχει υπάρξει πολύ και εξονυχιστική έρευνα σε αυτό το θέμα. Η ακεραιότητα του μοντέλου εκτίμησης της κατάστασης είναι ένα σημαντικό θέμα ασφάλειας στο έξυπνο δίκτυο.

Η δικτύωση πολλών διαφορετικών εξαρτημάτων του έξυπνου δικτύου μαζί σημαίνει ότι πολλά διαφορετικά εξαρτήματα πρέπει να αλληλεπιδράσουν με άλλα εξαρτήματα. Αυτό είναι ένα σημαντικό θέμα στο έξυπνο δίκτυο λόγω του μεγάλου αριθμού των εξαρτημάτων που πρέπει να επικοινωνήσουν μεταξύ τους. Υπάρχουν διαφορετικές απαιτήσεις για κάθε ζεύγος εξαρτημάτων που επικοινωνούν. Αυτές οι απαιτήσεις επικοινωνίας περιλαμβάνουν την καθυστέρηση, το διαθέσιμο εύρος ζώνης, την αξιοπιστία και τις απαιτήσεις ασφάλειας. Αυτό σημαίνει ότι πρέπει να χρησιμοποιηθούν πολλά διαφορετικά πρωτόκολλα στο έξυπνο δίκτυο για να είναι δυνατή η επικοινωνία μεταξύ των εξαρτημάτων του [1].

2. ΈΞΥΠΝΟ ΔΙΚΤΥΟ: ΕΙΣΑΓΩΓΗ

2.1. ΟΡΙΣΜΟΣ

Το έξυπνο δίκτυο είναι μια αναβάθμιση του υπάρχοντος δικτύου ηλεκτρικής ενέργειας. Αυτή η αναβάθμιση μπορεί να ενσωματώσει με ένα ικανό κόστος την συμπεριφορά και όλες τις ενέργειες των χρηστών που συνδέονται στο έξυπνο δίκτυο. Οι χρήστες μπορεί να είναι παραγωγοί ηλεκτρικής ενέργειας, καταναλωτές ή και τα δύο μαζί. Σκοπός του έξυπνου δικτύου είναι η διασφάλιση ενός οικονομικά αποδοτικού και βιώσιμου συστήματος ενέργειας με χαμηλές απώλειες και υψηλά επίπεδα ποιότητας και ασφάλειας.

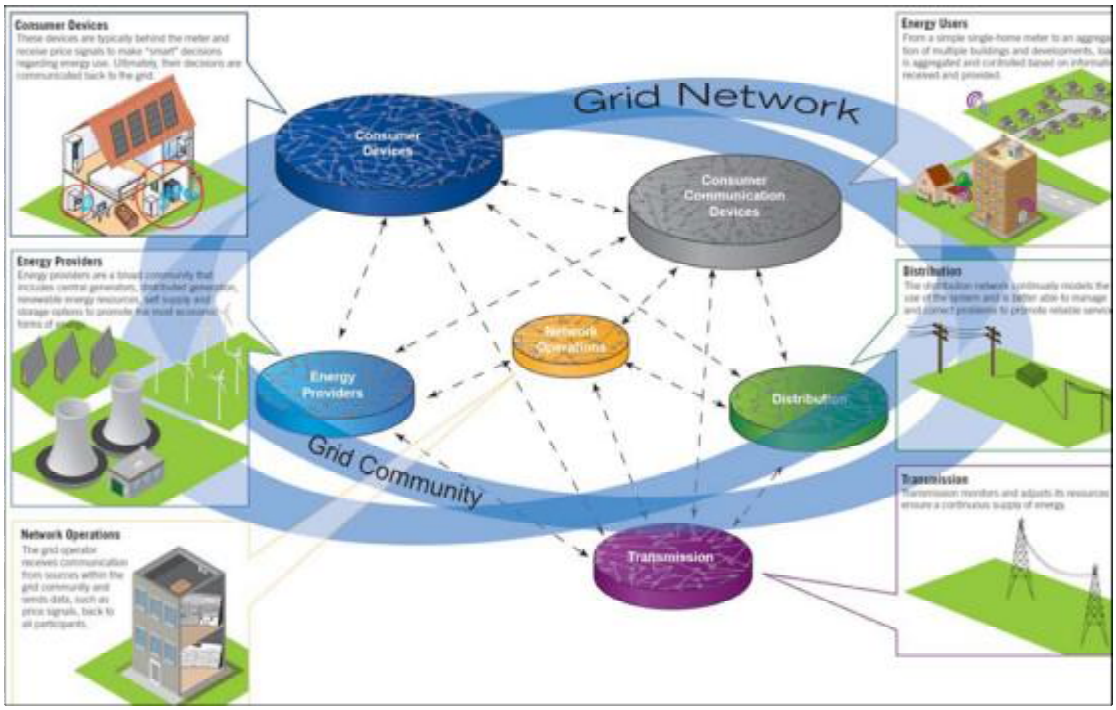
Αν και υπάρχουν εμφανή στοιχεία εξυπνάδας σε πολλά μέρη υφιστάμενων δικτύων, η διαφορά μεταξύ ενός σημερινού πλέγματος και του έξυπνου δικτύου του μέλλοντος εντοπίζεται κυρίως στην δυνατότητα του έξυπνου δικτύου να χειριστεί μεγαλύτερη πολυπλοκότητα από τα σημερινά πλέγματα με έναν ποιο αποδοτικό και αποτελεσματικό τρόπο. Το έξυπνο δίκτυο χρησιμοποιεί καινοτόμα προϊόντα και υπηρεσίες σε συνδυασμό με τεχνολογίες έξυπνης παρακολούθησης, ελέγχου, επικοινωνίας και αυτό-ίασης. Οι στόχοι που καλείται να υλοποιήσει το έξυπνο δίκτυο είναι να:

- διευκολύνει την σύνδεση και την λειτουργία γεννητριών όλων των μεγεθών και τεχνολογιών,
- επιτρέπει στους καταναλωτές να διαδραματίζουν ρόλο στην βελτιστοποίηση της λειτουργίας του συστήματος,
- παρέχει στους καταναλωτές μεγαλύτερη πληροφόρηση και επιλογές για το πως να χρησιμοποιούν το ηλεκτρικό ρεύμα που προμηθεύονται,
- ανταποκρίνεται στις κορυφώσεις παραγωγής ηλεκτρικής ενέργειας από τις ανανεώσιμες πηγές ενέργειας και να επιτρέπει την διαχείριση φορτίου,
- μειώνει σημαντικά τις περιβαλλοντικές επιπτώσεις του συστήματος ηλεκτρικής ενέργειας,
- διατηρεί ή ακόμα και να βελτιώνει τα υψηλά επίπεδα αξιοπιστίας, ποιότητας, ασφάλειας και εφοδιασμού του συστήματος,
- περιορίζει το κόστος μετάβασης σε ενεργειακές πηγές με χαμηλές εκπομπές ρύπων, επενδύοντας στον ευφυή σχεδιασμό και λειτουργία και όχι μόνο στην ενίσχυση του δικτύου,
- διατηρεί και βελτιώνει αποτελεσματικά τις υφιστάμενες υπηρεσίες,
- παρέχει τα προγράμματα που ανταποκρίνονται στην ζήτηση, στις υπηρεσίες και τα προϊόντα σε όλες τις κατηγορίες πελατών και
- τέλος να προωθεί την ενοποίηση της αγοράς.

Όσοι συμμετέχουν σε ένα έξυπνο δίκτυο μπορούν να κατηγοριοποιηθούν ως εξής:

- **φορείς εκμετάλλευσης των δικτύων**: σύστημα μεταφοράς και διανομής / φορείς εκμετάλλευσης των δικτύων (TSO/DSO και NSO)
- **χρήστες του πλέγματος**: οι γεννήτριες, οι καταναλωτές (συμπεριλαμβάνονται οι συνδρομητές κινητής τηλεφωνίας) και οι ιδιοκτήτες αποθήκευσης
- **άλλοι παράγοντες**: οι προμηθευτές, οι φορείς μέτρησης, οι ΕΕΥ (Εταιρείες Ενεργειακών Υπηρεσιών), οι πάροχοι υπηρεσιών και εφαρμογών και οι φορείς εκμετάλλευσης των πλατφορμών ανταλλαγής (αντίστοιχες των χρηματιστηρίων) ηλεκτρικής ενέργειας.

Ένα σχέδιο για το υπό-ανάπτυξη έξυπνο δίκτυο με βάση τα όσα έχουμε αναφέρει μέχρι στιγμής είναι το ακόλουθο.



Εικόνα 1, Σχέδιο έξυπνου δικτύου [3]

Μια υπηρεσία στο έξυπνο δίκτυο προσδιορίζει τόσο το αποτέλεσμα που χρειάζεται ο χρήστης από ηλεκτρικό δίκτυο όσο και αυτό που θα χρειαστεί μελλοντικά από αυτό σε μια πλήρως απελευθερωμένη αγορά ηλεκτρικής ενέργειας. Για την χρησιμοποίηση οποιασδήποτε υπηρεσίας ο χρήστης θα πρέπει να συνδεθεί σε έναν πάροχο και σε έναν αριθμό από πρωτοβάθμιους δικαιούχους. Θα πρέπει όλοι οι χρήστες να γνωρίζουν ότι τα οφέλη που προέρχονται από την χρησιμοποίηση οποιασδήποτε υπηρεσίας που παρέχεται στο έξυπνο δίκτυο αντικατοπτρίζονται από την άποψη των καταναλωτών και την επίδραση που έχει στο περιβάλλον.

Σε αυτό το σημείο πρέπει να κάνουμε μια αναφορά στην τεχνολογία που χρησιμοποιούν οι έξυπνοι μετρητές οι οποίοι και ολοκληρώνουν την έννοια του έξυπνου δικτύου. Πρέπει να επισημάνουμε ότι οι έξυπνοι μετρητές είναι ένα αναπόσπαστο κομμάτι του έξυπνου δικτύου. Αποτελούνται από έναν μετρητή ηλεκτρικού ρεύματος που καταγράφει την κατανάλωση ηλεκτρικής ενέργειας και μεταδίδει αυτή την πληροφορία στον διαχειριστή του δικτύου καθώς και στον προμηθευτή ηλεκτρικής ενέργειας τόσο για παρακολούθηση όσο και για τιμολόγηση. Χάρη σε αυτή την πληροφορία οι καταναλωτές είναι σε θέση να ελέγχουν άμεσα και να διαχειρίζονται μεμονωμένα την κατανάλωσή τους. Επιπλέον, οι διαχειριστές δικτύου μπορούν να προγραμματίσουν καλύτερα τη χρήση των υποδομών και την ισορροπία του συστήματος, για παράδειγμα όσον αφορά την ένταξη των ανανεώσιμων πηγών ενέργειας. Οι έξυπνοι μετρητές επιτρέπουν την αμφίδρομη επικοινωνία μεταξύ του μετρητή και του κεντρικού συστήματος [24].

2.2. ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΕΞΥΠΝΟΥ ΔΙΚΤΥΟΥ

Το έξυπνο δίκτυο είναι μια υποδομή ηλεκτρικής ενέργειας η οποία παίρνει έξυπνες αποφάσεις σχετικά με την κατάσταση του συστήματος ηλεκτρικής ενέργειας, έτσι ώστε να διατηρείται ένα σταθερό περιβάλλον. Ο πιο εύκολος τρόπος για να ορίσουμε το έξυπνο δίκτυο είναι μελετώντας τα χαρακτηριστικά του. Το έξυπνο δίκτυο είναι μια αναβάθμιση του υπάρχοντος συστήματος ηλεκτρικής ενέργειας, οπότε έχει όλα εκείνα τα χαρακτηριστικά του υπάρχοντος συστήματος ενέργειας καθώς επίσης και τα ακόλουθα:

[3] Η εικόνα είναι διαθέσιμη στην ιστοσελίδα http://leadinggreen.ca/2013/06/11/alternative-energy-how-the-power-grid-is-adapting-and-why-it-is-happening-now/

1. Αυτό-ίαση
2. Παρακινεί και περιλαμβάνει τον καταναλωτή
3. Ανθεκτικό στις επιθέσεις
4. Αυξάνει την ποιότητα της ενέργειας
5. Εξυπηρετεί όλη την παραγωγή και τις επιλογές αποθήκευσης
6. Επιτρέπει την αγορά ηλεκτρικής ενέργειας
7. Βελτιστοποιεί τα περιουσιακά στοιχεία και λειτουργεί αποτελεσματικά

Το έξυπνο δίκτυο θα έχει δυνατότητα αυτό-ίασης. Το έξυπνο δίκτυο θα μπορεί να ανακατευθύνει και να ρυθμίζει την ροή του ηλεκτρικού ρεύματος στην περίπτωση που μία διαδρομή διανομής ηλεκτρικής ενέργειας έχει πρόβλημα (π.χ. πτώση καλωδίων). Αυτό καθίσταται δυνατό μέσα από μια συνεχόμενη διαδικασία αυτό-αξιολόγησης της κατάστασης του συστήματος ενέργειας. Συνεπώς, μέσα από αυτή την διαδικασία μπορεί να μειωθεί η συχνότητα και η διάρκεια των μεγάλων διακοπών ρεύματος. Χαρακτηριστικό παράδειγμα είναι η διακοπή ρεύματος στις 13 Αυγούστου του 2003 στις ΗΠΑ και στον Καναδά που είχε κοινωνικό κόστος 10 δισεκατομμυρίων δολαρίων. Η μείωση του αριθμού των μεγάλων διακοπών ρεύματος και της σημαντικότητάς τους θα μειώσει τις οικονομικές απώλειες που προκαλούνται στην κοινωνία.

Το έξυπνο δίκτυο θα παρακινεί και θα περιλαμβάνει τους πελάτες. Με το υφιστάμενο δίκτυο ηλεκτρικής ενέργειας υπάρχει ελάχιστη αλληλεπίδραση μεταξύ των πελατών και των προμηθευτών. Το έξυπνο δίκτυο παρέχει στους πελάτες περισσότερες πληροφορίες και επιλογές σχετικά με την ηλεκτρική ενέργεια που χρησιμοποιούν και εν κατακλείδι καταναλώνουν. Στην θεωρία αυτό θα επιτρέψει στους πελάτες να πάρουν καλύτερες αποφάσεις σχετικά με την ηλεκτρική ενέργεια που θα καταναλώσουν. Αυτό θα οδηγήσει όχι μόνο στην εξοικονόμηση χρημάτων από τους πελάτες, αλλά θα αυξήσει και τον ανταγωνισμό μεταξύ των προμηθευτών. Η αλληλεπίδραση καθίσταται δυνατή με την ενεργοποίηση της αμφίδρομης επικοινωνίας μεταξύ πελατών και προμηθευτών. Το έξυπνο δίκτυο μπορεί επίσης να αλληλεπιδράσει με τις ηλεκτρικές συσκευές στο σπίτι του πελάτη. Αυτή η αλληλεπίδραση δίνει την δυνατότητα στον χρήστη να προγραμματίσει τις ηλεκτρικές του συσκευές, έτσι ώστε να δουλεύουν την χρονική περίοδο που το κόστος του ηλεκτρικού ρεύματος είναι το χαμηλότερο δυνατό.

Το έξυπνο δίκτυο θα είναι ανθεκτικό στις επιθέσεις και στις φυσικές καταστροφές. Το έξυπνο δίκτυο θα είναι ανθεκτικό όχι μόνο στις φυσικές επιθέσεις, αλλά και στις κυβερνο-επιθέσεις. Το δίκτυο ηλεκτρικής ενέργειας είναι ένα πολυσύνθετο σύστημα το οποίο βρίσκεται στην καρδιά της οικονομίας κάθε χώρας. Αυτό το κάνει ένα κρίσιμο κεφάλαιο και οποιαδήποτε ζημιά σε αυτό μπορεί να επιφέρει πλήγμα στην οικονομική δραστηριότητα της εκάστοτε χώρας. Το δίκτυο ηλεκτρικής ενέργειας είναι ένα πολύτιμο κεφάλαιο πάνω στο οποίο βασιζόμαστε και θα πρέπει να είναι ανθεκτικό σε όλους τους τύπους των επιθέσεων.

Το έξυπνο δίκτυο θα αυξήσει την ποιότητα της ηλεκτρικής ενέργειας. Το ηλεκτρικό ρεύμα πρέπει να είναι διαθέσιμο στο ηλεκτρικό δίκτυο όχι μόνο ανά πάσα χρονική στιγμή, αλλά πρέπει να έχει και σταθερή τάση. Ορισμένες διαδικασίες παραγωγής είναι εξαιρετικά ευαίσθητες στην διακύμανση της τάσης. Μια πτώση τάσης για περισσότερα από 100 χιλιοστά του δευτερολέπτου μπορεί να έχει το ίδιο αποτέλεσμα όπως η απώλεια ηλεκτρικής ενέργειας για αρκετά ή περισσότερα λεπτά σε ορισμένες βιομηχανικές διαδικασίες. Πρόσφατα έχει εκτιμηθεί ότι αυτές οι διακυμάνσεις στην τάση προκαλούν απώλειες στην παραγωγή από μερικές χιλιάδες ευρώ έως και αρκετά εκατομμύρια ανά εκδήλωσή τους.

Το έξυπνο δίκτυο θα εξυπηρετεί όλη την παραγωγή και θα έχει διαθέσιμες επιλογές αποθήκευσης. Η ενσωμάτωση των ανανεώσιμων πηγών ενέργειας στο δίκτυο ηλεκτρικής ενέργειας είχε αρκετές επιπλοκές. Η τρέχουσα δομή του ηλεκτρικού δικτύου βασίζεται σε ένα μοντέλο μετάδοσης που επιτρέπει μόνο την μονόδρομη ροή του ηλεκτρικού ρεύματος, δηλαδή από μία πηγή δημιουργίας σε πολλούς καταναλωτές. Οι ανανεώσιμες πηγές ενέργειας είναι συχνά γεωγραφικά διαχωρισμένες από τις παραδοσιακές πηγές ενέργειας.

Αυτό έχει σαν αποτέλεσμα όταν ενσωματώνονται στο δίκτυο ηλεκτρικής ενέργειας να είναι ως κατανεμημένες πηγές ενέργειας. Από την στιγμή που το δίκτυο ηλεκτρικής ενέργειας έχει σχεδιαστεί για μία και μοναδική πηγή ενέργειας και όχι για πολλαπλές κατανεμημένες πηγές ενέργειας δημιουργούνται επιπλοκές. Τα ορυκτά καύσιμα δεν είναι μια βιώσιμη πηγή ενέργειας και εκ' τούτου πρέπει να διερευνηθούν νέες εναλλακτικές πηγές ενέργειας. Το έξυπνο δίκτυο θα είναι σε θέση να υποστηρίζει αυτές τις νέες πηγές ενέργειας μαζί με τις παραδοσιακές.

Το έξυπνο δίκτυο θα ενεργοποιήσει την αγορά ηλεκτρικής ενέργειας. Οι αγορές ηλεκτρικής ενέργειας στο έξυπνο δίκτυο θα ενθαρρύνουν τον ανταγωνισμό μεταξύ των προμηθευτών ηλεκτρικής ενέργειας. Αυτός ο ανταγωνισμός θα παροτρύνει τους προμηθευτές ηλεκτρικής ενέργειας για να αναπτύξουν φθηνότερα και αποδοτικότερα μέσα παραγωγής. Αυτό σταδιακά θα οδηγήσει σε μείωση της τιμής της ηλεκτρικής ενέργειας για τους καταναλωτές, καθώς οι προμηθευτές θα ανταγωνίζονται για τις υπηρεσίες που παρέχουν. Επίσης, το έξυπνο δίκτυο θα υποστηρίζει κατανεμημένες πηγές ηλεκτρικής ενέργειας. Αυτή η δυνατότητα θα ανοίξει την πόρτα σε νέους προμηθευτές ηλεκτρικής ενέργειας, καθώς και σε παρόχους υπηρεσιών ηλεκτρικής ενέργειας για να μπορέσουν να μπουν στην αγορά ηλεκτρική ενέργειας. Η αγορά της ηλεκτρικής ενέργειας θα ρυθμίζει την τρέχουσα τιμή του ηλεκτρικού ρεύματος βασιζόμενη στο μοντέλο προσφοράς-ζήτησης. Το ηλεκτρικό ρεύμα θα είναι ποιο ακριβό όταν η ζήτηση ή το φορτίο είναι μεγάλο, ενώ θα είναι φθηνότερο όταν υπάρχει μεγάλη προσφορά ηλεκτρικού ρεύματος. Οι πελάτες μπορούν να χρησιμοποιήσουν αυτή την πληροφορία για να προγραμματίσουν εργασίες που χρησιμοποιούν μεγάλη ποσότητα ηλεκτρικού ρεύματος σε μια χρονική στιγμή που το ηλεκτρικό ρεύμα είναι φθηνότερο.

Το έξυπνο δίκτυο θα βελτιστοποιεί τα περιουσιακά στοιχεία και θα λειτουργεί αποτελεσματικά. Τα χαρακτηριστικά που θα κάνουν το έξυπνο δίκτυο αυτό-θεραπευόμενο μπορούν επίσης να χρησιμοποιηθούν στην διαχείριση περιουσιακών στοιχείων. Το έξυπνο δίκτυο θα μπορεί αυτόματα να αξιολογήσει την κατάσταση του εξοπλισμού καθώς και να διαχειριστεί τις ρυθμίσεις του εξοπλισμού. Αυτή η αυτοματοποιημένη διαχείριση μπορεί να γίνει σε σημαντικά μειωμένα κόστη σε σύγκριση με την χειροκίνητη διαχείριση. Η αυτοματοποίηση της διαχείρισης του εξοπλισμού επίσης θα μειώσει την πιθανότητα αποτυχίας του εξοπλισμού, καθώς η υποβάθμισης της λειτουργίας του θα μπορεί να ανιχνευθεί. Επίσης, το έξυπνο δίκτυο θα εισάγει νέες τεχνολογίες που θα μειώσουν τις ενεργειακές απώλειες κατά την διάρκεια μεταφοράς της ηλεκτρικής ενέργειας. Η μείωση των ενεργειακών απωλειών θα βελτιώσει την αποτελεσματικότητα ηλεκτρικού δικτύου ελαχιστοποιώντας την εξάλειψη της υπερβολικής σπατάλης ηλεκτρικής ενέργειας [1].

2.3. ΚΙΝΔΥΝΟΙ ΚΑΙ ΩΦΕΛΕΙΕΣ

Στην περίπτωση των συστημάτων και των ευφυών ηλεκτρικών δικτύων, με την ενσωμάτωση των ανανεώσιμων πηγών ενέργειας και των ευέλικτων καταναλωτών ηλεκτρικής ενέργειας (επαγγελματίες, συμπεριλαμβανομένης της αποθήκευσης και της κατανεμημένης παραγωγής στις θέσεις των καταναλωτών), έχουν καθοριστεί ορισμένες βασικές κινητήριες δυνάμεις για τη μελλοντική ανάπτυξη της έννοιας του έξυπνου δικτύου:

- ο βαθμός και η μορφή της αποκέντρωσης του συστήματος παραγωγής και του δικτύου διανομής,
- το επίπεδο νοημοσύνης των εμπλεκόμενων συστημάτων που υλοποιείται από έξυπνα προϊόντα και τις συναφείς έξυπνες υπηρεσίες,
- το νομικό πλαίσιο και ο σχετικός κανονισμός για την ρύθμιση ανταγωνιστικών προϊόντων και επιλογών υπηρεσιών απέναντι σε μονοπωλιακά προϊόντα και υπηρεσίες και
- οι κανόνες των επιχειρήσεων για τους παράγοντες που εμπλέκονται σε όλες τις πτυχές των δικτύων και των έξυπνων ηλεκτρικών συστημάτων.

Το έξυπνο δίκτυο είναι μια τεχνολογική έννοια που πρόκειται να αλλάξει δραματικά το τοπίο παραγωγής ηλεκτρικής ενέργειας. Σε όλο το πέρασμα των δεκαετιών όλο και περισσότερες προκλήσεις πρόκειται να προκύψουν από τις κυβερνήσεις, τις κοινωνίες, τις αγορές και τις βιομηχανίες και θα πρέπει να αντιμετωπιστούν αποτελεσματικά. Στην συνέχεια περιγράφονται οι πιθανές προκλήσεις και τα εμπόδια σε αυτή την μετάλλαξη του ηλεκτρικού δικτύου προς ένα έξυπνο σύστημα παροχής ηλεκτρικής ενέργειας.

2.3.1. ΗΛΕΚΤΡΙΚΕΣ ΤΕΧΝΟΛΟΓΙΕΣ

Πρέπει να υπάρχει μεγαλύτερη δυνατότητα ελέγχου της ποιότητας του συστήματος ηλεκτρικής ενέργειας, της ασφάλειας εφοδιασμού και των αντίστοιχων συστημάτων. Για να καταστεί αυτό δυνατόν θα πρέπει να αυξηθεί η ευελιξία κατανάλωσης ηλεκτρικής ενέργειας, χωρικά και χρονικά, με την χρήση κατάλληλων τεχνολογιών. Θα πρέπει να υπάρχουν όσο το δυνατόν περισσότερες τεχνολογίες που θα εξυπηρετούν τον στόχο για καλύτερη κατανομή του παραγόμενου φορτίου ηλεκτρικής ενέργειας ανά πάσα χρονική στιγμή και σε ευέλικτες γεωγραφικές ομαδοποιήσεις. Αυτές οι τεχνολογίες θα πρέπει οπωσδήποτε να συνδυάζουν βελτιωμένη διαχείριση των περιορισμών του συστήματος δικτύου.

Είναι απαραίτητο να υπάρχουν τεχνολογίες ελέγχου για τα στοιχεία ηλεκτρικής ενέργειας και την αποθήκευσης της. Αυτές οι τεχνολογίες θα είναι ικανές να χειρίζονται την αστάθεια των ανανεώσιμων πηγών ενέργειας με βάση την παραγωγή τους.

Πρέπει να γίνεται ασφαλή μεταφορά της ηλεκτρικής ενέργειας σε μεγάλες αποστάσεις και σε διασυνδεμένα δίκτυα. Η τεχνολογία εναλλασσόμενης HDVC για διασυνδεδεμένα δίκτυα συνεχούς ρεύματος υψηλής τάσης είναι το κλειδί για την επιτυχία. Αυτή η τεχνολογία μπορεί να μεταφέρει με ασφάλεια την υπερπροσφορά ηλεκτρικής ενέργειας από τις ανανεώσιμες πηγές ενέργειας.

Τα υλικά που απαρτίζουν τα εξαρτήματα του έξυπνου δικτύου πρέπει να είναι ισχυρότερα, ποιο ευέλικτα και αποδοτικότερα από πλευράς κόστους. Ο σκοπός είναι αποφεύγεται μια ξαφνική δυσλειτουργία του συστήματος. Στην περίπτωση όμως που συμβαίνει μια βλάβη σε ένα εξάρτημα του έξυπνου δικτύου πρέπει να γίνονται άμεσες και σχεδόν αυτόματες ενέργειες, όπου αυτό είναι δυνατόν, για την αποκατάσταση της βλάβης. Αυτό είναι απαραίτητο για να παρέχεται αδιάλειπτη διαθεσιμότητα των προϊόντων και υπηρεσιών του έξυπνου δικτύου στους χρήστες του.

2.3.2. ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

Για να υπάρχει καλύτερη παρακολούθηση και μετρήσεις είναι απαραίτητη η ύπαρξη αισθητήρων, τεχνολογιών επικοινωνίας και κατανεμημένων πλατφορμών πραγματικού χρόνου. Αυτές οι τεχνολογίες θα είναι βασικός παράγοντας για την παρακολούθηση και την μέτρηση της απόδοσης των διαφόρων εξαρτημάτων του έξυπνου δικτύου. Επίσης, θα χρησιμοποιηθούν για την παρακολούθηση της τρέχουσας κατάστασης του συστήματος. Η πληροφορία που θα συλλέγεται θα χρησιμοποιείται ως είσοδος για πολλούς αλγόριθμους πρόβλεψης μοντέλων. Η έξοδος αυτών των μοντέλων θα υποστηρίζει τις αποφάσεις για να επιτευχθούν οι στόχοι των μελλοντικών υλοποιήσεων στο έξυπνο δίκτυο.

Θα χρησιμοποιηθούν κατάλληλες τεχνολογίες για τον αποκεντρωμένο έλεγχο τόσο του έξυπνου δικτύου όσο και εξαρτημάτων του. Επιπλέον, θα ελέγχεται και θα σταθεροποιείται το δίκτυο με ελάχιστες παρεμβάσεις σε φυσικό και μηχανολογικό επίπεδο (αλλαγή εξαρτημάτων).

Θα απαιτηθούν βελτιωμένα μοντέλα βασισμένα σε υπολογιστές και αλγορίθμους που θα χρησιμοποιηθούν από διάφορα εξαρτήματα του δικτύου όπως: γραμμές μεταφοράς και διανομής, μετασχηματιστές τάσης και ρεύματος, ευέλικτο AC και εξαρτήματα του DC, διακόπτες, διακλαδώσεις, εξοπλισμός προστασίας, αλλά και από όλους του χρήστες του έξυπνου δικτύου (συμπεριλαμβάνονται οι γεννήτριες, η αποθήκευση, ο εξοπλισμός των καταναλωτών καθώς και η συμπεριφορά τους).

Θα πρέπει να υφίσταται μια κατάλληλη αρχιτεκτονική λογισμικού που θα επιτρέπει στους καταναλωτές και στους φορείς της αγοράς την δημιουργία νέων υπηρεσιών. Αυτές οι νέες υπηρεσίες θα ικανοποιούν τις απαιτήσεις που σχετίζονται με τις ενεργειακές υπηρεσίες και τα υπάρχοντα προϊόντα, χρησιμοποιώντας τις διασυνδέσεις της αγοράς. Επίσης, την ίδια χρονική στιγμή θα υποστηρίζουν την ποιότητα και την ασφάλεια του έξυπνου δικτύου.

2.3.3. ΝΟΜΙΚΑ ΠΛΑΙΣΙΑ ΚΑΙ ΔΟΜΕΣ ΤΗΣ ΑΓΟΡΑΣ

Οι κανόνες είναι αναγκαίοι για την χρήση μονοπωλιακών προϊόντων και υπηρεσιών. Τα νομικά πλαίσια πρέπει να θέτουν τι τιμές βασιζόμενα στα κόστη που προκύπτουν από τις ρυθμίσεις και τα κίνητρα για το ίδιο το ηλεκτρικό δίκτυο (όπου δεν υφίσταται μια αγορά βασισμένη στις επενδύσεις των εμπόρων). Επιπλέον, θα πρέπει να θέτουν τις τιμές για τις συναφείς υπηρεσίες, όπου δεν χρησιμοποιούνται σχετικές με την αγορά προσεγγίσεις. Αυτό εισάγει ερωτήσεις για το ποια ενδιαφερόμενα μέρη πρέπει να πληρώσουν για ποια τμήματα του κόστους και με ποιους κανόνες.

Πρέπει να σχεδιαστούν νομικά πλαίσια για τους κανόνες της αγοράς και για τις συναφείς αρχές τιμολόγησης. Θα πρέπει να χειριστούν το γεγονός ότι το έξυπνο δίκτυο των επόμενων δεκαετιών θα είναι σχεδιασμένο και λειτουργικό σε ένα πλαίσιο με φυσικούς, θερμικούς, κοινωνικούς και περιβαλλοντικούς περιορισμούς. Αυτοί οι περιορισμοί συχνά θα προέρχονται από το μονοπώλιο που βασίζεται στην υποδομή του δικτύου. Οι αρχές τιμολόγησης που θα σχεδιαστούν για τα προϊόντα και τις υπηρεσίες θα πρέπει να αντιμετωπίζουν και να ξεπερνούν αυτούς τους περιορισμούς, έτσι ώστε να μην υπάρχουν αποκλεισμοί και μονοπώλια.

2.4. ΡΥΘΜΙΣΤΙΚΟ ΠΛΑΙΣΙΟ, ΠΡΟΤΥΠΑ

Όπως όλα τα συστήματα έτσι και το έξυπνο δίκτυο θα πρέπει να διέπεται από κάποιο ρυθμιστικό πλαίσιο και να ακολουθεί κάποια πρότυπα. Υπάρχουν συγκεκριμένοι οργανισμοί και υπηρεσίες που ασχολούνται με την επιβολή των ρυθμιστικών πλαισίων και τον έλεγχο συμμόρφωσης με τα πρότυπα. Γι' αυτό το λόγο στην παρούσα ενότητα θα εξετάσουμε τι συμβαίνει στην Ευρωπαϊκή Ένωση.

2.4.1. ΕΥΡΩΠΑΙΚΟ ΔΙΚΤΥΟ ΔΙΑΧΕΙΡΙΣΤΩΝ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΦΟΡΑΣ

Το Ευρωπαϊκό Δίκτυο Διαχειριστών Συστημάτων Μεταφοράς (ENTSO) για την ηλεκτρική ενέργεια είναι υπεύθυνο για τη διαχείριση του συστήματος μεταφοράς ηλεκτρικής ενέργειας και για να επιτραπεί η εμπορία και προμήθεια ηλεκτρικής ενέργειας πέραν των συνόρων της Κοινότητας. Η Ευρωπαϊκή Επιτροπή συμβουλεύεται τον Οργανισμό Συνεργασίας των Ρυθμιστικών Αρχών Ενέργειας και τον ENTSO για την ηλεκτρική ενέργεια, προκειμένου να δημιουργηθεί ένας ετήσιος κατάλογος των προτεραιοτήτων που θα συμβάλει στην ανάπτυξη των κωδικών του δικτύου. Οι κωδικοί αυτοί αναπτύσσονται χρησιμοποιώντας μια μη δεσμευτική κατευθυντήρια γραμμή που υποβάλλονται στην Επιτροπή από τον Οργανισμό. Οι κωδικοί περιλαμβάνουν κανόνες και διαδικασίες που αφορούν κυρίως:

- την ασφάλεια των δικτύων και την αξιοπιστία,
- την ανταλλαγή δεδομένων,
- τις τεχνικές και επιχειρησιακές ανταλλαγές,
- τους κανόνες διαφάνειας,
- τα εναρμονισμένα τιμολόγια μεταφοράς και
- την ενεργειακή απόδοση.

Ο ENTSO για την ηλεκτρική ενέργεια είναι υπεύθυνος για την έγκριση:

- κοινών εργαλείων λειτουργίας του δικτύου,
- ενός δεκαετούς προγράμματος ανάπτυξης του δικτύου,
- συστάσεων σχετικά με το συντονισμό της τεχνικής συνεργασίας μεταξύ των διαχειριστών συστημάτων μεταφοράς της Κοινότητας,
- ενός ετησίου προγράμματος εργασίας,

- μιας ετήσιας έκθεσης,
- ετήσιων προβλέψεων επάρκειας θερινής και χειμερινής παραγωγής ενέργειας και
- κόστους και χρηματοδότησης.

2.4.2. ΟΡΓΑΝΙΣΜΟΣ ΣΥΝΕΡΓΑΣΙΑΣ ΡΥΘΜΙΣΤΙΚΩΝ ΑΡΧΩΝ ΕΝΕΡΓΕΙΑΣ

Ο Οργανισμός Συνεργασίας των Ρυθμιστικών Αρχών Ενέργειας (ACER) είναι ένας κοινοτικός οργανισμός και διαθέτει νομική προσωπικότητα. Εκδίδει γνωματεύσεις για όλα τα θέματα που σχετίζονται με τον τομέα των ρυθμιστικών αρχών ενέργειας. Συμμετέχει στη δημιουργία των κωδικών του δικτύου στους τομείς της ηλεκτρικής ενέργειας και του φυσικού αερίου. Επίσης, λαμβάνει αποφάσεις σχετικά με τις διασυνοριακές υποδομές, συμπεριλαμβανομένων των παρεκκλίσεων από ορισμένες διατάξεις των ισχυόντων κανονισμών.

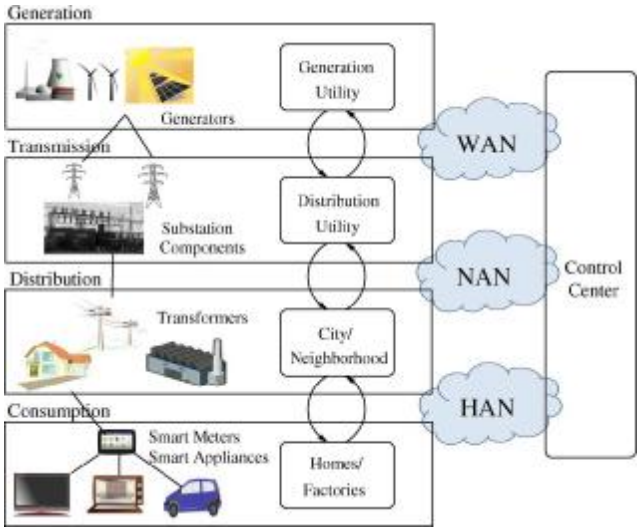
Ο Οργανισμός είναι υπεύθυνος για την έκδοση γνωματεύσεων σχετικά με το σχέδιο καταστατικού, τον κατάλογο των μελών και το σχέδιο κανόνων των διαδικασιών των ENTSO για την ηλεκτρική ενέργεια και το φυσικό αέριο, καθώς και για την παρακολούθηση της εκτέλεσης των καθηκόντων. Ο Οργανισμός διαδραματίζει σημαντικό ρόλο στη διαμόρφωση των κατευθυντήριων γραμμών με τις οποίες οι κωδικοί του δικτύου πρέπει να συμμορφώνονται. Επιπλέον, ο Οργανισμός παρακολουθεί την περιφερειακή συνεργασία μεταξύ των διαχειριστών συστημάτων μεταφοράς στους τομείς του ηλεκτρισμού και του φυσικού αερίου, καθώς και την εκτέλεση των καθηκόντων των ENTSO για την ηλεκτρική ενέργεια και το φυσικό αέριο.

Είναι επίσης υπεύθυνος για την έγκριση, υπό ορισμένες προϋποθέσεις, μεμονωμένων αποφάσεων σχετικά με τεχνικά ζητήματα. Μπορεί να προβεί σε συστάσεις με στόχο την προώθηση της ανταλλαγής ορθών πρακτικών μεταξύ των ρυθμιστικών αρχών και των φορέων της αγοράς. Παρέχει επίσης ένα πλαίσιο για τη συνεργασία μεταξύ των εθνικών ρυθμιστικών αρχών.

Ο Οργανισμός μπορεί να εκδώσει γνωμάτευση σχετικά με το αν η απόφαση που ελήφθη από μια ρυθμιστική αρχή συμμορφώνεται με τους ισχύοντες κοινοτικούς κανόνες. Αν η γνώμη του δεν ακολουθείται, ο οργανισμός ενημερώνει την Ευρωπαϊκή Επιτροπή και το ενδιαφερόμενο κράτος μέλος. Τέλος, είναι αρμόδιο για τον καθορισμό των όρων και των προϋποθέσεων για την πρόσβαση στην ηλεκτρική ενέργεια και στις υποδομές του φυσικού αερίου μεταξύ δύο τουλάχιστον κρατών μελών. Επίσης, ασχολείται και με την ασφάλεια λειτουργίας του συστήματος.

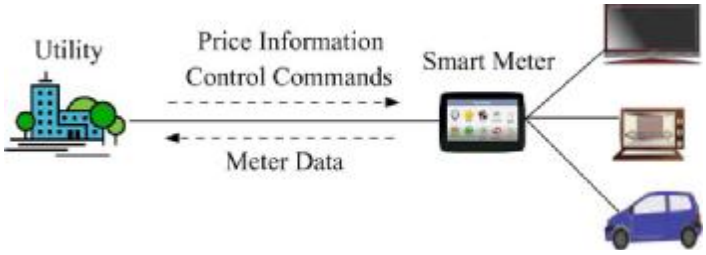
2.5. ΠΛΑΙΣΙΟ ΔΙΑΧΕΙΡΙΣΗΣ ΑΣΦΑΛΕΙΑΣ ΣΤΟ SMART GRID

Το έξυπνο δίκτυο αποτελείται από τέσσερα κύρια μέρη: παραγωγή, μεταφορά, διανομή και κατανάλωση. Στο μέρος του έξυπνου δικτύου που αφορά την κατανάλωση οι καταναλωτές χρησιμοποιούν ηλεκτρικές συσκευές (π.χ. έξυπνες εφαρμογές, ηλεκτρικά οχήματα) των οποίων η κατανάλωση ηλεκτρικής ενέργειας θα μετριέται από έξυπνους μετρητές. Ο έξυπνος μετρητής είναι ένα από τα βασικά στοιχεία των προηγμένων υποδομών μέτρησης (OEM). Ο μετρητής μπορεί να ομαδοποιείται και να αλληλεπιδρά με μια πύλη ενός οικιακού δικτύου περιοχής (HAN) ή ενός δικτύου επιχείρησης (BAN). Π.χ., ορίζουμε έναν έξυπνο μετρητή στην εικόνα 2 ως πύλη της XAN. Ένα γειτονικό δίκτυο (NAN) διαμορφώνεται σε ένα υποσταθμό, όπου πολλαπλές HAN φιλοξενούνται. Τέλος, μια εταιρεία κοινής ωφέλειας μπορεί να εκμεταλλευτεί ένα δίκτυο ευρείας περιοχής (WAN) για την σύνδεση κατανεμημένων NAN.



Εικόνα 2, Άποψη ασφάλειας στον κυβερνοχώρο του έξυπνου δικτύου [12]

Όπως έχουμε αναφέρει και σε προηγούμενη ενότητα οι απαιτήσεις ασφάλειας για ένα σύστημα περιλαμβάνουν τρεις κύριους στόχους: την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα. Η εμπιστευτικότητα αποτρέπει μη εξουσιοδοτημένους χρήστες από το να αποκτήσουν μυστικές ή ιδιωτικές πληροφορίες. Η ακεραιότητα εμποδίζει μη εξουσιοδοτημένους χρήστες να τροποποιούν πληροφορίες. Τέλος, η διαθεσιμότητα εξασφαλίζει ότι οι πόροι μπορούν να χρησιμοποιηθούν όταν ζητηθούν. Όπως μπορείτε να παρατηρήσετε στην εικόνα 3 οι πληροφορίες για την τιμή, τα δεδομένα των μετρητών και οι εντολές ελέγχου είναι οι κύριες πληροφορίες που ανταλλάσσονται στο έξυπνο δίκτυο. Παρόλο που στην πραγματικότητα ανταλλάσσονται περισσότεροι τύποι πληροφοριών, αυτοί οι κύριοι τύποι πληροφορίας παρέχουν ένα επαρκές παράδειγμα για τα ζητήματα ασφάλειας που μπορεί να προκύψουν.



Εικόνα 3, Πληροφορίες ροών προς / από έναν έξυπνο μετρητή [12]

Τώρα θα εξετάσουμε την σημασία της προστασίας των βασικών τύπων πληροφοριών σε σχέση με του κύριους στόχους για την ασφάλεια. Ο βαθμός της σημασίας των πληροφοριών για τις τιμές, οι εντολές ελέγχου και τα δεδομένα των μετρητών είναι ισοδύναμος με τις περιπτώσεις χρήσης της NISTIR 7628, στην οποία προστίθεται ο βαθμός σημασίας για το λογισμικό. Οι ποιο σημαντικές προϋποθέσεις για την προστασία των έξυπνων δικτύων είναι οι ακόλουθες:

- **Εμπιστευτικότητα χρήσης της ενέργειας**: Η μυστικότητα των στοιχείων των μετρητών είναι σημαντική, γιατί τα δεδομένα χρήσης της ηλεκτρικής ενέργειας παρέχουν πληροφορίες σχετικά με τα πρότυπα χρήσης των επιμέρους συσκευών. Αυτές οι πληροφορίες μπορούν να αποκαλύψουν τις δραστηριότητες των καταναλωτών με την χρήση μη παρεμβατικών συσκευών παρακολούθησης. Η εμπιστευτικότητα των τιμών και οι εντολές ελέγχου δεν είναι σημαντικά στις περιπτώσεις που αυτή η γνώση είναι δημόσια. Η εμπιστευτικότητα του λογισμικού δεν θα πρέπει να είναι κρίσιμη γιατί η ασφάλεια του συστήματος δεν θα πρέπει να βασίζεται στην μυστικότητα του λογισμικού, παρά μόνο στο απόρρητο των κλειδιών.

- **Ακεραιότητα δεδομένων, εντολών και λογισμικού**: Η ακεραιότητα των πληροφοριών για τις τιμές είναι σημαντική. Για παράδειγμα, εάν ένας εισβολέας στο σύστημα έχει εισάγει αρνητικές τιμές για την χρήση ηλεκτρικής ενέργειας, τότε μπορεί να προκαλέσει μια απότομη αύξηση στην χρήση της γιατί πολλές συσκευές θα λειτουργήσουν ταυτόχρονα εκμεταλλευόμενες τις χαμηλές τιμές του ηλεκτρικού ρεύματος. Παρά το γεγονός ότι είναι σημαντική η ακεραιότητα των δεδομένων του μετρητή και των εντολών, ο αντίκτυπος της περιορίζεται κυρίως στην απώλεια εσόδων. Από την άλλη πλευρά η ακεραιότητα του λογισμικού είναι κρίσιμη δεδομένου ότι είτε αλλοιωμένο λογισμικό είτε κακόβουλο μπορεί να ελέγξει οποιαδήποτε συσκευή ή εξάρτημα του έξυπνου δικτύου.
- **Διαθεσιμότητα από DoS / DDoS επιθέσεις**: Οι επιθέσεις άρνησης υπηρεσίας (DoS) είναι επιθέσεις κατανάλωσης πόρων που στέλνουν πλαστά αιτήματα σε ένα διακομιστή ή σε ένα δίκτυο. Η κατανεμημένη DoS (DDoS) επίθεση επιτυγχάνεται χρησιμοποιώντας κατανεμημένες πηγές επιθέσεων όπως χαλκευμένοι έξυπνοι μετρητές και συσκευές. Στα ευφυή δίκτυα η διαθεσιμότητα των πληροφοριών και της ενέργειας είναι ένα βασικό θέμα. Πιο συγκεκριμένα, η διαθεσιμότητα πληροφοριών για τις τιμές είναι κρίσιμη λόγω των σοβαρών οικονομικών και ενδεχομένως νομικών συνεπειών. Επιπλέον, ξεπερασμένες πληροφορίες τιμών μπορεί να επηρεάσουν αρνητικά τη ζήτηση. Η διαθεσιμότητα των εντολών είναι επίσης σημαντική, ειδικά όταν γυρίζεται προς τα πίσω ένας μετρητής μετά την ολοκλήρωση της πληρωμής ενός ηλεκτρικού λογαριασμού. Από την άλλη πλευρά, η διαθεσιμότητα των δεδομένων μέτρησης (π.χ., χρήση ενέργειας) μπορεί να μην είναι τόσο κρίσιμη, διότι τα δεδομένα μπορούν να διαβαστούν συνήθως σε μεταγενέστερο σημείο.

Με βάση τα παραπάνω μπορούμε να συνοψίσουμε στον πίνακα 2 την σημασία των δεδομένων, των εντολών και του λογισμικού. Υψηλός κίνδυνος σημαίνει ότι τα στοιχεία που εμπεριέχει μια πληροφορία είναι πολύ σημαντικά / κρίσιμα, ενώ ως μέσοι και χαμηλοί κίνδυνοι κατατάσσονται αυτοί των οποίων τα στοιχεία είναι σημαντικά και μη κρίσιμα αντίστοιχα. Αυτή η ταξινόμηση επιτρέπει την ιεράρχηση των κινδύνων, έτσι ώστε να επικεντρώνονται πρώτα οι προσπάθειες στις πιο κρίσιμες απαιτήσεις ασφάλειας. Για παράδειγμα, η ακεραιότητα των πληροφοριών των τιμών είναι πιο σημαντική από την εμπιστευτικότητα. Κατά συνέπεια θα πρέπει να επικεντρωθούμε στους αποτελεσματικούς μηχανισμούς ελέγχου ταυτότητας πριν την κρυπτογράφηση [11], [12] & [13].

	Πληροφορίες Τιμών	Εντολές Ελέγχου	Δεδομένα Μετρητών	Λογισμικό
Εμπιστευτικότητα	Χαμηλή	Χαμηλή	Μεσαία	Χαμηλή
Ακεραιότητα	Υψηλή	Υψηλή	Υψηλή	Υψηλή
Διαθεσιμότητα	Υψηλή	Υψηλή	Χαμηλή	

Πίνακας 2, Σημασία ιδιοτήτων ασφαλείας για τα δεδομένα, τις εντολές και το λογισμικό [12]

2.6. ΚΑΤΗΓΟΡΙΕΣ ΚΙΝΔΥΝΩΝ

Το έξυπνο δίκτυο αποτελείται από πολλά διαφορετικά εξαρτήματα. Καθένα από αυτά τα εξαρτήματα ενέχει κινδύνους για την ασφάλεια του δικτύου. Λόγω των διαφορετικών χαρακτηριστικών του κάθε εξαρτήματος θα εξετάσουμε τους κινδύνους στις ακόλουθες πέντε κατηγορίες εξαρτημάτων [1]:

- PCS
- Έξυπνοι μετρητές
- Εκτίμηση της κατάστασης του έξυπνου δικτύου
- Πρωτόκολλα επικοινωνίας του έξυπνου δικτύου
- Προσομοίωση του έξυπνου δικτύου για ανάλυση ασφάλειας

2.6.1. PCS

Τα PCS χρησιμοποιούνται από το έξυπνο δίκτυο για την παρακολούθηση και τον έλεγχο των φυσικών πτυχών του ηλεκτρικού δικτύου. Τα παραδοσιακά PCS έχουν σχεδιαστεί για να λειτουργούν σε απομονωμένα περιβάλλοντα στα οποία δεν υπάρχει καμία εξωτερική δικτυακή σύνδεση, οπότε τυπικά δεν έχουν ενσωματωμένες δυνατότητες ασφάλειας. Αυτό είναι θέμα για το έξυπνο δίκτυο από την στιγμή που τα PCS θα παρακολουθούν μεγάλες γεωγραφικές περιοχές του ηλεκτρικού δικτύου. Αυτό σημαίνει ότι θα υπάρχουν πολλά σημεία εισόδου για να μπει κάποιος στο δίκτυο. Τα PCS που θα χρησιμοποιηθούν θα πρέπει να αντιμετωπίσουν αυτά τα ζητήματα ασφάλειας. Υπάρχουν πολλά διαφορετικά είδη PCSs, αλλά αυτά που χρησιμοποιούνται κατά κόρον στο έξυπνο δίκτυο είναι τα συστήματα τύπου SCADA.

Δεδομένου ότι τα PCS θα ελέγχουν φυσικές πτυχές του ηλεκτρικού δικτύου η ασφάλεια αυτών των συστημάτων είναι πολύ σημαντική. Όταν ένας υπολογιστής έχει προβλήματα ασφάλειας μόνο τα δεδομένα που υπάρχουν σε αυτό τον υπολογιστή κινδυνεύουν. Σε κάποιες ακραίες περιπτώσεις μπορεί κάποιο από το υλικό του υπολογιστή να καταστραφεί. Ενώ όταν τα PCS αντιμετωπίσουν προβλήματα ασφάλειας, εξοπλισμός αξίας πολλών εκατομμυρίων μπορεί να πάθει ζημιά πέρα από την απώλεια δεδομένων. Σε ακραίες περιπτώσεις μπορεί να υπάρξουν τραυματισμοί ανθρώπων ακόμα και απώλεια ανθρώπινων ζωών. Ο ποιο σημαντικός στόχος για την ασφάλεια των PCS είναι η διαθεσιμότητα. Το σύστημα ηλεκτρικής ενέργειας πρέπει να είναι συνέχεια διαθέσιμο, συνεπώς τα PCS που ελέγχουν το σύστημα πρέπει να είναι πάντα διαθέσιμα. Η ακεραιότητα των PCS είναι ο επόμενος σημαντικός στόχος ασφάλειας. Δεν θα είναι δυνατόν να πάρουν σωστές αποφάσεις εάν έχουν δοθεί ψευδή / λανθασμένα στοιχεία. Η εμπιστευτικότητα είναι ο λιγότερο σημαντικός στόχος ασφάλειας. Τα PCS χρειάζεται να λειτουργούν σε πραγματικό χρόνο και αυτό σημαίνει ότι το σύστημα πρέπει να έχει ελάχιστη επιβάρυνση. Η υλοποίηση που θα γίνει για να ικανοποιηθεί η εμπιστευτικότητα μπορεί να είναι πολύ χρονοβόρα για να ανταποκριθεί στις απαιτήσεις καθυστέρησης.

Παραδοσιακά η ασφάλεια στα PCS έχει αγνοηθεί. Πολλά από τα PCS λειτουργούν σε απομονωμένες τοποθεσίες χωρίς εξωτερικές δικτυακές συνδέσεις, συνεπώς έχουν σχεδιαστεί με ελάχιστες ή και καθόλου δυνατότητες ασφάλειας. Στο πέρασμα των χρόνων οι απαιτήσεις των επιχειρήσεων έχουν οδηγήσει τα εταιρικά δίκτυα να συνδέονται με PCS. Αυτό έχει οδηγήσει σε παραβιάσεις ασφάλειας που μπορεί να καταλήξουν σε φυσικές καταστροφές ή και τραυματισμούς. Το έξυπνο δίκτυο χρησιμοποιεί PCS που είναι συνδεδεμένα σε ένα μεγάλο δίκτυο που έχει πολλά σημεία πρόσβασης. Γι' αυτό το λόγο τα PCSπρέπει να αντιμετωπίσουν τα προβλήματα ασφάλειας που έχουν τα μεγάλα δίκτυα.

2.6.2. ΕΞΥΠΝΟΙ ΜΕΤΡΗΤΕΣ

Η ασφάλεια των έξυπνων μετρητών είναι σημαντική γιατί πειραγμένες καταγραφές από μια τέτοια συσκευή μπορεί να οδηγήσουν σε εσφαλμένους λογαριασμούς και σε λανθασμένες εκτιμήσεις για την χρησιμοποίηση ενέργειας. Οι τροποποιήσεις στους έξυπνους μετρητές μπορεί να αποφέρουν χρηματικά οφέλη στους επιτιθέμενους και δεδομένου ότι οι συσκευές είναι εγκατεστημένες στο χώρο του πελάτη η πρόσβαση σε αυτές είναι σχετικά εύκολη. Στις Η.Π.Α. εκτιμάται ότι το ετήσιο κόστος από την κλοπή ηλεκτρικού ρεύματος ανέρχεται στα 6 δισ. δολάρια. Οι ποιο σημαντικοί στόχοι για την ασφάλεια στους έξυπνους μετρητές είναι η ακεραιότητα και η εμπιστευτικότητα. Είναι σημαντικό οι καταγραφές των έξυπνων μετρητών να είναι σωστές και όχι τροποποιημένες. Η εμπιστευτικότητα είναι επίσης σημαντική. Έχουν κατασκευαστεί εργαλεία που μπορούν να δημιουργήσουν ένα προφίλ από τις καταγραφές ηλεκτρικής ενέργειας των χρηστών, έτσι ώστε να καθοριστεί ποιες ηλεκτρικές συσκευές χρησιμοποιούνται. Αυτή η πληροφορία μπορεί να χρησιμοποιηθεί από διαφορετικές εταιρείες αλλά και από ιδιώτες. Αυτό βέβαια δημιουργεί ανησυχία και προβληματισμό για την προστασία της ιδιωτικής ζωής. Η διαθεσιμότητα των έξυπνων μετρητών είναι πιο ευέλικτη από τα υπόλοιπα εξαρτήματα του έξυπνου δικτύου. Η μέγιστη καθυστέρηση στην επικοινωνία των έξυπνων μετρητών μπορεί να είναι και ώρες. Αυτή η καθυστέρηση είναι

πολύ μεγαλύτερη από τις απαιτήσεις για καθυστέρηση σε πραγματικό χρόνο που είναι της τάξης χιλιοστών του δευτερολέπτου.

Η ασφάλεια στους έξυπνους μετρητές είναι πρόκληση, γιατί είναι εύκολο κάποιος να αποκτήσει πρόσβαση σε μια τέτοια συσκευή και να υπάρχουν άμεσα χρηματικά κέρδη από την τροποποίηση τους. Η ακεραιότητα των έξυπνων μετρητών και των δεδομένων τους πρέπει να επαληθευτούν από το έξυπνο δίκτυο πριν από την χρησιμοποίησή τους. Οι έξυπνοι μετρητές θα πρέπει να δικτυωθούν με τους προμηθευτές ηλεκτρικής ενέργειας, έτσι ώστε να μπορέσουν να επιτελούν την λειτουργικότητά τους. Αυτό σημαίνει ότι είναι δυνατή η παρατήρηση καταγραφών χρήσης ηλεκτρικής ενέργειας χρηστών από οποιονδήποτε άλλο είναι συνδεδεμένο στο ίδιο δίκτυο. Αυτή η πληροφορία μπορεί να χρησιμοποιηθεί για την καταγραφή της συμπεριφοράς των χρηστών.

2.6.3. ΕΚΤΙΜΗΣΗ ΤΗΣ ΚΑΤΑΣΤΑΣΗΣ ΤΟΥ ΕΞΥΠΝΟΥ ΔΙΚΤΥΟΥ

Η ασφάλεια του μοντέλου εκτίμησης της κατάστασης του συστήματος ηλεκτρικής ενέργειας είναι σημαντική, γιατί χρησιμοποιείται από το έξυπνο δίκτυο για την διατήρηση του συστήματος ενέργειας. Το μοντέλο εκτίμησης της κατάστασης του συστήματος ηλεκτρικής ενέργειας είναι ένα εργαλείο που χρησιμοποιούν τα PCS του έξυπνου δικτύου για να μοντελοποιήσουν τα δεδομένα των αισθητήρων και των πρακτόρων. Αυτό σημαίνει ότι οι στόχοι ασφάλειας που έχουν τεθεί για τα PCS είναι επίσης σημαντικοί και εδώ. Η διαθεσιμότητα είναι πολύ σημαντική και ακολουθείται από την ακεραιότητα. Η εμπιστευτικότητα είναι ο λιγότερο σημαντικός στόχος γιατί προσθέτει επιπλέον φόρτο σε ένα σύστημα πραγματικού χρόνου.

Η ασφάλεια στο μοντέλο εκτίμησης κατάστασης αποτελεί πρόκληση λόγω της δυνατότητας λήψης πλαστών στοιχείων εισόδου για το μοντέλο. Υπάρχουν αρκετοί λόγοι για την εισαγωγή πλαστών στοιχείων εισόδου στο μοντέλο. Η αστάθεια του συστήματος καθώς και τα οικονομικά κέρδη είναι μερικά από τα κίνητρα για τους επιτιθέμενους. Πολλά από τα PCS δημιουργούν ζητήματα ασφάλειας με την απευθείας εισαγωγή πλαστών στοιχείων. Η διάκριση μεταξύ πλαστών και πραγματικών στοιχείων είναι ένα δύσκολο πρόβλημα. Συνήθως, υπάρχουν μηχανισμοί που μπορούν να διακρίνουν υπό κανονικές συνθήκες τα «καλά» από τα «κακά» δεδομένα, αλλά αυτοί οι μηχανισμοί δεν είναι αποδοτικοί απέναντι σε επιθέσεις με πλαστά δεδομένα.

2.6.4. ΠΡΩΤΟΚΟΛΛΑ ΕΠΙΚΟΙΝΩΝΙΑΣ ΤΟΥ ΕΞΥΠΝΟΥ ΔΙΚΤΥΟΥ

Η ασφάλεια στα πρωτόκολλα επικοινωνίας που χρησιμοποιεί το έξυπνο δίκτυο είναι ένα σημαντικό ζήτημα γιατί η δικτυακή επικοινωνία είναι η ραχοκοκαλιά του έξυπνου δικτύου. Πολλές από τις κύριες λειτουργίες του έξυπνου δικτύου δεν μπορούν να πραγματοποιηθούν χωρίς την ύπαρξη δικτυακών επικοινωνιών. Οι στόχοι ασφάλειας που είναι σημαντικοί εξαρτώνται από τα εξαρτήματα του έξυπνου δικτύου που επικοινωνούν μεταξύ τους και του είδους των πληροφοριών που ανταλλάσουν.

Η ασφάλεια στα πρωτόκολλα επικοινωνίας που χρησιμοποιεί το έξυπνο δίκτυο είναι πρόκληση, γιατί υπάρχουν πολλά διαφορετικά εξαρτήματα που επικοινωνούν μεταξύ τους, καθένα από τα οποία έχει ένα διαφορετικό σύνολο από απαιτήσεις που πρέπει να ικανοποιήσει. Ένα άλλο πολύ σημαντικό ζήτημα είναι ότι η τεχνολογία που θα χρησιμοποιήσει το έξυπνο δίκτυο θα πρέπει να επικοινωνήσει με παραδοσιακά / απαρχαιωμένα συστήματα ενέργειας (legacy power systems) που έχουν περιορισμούς στην ασφάλεια οι οποίοι πρέπει να ληφθούν υπόψη. Τα παραδοσιακά / απαρχαιωμένα συστήματα ενέργειας θα εισάγουν ευπάθειες στην ασφάλεια του έξυπνου δικτύου λόγω της έλλειψης που έχουν στην υποστήριξη δυνατοτήτων ασφάλειας.

2.6.5. ΠΡΟΣΟΜΟΙΩΣΗ ΤΟΥ ΕΞΥΠΝΟΥ ΔΙΚΤΥΟΥ ΓΙΑ ΑΝΑΛΥΣΗ ΑΣΦΑΛΕΙΑΣ

Η τελευταία κατηγορία κινδύνων για το έξυπνο δίκτυο είναι η ανάλυση της ασφάλειας με προσομοίωση. Οι δοκιμές διαφορετικών σχεδιαστικών προσεγγίσεων για το έξυπνο δίκτυο ή τυχόν αλλαγές σε αυτό είναι πολύ δύσκολο να γίνουν στην πράξη. Το σύστημα ηλεκτρικής

ενέργειας πρέπει να είναι πάντοτε διαθέσιμο, οπότε δεν είναι δυνατόν να βγει εκτός παραγωγής για την πραγματοποίηση δοκιμών. Αντί αυτού είναι δυνατή η μοντελοποίηση του έξυπνου δικτύου με την χρήση λογισμικού ή υλικού. Αυτά τα μοντέλα μπορούν να χρησιμοποιηθούν για την ανάλυση ζητημάτων ασφαλείας ή άλλων πτυχών του έξυπνου δικτύου.

Η προσομοίωση του έξυπνου δικτύου είναι σημαντική λόγω των ζητημάτων που μπορεί να προκύψουν από τις προσομοιώσεις / δοκιμές που θα πραγματοποιηθούν σε αυτό. Η δημιουργία ενός έξυπνου δικτύου είναι πολύ ακριβή. Χαρακτηριστικό παράδειγμα είναι η περίπτωση της περιοχής Boulder του Κολοράντο των Η.Π.Α., όπου το κόστος για την εγκατάσταση του έξυπνου δικτύου είναι 42,1 εκατομμύρια δολάρια. Ως εκ τούτου είναι ανέφικτη η δημιουργία ενός ξεχωριστού έξυπνου δικτύου σε μεγάλη έκταση μόνο και μόνο για την πραγματοποίηση δοκιμών. Επίσης, είναι δύσκολη έως και αδύνατη η χρησιμοποίηση οποιουδήποτε παραγωγικού συστήματος ενέργειας για δοκιμές, γιατί αυτές οι δοκιμές μπορεί να θέσουν σε κίνδυνο την διαθεσιμότητα του συστήματος.

2.7. ΑΝΤΙΜΕΤΩΠΙΣΗ ΚΙΝΔΥΝΩΝ

2.7.1. ΔΙΑΧΕΙΡΙΣΗ ΚΛΕΙΔΙΩΝ

Η διαχείριση των κλειδιών αποτελεί θεμελιώδη προσέγγιση για την ασφάλεια των πληροφοριών. Τα κοινόχρηστα μυστικά κλειδιά ή τα αυθεντικά δημόσια κλειδιά μπορούν να χρησιμοποιηθούν για να επιτευχθεί μυστικότητα και αυθεντικότητα στην επικοινωνία. Η γνησιότητα είναι ιδιαίτερα σημαντική για την επαλήθευση της προέλευσης η οποία με την σειρά της είναι κλειδί για τον έλεγχο πρόσβασης.

Η εγκατάσταση των κλειδιών σε ένα σύστημα καθορίζει την ρίζα της εμπιστοσύνης. Π.χ., ένα σύστημα που βασίζεται σε δημόσια / ιδιωτικά κλειδιά μπορεί να καθορίσει το δημόσιο κλειδί ως την ρίζα της εμπιστοσύνης και το ιδιωτικό κλειδί του κέντρου εμπιστοσύνης να χρησιμοποιείται για την υπογραφή πιστοποιητικών και την ανάθεση εμπιστοσύνης σε άλλα δημόσια κλειδιά. Σε ένα σύστημα με συμμετρικό κλειδί κάθε φορέας καθώς και το κέντρο εμπιστοσύνης θα πρέπει να δημιουργούν κοινά μυστικά κλειδιά. Επίσης, θα πρέπει να θέτουν πρόσθετες σχέσεις εμπιστοσύνης μεταξύ των κόμβων μοχλεύοντας το κέντρο εμπιστοσύνης, όπως συμβαίνει με το σύστημα διαχείρισης κλειδιών και ταυτοποίησης Kerberos.

Στο έξυπνο δίκτυο η διαχείριση των κλειδιών συνιστά πρόκληση γιατί υπάρχει ευρεία και ποικίλη υποδομή. Σε μια πρόσφατη αναφορά του NIST [13] αναφέρεται ότι απαιτούνται αρκετές δεκάδες σενάρια ασφαλούς επικοινωνίας, που κυμαίνονται από την επικοινωνία του διανομέα ρεύματος με τον έξυπνο μετρητή μέχρι και την επικοινωνία του εξοπλισμού με τους τεχνικούς. Για όλα αυτά τα σενάρια επικοινωνίας πρέπει να δημιουργηθούν κλειδιά για να εξασφαλίσουν την αυθεντικότητα και την μυστικότητα. Εκτός από την τεράστια ποικιλία του εξοπλισμού, υπάρχει επίσης και ένα ευρύ φάσμα ενδιαφερομένων, όπως η κυβέρνηση, οι επιχειρήσεις και οι καταναλωτές. Ακόμα και η ασφαλή επικοινωνία με email συνιστά μια πρόκληση στις μέρες μας. Η ασφαλής επικοινωνία μεταξύ του εξοπλισμού της μίας εταιρείας με τους τεχνικούς της άλλης δημιουργεί πολλές πρόσθετες προκλήσεις. Με την προσθήκη μιας ποικιλίας βασικών λειτουργιών διαχείρισης για τα κλειδιά στο μίγμα (π.χ., ανανέωση, ανάκληση, αποθήκευση, ανάκτηση), η πολυπλοκότητα της διαχείρισης κλειδιών γίνεται πραγματικά πολύ μεγάλη. Επιπλέον, πρέπει να εξεταστούν οι επιχειρηματικές, οι πολιτικές και οι νομικές πτυχές καθώς η υπογραφή ενός μηνύματος από ένα δημόσιο κλειδί μπορεί να καταστήσει τον κάτοχο του κλειδιού υπεύθυνο για το περιεχόμενο των πληροφοριών. Μια πρόσφατη δημοσίευση από το NIST [13] παρέχει μια καλή κατευθυντήρια γραμμή για το σχεδιασμό συστημάτων διαχείρισης κρυπτογραφικών κλειδιών για τη στήριξη μιας οργάνωσης, αλλά δεν λαμβάνονται υπόψη οι ποικίλες απαιτήσεις των έξυπνων υποδομών του πλέγματος [12] & [13].

2.7.2. ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΑΣΦΑΛΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

Ο σχεδιασμός μιας εξαιρετικά ανθεκτικής αρχιτεκτονικής επικοινωνιών για ένα έξυπνο δίκτυο είναι ζωτικής σημασίας για τον περιορισμό των επιθέσεων. Παράλληλα θα πρέπει να επιτυγχάνεται και πολύ υψηλή διαθεσιμότητα. Στην συνέχεια παρουσιάζονται τα απαραίτητα στοιχεία που πρέπει να έχει αυτή η αρχιτεκτονική [12] & [13].

- **Σχεδιασμός τοπολογίας δικτύου**: Μια τοπολογία δικτύου αντιπροσωπεύει την δομή σύνδεσης μεταξύ των κόμβων, η οποία μπορεί να έχει επιπτώσεις στην ευρωστία απέναντι στις επιθέσεις. Συνεπώς, η σύνδεση των κόμβων δικτύωσης έτσι ώστε να είναι ιδιαίτερα ανθεκτικοί στις επιθέσεις μπορεί να είναι η βάση για την δημιουργία μιας ασφαλούς αρχιτεκτονικής επικοινωνιών.
- **Ασφαλή πρωτόκολλα δρομολόγησης**: Ένα πρωτόκολλο δρομολόγησης χρησιμοποιείται σε ένα δίκτυο για να οικοδομηθεί η λογική σύνδεση μεταξύ των κόμβων. Ένα απλός τρόπος για να διαταραχθεί η επικοινωνία είναι κάνοντας επίθεση στο πρωτόκολλο δρομολόγησης. Η επικοινωνία σε ένα ολόκληρο δίκτυο μπορεί να παρουσιάσει πρόβλημα θέτοντας είτε σε κίνδυνο έναν δρομολογητή (router) είτε εισάγοντας ψεύτικες δρομολογήσεις. Συνεπώς, θα πρέπει να εξεταστεί η ασφάλεια του πρωτόκολλου δρομολόγησης που τρέχει πάνω σε μια τοπολογία δικτύου.
- **Ασφαλής προώθηση**: Ένας αντίπαλος που ελέγχει έναν δρομολογητή μπορεί να αλλάξει, να εξαφανίσει και να καθυστερήσει τα υφιστάμενα πακέτα δεδομένων ή ακόμα και να εισάγει νέα πακέτα. Συνεπώς, θα απαιτηθεί η εξασφάλιση των μεμονωμένων δρομολογητών και η ανίχνευση των κακόβουλων συμπεριφορών για την επίτευξη της ασφαλούς προώθησης των πακέτων.
- **Επικοινωνία από άκρο σε άκρο**: Από την πλευρά της επικοινωνίας από άκρο σε άκρο το απόρρητο και η αυθεντικότητα των δεδομένων είναι από τις ποιο κρίσιμες ιδιότητες. Η μυστικότητα εμποδίζει έναν ωτακουστή από την εκμάθηση του περιεχομένου των δεδομένων, ενώ η αυθεντικότητα (μερικές φορές αναφέρεται ως ακεραιότητα) δίνει τη δυνατότητα στον δέκτη να βεβαιωθεί ότι τα δεδομένα πράγματι προέρχονται από τον αποστολέα, αποτρέποντας έτσι έναν επιτιθέμενο από το να τροποποιήσει τα δεδομένα.

Ενώ υπάρχουν πολλά πρωτόκολλα (π.χ., SSL / TLS, IPsec, SSH), ορισμένες συσκευές χαμηλής ισχύος μπορεί να χρειαστούν ποιο ελαφριά πρωτόκολλα για την εκτέλεση λειτουργιών σχετικών με την κρυπτογραφία.

- **Ασφαλής μετάδοση**: Πολλά έξυπνα περιβάλλοντα βασίζονται στην επικοινωνία με εκπομπές δεδομένων. Ειδικά για τη διάδοση των τιμών η αυθεντικότητα των πληροφοριών είναι σημαντική, γιατί ο αντίπαλος θα μπορούσε να δώσει ένα αρνητικό κόστος και να κορυφωθεί η κατανάλωση της ηλεκτρικής ενέργειας. Αυτό θα συνέβαινε γιατί πολλές ηλεκτρικές συσκευές θα ενεργοποιούνταν ταυτόχρονα για να επωφεληθούν από την χαμηλή τιμή του ηλεκτρικού ρεύματος.
- **Άμυνα στις επιθέσεις DoS**: Λαμβάνοντας υπόψη όλους τους παραπάνω μηχανισμούς, ένας αντίπαλος θα μπορούσε να εξακολουθεί να εμποδίζει τις επικοινωνίες εκκινώντας επιθέσεις DoS. Π.χ., εάν ένας αντίπαλος ελέγχει πολλά τερματικά σημεία, μετά από επιθέσεις σε αυτά, θα μπορεί να τα χρησιμοποιήσει σαν τερματικά σημεία για να πλημμυρίσει το δίκτυο με δεδομένα. Ως εκ' τούτου είναι ζωτικής σημασίας να υπάρχει επικοινωνία και κάτω από αυτές τις συνθήκες. Επιπλέον, η ίδια ηλεκτρική ενέργεια και όχι τα δίκτυα επικοινωνίας μπορεί να είναι στόχος μια επίθεσης DoS.
- **Άμυνα στις παρεμβολές**: Για να αποτραπεί ένας εξωτερικός αντίπαλος από την χρησιμοποίηση του ασύρματου δικτύου, μπορεί να γίνει εμπλοκή των μηχανισμών ανίχνευσης για τον εντοπισμό επιθέσεων και την ενεργοποίηση των συναγερμών. Έχει αναπτυχθεί ένας πλήθος μεθόδων για την αντιμετώπιση επιθέσεων παρεμβολών, επιτρέποντας την λειτουργία κατά την διάρκεια παρεμβολών.

2.7.3. ΑΣΦΑΛΕΙΑ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΣΥΣΚΕΥΩΝ

Ένας σημαντικός τομέας είναι η αντιμετώπιση των αδυναμιών που επιτρέπουν την εκμετάλλευση ενός συστήματος μέσω επιθέσεων που πραγματοποιούνται με την χρήση λογισμικού. Αυτού του είδους οι επιθέσεις μπορούν να συμβούν είτε όταν ένα επιτιθέμενος εκμεταλλεύεται μια ευπάθεια του λογισμικού για να εισάγει κακόβουλο κώδικα, είτε όταν ένας κακόβουλος χρήστης χρησιμοποιεί δικαιώματα διαχειριστή για να εγκαταστήσει κακόβουλο κώδικα. Η πρόκληση σε ένα τέτοιο περιβάλλον είναι να έχει ο εξουσιοδοτημένος χρήστης την σωστή απάντηση στο ακόλουθο ερώτημα, κατά την επικοινωνία με ένα σύστημα σε εν δυνάμει κίνδυνο. Η απάντηση που έλαβε ο εξουσιοδοτημένος χρήστης προήλθε από το νόμιμο κώδικα ή από τον κακόβουλο; Ένα παράδειγμα αυτού του προβλήματος είναι όταν προσπαθείτε να εκτελέσετε ένα πρόγραμμα ανίχνευσης ιών σε ένα σύστημα που βρίσκεται δυνητικά σε κίνδυνο. Εάν το πρόγραμμα ανίχνευσης ιών επιστρέψει αποτέλεσμα ότι δεν υπάρχει ιός δύο πράγματα δυνητικά θα μπορούν να συμβαίνουν, είτε ότι δεν μπόρεσε να προσδιοριστεί κανένα ιός είτε ότι ο ιός έχει απενεργοποιήσει το πρόγραμμα ανίχνευσης ιών. Ένα παρόμοιο πρόβλημα είναι ότι τα προγράμματα ανίχνευσης ιών έχουν ατελείς καταλόγους με υπογραφές ιών. Συνεπώς, η απουσία ανίχνευσης του ιού θα μπορούσε να είναι επειδή το πρόγραμμα ανίχνευσης ιών δεν αναγνωρίζει ακόμη το νέο ιό.

Στο πλαίσιο των έξυπνων δικτύων οι ερευνητές έχουν προτείνει διάφορες τεχνικές για να εξασφαλίσουν μηχανισμούς πρόληψης και εντοπισμού κακόβουλων προγραμμάτων. Οι Mc Laughlin et al. έχουν προτείνει πολυμορφία στο ενσωματωμένο firmware για να αποφευχθούν τα σενάρια όπου ένα κακόβουλο λογισμικό θέτει σε κίνδυνο εξοπλισμό. Με αυτή την πρόταση κάθε συσκευή θα εκτελεί διαφορετικό λογισμικό, έτσι ώστε να αποφεύγονται κοινές αδυναμίες.

Μια πολλά υποσχόμενη νέα προσέγγιση για την παροχή εξ αποστάσεως επαλήθευσης του κώδικα είναι μια τεχνολογία που ονομάζεται βεβαίωση. Η βεβαίωση κώδικα επιτρέπει σε έναν εξωτερικό φορέα να ερευνήσει το λογισμικό που εκτελείται σε ένα σύστημα, με έναν τέτοιο τρόπο που δεν επιτρέπει στο κακόβουλο λογισμικό να κρυφτεί. Από την στιγμή που η βεβαίωση αποκαλύπτει μια υπογραφή του εκτελούμενου κώδικα, ακόμα και ένα άγνωστο κακόβουλο λογισμικό να μεταβάλλει αυτήν την υπογραφή θα καταστεί δυνατόν να ανιχνευθεί. Σε αυτή την κατεύθυνση οι LeMay et al. έχουν μελετήσει προσεγγίσεις για την βεβαίωση βασιζόμενοι στο υλικό. Η βεβαίωση βασιζόμενη στο λογισμικό είναι μια προσέγγιση που δεν βασίζεται σε εξειδικευμένο υλικό, αλλά κάνει κάποιες παραδοχές κατά τις οποίες ο ελεγκτής μπορεί να επικοινωνεί μοναδικά με τη συσκευή που ελέγχεται. Οι Shah et al. έχουν αποδείξει την σκοπιμότητα αυτής της αντίληψης για τις συσκευές SCADA [12] & [13].

3. ΄ΕΞΥΠΝΟΙ ΜΕΤΡΗΤΕΣ – ΤΕΛΙΚΟΣ ΚΑΤΑΝΑΛΩΤΗΣ

3.1. ΟΡΙΣΜΟΣ

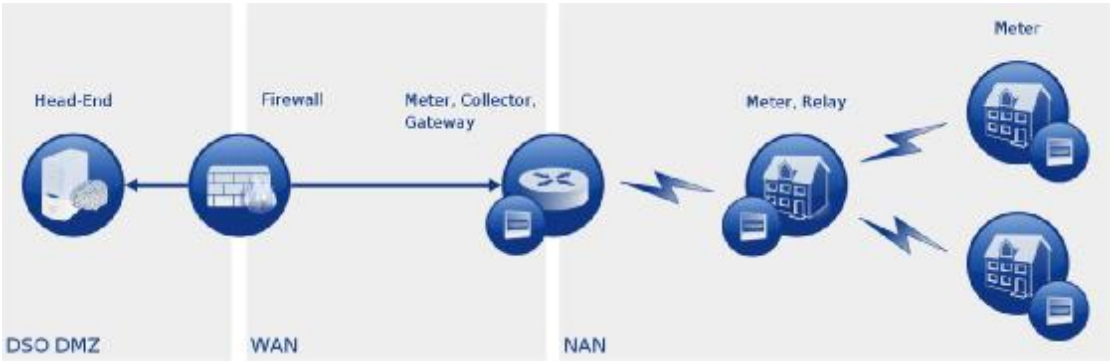
Ένα από τα βασικά εξαρτήματα του έξυπνου δικτύου τα οποία βρίσκονται στην πρώτη γραμμή του είναι οι έξυπνοι μετρητές. Ο κύριος σκοπός ενός μετρητή είναι η παρακολούθηση της ενέργειας που καταναλώνεται με την χρήση της μετρολογίας, η οποία μετράει το ποσό του φορτίου που λαμβάνει μια οντότητα. Οι μετρητές χρησιμοποιούνται κατά κόρον σε οικιακά και επαγγελματικά κτίσματα. Στο παρελθόν οι εταιρείες κοινής ωφέλειας επισκεπτόντουσαν στο φυσικό του χώρο κάθε μετρητή, σε προκαθορισμένες χρονικές στιγμές, για να τον διαβάσουν και να καθορίσουν το ποσό της ενέργειας που έχει καταναλώσει ο πελάτης. Χρησιμοποιούσαν πολύπλοκους μηχανισμούς για να προβλέψουν το ποσό της ενέργειας που θα καταναλώσει ο πελάτης, έτσι ώστε να μπορέσουν να εκδώσουν τον λογαριασμό του (πληρωμή έναντι).

Ένας τρόπος για να εκδοθούν οι λογαριασμοί έναντι είναι με την χρήση ιστορικότητας. Χρησιμοποιούνται δεδομένα μετρητών που έχουν καταγραφεί σε βάθος ενός έτους και με βάση αυτά γίνεται πρόβλεψη της ηλεκτρικής ενέργειας που θα καταναλώσει ο πελάτης. Οι εταιρείες κοινής ωφέλειας θα μπορούσαν να πάρουν την μέση τιμή των λογαριασμών για ένα έτος και να υποθέσουν ότι οι καταναλωτές της ίδιας περιοχής θα καταναλώσουν περίπου το ίδιο ποσό ενέργειας. Προφανώς, αυτή η διαδικασία είναι αναποτελεσματική γιατί οι χρεώσεις των καταναλωτών δεν βασίζονται σε πραγματικά δεδομένα, αλλά σε προβλέψεις οι οποίες πολλές φορές δεν αναπαριστούν την πραγματικότητα. Σε αυτό το σημείο πρέπει να επισημάνουμε ότι οι εταιρείες κοινής ωφέλειας χρησιμοποιούν πολύπλοκους αλγορίθμους για να πραγματοποιήσουν αυτές τις προβλέψεις. Αυτοί οι αλγόριθμοι θεωρούνται εμπορικά μυστικά και υποτίθεται ότι εξασφαλίζουν ισότητα και ισονομία στους πελάτες. Επιπλέον, οι πελάτες αρκετές φορές χρεώνονται για λιγότερο ποσό από ότι τους αναλογεί, έτσι ώστε να μην κατηγορηθούν οι εταιρείες κοινής ωφέλειας για ακατάλληλες λογιστικές πρακτικές.

Η χρήση παλαιών μετρητών έχει οδηγήσει στην απώλεια εσόδων στις εταιρείες κοινής ωφέλειας. Εάν μπορούσαν με κάποιον τρόπο να έχουν ακριβή δεδομένα για την κατανάλωση ηλεκτρικής ενέργειας σε ευρεία κλίμακα, θα μπορούσαν να εκδώσουν ακριβείς λογαριασμούς και να έχουν μεγαλύτερα κέρδη σε βάθος χρόνου. Αυτό το πρόβλημα λύνεται με την χρήση έξυπνων μετρητών. Ωστόσο δημιουργείται ένα άλλο πρόβλημα, γιατί θα πρέπει να εγκατασταθούν οι έξυπνοι μετρητές σε κάθε πελάτη και κάθε εταιρεία κοινής ωφέλειας μπορεί να έχει μερικές εκατοντάδες χιλιάδες πελάτες ακόμα και εκατομμύρια. Στην ουσία όμως το κύριο πρόβλημα είναι τα κόστη αντικατάστασης τόσου εξοπλισμού (ένας έξυπνος μετρητής για κάθε πελάτη) και το πώς θα υλοποιηθεί ένα δίκτυο επικοινωνίας που θα υποστηρίζει τόσους πολλούς πελάτες. Σαν αποτέλεσμα οι εταιρείες κοινής ωφέλειας δεν έχουν αναπτύξει τους έξυπνους μετρητές, γιατί τα κόστη εγκατάστασης και χρησιμοποίησή τέτοιας τεχνολογίας δεν θα κατανοηθούν παρά μονάχα σε πολλά χρόνια στο μέλλον [17] & [28].

3.2. ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΚΑΙ ΥΠΟΔΟΜΗ AMI

Η προηγμένη υποδομή μέτρησης (AMI) είναι συνήθως δομημένη σε μια δέσμη δικτύων και αποτελείται από αρκετά βασικά συστατικά. Η εικόνα 4 παρέχει μια επισκόπηση των περισσότερων βασικών συστατικών και δικτύων. Η AMI αποτελείται από τον έξυπνο μετρητή, τον συλλέκτη και τα συστήματα διακομιστών που βρίσκονται είστε στο διαχειριστή του συστήματος διανομής (DSO) είτε στην εταιρεία μετρήσεων [17], [25] & [28].



Εικόνα 4, Υποδομή δικτύων και συστατικών της AMI [25]

3.2.1. ΕΠΙΚΟΙΝΩΝΙΕΣ

Η επικοινωνιακή υποδομή αποτελείται από διάφορα δίκτυα τα οποία μπορούν να βασίζονται σε εντελώς διαφορετικά μέσα και σε μια πληθώρα πρωτοκόλλων. Όταν αναφερόμαστε στην AMI συνήθως υπάρχουν τρία διαφορετικά δίκτυα: το δίκτυο ευρείας περιοχής (WAN), το δίκτυο γειτονιάς(NAN) και το οικιακό δίκτυο (HAN). Επιπλέον, παρέχεται και ένας τοπικός δίαυλος (bus) με κοινές επαφές, π.χ. σειριακή θύρα, οπτική διεπαφή, κλπ., για διαγνωστικούς σκοπούς.

3.2.4.1. WAN

Το WAN συνδέει έναν μετρητή ή έναν συλλέκτη στο HES και μερικές φορές αναφέρεται στην βιβλιογραφία ως backhaul δίκτυο. Η επικοινωνία στο WAN βασίζεται ως επί το πλείστον στο πρωτόκολλο IPκαι σε μέσα και τεχνολογίες της επιστήμης των υπολογιστών, όπως καλώδια οπτικών ινών, DSL, GRPS, MPLS, PLS, ή κάποιου είδους ιδιωτικό δίκτυο. Η συντονιστική ομάδα για το έξυπνο δίκτυο (SMCG) της Ευρωπαϊκής Ένωσης δεν προσδιορίζει ένα συγκεκριμένο πρωτόκολλο, αλλά προτείνει οι επικοινωνίες να βασίζονται σε ασφαλή και μη ιδιωτικά (nonproprietary) πρωτόκολλα και πλατφόρμες επικοινωνίας για την «χύμα» μετάδοση δεδομένων από συλλέκτες που περιέχουν έναν μεγάλο αριθμό έξυπνων μετρητών.

3.2.4.2. NAN

Το NAN συνδέει τους έξυπνους μετρητές και τους συλλέκτες. Τυπικές συσκευές που συνδέονται στο NAN είναι οι μετρητές ηλεκτρικής ενέργειας, αερίου, νερού ή θερμότητας. Οι επιχειρήσεις μερικές φορές αναφέρονται στα NAN ως τοπικό μετρολογικό δίκτυο (LMS), δίκτυο τομέα (FAN), ή τοπικό δίκτυο (LAN) μέτρησης. Αν και κερδίζουν εμπιστοσύνη τα πρότυπα όπως το IEEE 802.15.4, στο οποίο βασίζεται το ZigBee, ωστόσο οι κατασκευαστές δυσκολεύονται να συμφωνήσουν σε ένα κοινό πρότυπο. Οι εταιρείες κοινής ωφέλειας που εδράζονται στην Ευρωπαϊκή Ένωση φαίνεται να προτιμούν το πρότυπο μετρητή διαύλου για την επικοινωνία στο NAN, ωστόσο η ENISA δεν αναφέρει τον μετρητή διαύλου ως πρότυπο για το NAN.

3.2.4.3. HAN

Ανάλογα με τον τύπο του καταναλωτή το HAN θα μπορούσε επίσης να ονομαστεί ως δίκτυο κτιρίου (BAN) ή βιομηχανικό δίκτυο περιοχής (IAN). Όποιο και εάν είναι το όνομα του ο σκοπός του HAN είναι η ενσωμάτωση επιπλέον μετρητών αερίου, νερού και θερμότητας. Το HAN θα μπορούσε να επιτρέψει τον ευφυή αυτοματισμό κτιρίων καθώς επίσης και την διασύνδεση των DER με το έξυπνο δίκτυο.

Για τη βελτιστοποίηση της κατανάλωσης κατά τις ώρες αιχμής ένα βοηθητικό πρόγραμμα θα μπορούσε για παράδειγμα να αποφασίσει να μην απενεργοποιήσει εντελώς, αλλά να μειώσει την χρήση συσκευών θέρμανσης, κλιματισμού και εξαερισμού (HVAC) για να επιτευχθεί εξισορρόπηση του δικτύου. Για αυτό το σκοπό θα πρέπει οι καταναλωτές να επιτρέπουν την πρόσβαση στις ηλεκτρικές τους συσκευές από τις εταιρείες κοινής ωφέλειας. Ωστόσο, ο ευφυής έλεγχος δεν απαιτεί κατ 'ανάγκη την παρέμβαση ενός εξωτερικού μέρους. Με αυτό το τρόπο μια έξυπνη HVAC θα μπορούσε να αποφασίσει αυτόματα την μείωση της

χρησιμοποιούμενης ενέργειας, με βάση την πληροφόρηση σε πραγματικό χρόνο από το πρόγραμμα για την τιμή του ηλεκτρικού ρεύματος.

3.2.2. HES

Το HES (Head-End System) είναι επίσης γνωστό και ως σύστημα ελέγχου μέτρησης και βρίσκεται στο δίκτυο της εταιρείας μετρήσεων. Στις περισσότερες περιπτώσεις η εταιρεία μετρήσεων είναι η υπεύθυνη DSO. Το HES επικοινωνεί άμεσα με τους έξυπνους μετρητές και ως εκ' τούτου θα πρέπει να βρίσκεται σε κάποια αποστρατικοποιημένη ζώνη (DMZ), δεδομένου ότι οι υπηρεσίες και λειτουργίες του θα παρέχονται προς τα έξω (π.χ. στο διαδίκτυο).

Υπάρχουν πολλές περισσότερες υποδομές στις DSO και στις εταιρείες μετρήσεων. Τα δεδομένα που συλλέγονται θα διαχειρίζονται μέσα σε ένα σύστημα διαχείρισης δεδομένων μέτρησης (MDM), το οποίο επίσης χαρτογραφεί δεδομένα του οικιακού χρήστη. Ανάλογα με το επίπεδο αυτοματοποίησης τα δεδομένα μέτρησης θα έχουν επίδραση στις ενέργειες της DSO, προκειμένου αυτή να εξισορροπήσει το δίκτυο.

Η έκθεση του HES στους καταναλωτές εγείρει κάποιες σημαντικές απειλές για την DSO. Για παράδειγμα, εάν ένας αντίπαλος καταφέρει να αποκτήσει πρόσβαση στο HES θα μπορέσει να διαβάσει όλα τα δεδομένα των καταναλωτών. Επιπλέον, θα μπορούσε κάποιος να ελέγξει τους έξυπνους μετρητές και να χειραγωγήσει τα δεδομένα μέτρησης ή να δημιουργήσει μηνύματα προειδοποιήσεων (alarms). Αυτό θα μπορούσε να διαταράξει τις λειτουργίες τις DSO ή να προκαλέσει την ενεργοποίηση της ομάδας αντιμετώπισης περιστατικών στους υπολογιστές (CIRT) και ίσως να αναγκάσει την DSO να εφαρμόσει κάποιο σχέδιο επιχειρησιακής συνέχειας (BCP), ενώ παράλληλα θα αναλύει και θα προβαίνει σε ανάκτηση του HES.

3.2.3. ΣΥΛΛΕΚΤΗΣ

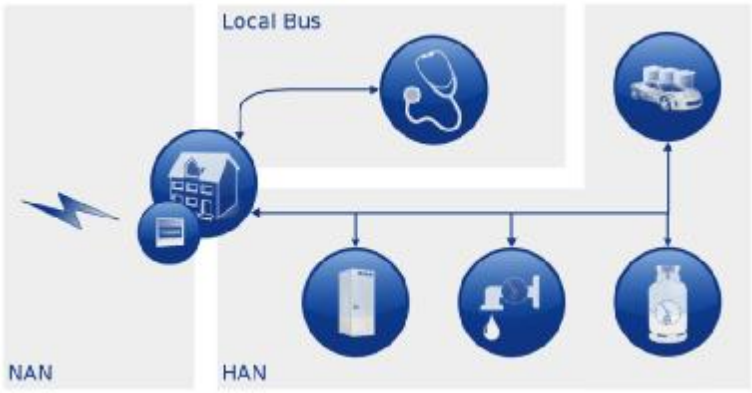
Ο συλλέκτης, επίσης γνωστός ως συγκεντρωτής ή πύλη, χρησιμεύει ως κόμβος επικοινωνίας για το HES. Ανάλογα με την υποδομή ο συλλέκτης θα μπορούσε να είναι και ο ίδιος ένας έξυπνος μετρητής. Η κύρια λειτουργία του είναι η δημιουργία μιας διεπαφής μεταξύ του HES και των έξυπνων μετρητών και / ή άλλων συλλεκτών μέσα σε ένα δίκτυο γειτονιάς (NAN).

Όχι μόνο το HES αλλά και ο συλλέκτης εγείρει απειλές για το έξυπνο δίκτυο. Ο συλλέκτης εκτίθεται φυσικά στους αντιπάλους (λόγω της εγκατάστασης στο φυσικό περιβάλλον). Επιπλέον, έχει μια εμπιστευτική διασύνδεση τόσο με το HES όσο και με την πλευρά του NAN και έτσι έχει το προνόμιο να μπορεί να επικοινωνεί και με τις δύο άκρες. Οι αντίπαλοι μπορεί να εκμεταλλευτούν αυτό το γεγονός προκειμένου να επιτεθούν στο HES. Επιπλέον, από την πλευρά του NAN οι αντίπαλοι θα μπορούσαν να μιμηθούν τον συλλέκτη για να στήσουν ένα MitM σενάριο[4] ή να στείλουν αυθαίρετες εντολές στους έξυπνους μετρητές.

3.2.4. ΕΞΥΠΝΟΣ ΜΕΤΡΗΤΗΣ

Ο έξυπνος μετρητής τοποθετείται στις εγκαταστάσεις των καταναλωτών και όταν ενσωματωθεί σε έναν συλλέκτη επικοινωνεί απευθείας με το HES. Ένας έξυπνος μετρητής μπορεί είτε να επικοινωνεί με τον συλλέκτη είτε να λειτουργεί ως συνδετικός κρίκος για την δρομολόγηση πακέτων μεταξύ κοντινών έξυπνων μετρητών και του συλλέκτη. Μερικοί έξυπνοι μετρητές προσφέρουν και διασύνδεση με οικιακές ηλεκτρικές συσκευές. Για έναν πελάτη λιανικής αυτό το δίκτυο ονομάζεται οικιακό δίκτυο (HAN). Οι έξυπνοι μετρητές παρέχουν επίσης τοπικές διαγνωστικές θύρες για λειτουργίες ανάγνωσης, εγκατάστασης και συντήρησης, όπως φαίνεται στην εικόνα 5.

[4] Η επίθεση MitM είναι μια κοινή παραβίαση ασφάλειας. Ο επιτιθέμενος παρεμποδίζει την νόμιμη επικοινωνία μεταξύ δύο μερών, τα οποία είναι φιλικά μεταξύ τους. Στη συνέχεια, ο κακόβουλος host ελέγχει τη ροή επικοινωνίας και μπορεί να αποσπάσει ή να αλλάξει πληροφορίες που στέλνονται από έναν από τους αρχικούς συμμετέχοντες. Οι επιθέσεις MitM εφαρμόζονται ιδιαίτερα στο πρωτόκολλο Diffie-Hellman, όταν η συμφωνία ανταλλαγής κλειδιών γίνεται χωρίς ταυτοποίηση.



Εικόνα 5, Σχεδιάγραμμα HANκαι τοπικού διαύλου [25]

Από την πλευρά των επιτιθέμενων ο έξυπνος μετρητής είναι το σημείο εισόδου για το κτήριο αυτοματισμού, το DER και για τα δεδομένα των χρηστών. Αλλά ο έξυπνος μετρητής είναι ένα τμήμα του έξυπνου δικτύου και δεν πρέπει σε καμία περίπτωση η χειραγώγησή του να επηρεάσει σε κρίσιμο βαθμό το έξυπνο δίκτυο ή την διαθεσιμότητα τόσο του ίδιου του έξυπνου δικτύου όσο και των μερών του.

3.3. ΔΙΑΧΕΙΡΙΣΗ ΑΣΦΑΛΕΙΑΣ ΕΠΙΚΟΙΝΩΝΙΩΝ

Η εξασφάλιση των επικοινωνιών στο έξυπνο δίκτυο εξαρτάται από δύο σημαντικούς παράγοντες, από την καθυστέρηση στην επικοινωνία και από τον όγκων των μηνυμάτων. Εάν το κέντρο λειτουργίας χάσει οποιαδήποτε είσοδο από έναν έξυπνο μετρητή ενός HAN, αυτό μπορεί να επηρεάσει οποιαδήποτε απόφαση που πήρε το έξυπνο κέντρο και η οποία μπορεί να ήταν και σημαντική. Ο πίνακας 3 περιέχει στοιχεία σχετικά με την διαχείριση ασφάλειας σε εξοπλισμό που βρίσκεται σε ένα HAN. Προκειμένου να αποφευχθεί κάθε πιθανή κατάσταση έκτακτης ανάγκης, η οποία μπορεί να συμβεί ανά πάσα στιγμή, το σύστημα επικοινωνίας του έξυπνου δικτύου πρέπει να είναι σε θέση να χειριστεί την παράδοση των μηνυμάτων στο κέντρο λειτουργίας μέσω των πυλών (gateways) των NAN & BAN με την ελάχιστη δυνατή καθυστέρηση.

Επίθεση	Αντίκτυπο στο έξυπνο δίκτυο	Απαίτηση ασφάλειας
Παρακολούθηση έξυπνων μετρητών	Το ίδιο πρόβλημα όπως και σε ένα παραδοσιακό δίκτυο	Κωδικοποιημένα πακέτα: δυσκολία για αποκωδικοποίηση της κίνησης
Ανάλυση της κίνησης	Δυσκολία στην ανίχνευση	Περιοδική αλλαγή των κρυπτογραφικών κλειδιών
DoS, παρεμβολές & εμπλοκές στο ασύρματο δίκτυο	Μπορεί να εξαχθούν κλειδιά από τα δεύτερης γενιάς ολοκληρωμένα κυκλώματα ZigBee	Έλεγχος χρηστών στον διαμοιρασμό των πηγών ή και των καναλιών
Πλημμύρισμα μνήμης προσωρινής αποθήκευσης με DoS	Μπορεί να διαγράψουν την μνήμη προσωρινής αποθήκευσης των έξυπνων μετρητών	Εξονυχιστική αποσφαλμάτωση (debug) των προγραμμάτων και των πρωτοκόλλων
Επανακαθορισμός της επίθεσης	Εγκατάσταση ασταθούς firmwareστους έξυπνους μετρητές και στις ηλεκτρονικές συσκευές	Ασφαλής αναβάθμιση firmwareμόνο από πιστοποιημένα κέντρα λειτουργίας
Εξαπάτηση	• Υποδύονται τους έξυπνους μετρητές • Αύξηση του	Ταυτοποίηση των έξυπνων μετρητών με την χρήση του πρωτοκόλλου IPSec

	λογαριασμού των καταναλωτών • Χαμηλότερος λογαριασμός για τους επιτιθέμενους	
MitM	Μπορεί να υποδυθούν τον έξυπνο μετρητή	Ασφαλής επικοινωνία πάνω από IPSec
Επαναληπτική	• Αποθήκευση τρεχόντων δεδομένων (κατά την χαμηλή χρήση ενέργειας) των έξυπνων μετρητών • Αποστολή των αποθηκευμένων δεδομένων στην εταιρεία κοινής ωφέλειας σε μεταγενέστερο χρόνο (κατά την υψηλή χρήση ενέργειας)	• Χρησιμοποίηση χρονοσήμανσης και συγχρονισμού ώρας στους έξυπνους μετρητές και στα κέντρα λειτουργίας • Χρησιμοποίηση nonceπου διαφέρουν με το χρόνο

Πίνακας 3, Διαχείριση κινδύνων ασφάλειας [3]

Οι απαιτήσεις ισχύος των ηλεκτρικών συσκευών ενός HAN στέλνονται στο αντίστοιχο BAN κατά την περιοδική ανάγνωση των δεδομένων που κάνει ο μετρητής. Το μέγεθος κάθε περιοδικού αιτήματος είναι 32 bytes. Υπολογίζοντας τις υποχρεωτικές επικεφαλίδες το μέγεθος του πακέτου μπορεί να είναι περίπου (50+32=) 82 bytes. Επιπλέον, υπάρχουν και οι επικεφαλίδες του TCP/IP καθώς και επιπλέον επικεφαλίδες για την ασφάλεια, εάν χρησιμοποιηθεί κάποιο επιπλέον πρωτόκολλο ασφάλειας. Εάν συμβεί κάποια καθυστέρηση στην πύλη του BAN, το πακέτο μπορεί να καθυστερήσει να αποσταλεί στην πύλη του NAN και από εκεί στο κέντρο λειτουργίας. Επιπλέον, μπορεί επίσης και να χαθεί εάν η μνήμη του αντίστοιχου ολοκληρωμένου κυκλώματος της πύλης του BAN γεμίσει λόγω: 1) πολλαπλών μηνυμάτων που φθάνουν από διαφορετικές HAN την ίδια χρονική στιγμή και 2) περιορισμένης επεξεργαστικής δυνατότητας της πύλης του BAN. Σε αυτή την περίπτωση η πύλη του BAN μπορεί να ζητήσει από την πύλη του HAN να μεταδώσει πάλι τα απαιτούμενα πακέτα. Αυτό συμβάλλει στην αύξηση της καθυστέρησης των επικοινωνιών.

Οι Hauser et al. αναφέρουν ότι το δίκτυο επικοινωνίας του έξυπνου δικτύου θα πρέπει να είναι σε θέση να εξυπηρετεί πολλά μηνύματα ταυτόχρονα. Αυτό θα πρέπει να συμβαίνει τόσο χωρίς σημαντική καθυστέρηση στην επικοινωνία όσο και χωρίς καμία απολύτως επίπτωση στην ασφάλεια. Σε αυτό το σημείο πρέπει να αναφερθεί ότι ο μεγάλος όγκος των μηνυμάτων θα επηρεάσει το απαιτούμενο εύρος ζώνης. Συνεπώς, κάθε ασφαλές πλαίσιο επικοινωνίας για έξυπνα δίκτυα θα πρέπει να έχει «ελαφριές» λειτουργίες. Οι λόγοι πίσω από αυτό είναι δύο: 1) πρέπει να αποφευχθούν ενδεχόμενες υψηλές καθυστερήσεις στην επικοινωνία και 2) πρέπει να μειωθούν τα γενικά έξοδα επικοινωνίας περιορίζοντας τα περιττά μηνύματα σηματοδοσίας. Επιπλέον, σημειώστε ότι οι επικεφαλίδες ασφάλειας συμβάλλουν στην αύξηση του μεγέθους του πακέτου. Ως εκ τούτου ο μηχανισμός ελέγχου που θα χρησιμοποιηθεί πρέπει να είναι ελαφρύς για τον σχεδιασμό αποτελεσματικών αλγορίθμων ταυτότητας για τις πύλες των HAN/BAN/NAN.

Ωστόσο, οι διαθέσιμες προτάσεις για ασφαλείας για τα έξυπνα δίκτυα δεν έχουν αναλυτική τεκμηρίωση, συμπεριλαμβανομένης της επιλογής των κατάλληλων κρυπτοσυστημάτων. Επίσης, μέχρι στιγμής δεν υπάρχει ασφαλές πλαίσιο για την πραγματοποίηση αξιόπιστου ελέγχου ταυτότητας στους έξυπνους μετρητές. Για παράδειγμα μια πύλη του BAN πρέπει να κάνει έλεγχο ταυτότητας στην αιτούσα πύλη του HAN ενώ η πύλη του NAN πρέπει να κάνει έλεγχο ταυτότητας στις δικές της πύλες των BAN. Η προσθήκη κρυπτογραφικών

δυνατοτήτων στην επικοινωνία καταλαμβάνει ένα σημαντικό μέρος από το συνολικό μέγεθος του πακέτου. Επιπλέον, αυτές οι δυνατότητες αυξάνουν το υπολογιστικό κόστος, ειδικά στην πλευρά του δέκτη που επαληθεύει το μήνυμα. Στο έξυπνο δίκτυο στέλνονται μηνύματα κάθε δευτερόλεπτο από τους έξυπνους μετρητές, συνεπώς ο αριθμός των μηνυμάτων που πρέπει να επαληθευτεί είναι υψηλός. Επίσης, υπάρχει και καθυστέρηση στην επεξεργασία των μηνυμάτων λόγω των πρόσθετων κρυπτογραφικών δυνατοτήτων. Όλα τα παραπάνω αυξάνουν την καθυστέρηση στην επικοινωνία.

Επειδή η συμβατική υποδομή δημόσιου κλειδιού (PKI)δεν είναι επαρκής για αυτά τα συστήματα λόγω των αυστηρών χρονικών περιορισμών για τις επικοινωνίες, είναι απαραίτητη η ύπαρξη ενός «ελαφριού» αλγορίθμου επαλήθευσης. Με την χρήση αυτού του «ελαφριού» αλγορίθμου τα εισερχόμενα μηνύματα θα μπορούν να υποβληθούν γρηγορότερα σε επεξεργασία. Επιπλέον, οι έξυπνοι μετρητές είναι ευάλωτοι σε διάφορες επιθέσεις και η χρήση τεχνολογιών βασισμένες στην IP καθιστούν το έξυπνο δίκτυο ποιο ευάλωτο σε κυβερνο-επιθέσεις. Το χρησιμοποιούμενο πλαίσιο ασφάλειας θα πρέπει να λάβει υπόψη του αυτές τις απειλές για να μπορέσει να τις αντιμετωπίσει κατάλληλα [3].

3.4. ΜΗΧΑΝΙΣΜΟΣ ΤΑΥΤΟΠΟΙΗΣΗΣ ΧΡΗΣΤΩΝ

Σε αυτή την ενότητα θα ασχοληθούμε με την ασφάλεια του έξυπνου δικτύου από την πλευράς της δημιουργίας διασυνδεδεμένων σφαιρών εμπιστοσύνης[5] (trust realms). Οι τέσσερις τύποι των εντολέων που απαιτούνται σε μια σφαίρα αναλύονται ως εξής [14], [18], [22] & [28]:

- **Άγκυρες εμπιστοσύνης (trust anchors)**: διαχειρίζονται τα κλειδιά κατανομής σε μια σφαίρα, συνεπώς κάθε άγκυρα εμπιστοσύνης έχει ένα δημόσιο και ένα ιδιωτικό κλειδί.
- **Συναθροιστές δεδομένων (data aggregators)**: είναι πράκτορες που είναι σε θέση να εκτελούν περίπλοκες εργασίες επεξεργασίας δεδομένων. Κάθε συναθροιστής δεδομένων έχει ένα πιστοποιημένο δημόσιο και ένα ιδιωτικό κλειδί για τα δεδομένα των επικοινωνιών.
- **Συλλέκτες δεδομένων (data collectors)**: είναι πράκτορες που ασχολούνται με την συλλογή και την πραγματοποίηση αναλύσεων ευαισθησίας στα δεδομένα. Κάθε συλλέκτης δεδομένων έχει ένα πιστοποιημένο δημόσιο κλειδί και ένα ιδιωτικό κλειδί για την επικοινωνία με άλλες αρχές σε μια σφαίρα.
- **Αισθητήρες (sensors)**: είναι χαμηλής ισχύος συσκευές για τη συλλογή δεδομένων. Κάθε αισθητήρας έχει μια έξυπνη κάρτα που περιέχει δύο πιστοποιητικά για την ανάθεση εμπιστοσύνης που εκδίδεται από τις άγκυρες εμπιστοσύνης. Με αυτά τα πιστοποιητικά διευκολύνεται η πραγματοποίηση ασφαλών και αποτελεσματικών επικοινωνιών από τους αισθητήρες με άλλους εντολείς στην σφαίρα.

3.5. ΠΡΟΤΑΣΗ ΔΙΑΧΕΙΡΙΣΗΣ ΚΛΕΙΔΙΩΝ

Προτείνεται η συνδυασμένη χρησιμοποίηση ενός δημοσίου και ενός ιδιωτικού κλειδιού για λόγους απλότητας και επεκτασιμότητας της διαχείρισης κλειδιών. Το σχήμα του συμμετρικού κλειδιού βασίζεται στο πρωτόκολλο ελέγχου ταυτότητας των Needham-Schroeder. Το σχήμα του δημόσιου κλειδιού βασίζεται σε ελλειπτική κρυπτογραφία για υψηλή αποδοτικότητα και ισχυρή ασφάλεια. Η χρήση των δημοσίων κλειδιών διαθέτει επίσης μια όμορφη ιδιότητα που δεν απαιτεί την χρήση ενός στατικού συμμετρικού κλειδιού μεταξύ των συναθροιστών δεδομένων και των συλλεκτών.

Δεδομένου ότι στο πρωτόκολλο ελέγχου ταυτότητας των Needham-Schroeder η χρησιμοποίηση σημασιολογίας στα εμπλεκόμενα μηνύματα είναι ζωτικής σημασίας ως

[5] Ως σφαίρα εμπιστοσύνης ορίζεται εκείνο το τμήμα του δικτύου υπολογιστών στο οποίο όσοι βρίσκονται και επικοινωνούν εμπιστεύονται ο ένας τον άλλο και ανταλλάσουν με ασφάλεια δεδομένα και πληροφορίες.

αντίμετρο για τις επιθέσεις επανάληψης[6] (replay attacks). Η χρήση χρονοσήμανσης ή η χρήση του nonce συνήθως θεωρούνται επαρκείς για την αντιμετώπιση επιθέσεων επανάληψης. Ωστόσο, από την μία πλευρά, τα ρολόγια πραγματικού χρόνου στους περισσότερους αισθητήρες χαμηλής ισχύος έχουν κάποια εγγενή ηλεκτρική τάση που δεν τους επιτρέπει να συγχρονιστούν με επαρκή ακρίβεια στο πρωτόκολλο ελέγχου ταυτότητας. Από την άλλη πλευρά καθώς αυξάνεται το εύρος ζώνης του δικτύου απαιτείται λιγότερος χρόνος για την μετάδοση των μηνυμάτων σε αυτά τα πρωτόκολλα και σχήματα. Οι δύο αυτοί παράγοντες κάνουν τις ευκαιριακές επιθέσεις τύπου επανάληψης ιδιαίτερα δυνατές. Έχει προταθεί η δημιουργία μεθόδων που συνδυάζουν την χρήση χρονοσήμανσης και την χρήση του nonce μία μόνο φορά. Αυτές οι μέθοδοι έχουν αναπτυχθεί ως αντίμετρα στις επιθέσεις επανάληψης στους ασύρματους αισθητήρες ZigBee. Επίσης, έχουν προταθεί υλοποιήσεις βασιζόμενες στο υλικό για να εξασφαλίσουν την μοναδική σημασιολογία των μηνυμάτων. Αυτές οι υλοποιήσεις είναι αντίμετρα στις επιθέσεις τύπου επανάληψης, με βάση τους περιορισμούς για επικοινωνία σε πραγματικό χρόνο σε ένα παραγωγικό περιβάλλον, χωρίς να υπάρχει κανένας συμβιβασμός σε θέματα απόδοσης.

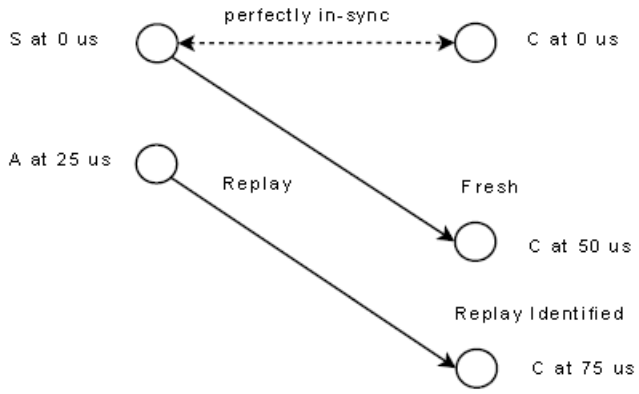
Η διαφορά στο ρολόι μεταξύ μιας μεταδιδόμενης ασύρματης συσκευής και μιας συσκευής λήψης είναι ένα κοινό πρόβλημα στα ασύρματα δίκτυα. Για χαμηλής ισχύος ασύρματες συσκευές, όπως είναι οι αισθητήρες ZigBee που χρησιμοποιούνται στο ασύρματο δίκτυο, το πρόβλημα μεγεθύνεται ακόμη περισσότερο από τη γήρανση του κρυστάλλου (το οποίο είναι το ουσιαστικό μέρος του κυκλώματος του ρολογιού πραγματικού χρόνου (RTC)), την διακύμανση της θερμοκρασίας του περιβάλλοντος, την χωρητικότητα των αδέσποτων φορτίων, κλπ. Για παράδειγμα, σε έναν τυπικό RTC ταλαντωτή των 32,768 kHz αυτή η διαφορά στο ρολόι μπορεί να είναι περισσότερη από 20 ppm, η οποία ανέρχεται σε τουλάχιστον 1,7 δευτερόλεπτα ανά ημέρα. Από την μία πλευρά, όταν ο χρόνος μετάδοσης ενός μηνύματος από άκρο σε άκρο μικραίνει εξαιτίας των νέων τεχνολογιών για τα ασύρματα δίκτυα, η ακρίβεια συγχρονισμού στο δίκτυο πρέπει να είναι αυστηρή .Αυτό συμβαίνει γιατί η χρονοσήμανση θα ήταν πολύ λιγότερο αποτελεσματική όταν η ακρίβεια του συγχρονισμού βρίσκεται κοντά στο τέλος της μετάδοσης του μηνύματος από άκρο σε άκρο. Από την άλλη πλευρά, λόγω της διακύμανσης του ρολογιού ο συγχρονισμός του δικτύου πρέπει να εκτελείται περιοδικά, αλλά λόγω του περιοδικού συγχρονισμού του δικτύου ο μηχανισμός ο οποίος χρησιμοποιεί χρονοσημάνσεις όπως τα nonce θα παραβιάσει την μοναδικότητα των σημασιολογιών. Επιπλέον, μπορεί να μην είναι σε θέση να παρέχουν επαρκείς εγγυήσεις σχετικά με την «φρεσκάδα» των μηνυμάτων. Αυτό προκαλείται από το γεγονός ότι κατά την προέλευση των μηνυμάτων ο χρόνος δεν είναι μια μονότονη συνάρτηση.

Το παράδειγμα στην εικόνα 6 δείχνει ένα επαναληπτικό μήνυμα ενός επιτιθέμενου που έχει αναγνωριστεί σωστά ως «μπαγιάτικο», όταν ο συλλέκτης και ο αισθητήρας είναι τέλεια συγχρονισμένοι. Στην εικόνα 6 το S αντιπροσωπεύει έναν αισθητήρα, το A αντιπροσωπεύει έναν αντίπαλο και το C αντιπροσωπεύει τον συλλέκτη. Σε αυτό το παράδειγμα υποτίθεται ότι η από άκρο σε άκρο καθυστέρηση ενός μηνύματος από το S στο C είναι 50 μs και ο C γνωρίζει ότι η από άκρο σε άκρο καθυστέρηση είναι 50 μs. Η καθυστέρηση των 50 μs μπορεί να οφείλεται στην καθυστέρηση των κυκλωμάτων των πομποδεκτών, ή και στην καθυστέρηση του buffering στους κόμβους της διαδρομής μετάδοσης μεταξύ άλλων. Όπως φαίνεται στην εικόνα 6 το μήνυμα μεταδίδεται από τον S την χρονική στιγμή 0 μs και έχει χρονοσήμανση 0 μs. Το μήνυμα φτάνει στο C την χρονική στιγμή 50 μs. Από την στιγμή που η χρονοσήμανση των 0 μs μαζί με την επιπλέον καθυστέρηση των 50μs δεν είναι μικρότερη από την τρέχουσα ώρα στο C, το C δηλώνει το μήνυμα από τον C ως «φρέσκο».

Την χρονική στιγμή 25μs ο A εγκαινιάζει μια επαναληπτική επίθεση στέλνοντας μηνύματα έχοντας κρυφακούσει τον S. Αυτά τα μηνύματα έχουν χρονοσήμανση 0 μs. Ας υποθέσουμε ότι η καθυστέρηση ενός μηνύματος από άκρο σε άκρο από τον A στο C είναι επίσης 50μs, δεδομένου ότι ο A πρέπει να είναι κοντά στον Sπροκειμένου να κρυφακούσει /

[6] Η επίθεση επανάληψης είναι μια μορφή δικτυακής επίθεσης κατά την οποία μια έγκυρη μετάδοση δεδομένων κακόβουλα ή ψευδώς επαναλαμβάνεται ή καθυστερεί.

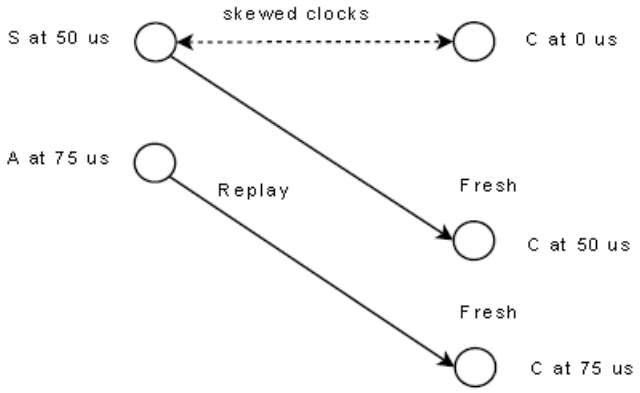
παρακολουθήσει τα μηνύματα από τον S. Στην συνέχεια το επαναληπτικό μήνυμα φτάνει στον Cτην χρονική στιγμή 75μs. Η χρονοσήμανση είναι 0μs και μαζί με την καθυστέρηση των 50μs είναι μικρότερη από την τρέχουσα ώρα στον C, δηλαδή το επαναληπτικό μήνυμα αναμένεται να φτάσει την χρονική στιγμή 50μs, αλλά η τρέχουσα χρονική στιγμή είναι 75μs. Αυτό έχει σαν αποτέλεσμα ο C να δηλώσει το μήνυμα ως «μπαγιάτικο». Συνεπώς, η επαναληπτική επίθεση αποτυγχάνει.



Εικόνα 6, Αποτυχημένη επαναληπτική επίθεση σε ένα τέλεια συγχρονισμένο δίκτυο [18]

Η εικόνα 7 παρουσιάζει ένα παράδειγμα όπου ένας αντίπαλος εκμεταλλεύεται την διαφορά του ρολογιού. Στο εικονιζόμενο παράδειγμα ο επιτιθέμενος ξεκινάει μια αποτελεσματική επαναληπτική επίθεση όταν το ρολόι του αισθητήρα S υπολείπεται του ρολογιού του συλλέκτη C κατά 50 μs. Όπως φαίνεται στην εικόνα 7 ένα μήνυμα μεταδίδεται από τον S την χρονική στιγμή 50 μs (σε σχέση με το ρολόι του S) και συνεπώς έχει χρονοσήμανση 50 μs. Το μήνυμα φτάνει στον C την χρονική στιγμή 50 μs (σε σχέση με το ρολόι του C). Δεδομένου ότι η χρονική σήμανση των 50 μs μαζί με την καθυστέρηση των 50 μs δεν είναι μικρότερη από την τρέχουσα ώρα του C, ο C δηλώνει το μήνυμα από τον S ως «φρέσκο».

Την χρονική στιγμή 75 μs (σε σχέση με το ρολόι του S) ο A εγκαινιάζει μια επαναληπτική επίθεση στέλνοντας μηνύματα έχοντας κρυφακούσει τον S. Αυτά τα μηνύματα έχουν χρονοσήμανση 50μs. Τότε το επαναληπτικό μήνυμα φτάνει στον C την χρονική στιγμή 75 μs(σε σχέση με το ρολόι του C). Δεδομένου ότι η χρονική σήμανση των 50 μs μαζί με την καθυστέρηση των 50 μs δεν είναι μικρότερη από την τρέχουσα ώρα του C, ο C δηλώνει το επαναληπτικό μήνυμα ως «φρέσκο». Συνεπώς, η επαναληπτική επίθεση είναι επιτυγχάνει.



Εικόνα 7, Επιτυχημένη επίθεση σε ένα ασυγχρόνιστο δίκτυο [18]

Είναι γνωστό ότι η ιδανική περίπτωση για να εξασφαλιστεί η μοναδικότητα των σημασιολογιών είναι η χρήση μιας αμιγώς τυχαίας ακολουθίας bit ως nonce. Ο πρακτικός

συμβιβασμός είναι να χρησιμοποιήσετε μια ψευδό τυχαία ακολουθία bit για nonce. Ωστόσο, είναι πρακτικά αδύνατο να απαιτήσει κάποιος από έναν χαμηλής ισχύος δέκτη να ελέγξει για nonce σε πραγματικό χρόνο για την εκπλήρωση αυτής της σημασιολογίας, ειδικά σε σύγκριση με όλα τα χρησιμοποιούμενα nonceσε ένα μεγάλο έξυπνο δίκτυο. Είναι δυνατό να εξασφαλιστεί η μοναδικότητα των σημασιολογιών σε έναν δέκτη εάν συνδυάσουμε την χρονοσήμανση και nonce χρησιμοποιώντας μια ψευδό τυχαία ακολουθία bitστον δημιουργό του μηνύματος. Δεδομένου ότι ο δημιουργός του μηνύματος μπορεί να δημιουργήσει με εύκολο τρόπο έναν ψευδό τυχαίο αριθμό με επαρκή αριθμό bits, μια σύγκρουση nonceμεταξύ δύο περιπτώσεων / παρουσιών είναι εξαιρετικά απίθανο να συμβεί στην πηγή του μηνύματος. Για τον λόγο αυτό επικεντρωνόμαστε στην μοναδικότητα των σημασιολογιών στην πλευρά του αποδέκτη του μηνύματος [18].

4. ΑΥΤΟΜΑΤΟΠΟΙΗΜΕΝΗ ΔΙΑΝΟΜΗ ΦΟΡΤΙΟΥ

4.1. ΟΡΙΣΜΟΣ

Για τους περισσότερους που ασχολούνται με την βιομηχανία της ηλεκτρικής ενέργειας, η διανομή φορτίου θεωρείται το άγιο δισκοπότηρο. Σε αντίθεση με την μεταφορά φορτίου και την παραγωγή ηλεκτρικής ενέργειας η διανομή φορτίου δεν μπορεί να έχει επικαλύψεις και είναι το μέρος του δικτύου στο οποίο συμβαίνουν διακοπές. Π.χ. διακοπές ηλεκτρικού ρεύματος μπορεί να προκύψουν από κομμένα δένδρα μέχρι και για καιρικά φαινόμενα. Υπάρχουν κάποιοι πελάτες που έχουν εφεδρικές πηγές ηλεκτρικής ενέργειας, όπως τα νοσοκομεία ή μεγάλοι εμπορικοί πελάτες, ωστόσο στην πλειονότητα των πελατών οποιοδήποτε πρόβλημα στην διανομή φορτίου τους αφήνει χωρίς ηλεκτρική ενέργεια. Επειδή η ηλεκτρική ενέργεια είναι κοινωνικό αγαθό πρέπει να είναι διαθέσιμη αδιάλειπτα και στο ποιο απομακρυσμένο μέρος. Αυτό όμως πολλές φορές έχει μεγάλο κόστος που επιβαρύνει την εταιρεία κοινής ωφέλειας και το οποίο δεν μπορεί να αποσβεστεί στην πλειονότητα των περιπτώσεων. Επιπλέον, πρέπει να δημιουργηθεί κατάλληλα το δίκτυο και ειδικότερα η διανομή φορτίου, έτσι ώστε να υπάρχει παντού επάρκεια φορτίου και να αντιμετωπίζονται όλες οι προβληματικές καταστάσεις που μπορεί να προκύψουν.

Ο πρωταρχικός σκοπός της διανομής φορτίου είναι η παράδοση αξιόπιστης ηλεκτρικής ενέργειας σε όλες τις εγκαταστάσεις κάθε χρονική στιγμή. Η εγκατάσταση ή η βελτίωση της υπάρχουσας υποδομής σημαίνει ότι οι πελάτες μπορεί να μείνουν για κάποιο χρονικό διάστημα χωρίς ηλεκτρική ενέργεια. Επίσης, οι πελάτες μπορεί να μείνουν χωρίς ηλεκτρική ενέργεια και κατά την διάρκεια αποκατάστασης των βλαβών. Στο έξυπνο δίκτυο η εγκατάσταση ευφυΐας στην διανομή φορτίου δεν αποσκοπεί μόνο στην αναφορά βλαβών και στην παρακολούθηση του δικτύου, αλλά και στην ικανότητα του δικτύου να μπορεί να αντιμετωπίζει προβλήματα και καταστάσεις έκτακτης ανάγκης. Εξελιγμένες εφαρμογές θα μπορούν να λειτουργούν σε συνδυασμό με τους υποσταθμούς και την μεταφορά φορτίου, έτσι ώστε να παρακολουθούν το ηλεκτρικό δίκτυο, να αλλάζουν τις ρυθμίσεις του και να μπορούν να διακόπτουν την παροχή ρεύματος στην περίπτωση σοβαρών διαταραχών.

Οι εφαρμογές που βρίσκονται κοντύτερα στις άκρες του δικτύου και στις ποιο ευαίσθητες περιοχές του, συνήθως τρέχουν σε δυνατές πλατφόρμες με εφεδρικές δυνατότητες λειτουργίας και με ενσωματωμένα εξελιγμένα συστήματα ελέγχου ασφάλειας. Σε πολλές περιπτώσεις προσφέρουν τον ιδανικότερο συνδυασμό αποτελεσματικότητας, αποδοτικότητας και ασφάλειας. Ωστόσο, οτιδήποτε μπορεί να πάρει στραβά οποιαδήποτε χρονική στιγμή. Χαρακτηριστικό παράδειγμα αποτελεί η AMI όπου ο εξελιγμένος αυτοματισμός και ο κεντρικός έλεγχος είναι ευαίσθητος σε ανακριβή δεδομένα από αναξιόπιστους χρήστες, γιατί μπορούν να δημιουργήσουν ζημιά στο σύστημα όταν εντοπιστεί μία ευπάθεια σε αυτό. Επιπλέον, ο τοπικός έλεγχος (σε αναντιστοιχία με την AMI), όπως στους έξυπνους μετρητές, δημιουργεί πολλά πιθανά σημεία εισόδου στους επιτιθέμενους, τα οποία μπορούν να εντοπίσουν και να εκμεταλλευτούν. Όλα αυτά τα παραπάνω σημαίνουν ότι οποιαδήποτε λύση επιλεγεί για την ασφάλεια της αυτοματοποιημένης διανομής φορτίου πρέπει να υπολογίσει πολύ σοβαρά τον αντίκτυπο που σχετίζεται με τις διαδικασίες που επιτελεί η αυτοματοποιημένη διανομή φορτίου, καθώς επίσης και με τις πιθανές συνέπειες που μπορεί να προκύψουν [24].

4.2. ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΗΛΕΚΤΡΙΚΟΥ ΔΙΚΤΥΟΥ

Το προτεινόμενο μοντέλο από το NIST για την αρχιτεκτονική του έξυπνου δικτύου περιλαμβάνει έξι κύριους τομείς, όπως αυτοί αναπαρίστανται στην εικόνα 8. Στην αυτοματοποιημένη διανομή φορτίου εμπλέκονται κατά κύριο λόγο οι τομείς του συστήματος και του δικτύου.

Εικόνα 8, Προτεινόμενη αρχιτεκτονική του έξυπνου δικτύου από το NIST [4]

Τα κύρια συστατικά του ηλεκτρικού συστήματος στο έξυπνο δίκτυο είναι τα ακόλουθα:

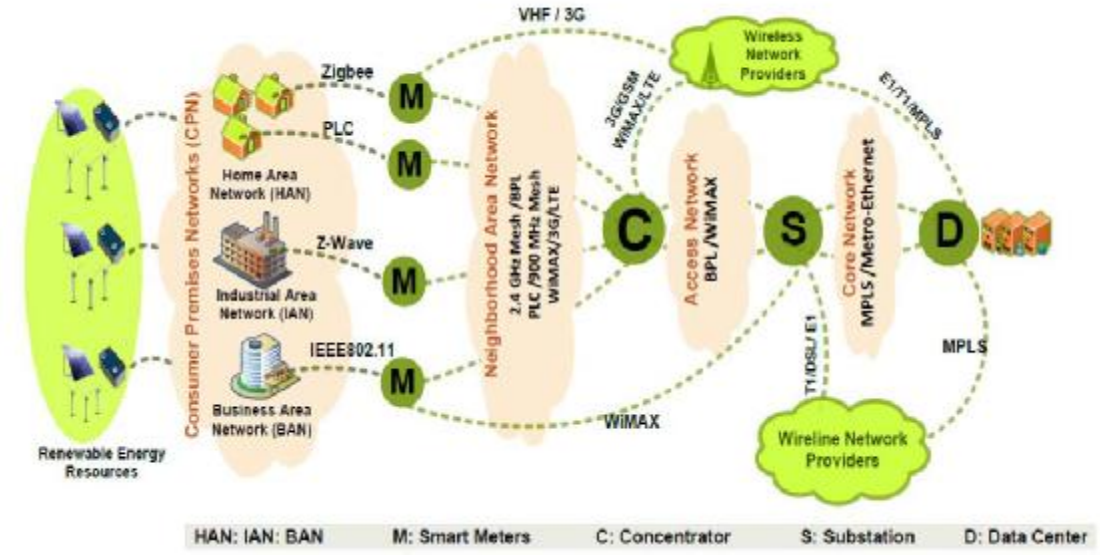
- Ηλεκτρικές οικιακές συσκευές,
- Ανανεώσιμες πηγές ενέργειας,
- Έξυπνοι μετρητές,
- Κέντρο λειτουργίας και
- Πάροχοι υπηρεσιών.

Οι ηλεκτρικές οικιακές συσκευές (έξυπνες και παραδοσιακές) είναι σε θέση να επικοινωνούν με έξυπνους μετρητές μέσω ενός HAN. Με αυτό το τρόπο διευκολύνεται η αποτελεσματική διαχείριση της ενέργειας που καταναλώνεται στις οικιακές συσκευές. Υπάρχει η δυνατότητα με την χρήση ανανεώσιμων πηγών ενέργειας (κατά βάση ηλιακή και αιολική) να μπορούν να τροφοδοτούνται με ηλεκτρική ενέργεια οι οικιακές συσκευές. Εάν υπάρχει περίσσεια ενέργειας από τις ανανεώσιμες πηγές ενέργειας, όταν καταναλώνεται λιγότερη από ότι παράγεται, τότε αυτή η ενέργεια θα διανέμεται στο ηλεκτρικό δίκτυο. Το κέντρο λειτουργίας αλληλεπιδρά με τους έξυπνους μετρητές για να ρυθμίζει την κατανάλωση ηλεκτρικής ενέργειας. Επίσης, στέλνει οδηγίες σχετικά με την κατανάλωση ηλεκτρικής ενέργειας στους έξυπνους μετρητές και συλλέγει υπό-ωριαίες αναφορές για την χρήση ηλεκτρικής ενέργειας. Χρησιμοποιώντας τεχνολογία GPRS το κέντρο λειτουργίας μπορεί να λαμβάνει και να στέλνει κοινοποιήσεις λαθών και εκτάκτων αναγκών. Οι πάροχοι υπηρεσιών αλληλεπιδρούν με εσωτερικές συσκευές μέσω μηνυμάτων που αναμεταδίδονται από τον έξυπνο μετρητή. Για τη δημιουργία αυτής της αλληλεπίδρασης οι πάροχοι υπηρεσιών θα πρέπει να εγγραφούν στο ηλεκτρικό δίκτυο και να αποκτήσουν ψηφιακά πιστοποιητικά για την ταυτότητά τους καθώς και δημόσια κλειδιά. Τα πιστοποιητικά χρησιμοποιούνται στη συνέχεια για να διευκολύνουν την ασφαλή επικοινωνία με τους χρήστες.

Το έξυπνο δίκτυο περιλαμβάνει δύο είδη επικοινωνίας: τα οικιακά δίκτυα (HAN) και τα δίκτυα ευρείας περιοχής (WAN). Σε ένα δίκτυο HAN συνδέονται οι έξυπνες οικιακές ηλεκτρικές συσκευές με τον έξυπνο μετρητή. Η δικτύωση των συσκευών στο HAN μπορεί να γίνει είτε χρησιμοποιώντας ZigBee είτε με ενσύρματη ή ασύρματη σύνδεση Ethernet ή Bluetooth. Από την άλλη πλευρά το WAN είναι ένα μεγαλύτερο δίκτυο που συνδέει τους έξυπνους μετρητές, τους παρόχους υπηρεσιών και την ηλεκτρική εταιρεία. Το WAN μπορεί να επικοινωνήσει χρησιμοποιώντας WiMAX, 3G/GSM/LTEή οπτικές ίνες.

Οι έξυπνοι μετρητές λειτουργούν ως πύλες μεταξύ των οικιακών ηλεκτρικών συσκευών και των εξωτερικών μερών για να παρέχουν την απαιτούμενη πληροφορία. Η ηλεκτρική εταιρεία διαχειρίζεται την διανομή φορτίου εντός του έξυπνου δικτύου, συλλέγει αναφορές υπό-ωριαίας κατανάλωσης ηλεκτρικής ενέργειας και στέλνει ειδοποιήσεις στους έξυπνους

μετρητές όποτε απαιτείται. Ο έξυπνος μετρητής λαμβάνει μηνύματα από τις συσκευές που βρίσκονται στο HAN και τα στέλνει στον κατάλληλο πάροχο υπηρεσιών. Τα HAN χρησιμοποιούνται σε κατοικίες, δίκτυα επιχειρήσεων (BAN) και βιομηχανικά δίκτυα (IAN). Στην εικόνα 9 απεικονίζεται η αρχιτεκτονική που μόλις περιγράψαμε [4], [5], [6], [8] & [14].

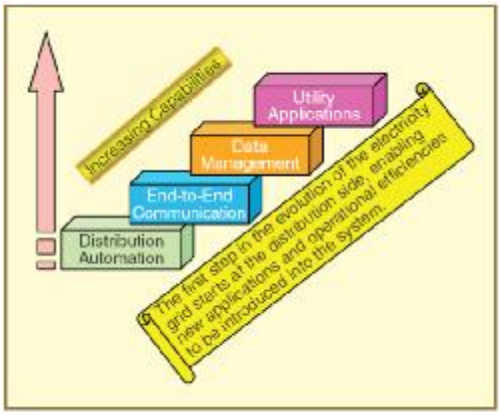


Εικόνα 9, Βασική αρχιτεκτονική του δικτύου [4]

4.3. ΑΥΤΟΜΑΤΟΠΟΙΗΣΗ ΔΙΑΝΟΜΗΣ

Λόγω του μεγέθους, της πολυπλοκότητας και του κόστους ο μετασχηματισμός του υπάρχοντος ηλεκτρικού δικτύου σε ένα έξυπνο δίκτυο θα πρέπει να γίνει σε διάφορα στάδια με την πάροδο του χρόνου. Δεδομένου ότι σχεδόν το 90% του συνόλου των διακοπών ρεύματος και οι διαταραχές του έχουν τις ρίζες τους στο δίκτυο διανομής, αυτή η μετατροπή θα πρέπει να αρχίσει από το επίπεδο της διανομής. Τα συστήματα διανομής είναι υπεύθυνα για την μεταφορά ηλεκτρικής ενέργειας από το ηλεκτρικό δίκτυο υψηλής τάσης 100-800kV στους εμπορικούς, βιομηχανικούς και οικιακούς πελάτες. Οι γραμμές διανομής αποτελούνται από μέσης τάσης και χαμηλής τάσης κυκλώματα που κυμαίνονται από 35kV μέχρι 110V.

Ένα πρώτο βήμα για την μετατροπή θα είναι η ανάπτυξη και η εγκατάσταση σε ευρεία κλίμακα συστημάτων αυτοματισμού διανομής (DAS). Τα DAS έχουν την δυνατότητα να μετατρέπουν τις μακράς διάρκειας διακοπές ηλεκτρικού ρεύματος σε στιγμιαίες διακοπές, επιτρέποντας την ταχεία απομόνωση των βλαβών και την αποκατάσταση του δικτύου. Μέχρι στιγμής μόνο ένα μικρό ποσοστό των συστημάτων διανομής σε όλο τον κόσμο είναι εξοπλισμένα με τέτοιες δυνατότητες. Ακόμα και στην Βόρεια Αμερική που έχει ένα από τα ποιο προηγμένα συστήματα παραγωγής ενέργειας στον κόσμο, λιγότερο από το ένα τέταρτο του συστήματος διανομής είναι εξοπλισμένο με συστήματα πληροφοριών και επικοινωνιών, και μόνο περίπου 15% έως 20% του συστήματος σε επίπεδο τροφοδότη. Αυτό έχει σαν αποτέλεσμα πολλές επιχειρήσεις κοινής ωφέλειας να πιστεύουν ότι η αρχική επένδυση στην αυτοματοποίηση της διανομής θα τους παρέχει αυξημένες δυνατότητες με την πάροδο του χρόνου, όπως φαίνεται και στην εικόνα 10.



Εικόνα 10, Επιθυμητές δυνατότητες από εταιρείες κοινής ωφέλειας [26]

Τα συστήματα αυτοματισμού διανομής είναι εξοπλισμένα με συστήματα πληροφοριών και επικοινωνιών για να παρέχουν αδιάλειπτη υποστήριξη στους διεκπεραιωτές του συστήματος. Οι κοινές λειτουργίες που παρέχουν περιλαμβάνουν:

- Αυτόματη δημιουργία τομέων στους διαύλους
- Μεταγωγή, εγκατάσταση και αυτόματη δημιουργία τομέων στους τροφοδότες
- Ολοκληρωμένο έλεγχο στα volt / var
- Εξισορρόπηση φορτίου σε μετασχηματιστή υποσταθμού
- Εξισορρόπηση φορτίου στον τροφοδότη
- Απομακρυσμένες μετρήσεις
- Έλεγχος φόρτωσης δικτύου

Ο έλεγχος του DAS μπορεί να είναι είτε κεντρικός είτε αποκεντρωμένος. Σε κεντρικά συστήματα ελέγχου όλες οι λειτουργίες υπολογισμού και ελέγχου γίνονται σε μία κεντρική τοποθεσία, ενώ στα αποκεντρωμένα συστήματα αυτές οι λειτουργίες μπορούν να διασπαρθούν σε πολλές διαφορετικές θέσεις. Ο κεντρικός έλεγχος είναι πολύ ποιο εύκολο να υλοποιηθεί από τον αποκεντρωμένο, ωστόσο δεν είναι σε θέση να ανταποκρίνεται άμεσα σε ανεπιθύμητες ενέργειες που συμβαίνουν σε κεντρικά σημεία ελέγχου. Από την άλλη πλευρά ενώ ο αποκεντρωμένος έλεγχος μπορεί να ανταποκριθεί άμεσα σε ανεπιθύμητες ενέργειες, η έλλειψη πληροφοριών μπορεί να οδηγήσει σε λήψη αναξιόπιστων ή προκατειλημμένων αποφάσεων. Συνεπώς, απαιτείται μια έξυπνη μορφή αποκεντρωμένου ελέγχου που να μπορεί να ανταποκρίνεται στις ανεπιθύμητες ενέργειες και να οδηγεί στην λήψη αξιόπιστων και αμερόληπτων αποφάσεων [26].

4.4. ΚΑΤΑΝΕΜΗΜΕΝΟΣ ΕΞΥΠΝΟΣ ΕΛΕΓΧΟΣ ΔΙΑΝΟΜΗΣ

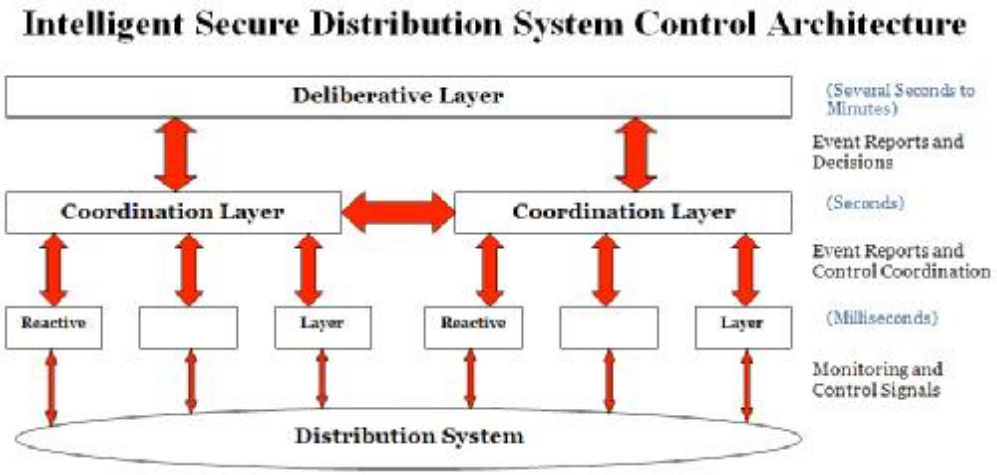
Όπως κάθε σύνθετο δυναμικό σύστημα υποδομών έτσι και το δίκτυο ηλεκτρικής ενέργειας έχει πολλά στρώματα και είναι ευάλωτο σε πολλούς διαφορετικούς τύπους διαταραχών. Ενώ είναι απαραίτητος ο «ισχυρός» κεντρικός έλεγχος για την αξιόπιστη λειτουργία του, αυτός απαιτείται να έχει τα ακόλουθα χαρακτηριστικά: πολλαπλές συνδέσεις υψηλού ρυθμού δεδομένων αμφίδρομης επικοινωνίας, μια ισχυρή κεντρική επεξεργαστική μονάδα και ένα πολύπλοκο κέντρο λειτουργίας. Αλλά όλα αυτά μπορούν να διαταραχθούν την ίδια χρονική στιγμή και όταν χρειάζονται περισσότερο (δηλαδή όταν το σύστημα ταλανίζεται από φυσικές καταστροφές, σκόπιμες επιθέσεις, ή ασυνήθιστα υψηλή ζήτηση). Σε περίπτωση βλαβών που συμβαίνουν σε διάφορες θέσεις σε ένα τέτοιο δίκτυο, όλο το δίκτυο κατακερματίζεται σε μικρές απομονωμένες νησίδες καθεμία από τις οποίες πρέπει στην συνέχεια να τα βγάλει πέρα μόνη της.

Για βαθύτερη και πολύ-επίπεδη προστασία απαιτείται κατανεμημένος έξυπνος έλεγχος διανομής. Αυτός ο έλεγχος θα μπορεί να ενεργοποιεί τα τμήματα του δικτύου, έτσι ώστε να παραμένουν λειτουργικά και να μπορούν να αλλάζουν αυτόματα τις ρυθμίσεις τους σε περιπτώσεις τοπικών απωλειών ή απειλών για αποτυχία. Με χρήση κατανεμημένης

εξυπνάδας και στοιχείων δικτύου που να μπορούν να λειτουργούν σαν ανεξάρτητοι πράκτορες, είναι δυνατόν οι απομονωμένες περιοχές να μπορούν να ανασυγκροτηθούν και να κάνουν αποτελεσματική χρήση των τοπικών πόρων ή ότι έχει απομείνει από αυτούς. Αυτές οι ενέργειες θα γίνονται με σύμφωνο τρόπο ως προς τις διεθνείς πρακτικές για την ελαχιστοποίηση των αρνητικών επιπτώσεων στο σύνολο του δικτύου. Τοπικοί ελεγκτές θα καθοδηγούν τις απομονωμένες περιοχές για να λειτουργούν ανεξάρτητα ενώ παράλληλα θα τις προετοιμάζουν για να ενταχθούν και πάλι στο συνολικό δίκτυο, χωρίς να δημιουργήσουν μη αποδεκτές τοπικές συνθήκες κατά την διάρκεια της μετάβασης ή μετά [26].

4.4.1. ΑΡΧΙΤΕΚΤΟΝΙΚΗ

Για την επίτευξη των επιθυμητών στόχων που αναφέρονται παραπάνω για τα συστήματα διανομής, υλοποιήθηκε ένας κατανεμημένος έξυπνος έλεγχος διανομής [27]. Το μοντέλο βασίστηκε στην αρχιτεκτονική του συστήματος ελέγχου SPID και αναπτύχθηκε από την EPRI / DOD Networks Complex Interactive / Systems Initiative (CIN / SI) για συστήματα με έξυπνη προστασία ευρείας περιοχής με δυνατότητες αναδιάρθρωσης. Χρησιμοποιώντας διάφορες κεντρικές έννοιες του μοντέλου SPID αναπτύχθηκε μια αρχιτεκτονική ειδικά για τα συστήματα διανομής. Στην εικόνα 11 παρουσιάζεται η προτεινόμενη αρχιτεκτονική ελέγχου.



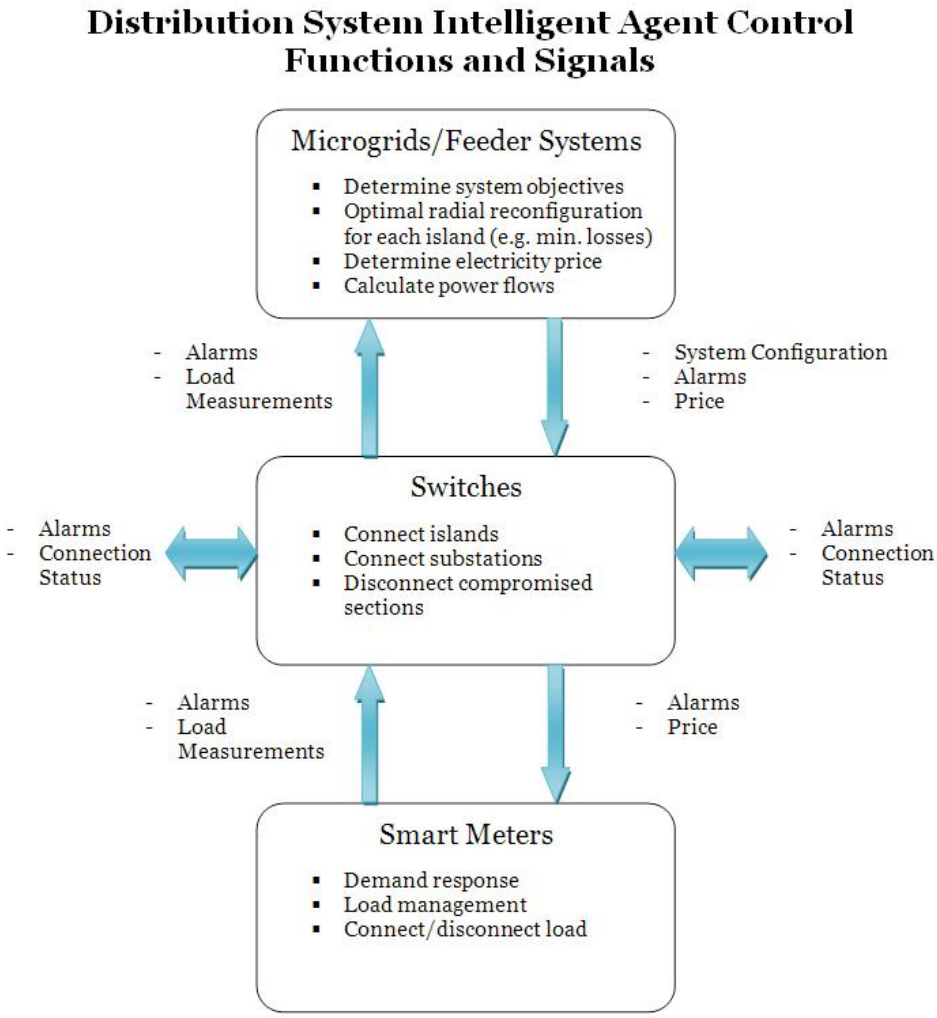
Εικόνα 11, Αρχιτεκτονική ασφαλούς κατανεμημένου έξυπνου ελέγχου διανομής [26]

Το παραπάνω μοντέλο χρησιμοποιεί τρία επίπεδα και αποτελείται από πολλαπλούς ανεξάρτητους ευφυείς πράκτορες. Αυτοί οι πράκτορες συλλέγουν και ανταλλάσουν μεταξύ τους πληροφορίες σε πραγματικό χρόνο, έτσι ώστε να παρέχουν συντονισμένη προστασία και βελτιστοποιημένη απόδοση του συστήματος. Η θέση των πρακτόρων σε κάθε επίπεδο της αρχιτεκτονικής ελέγχου και στις αντίστοιχες λειτουργίες ελέγχου παρατίθενται στον πίνακα που ακολουθεί. Επίσης, στην συνέχεια παρουσιάζεται και ένα διάγραμμα των λειτουργιών ελέγχου και των σημάτων (πίνακας 4).

Επίπεδο	Τοποθεσίες Πρακτόρων	Λειτουργίες Ελέγχου
Δραστικό (Reactive)	• Έξυπνοι Μετρητές • Υποσταθμοί	• Ανταπόκριση στην ζήτηση • Διαχείριση φορτίου • Σύνδεση / Αποσύνδεση φορτίου • Αποστολή σημάτων συναγερμού
Συντονισμού (Coordination)	• Μεταγωγοί (switches)	• Σύνδεση απομονωμένων περιοχών (νησίδες) • Σύνδεση υποσταθμών • Αποσύνδεση τμημάτων που έχουν εκτεθεί σε κίνδυνο • Αποστολή σημάτων συναγερμού
Συμβουλευτικό	• Μικρό-δίκτυα /	• Καθορισμός στόχων του συστήματος

(Deliberative)	Συστήματα τροφοδότησης	• Βέλτιστος επανακαθορισμός του δικτύου για κάθε απομονωμένη περιοχή (νησίδα), π.χ. για την μείωση των απωλειών • Καθορισμός της τιμής του ηλεκτρικού ρεύματος • Αποστολή σημάτων συναγερμού

Πίνακας 4, Λειτουργίες ευφυών πρακτόρων του συστήματος διανομής [26]



Εικόνα 12, Έλεγχος, λειτουργίες και σήματα των ευφυών πρακτόρων [26]

Η κατανεμημένη αρχιτεκτονική του συστήματος ελέγχου μπορεί στη συνέχεια να εφαρμοστεί σε συνδυασμό με ένα σύστημα πρόληψης εισβολών που βασίζεται σε πολλαπλούς πράκτορες, όπως αυτή που περιγράφεται, με σκοπό τον εντοπισμό και την πρόληψη των επιθέσεων στον κυβερνοχώρο μέσω του δικτύου. Μια προσέγγιση ασφάλειας στον κυβερνοχώρο που βασίζεται σε πολλαπλούς πράκτορες έχει πολλά πλεονεκτήματα τόσο για το δίκτυο όσο και για τα συστήματα διανομής. Τα πλεονεκτήματα αυτά περιλαμβάνουν: μειωμένο φορτίο δικτύου, αντιμετώπιση καθυστερήσεων του δικτύου, ανεξαρτησία πλατφορμών και ανοχή σε σφάλματα.

4.4.2. ΔΡΑΣΤΙΚΟ ΕΠΙΠΕΔΟ (REACTIVE LAYER)

Στο χαμηλότερο επίπεδο ελέγχου το δραστικό επίπεδο αποτελείται από πράκτορες που βρίσκονται σε κάθε έξυπνο μετρητή και υποσταθμό του συστήματος. Αυτοί οι πράκτορες συλλέγουν και ανταλλάσσουν πληροφορίες με πράκτορες που βρίσκονται σε μεταγωγούς

(switches) του γειτονικού επίπεδου συντονισμού. Ανταποκρίνονται σε εισερχόμενα μηνύματα τιμών και συναγερμών εκτελώντας λειτουργίες ανταπόκρισης στην ζήτηση και διαχείρισης φορτίου. Αυτές οι λειτουργίες μπορεί να περιλαμβάνουν αποβολή φορτίου ή μετατόπιση του φορτίου σε χαμηλότερη τιμή και σύνδεση ή αποσύνδεση φορτίου από το σύστημα διανομής για την αντιμετώπιση επιθέσεων ή φυσικών καταστροφών. Σε αντάλλαγμα, οι μετρήσεις φορτίου και τα σήματα συναγερμού στέλνονται προς τα πίσω μέχρι και στο επίπεδο συντονισμού. Για να αποτρέπονται οι πελάτες είτε από το να βλέπουν δεδομένα που αποστέλλονται μέσω του δικτύου από άλλους πελάτες είτε από το να αλλοιώνουν δεδομένα γειτονικών έξυπνων μετρητών, οι πράκτορες του δραστικού επιπέδου δεν επικοινωνούν απευθείας μεταξύ τους.

4.4.3. ΕΠΙΠΕΔΟ ΣΥΝΤΟΝΙΣΜΟΥ (COORDINATION LAYER)

Το επίπεδο συντονισμού αποτελείται από πολλούς πράκτορες που βρίσκονται σε κάθε σύστημα γραμμών / μεταγωγών του δικτύου διανομής. Οι πράκτορες αυτού του επιπέδου ανταλλάσσουν πληροφορίες μεταξύ τους. Επίσης, προωθούν τα μηνύματα που αποστέλλονται από τους πράκτορες που βρίσκονται στο δραστικό και συμβουλευτικό επίπεδο προς τους κατάλληλους προορισμούς. Παίρνουν αποφάσεις σχετικά με την κατάστασή τους και αναλαμβάνουν άμεσα δράση εάν εντοπίσουν βλάβες ή επιθέσεις στο σύστημα. Έχουν την ικανότητα να αναγνωρίσουν εάν έχουν απομονωθεί από το υπόλοιπο σύστημα, δηλαδή βρίσκονται σε κάποια νησίδα, και να χρησιμοποιήσουν όποιους τοπικούς πόρους έχουν στην διάθεσή τους. Επιπλέον, εφαρμόζουν βέλτιστες διαμορφώσεις του συστήματος, όπως καθορίζονται από τους πράκτορες του συμβουλευτικού επιπέδου.

4.4.4. ΣΥΜΒΟΥΛΕΥΤΙΚΟ ΕΠΙΠΕΔΟ (DELIBERATIVE LAYER)

Τέλος, το συμβουλευτικό επίπεδο αποτελείται από πράκτορες που βρίσκονται στο επίπεδο του μικρό-δικτύου / συστήματος τροφοδότησης. Αυτοί οι πράκτορες συλλέγουν και ανταλλάσσουν πληροφορίες με πράκτορες του γειτονικού επιπέδου συντονισμού και καθορίζουν τους γενικούς στόχους του συστήματος, όπως η αύξηση της αξιοπιστίας του δικτύου ή η ελαχιστοποίηση των απωλειών των γραμμών. Επίσης, μπορούν να καθορίσουν την βέλτιστη διαμόρφωση του δικτύου για κάθε νησίδα στο σύστημα τους, με βάση τους στόχους που έχουν επιλεγεί για το σύστημα. Όταν καθορίσουν την βέλτιστη διαμόρφωση στέλνουν σήματα ελέγχου στους πράκτορες του επιπέδου συντονισμού για να υλοποιήσουν τις αποφάσεις τους. Πραγματοποιούν ανάλυση στα συστήματά τους για να εξακριβώσουν εάν πληρούνται όλοι οι λειτουργικοί περιορισμοί και για να δουν το συνολικό φορτίο του συστήματος, έτσι ώστε να υποβάλλουν προσφορές σε πραγματικό χρόνο στις αγορές ηλεκτρικής ενέργειας. Τα κυκλώματα δικτύου χρησιμοποιούνται σε συστήματα τροφοδοσίας γιατί παρέχουν αρκετά πλεονεκτήματα. Αυτά περιλαμβάνουν:

- ευκολότερη προστασία από σφάλματα στο ρεύμα,
- μικρότερα σφάλματα ρεύματος στο μεγαλύτερο μέρος του κυκλώματος,
- ευκολότερος έλεγχος στην τάση,
- ευκολότερη πρόβλεψη και ο έλεγχος των ροών ενέργειας και
- χαμηλότερο κόστος.

5. ΑΥΤΟΜΑΤΟΠΟΙΗΜΕΝΗ ΜΕΤΑΦΟΡΑ ΦΟΡΤΙΟΥ

5.1. ΟΡΙΣΜΟΣ

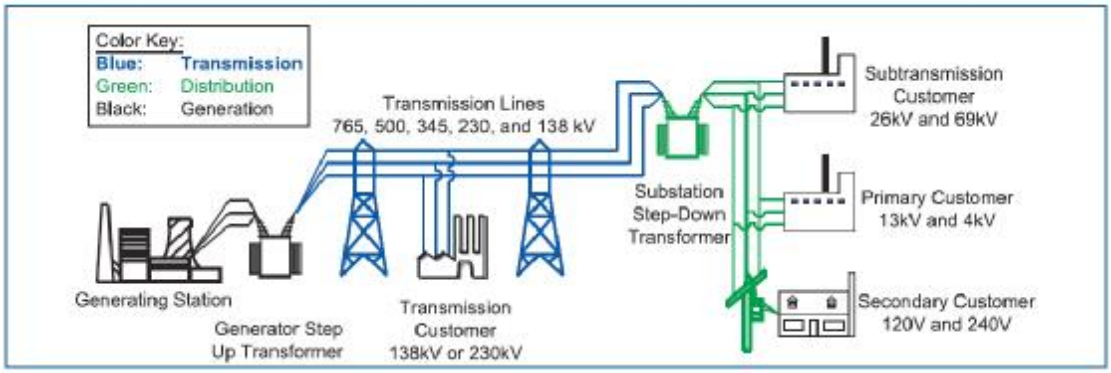
Το δίκτυο ηλεκτρικής ενέργειας μεταφέρει ενέργεια μέσω σειράς κόμβων ή αλλιώς υποσταθμών. Το σύνολο αυτών των υποσταθμών αποτελεί την Υποδομή Μεταφοράς Ηλεκτρικής Ενέργειας μέσω γραμμών υψηλής τάσης και σε όλο το μήκος και πλάτος μίας χώρας. Το χαρακτηριστικό είναι ότι το μεγαλύτερο μέρος του πληθυσμού που ζει σε πυκνοκατοικημένες πόλεις μπορεί μέσω αυτού του δικτύου να απολαμβάνει ενέργειας που παράγεται σε απομακρυσμένα μέρη από μη αισθητικά ευχάριστες πηγές. Αυτό δείχνει επίσης ότι η υποδομή μεταφοράς φορτίου που αξιοποιεί απομακρυσμένες ανανεώσιμες πηγές ενέργειας και μεταφέρει την όποια παραγωγή οπουδήποτε στη χώρα αντικαθιστώντας παραδοσιακές πηγές έχει τεράστια σημασία στην εξέλιξη του Έξυπνου Δικτύου Ενέργειας.

Από την άλλη η τοπική κρατική εξουσία και η ρυθμιστική πηγή ενέργειας καλούνται να διαχειριστούν τα κόστη από πλευράς, κατασκευής, λειτουργίας, επέκτασης του Δικτύου Μεταφοράς [24].

5.2. ΥΠΟΔΟΜΗ

Οι γραμμές μεταφοράς ηλεκτρικού φορτίου κατηγοριοποιούνται με βάση την τάση. Υψηλότερη η τάση, μεγαλύτερος ο όγκος του φορτίου που μπορεί να μεταφερθεί. Το δίκτυο μεταφοράς συνήθως λειτουργεί στο φάσμα υψηλής τάσης μεταξύ 115 και 800 KVolts:

- Υψηλή τάση: 33 έως 230 KVolts – χρησιμοποιείται για τη μεταφορά φορτίου σε μεγάλους καταναλωτές
- Πολύ υψηλή τάση: 230 έως 800 KVolts – χρησιμοποιείται για μεγάλη απόσταση, μεταφορά μεγάλου φορτίου ηλεκτρικής ενέργειας
- Πάρα πολύ υψηλή τάση: πάνω από 800 KVolts - χρησιμοποιείται για μεγάλη απόσταση, και μεταφορά αρκετά μεγάλου φορτίου ηλεκτρικής ενέργειας



Εικόνα 13, δίκτυο μεταφοράς ηλεκτρικού φορτίου [28]

5.3. ΤΕΧΝΟΛΟΓΙΚΗ ΥΠΟΔΟΜΗ

Η έξυπνη μεταφορά ηλεκτρικού φορτίου αφιερώνεται στην υλοποίηση οχτώ κύριων χαρακτηριστικών του σύγχρονου ηλεκτρικού δικτύου [10]:

- Αυτό-διόρθωση
- Παρότρυνση καταναλωτή
- Ξεπέρασμα εμποδίων και αντιδράσεων
- Ποιοτική ηλεκτρική ενέργεια
- Κατανεμημένη παραγωγή

- Αποθήκευση ενέργειας
- Δημιουργία νέας αγοράς
- Βελτιστοποίηση δικτύου

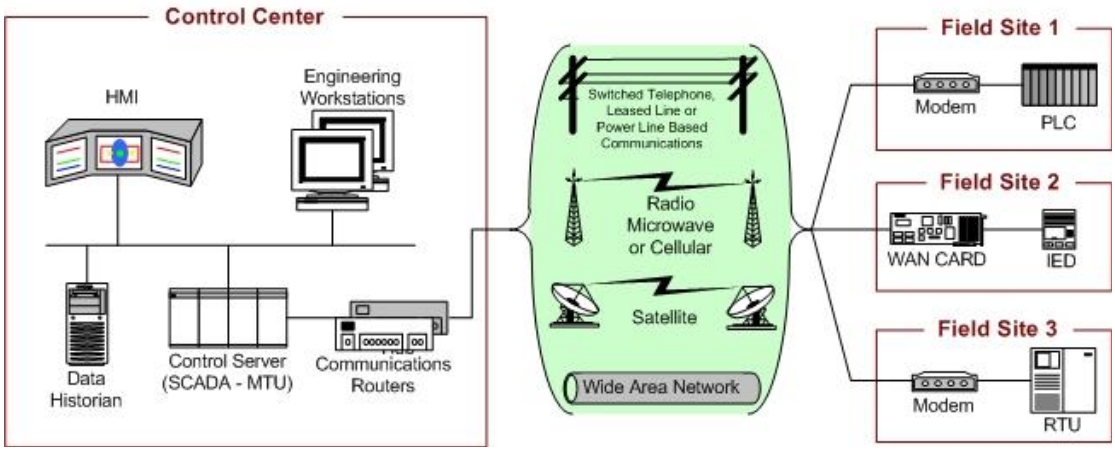
Η έξυπνη μεταφορά δικτύου εξελίσσεται τεχνολογικά για την ενσωμάτωση εργαλείων μοντελοποίησης, ανάλυσης και ελέγχου σε πραγματικό χρόνο

- Συμφόρηση στο υπάρχον σύστημα μεταφοράς εξασφαλίζοντας περισσότερη ευελιξία από τη παραγωγή ενέργειας ως τη μεταφορά του φορτίου
- Προγράμματα με περισσότερες λειτουργίες αυτοματισμού της διαχείρισης υποσταθμών
- Γεωγραφικά πληροφοριακά συστήματα για τη μεταφορά
- Συστήματα μέτρησης ευρείας κάλυψης
- Προστασία και έλεγχος με ιδιαίτερα χαρακτηριστικά
- Εργαλεία μοντελοποίησης, προσομοίωσης και γραφικής απεικόνισης
- Εφαρμογές ανά περιοχή για τοπική διαχείριση με εμπλουτισμένα χαρακτηριστικά

Ερμηνεύοντας τον τρόπο υλοποίησης των παραπάνω γίνεται αντιληπτό ότι η τεχνολογική τους βάση είναι εξαρτημένη στην Πληροφορική. Για παράδειγμα το σύστημα κεντρικού ελέγχου ελέγχει και παρακολουθεί όλα τα απομακρυσμένα σημεία του δικτύου μεταφοράς αποτελεί μία υπολογιστική εφαρμογή διαχείρισης ηλεκτρικού φορτίου, ενέργειας, ανταλλαγής δεδομένων και ελέγχου αυτόματης παραγωγής. Το σύστημα αυτό ονομάζεται Σύστημα Εποπτικού Ελέγχου και Απόκτησης Δεδομένων (SCADA) και αφιερώνεται τόσο στην παρακολούθηση (πχ για επείγουσες περιπτώσεις) όσο και στην καθημερινότητα.

Για την εκτέλεση των λειτουργιών ελέγχου και παρακολούθησης το SCADA βασίζεται στα παρακάτω υποσυστήματα:

- Σύστημα διαχείρισης ενέργειας (EMS)
- Σύστημα διαχείρισης ηλεκτρικού φορτίου (PMS)
- Σύστημα αυτόματου ελέγχου παραγωγής (AGC)
- Εφαρμογή ανταλλαγής δεδομένων σε πραγματικό χρόνο (RTDE)



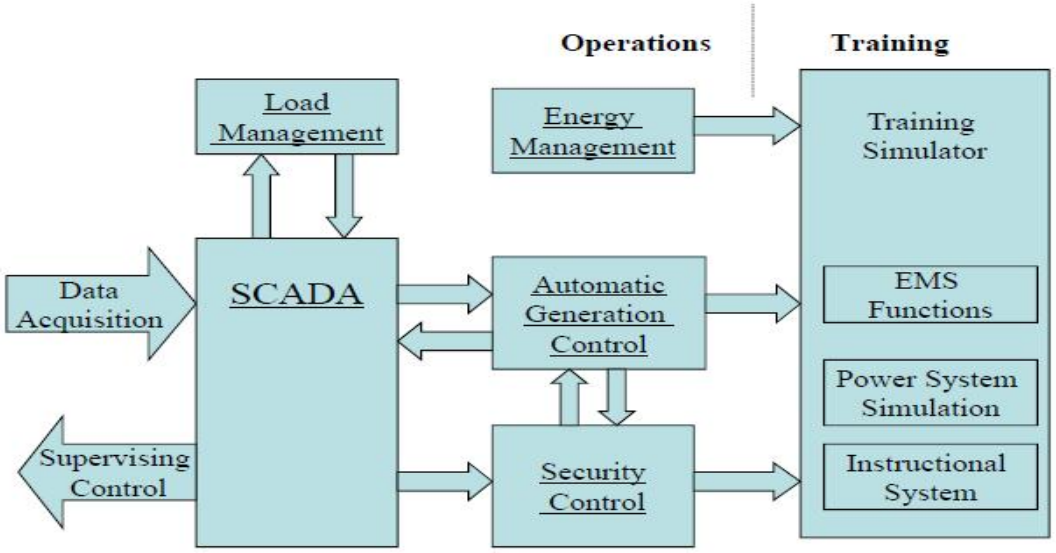
Εικόνα 14, υποσυστήματα και τερματικές συσκευές στην αρχιτεκτονική SCADA

Επιπλέον υποσυστήματα περιλαμβάνουν:

- SCADA κύρια τερματική μονάδα (MTU)
- SCADA επεξεργαστής δεδομένων
- SCADA κύρια βάση

5.3.1. ΣΥΣΤΗΜΑ ΔΙΑΧΕΙΡΙΣΗΣ ΕΝΕΡΓΕΙΑΣ

Το Σύστημα Διαχείρισης Ενέργειας (Energy Management System – ΣΔΕ) είναι μία σουίτα εφαρμογών που χρησιμοποιείται για την παρακολούθηση, έλεγχο και βελτιστοποίηση της απόδοσης του συστήματος παραγωγής και μεταφοράς. Οι ΣΔΕ εφαρμογές αξιοποιούν δεδομένα σε πραγματικό χρόνο όπως συχνότητα, παραγωγικά αποτελέσματα, ροές φορτίων ανά ζώνη, και την κατάσταση του ελεγκτή σε κάθε μονάδα παραγωγής για να καθορίσει τις επόμενες μεταβολές. Οι εφαρμογές αυτές περιλαμβάνουν τις παρακάτω:



Εικόνα 15, υποσυστήματα διαχείρισης ενέργειας στην αρχιτεκτονική SCADA [10]

- Πίνακας Απεικόνισης Δεδομένων: απεικονίζει τα δεδομένα της παραγωγής και τις προειδοποιήσεις που λαμβάνονται από την παραγωγή, μετάδοση και διανομή
- Αυτοματοποιημένος Έλεγχος Παραγωγής: υπολογίζει τις παραμέτρους που απαιτούνται για τη ρύθμιση της συχνότητας φόρτωσης, και την ανταλλαγή ρεύματος με γειτονικά συστήματα σε προγραμματισμένες χρονικές στιγμές.
- Εποπτικός Έλεγχος: εφαρμόζονται αλγόριθμοι ροής ρεύματος και λογικοί κανόνες που ορίζονται από τους χρήστες για τη βελτιστοποίηση των λειτουργιών του συστήματος. Για τους καταναλωτές βελτιστοποίηση σημαίνει λιγότερη κατανάλωση ρεύματος σε ώρα αιχμής, ή λιγότερες παρεμβάσεις για τον έλεγχο των λειτουργιών. Για τους παραγωγούς σημαίνει λιγότερο κόστος σε καύσιμα για την παραγωγή ρεύματος, καλύτερη δυνατή λειτουργία με το μικρότερο δυνατό κόστος και μέγιστη ασφάλεια του συστήματος.
- Διαχείριση Αποθεμάτων Ενέργειας: το υποσύστημα αυτό είναι υπεύθυνο για τη διαθεσιμότητα επαρκούς χωρητικότητας ρεύματος σε συγκεκριμένες χρονικές στιγμές για την αποφυγή απώλειας φορτίων σε περίπτωση έκτακτων γεγονότων. Έτσι οι κύριες λειτουργίες του υποσυστήματος περιλαμβάνουν:
  - Υπολογισμός απαιτήσεων για χωρητικότητα αποθεμάτων
  - Παρακολούθηση και διατήρηση αποθεμάτων ανά κατηγορία: απαιτούμενα από τη ρυθμιστική αρχή, αντιμετώπισης έκτακτων αναγκών, κατά ανάγκη.
- Προγραμματισμός ανταλλαγών ρεύματος: εξασφαλίζει τη δυνατότητα προγραμματισμού μεταφοράς ρεύματος από τη μία πλευρά ελέγχου στην άλλη ενώ ενσωματώνει λειτουργίες προγραμματισμού ενέργειας, διαχείρισης συναλλαγών, κοστολόγηση και αναφορά εξόδων. Αυτό επιτρέπει την εφαρμογή διαφορετικής τιμολογιακής πολιτικής ανά τοποθεσία. Τα παραπάνω είναι σημαντικά για την εμπορία του ηλεκτρικού ρεύματος (ρύθμιση ζήτησης – προσφοράς) με βάση συγκεκριμένα επιχειρησιακά σχέδια αλλά και διαχείριση κινδύνων (για παράδειγμα η ανταλλαγή ρεύματος σε πλήρη ισχύ μπορεί να προκαλέσει υπερφόρτωση).

5.3.2. SCADA – ΚΥΡΙΑ ΤΕΡΜΑΤΙΚΗ ΜΟΝΑΔΑ (MTU)

Η μονάδα αυτή αποτελεί τον κύριο εξυπηρετητή επεξεργασίας δεδομένων στο σύστημα SCADA. Βρίσκεται στο κέντρο ελέγχου του συστήματος και φιλοξενεί τις εφαρμογές Διαχείρισης Ενέργειας (EMS) και Διαχείρισης Ρεύματος (PMS). Επίσης διαχειρίζεται κάθε πληροφορία που εισέρχεται και εξέρχεται στην κύρια βάση του συστήματος καθώς επίσης παρέχει στους χρήστες κονσόλα εργαλείων και εντολών για να διαχειριστούν βασικά στοιχεία του δικτύου (μεταγωγείς, αποζεύκτες).

5.3.3. SCADA – ΠΡΟ-ΕΠΕΞΕΡΓΑΣΤΗΣ (FEP)

Ο επεξεργαστής αυτός έχει πολλαπλούς ρόλους καλύπτοντας τη βασική ανάγκη επεξεργασίας των δεδομένων που παράγονται κατά μήκος των λειτουργιών μεταφοράς και διανομής. Επιπλέον παρέχει λειτουργίες τερματικού εξυπηρετητή για τη πρόσβαση στη διεπαφή ενός απομακρυσμένου υπό-σταθμού. Ο FEP επεξεργαστής βρίσκεται συνήθως σε αποστρατικοποιημένη ζώνη (DMZ) με προς τα μέσα διασύνδεση προς τη κύρια τερματική μονάδα (MTU). Έτσι εγκαθιστώντας ένα συμβατικό firewall δικτύου υπολογιστών μπροστά από την MTU μονάδα διαχειρίζεται την πρόσβαση από και προς αυτό με σκοπό να απομονώσει τα δύο συστήματα (MTU και FEP). Αυτό είναι απαραίτητο καθώς υπάρχει ένας αριθμός από FEP επεξεργαστές οι οποίοι παρέχουν συγκέντρωση δεδομένων από διαφορετικά σημεία και ένα αριθμό υποσταθμούς.

5.3.4. ΥΠΟΣΤΑΘΜΟΙ ΜΕΤΑΦΟΡΑΣ

Οι υποσταθμοί χρησιμοποιούνται για την ένωση δύο ή περισσότερων γραμμών μετάδοσης. Ελέγχονται μέσω ευφυών ηλεκτρονικών συσκευών (intelligent electronic devices – IEDs) που υπάρχουν στους υποσταθμούς και επικοινωνούν με το κέντρο ελέγχου του ευρύτερου συστήματος. Η επικοινωνία με αυτές τις συσκευές γίνεται μέσω δικτύου: είτε με από άκρο σε άκρο διασύνδεση εναλλακτικών πρωτοκόλλων ή με τη χρήση τερματικών εξυπηρετητών.

PMUs (phasor measurement units) είναι μία κατηγορία ευφυών ηλεκτρονικών συσκευών που χρησιμοποιούνται στη λήψη μετρήσεων κατά μήκος του δικτύου. Οι μετρήσεις αυτές είναι πολύ χρήσιμες στην ασφάλεια του κυβερνοχώρου καθώς επιτρέπουν τη δημιουργία συνθηκών και προειδοποιήσεων που αξιοποιούνται στην υλοποίηση αυτόματων ελέγχων για την αποφυγή καταστροφών ή για τη βελτιστοποίηση της απόδοσης. Για παράδειγμα η διακοπή ρεύματος μπορεί να είναι το αποτέλεσμα μίας συνθήκης σφάλματος που έχει δημιουργηθεί από τις μετρήσεις σε ένα υποσταθμό.

Άλλες συσκευές – υποκατηγορίες των ευφυών ηλεκτρονικών συσκευών- περιλαμβάνουν ρελέ (relays) για τον έλεγχο των διακοπτών στους υποσταθμούς και ελεγκτές προγραμματιστικής λογικής (PLUs) οι οποίοι αυτοματοποιούν ηλεκτρομηχανικές διαδικασίες.

5.4. ΣΥΣΤΗΜΑ ΔΙΑΧΕΙΡΙΣΗΣ ΜΕΤΑΦΟΡΑΣ & ΑΣΦΑΛΕΙΑ ΜΕΤΑΦΟΡΑΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Η κυβερνο-ασφάλεια στο σύστημα μετάδοσης επικεντρώνεται κατά βάση σε χαρακτηριστικά που σχετίζονται με την διαθεσιμότητα όπως:

- Ικανότητα αυτό-θεράπευσης: αν επηρεαστεί η μεταφορά ενέργειας το σύστημα πρέπει να δράσει άμεσα
- Ποιότητα ρεύματος: υπάρχει άμεση συσχέτιση μεταξύ ποιότητας και επάρκειας ρεύματος. Υψηλότερη η επάρκεια, τότε υψηλότερη και η ποιότητα.
- Κατανεμημένη παραγωγή: αυξάνοντας τις πηγές ανανεώσιμων μορφών ενέργειας αυξάνεται και η πολυπλοκότητα του Έξυπνου Δικτύου αναζητώντας επιπλέον αξιοπιστία και αντοχή.
- Αποθήκευση ενέργειας: η διαθεσιμότητα αποθηκευμένης ενέργειας είναι ένας άλλος σημαντικός παράγοντας που ενεργοποιείται όταν η παραγωγή βρίσκεται για κάποιο λόγο εκτός στόχων

Επιπλέον υπάρχουν απαιτήσεις σχετικά με την ακεραιότητα του συστήματος με σκοπό την αποφυγή απειλών που θέτουν σε κίνδυνο τη λειτουργία του συστήματος [16] & [21].

5.4.1. ΚΥΒΕΡΝΟ ΑΣΦΑΛΕΙΑ ΣΤΟ ΚΕΝΤΡΙΚΟ ΣΥΣΤΗΜΑ ΕΛΕΓΧΟΥ

Το Κεντρικό Σύστημα Ελέγχου είναι απομονωμένο από το υπόλοιπο δίκτυο με τη χρήση Firewall. Αυτό δίνει τη δυνατότητα αποφυγής ελέγχων για την εύρεση ασφαλειών στο δίκτυο. Από την άλλη πλευρά μπορεί να υπάρχουν αδυναμίες που δεν έχουν εντοπιστεί εξαιτίας της παραπάνω απαίτησης. Το Firewall προστατεύει από μη εξουσιοδοτημένη πρόσβαση εφαρμόζοντας ένα σύνολο κανόνων που ελέγχουν την υποδομή. Από την άλλη τα εσωτερικά δίκτυα μπορεί να αποτελέσουν μία σημαντική απειλή. Για παράδειγμα η χρήση ανιχνευτή ευπαθειών μπορεί να καταστήσει το Firewall μη διαθέσιμο με αποτέλεσμα και το ηλεκτρικό δίκτυο να μην είναι διαθέσιμο.

Η αδυναμία παρακολούθησης διακυμάνσεων στο ρεύμα και η αδυναμία μέτρησης συχνότητας μπορεί να οδηγήσει σε κακή διαχείριση της ενέργειας και του δικτύου γενικότερα. Ειδικότερα οι λεγόμενες ADT απειλές διαρκούς επιχείρησης εφαρμόζουν τέτοιες μεθόδους εισβολής καλά οργανωμένες από εθνικές ή άλλες καλοπληρωμένες πηγές προκειμένου να αξιοποιήσουν τη παραμικρή αδυναμία του Firewall. Η πιθανότητα να συμβεί κάτι τέτοιο είναι χαμηλή γιατί δεν έχει προηγούμενο ωστόσο η επίδραση του θα είναι πολύ σημαντική. Αν επίσης λάβουμε υπόψη ότι ιδιωτικές εταιρίες που έχουν αναλάβει να τρέξουν τα συγκεκριμένα έργα δεν έχουν συγκεντρώσει τα απαραίτητα κεφάλαια τότε αυτό σημαίνει μεγαλύτερη ευπάθεια σε κυβερνο-απειλές λόγω φτωχότερης συντήρησης.

Ο Οργανισμός Ηλεκτρικής Αξιοπιστίας της Βόρειας Αμερικής (North American Electric Reliability Corporation – NERC) όρισε ένα αριθμό κριτηρίων με βάση τα οποία ένας πόρος θεωρείται κρίσιμος έτσι ώστε να είναι κατάλληλα διαχειρίσιμα από τα συστήματα κυβερνο-άμυνας.

- Το σύστημα ελέγχου ή το εφεδρικό σύστημα ελέγχου καθώς επίσης υποδομές σε κεντρικές και απομακρυσμένες εγκαταστάσεις που παρέχουν υπηρεσίες ελέγχου και παρακολούθησης, έλεγχο αυτόματης παραγωγής, μοντελοποίηση ηλεκτρικών δικτύων σε πραγματικό χρόνο θεωρούνται κρίσιμοι πόροι.
- Ένας υποσταθμός μεταφοράς ενέργειας που υποστηρίζει την αξιόπιστη λειτουργία του ηλεκτρικού δικτύου με τη βοήθεια κυβερνο-πόρων τότε θεωρείται κρίσιμων πόρων.
- Ένας παραγωγικός πόρος που είναι κρίσιμος στην αξιόπιστη λειτουργία του δικτύου είναι επίσης κρίσιμος.
- Πόροι που συμβάλλουν στην αποκατάσταση της λειτουργίας του δικτύου μετά από πτώση φορτίου πρέπει να αξιολογηθούν αν τα κυβερνο-συστήματα που περιέχονται σε αυτά είναι κρίσιμα.
- Συστήματα που ελέγχουν τον αυτόματο μετασχηματισμό φορτίων άνω των 300 megawatts ελέγχονται αν τα συστήματα ασφαλείας τους είναι κρίσιμα.
- Συστήματα ειδικής προστασίας (SPS) που συμβάλλουν στην αξιόπιστη λειτουργία του συστήματος και της ενεργοποίησης ενός σχήματος ενεργειών επίλυσης προβλημάτων.

Μία τεχνική ελέγχου της ακεραιότητας των δεδομένων στα παραπάνω συστήματα είναι η εφαρμογή του ελέγχου των δεδομένων που καλούνται να διαχειριστούν οι εκτελεστές εντολών στον πίνακα ελέγχου. Η λήψη παραπλανητικών ή εσφαλμένων παραμέτρων εισόδου θα οδηγήσει σε λαθεμένες εντολές προς εκτέλεσης με αρνητικές συνέπειες. Οι εκτελεστές των εντολών πρέπει να επαληθεύουν την πηγή των δεδομένων και να εξασφαλίζουν μηχανισμούς διασφάλισης ότι, για παράδειγμα, συναγερμοί θα αποστέλλονται με βάση πραγματικές συνθήκες.

5.4.2. ΑΣΦΑΛΕΙΑ ΥΠΟΣΤΑΘΜΩΝ ΜΕΤΑΔΟΣΗΣ

Οι υπολογιστές που διαχειρίζονται τις εφαρμογές και υπηρεσίες του υποσταθμού μετάδοσης πρέπει να ελεγχθούν για την ασφάλεια τους και να συμμορφωθούν σε συγκεκριμένες πολιτικές. Μέτρα εφαρμογής αυτών των πολιτικών περιλαμβάνουν:

- Προστασία από κακόβουλα προγράμματα
- Λογισμικό προστασίας από ιούς για συγκεκριμένη λίστα ιών
- Λογισμικό Παρακολούθησης Κατάστασης Ασφαλείας παρακολουθεί συμβάντα ασφαλείας που δεν έχουν προσδιοριστεί
- Παρακολούθηση απειλών στην ασφάλεια του δικτύου, μηχανισμούς ελέγχου των δικαιωμάτων πρόσβασης, προγραμμάτων προστασίας από ιούς, διαδικασία ελέγχου κώδικα για προγράμματα που εγκαθίστανται μέσα στην υποδομή, καταγραφή συμβάντων και ανταλλαγή συμβάντων με άλλα συστήματα για τον εντοπισμό απειλών.

Με λίγα λόγια το Έξυπνο Δίκτυο Ενέργειας έχει τις ίδιες απαιτήσεις με την Κυβερνο Άμυνα. Οι πληροφορίες για απειλές πρέπει να προσδιοριστούν, να αναλυθούν, και να χρησιμοποιηθούν για τη λήψη μέτρων. Έτσι η πρόκληση στα συστήματα διαχείρισης των υποσταθμών μεταφοράς ενέργειας είναι ο προσδιορισμός όλων των παραγόντων που μπορεί να αποτελέσουν απειλή και να ερμηνεύσουν κάτω από ποιες συνθήκες οι παράγοντες αυτοί ενεργοποιούνται. Η αντιμετώπιση αυτή απαιτεί διαχείριση αλλαγών (configuration management) και παρακολούθηση της επίδρασης των αλλαγών στα συστήματα για να οριστούν με ακρίβεια οι ανάγκες βελτίωσης των συστημάτων.

5.4.3. ΣΤΡΑΤΗΓΙΚΕΣ ΑΣΦΑΛΕΙΑΣ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ ΜΕΤΑΦΟΡΑΣ ΕΝΕΡΓΕΙΑΣ

Οι στρατηγικές ασφάλειας του συστήματος μεταφοράς ενέργειας είναι:

1. Εφαρμογή μηχανισμού ελέγχου αλλαγών, έγκριση αλλαγών πριν τη πραγματοποίηση τους και παρακολούθηση των αλλαγών στις όποιες παραμετροποιήσεις

   Για παράδειγμα καμία αλλαγή δεν μπορεί να πραγματοποιηθεί αν δεν συνοδεύεται από αριθμό εισιτηρίου που επικυρώνει την έγκριση των αρμόδιων τμημάτων για τις αλλαγές.

2. Εγκατάσταση, παρακολούθηση και αξιολόγηση ενός συστήματος ανίχνευσης εισβολών (Intrusion Detection System- IDS)

   Τα συστήματα ανίχνευσης εισβολών καταγράφουν μεγάλο όγκο δεδομένων για αυτό απαιτούνται επιπλέον εργαλεία φιλτραρίσματος όπως αυτό του τύπου της κίνησης.

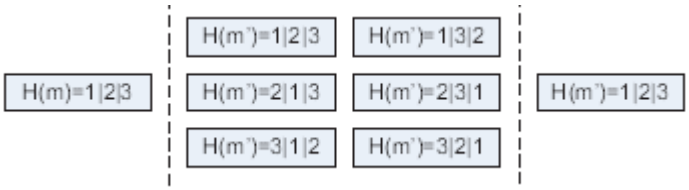
3. Επιπλέον ο έλεγχος φυσικής και λογικής πρόσβασης των χρηστών είναι αξιόπιστος μηχανισμός ελέγχου της πρόσβασης στο σύστημα ελέγχου του δικτύου.

   Οι μηχανισμοί αυτοί βοηθούν τους οργανισμούς και τους εργαζομένους να αντιληφθούν τη σπουδαιότητα του ελέγχου πρόσβασης. Ένας άλλος τρόπος είναι η εκπαίδευση και η υλοποίηση προτύπων κυβερνο ασφάλειας. Για παράδειγμα οι διαχειριστές των IT συστημάτων μπορεί να έχουν πρόσβαση στους υπολογιστές διαχείρισης του δικτύου αλλά δεν επιτρέπεται η επανεκκίνηση του υπολογιστή χωρίς την εξουσιοδότηση τρίτου προσώπου.

Ένας επιπλέον μηχανισμός κρυπτογράφησης των μηνυμάτων που αποστέλλονται σε πολλούς αποδέκτες (multicast) είναι η εφαρμογή υπογραφής στο μήνυμα (Li ,2011). Ο μηχανισμός αυτός ονομάζεται Υπογραφή Ορισμένης Διάρκειας (One Time Signature - ΥΟΔ) καθώς παρέχει στιγμιαία ταυτοποίηση χωρίς καθυστέρηση στην ενταμίευση μηνυμάτων και μπορεί να υποστεί ανεκτικά τη διαπραγμάτευση με ορισμένους από τους κόμβους οι οποίοι λαμβάνουν τα μηνύματα. Ο ΥΟΔ είναι ουσιαστικό παρεμφερής μηχανισμός κρυπτογράφησης του ιδιωτικού κλειδιού με την έννοια ότι ο αποστολέας χρησιμοποιεί ένα μυστικό κλειδί για να

κρυπτογραφήσει ένα μήνυμα και ο παραλήπτης χρησιμοποιεί ένα δημόσιο κλειδί για να αποκρυπτογραφήσει/επιβεβαιώσει τη γνησιότητα του μηνύματος. Ο ΥΟΔ είναι πολύ πιο αποδοτικός σε υπολογιστική ισχύ καθώς οι διαδικασίες υλοποίησης βασίζονται στην ροή των μηνυμάτων προς μία κατεύθυνση χωρίς επιπλέον σημεία ελέγχου.

Ένα αρχικό μειονέκτημα του ΥΟΔ ήταν το μέγεθος του (από μερικές εκατοντάδες σε μερικές χιλιάδες bytes). Ο Li (2011) πρότεινε μία εξέλιξη του που θεωρείται η πιο βελτιωμένη έκδοση του ΥΟΔ και ονομάζεται HORS.



Εικόνα 16,αλγόριθμος υπογραφής μηνύματος ορισμένης διάρκειας (ΥΟΔ)- επέκταση του αλγορίθμου με την ονομασία HORS [21]

- **Δημιουργία κλειδιού:** Δημιουργία t τυχαίων l-bit συμβολοσειρών (s1, s2, ..., st), οι οποίες σχηματίζουν το μυστικό κλειδί SK. Το δημόσιο κλειδί υπολογίζεται ως PK= (v1, v2, ..., vt), όπου vi= f(si) και f είναι συνάρτηση μονής κατεύθυνσης.
- **Δημιουργία υπογραφής:** Για την υπογραφή του μηνύματος m, θεωρούμε ότι h= H(m), όπου H είναι μία συνάρτηση κατακερματισμού. Το αποτέλεσμα h διασπάται σε k συμβολοσειρές h1, h2, ..., hk με $\log_2 t$ bits η κάθε μία. Το κάθε hj μεταφράζεται ως ένας ακέραιος ij. Η υπογραφή του m είναι τότε (si1 , si2 , ..., sik).
- **Επικύρωση υπογραφής:** Για την επικύρωση της υπογραφής (s′1, s′2, ..., s′k) που εφαρμόζεται στο μήνυμα m, υπολογίζεται h= H(m). Κατόπιν το αποτέλεσμα h διασπάται σε k συμβολοσειρές h1, h2, ..., hk των με $\log_2 t$ bits το καθένα. Το κάθε hj μεταφράζεται ως ένας ακέραιος ij και ελέγχεται αν η σχέση f(s′j) = vij είναι αληθής.

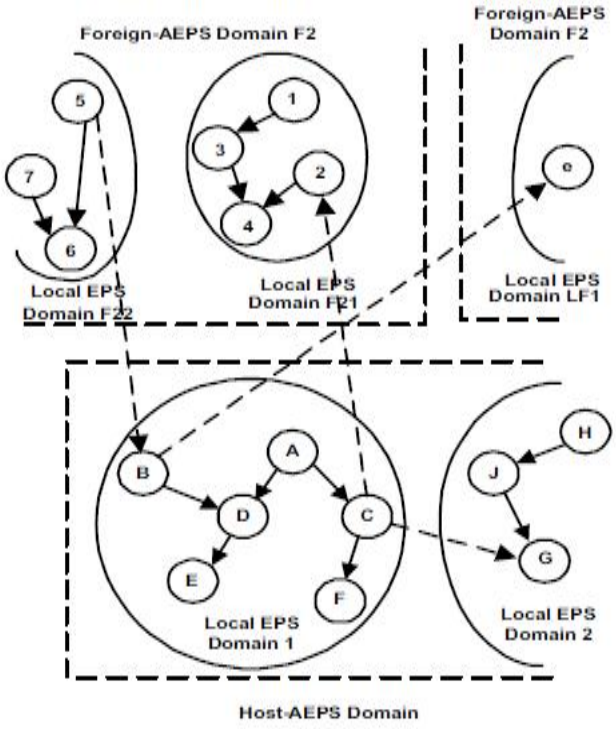
Ο αλγόριθμος αυτός γίνεται ακόμη πιο αποτελεσματικός αν τα k στοιχεία μίας υπογραφής οριστούν ως ένα πρότυπο ταξινομημένης ακολουθίας στην οποία η θέση του κάθε στοιχείου καθορίζει και τη διαδικασία επικύρωσης της υπογραφής. Έτσι από μία έγκυρη υπογραφή (s1, s2, ..., sk), αυτός που υποκλέπτει μπορεί να αντιγράψει μόνο μία ακολουθία υπογραφής και να τη ταιριάξει ακριβώς στο δικό του μήνυμα. Η πολυπλοκότητα για να το πετύχει αυξάνεται κατά k!. Επιπλέον ενώ στην αρχική έκδοση του HORS απαιτούνται 80 bits για να δημιουργηθεί ένας παράγοντας πολυπλοκότητας 2^{28}με k=13, t=1024. Η εξέλιξη του αλγορίθμου κατάφερε επιπλέον να μειώσει το μέγεθος του δημόσιου κλειδιού t συνεπώς μειώνει το κόστος της αποστολής και λήψης μηνυμάτων πολλαπλής εκπομπής. Στον ορισμό αυτό ορίζεται η σχέση C= $\frac{k(k+1)}{2d}l$ για να υπολογιστεί το υπολογιστικό κόστος μετάδοσης lbits σε κάθε μήνυμα ενώ d είναι μία τιμή μικρότερη k^2. Ο πίνακας 5 δείχνει πως διαμορφώνεται η τιμή C για διαφορετικές τιμές των παραμέτρων.

C	Min. Signing Cost	Signing Cost of Heuristic Solution	-	C	Min. Signing Cost	Signing Cost of Heuristic Solution
0	6.2×10^9	6.2×10^9		20	1152	1152
1	4.8×10^8	4.8×10^8		21	864	864
2	8.0×10^7	8.0×10^7		22, 23	576	576
3	2.2×10^7	2.2×10^7		24	532	532
4	7.3×10^6	7.3×10^6		25, 26	288	$432(C = 25)$, $288(C = 26)$
5	2.2×10^6	2.2×10^6		27	192	288
6	9.7×10^5	9.7×10^5		$28 \sim 30$	144	288
7	4.8×10^5	4.8×10^5		31	96	288
8	2.4×10^5	2.4×10^5		32, 33	72	$192(C = 3225)$, $96(C = 33)$
9	1.2×10^5	1.2×10^5		$34 \sim 37$	48	$96(C = 34, 35)$, $64(C = 36, 37)$
10	60480	60480		38	32	32
11	34560	34560		$39 \sim 41$	32	32
12	25920	25920		$42 \sim 45$	32	32
13	17280	17280		46, 47	32	32
14	8640	11520		$48 \sim 54$	8	$32(C = 48, 49)$, $16(C = 50 \sim 54)$
15	5760	5760		55	6	16
16	4320	4320		$56 \sim 65$	4	$16(C = 56 \sim 59)$, $8(C = 60 \sim 65)$]
17	2880	2880		$66 \sim 77$	2	$8(C = 66, 67)$, $4(C = 68 \sim 73)$, $2(C = 74 \sim 77)$
18	2304	2304		78	1	1
19	1440	1440				

Πίνακας 5, υπολογιστικό κόστος εύρεσης βέλτιστης λύσης κατά την εφαρμογή του αλγορίθμου HORS δοκιμάζοντας διαφορετικές τιμές C, και k=13 [21]

Επιπλέον απαιτούνται διαδικασίες ελέγχου και ταυτοποίησης των αιτημάτων εκτέλεσης εντολών προς ένα κύριο κόμβο του δικτύου ή άλλους γειτονικούς κόμβους. Για να επιτευχθεί αυτό ορίζονται συγκεκριμένοι κόμβοι με ιδιότητες από το πρότυπο AEPS (Assessment, Evaluation, Programming System). Το πρότυπο επιτρέπει την κατάτμηση του δικτύου σε επιμέρους τομείς και την αντίστοιχη κατανομή ρόλων και αρμοδιοτήτων ανάμεσα στους κόμβους. Έτσι σε ένα Έξυπνο Δίκτυο απαιτούνται οι ρόλοι του:

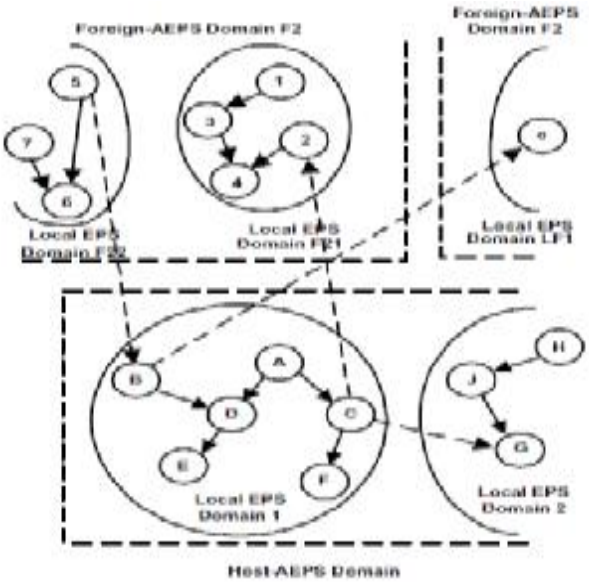
- επόπτη
- Καταγραφικού
- ελέγχου της ροής της ενέργειας
- σχεδιασμού του κάθε υποσταθμού
- Ανάλυσης
- Λειτουργίας του κάθε υποσταθμού
- Παρακολούθησης της ροής της ενέργειας
- Ελέγχου
- Ανάλυση της διαδρομής της τάσης



Εικόνα 17,εφαρμογή του πρότυπου AEPS: Assessment, Evaluation, Programming System στη διαχείριση των κόμβων στο Έξυπνο Δίκτυο [16]

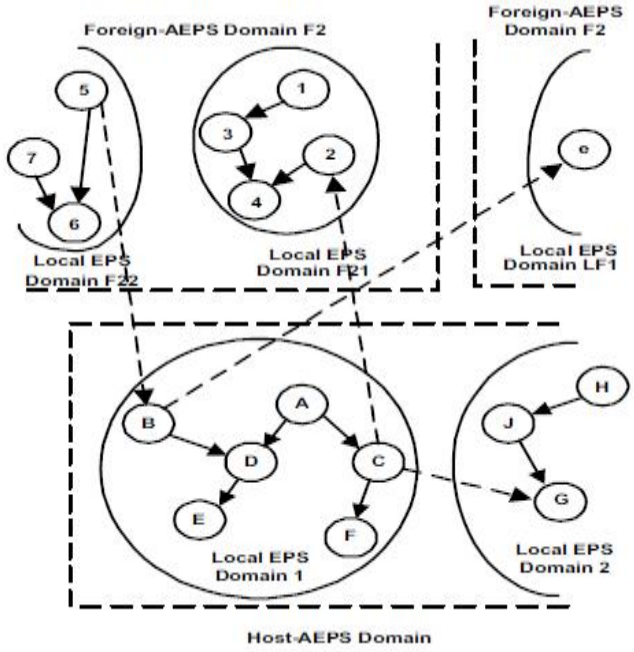
Ο ορισμός ρόλων επιτρέπει την αναγνώριση μίας συλλογής από δικαιώματα και την κατανομή τους σε συγκεκριμένους ανθρώπους μέσα στον ευρύτερο οργανισμό του Δικτύου. Το κάθε δικαίωμα αντιστοιχεί κατόπιν σε συγκεκριμένα στοιχεία και λειτουργίες του δικτύου (πχ ο εξοπλισμός του κάθε υποσταθμού, ο σταθμός παρακολούθησης της ροής της τάσης κλπ). Με τον τρόπο αυτό ορίζεται και ο ρόλος του ελεγκτή του δικτύου ο οποίος ταυτοποιεί τον χρήστη της κάθε συναλλαγής σε σχέση με τα δικαιώματα και τους περιορισμούς του ρόλου του. Για παράδειγμα ανά πάσα στιγμή γνωρίζει ότι ένας περιορισμένος αριθμός χρηστών έχει τα δικαιώματα ενός συγκεκριμένου ρόλου (πχ επόπτης υποσταθμού). Επιπλέον ο ελεγκτής διασταυρώνει τη μη ύπαρξη εμποδίων και συγκρούσεων στην ταυτόχρονη εκτέλεση των καθηκόντων που έχουν ανατεθεί σε ένα ή περισσότερους χρήστες.

Έχοντας ορίσει τους τομείς δραστηριότητας και λειτουργίας του δικτύου ορίζονται με τον ίδιο τρόπο και οι εξωτερικοί τομείς με τους οποίους ορίζονται σχέσεις εμπιστοσύνης και μπορούν να εκτελεστούν συναλλαγές ανάμεσα τους. Ο ελεγκτής διασταυρώνει σε δεδομένες συναλλαγές και σημεία του χρόνου ότι ψηφιακά διαπιστευτήρια έχουν δοθεί σε ένα ορισμένο αριθμό χρηστών του ξένου τομέα και εξακολουθούν να είναι σε ισχύ. Στο παρακάτω παράδειγμα, υποβάλλεται το αίτημα της μείωσης της ροής ενέργειας στον τοπικό τομέα EPS 1. Το αίτημα αυτό γίνεται αποδεκτό γιατί ο χρήστης έχει τον ρόλο C συνεπώς έχει τα εχέγγυα για να επιβάλλει τον έλεγχο της ροής ενέργειας στον τομέα 1.



Εικόνα 18, αποδοχή αιτήματος χρήστη με συγκεκριμένο ρόλο [16]

Σε ένα άλλο παράδειγμα το αίτημα για ανάλυση της διακύμανσης της διαδρομής της τάσης στον τομέα 1 απορρίπτεται καθώς ο απαιτούμενος ρόλος Ε δεν συμπεριλαμβάνεται στους ρόλους τους οποίους έχει ήδη ο συγκεκριμένος χρήστης.



Εικόνα 19, άρνηση αιτήματος χρήστη με συγκεκριμένο ρόλο [16]

6. ΚΑΤΑΝΕΜΗΜΕΝΗ ΠΑΡΑΓΩΓΗ ΕΝΕΡΓΕΙΑΣ

6.1. ΚΑΤΑΝΕΜΗΜΕΝΟΙ ΠΟΡΟΙ ΠΑΡΑΓΩΓΗΣ ΕΝΕΡΓΕΙΑΣ, ΤΑΞΙΝΟΜΗΣΗ

Η κατανεμημένη παραγωγή ενέργειας είναι αναπόφευκτη λαμβάνοντας υπόψη τον καταμερισμό τον διαφορετικών πηγών ενέργειας και την ανάγκη μείωσης του κινδύνου μη διαθεσιμότητας επαρκούς παραγωγής σε περίπτωση αποτυχίας ενός εκ των σταθμών. Η κατανεμημένη παραγωγή αυξάνει την αξιοπιστία του Δικτύου και το Έξυπνο Δίκτυο διευρύνει ακόμη περισσότερο την ευελιξία της κατανεμημένης διαθεσιμότητας καθώς αξιοποιείται και η προσφορά των οικιακών παραγωγών. Στο παραπάνω πλαίσιο ορίζεται η έννοια των Κατανεμημένων Ενεργειακών Πόρων (ΚΕΠ) ως οι πιο σημαντικοί πόροι που θα πρέπει να ληφθούν υπόψη και σε επίπεδο ασφάλειας.

Οι κύριες κατηγορίες κατανεμημένων ενεργειακών πόρων περιλαμβάνουν

- Πυρηνικούς σταθμούς
- Σταθμούς καύσης ορυκτών καυσίμων (λιγνίτη, φυσικού αερίου, ή πετρελαίου)
- Υδροηλεκτρικοί σταθμοί

Κεντρικοί σταθμοί παραγωγής είναι κρίσιμοι στη κάλυψη της απαιτούμενης ζήτησης σε κάθε χώρα. Αυξάνοντας τον αριθμό των μικρότερων σταθμών για να αυξηθεί και ο βαθμός κατανομής σημαίνει αυτόματα και απαίτηση για κάλυψη της παραγωγής που θα πρόσφεραν εναλλακτικά μεγάλοι κεντρικοί σταθμοί.

Οι ΚΕΠ ουσιαστικά επιτρέπουν την συμβολή οικιακών μικρό-παραγωγών στο ηλεκτρικό δίκτυο μίας χώρας. Τυπικά η παραγωγή αυτού του τύπου δεν ξεπερνά τα 10 MWs και διατίθεται στο τοπικό δίκτυο διανομής. Δεν μπορούν να συνδεθούν στο σύστημα μεταφοράς γιατί δεν αποτελούν συστήματα παραγωγής υψηλής τάσης. Ανήκουν στα συστήματα χαμηλής τάσης και καλύπτουν δύο τύπους ενέργειας:

- Παραγωγή ενέργειας
- Αποθήκευση ενέργειας

Στην 1^{η} κατηγορία υπάγονται τεχνολογίες παραγωγής ενέργειας όπως: ανεμογεννήτριες, ντιζελογεννήτριες, γεννήτριες φυσικού αερίου, διπλού καυσίμου, γεννήτριες υγραερίου, μικρό-γεννήτριες αερίου, κελιών καυσίμου (υδρογόνου), και φωτοβολταϊκά. Στη 2^{η} κατηγορία τα συστήματα αυτά αποθηκεύουν ενέργεια όπως στη περίπτωση των επαναφορτιζόμενων μπαταριών. Παρόλο που υπάρχει πληθώρα συσκευών αποθήκευσης ενέργειας η τεχνολογία περιορίζεται στην αποθήκευση μικρού ποσοστού ενέργειας. Συσκευές αποθήκευσης ενέργειας περιλαμβάνουν:

- Συστήματα Αδιάλειπτης Παροχή Ενέργειας (UPS)
- Συστήματα υπεραγώγιμων υλικών
- Συστήματα χρήσης μηχανικής ενέργειας (αντλησιοταμίευση, συμπιεσμένος αέρας, στρεφόμενοι σφόνδυλοι)
- Συστήματα χρήσης χημικών μεθόδων (μπαταρίες, μπαταρίες ροής, προχωρημένου τύπου μπαταρίες)

Επιπλέον οι ΚΕΠ αξιοποιούνται με βάση την επιλογή ενός προγράμματος κατανάλωσης της ενέργειας τους.

- Απορρόφηση αυξημένης ζήτησης: στη περίπτωση αυτή οι εταιρίες χρεώνουν διαφορετική τιμή για τη χρήση της ενέργειας σε ώρα αιχμής. Καθώς αυξάνει η ζήτηση αυξάνει η τιμή γιατί μειώνεται η διαθέσιμη παραγωγή.

- Βελτιωμένη ποιότητα ρεύματος: για παράδειγμα πτώσεις ρεύματος θα πρέπει να αποφεύγονται με τη χρήση κάποιου συστήματος όπως αυτά που περιγράφηκαν παραπάνω
- Πράσινη ενέργεια: το πρόγραμμα αυτό περιορίζει τους ΚΕΠ αποκλειστικά σε ανανεώσιμες πηγές ενέργειας (πχ ανεμογεννήτριες, φωτοβολταϊκά)

6.2. ΣΥΣΤΗΜΑ ΔΙΑΧΕΙΡΙΣΗΣ ΠΑΡΑΓΩΓΗΣ ΕΝΕΡΓΕΙΑΣ & ΑΣΦΑΛΕΙΑ ΠΑΡΑΓΩΓΗΣ ΕΝΕΡΓΕΙΑΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Η επίδραση των Κατανεμημένων Ενεργειακών Πόρων στην Κυβερνο-Ασφάλεια δεν έχει προσδιοριστεί ακόμη με ακρίβεια. Τα συστήματα αυτά οριοθετούνται σε τοπικές περιφέρειες στις οποίες αξιοποιούνται από διάφορους οργανισμούς για την κάλυψη των ενεργειακών τους αναγκών. Από τη στιγμή όμως που θα αρχίσουν να διασυνδέονται στην ευρύτερη ενεργειακή υποδομή και θα αποτελούν αξιόλογους κατανεμημένους πόρους μίας ευρύτερης παραγωγής σημαίνει ταυτόχρονα ότι η υπολογιστική τους υποδομή θα είναι μέρος ενός ευρύτερου δικτύου επικοινωνιών. Η έκθεση της δικτυακής υποδομής στους κινδύνους που μπορεί να εμπεριέχουν οι υπολογιστικές οντότητες των ΚΕΠ είναι η σημαντικότερη απειλή που πρέπει να ληφθεί υπόψη.

Πράγματι αποτελεί σημαντικό παράγοντα κινδύνου που πρέπει να αξιολογηθεί καθώς οι ΚΕΠ αλληλεπιδρούν με άλλους πόρους παραγωγής και άλλα ενεργειακά συστήματα μέσω της δικτυακής υποδομής. Ο πίνακας ελέγχου του Έξυπνου Δικτύου πρέπει να παρακολουθεί και τη λειτουργία των ΚΕΠ, να γνωρίζει ποιοι πόροι είναι διαθέσιμοι ειδικά σε συμβάντα επείγουσας αύξησης της παραγωγής και την ανταπόκριση σε ξαφνική ζήτηση. Με λίγα λόγια, το πρόβλημα όσον αφορά την κυβερνο-ασφάλεια δεν είναι η λειτουργία των ΚΕΠ αλλά η επικοινωνία με αυτούς.

Η επικοινωνία με τους ΚΕΠ μέσω του κέντρου ελέγχου ίσως αποτελεί πρόβλημα εξαιτίας της κατανεμημένης και μη ασφαλούς φύσης λειτουργίας τους. Το τελευταίο συνεπάγεται από το γεγονός ότι οποιοσδήποτε μπορεί να παράγει και να πουλά ενέργεια στο κεντρικό δίκτυο ως ένας αυτόνομος ΚΕΠ. Αυτό επίσης σημαίνει ότι το κέντρο ελέγχου δεν μπορεί να ελέγξει το τελικό σημείο του δικτύου που συγκεντρώνει τα δεδομένα από το ΚΕΠ. Για παράδειγμα, αν κάποια απειλή παρεισφρήσει ανάμεσα στο τελικό σημείο του δικτύου και το ΚΕΠ τότε μπορεί να αλλοιώσει και τα δεδομένα που υποτίθεται ότι το ΚΕΠ αποστέλλει στο δίκτυο. Ένα άλλο θέμα κυβερνο-ασφάλειας είναι η επίπτωση που θα υπάρξει στη διαθεσιμότητα ενέργειας αν ληφθούν αλλοιωμένα δεδομένα ειδικότερα σε κρίσιμες περιπτώσεις ανταπόκρισης σε αυξημένη ζήτηση.

6.2.1. ΕΞΥΠΝΑ ΔΙΚΤΥΑ ΜΙΚΡΗΣ ΚΛΙΜΑΚΑΣ (MICRO-GRIDS)

Μία πρόταση αυτοματοποιημένου ελέγχου και καταγραφής της ενέργειας που παράγεται και μεταφέρεται από οικιακά δίκτυα είναι τα έξυπνα δίκτυα μικρής κλίμακας. Τυπικά ένα τέτοιο μικρό-δίκτυο μπορεί να διαχειριστεί τη παραγωγή και κατανομή ηλεκτρικών φορτίων σε μικρά οικοσυστήματα όπως ένα πολυώροφο κτίριο, ένα πανεπιστήμιο, μία γειτονιά κ.α.. Ουσιαστικά ένα μικρό-δίκτυο εξομοιώνει τις λειτουργίες ενός ενεργού δικτύου διανομής ενώ μπορεί να διαθέτει και μπορεί επίσης να διαθέτει γεννήτριες ντίζελ για έκτακτες ανάγκες. Οι μικρό-πηγές παραγωγής σε αυτό το δίκτυο, στη σύγχρονη μορφή αυτών των δικτύων, είναι ανανεώσιμες πηγές ενέργειας και καθαρές μορφές ορυκτών καυσίμων (φυσικό αέριο). Επιπλέον, ένα σημαντικό χαρακτηριστικό των μικρό-δικτύων είναι η τηλε-θέρμανση καθώς η θέρμανση που παράγεται συνήθως στη μορφή ατμού κατά την παραγωγική διαδικασία μπορεί να μοιραστεί στο οικοσύστημα μέσω κεντρικών αγωγών.

Τα μικρό-δίκτυα δεν έχουν φυσικά δίκτυα μεταφοράς γιατί η παραγωγή και διανομή είναι τοπική. Αντί αυτού, ένας κρίσιμος συντελεστής ορθής λειτουργίας του είναι ο συγχρονισμός του με το ευρύτερο δίκτυο. Οποιαδήποτε ανωμαλία στη λειτουργία ενός μικρό-δικτύου δεν πρέπει να μεταδοθεί στο μεγαλύτερο δίκτυο. Ειδικά στη σύγχρονη τους έκδοση οι λειτουργίες των περισσότερων δικτύων δεν έχουν δοκιμαστεί. Επιπρόσθετα καλούνται να εφαρμόσουν

τοπικές πολιτικές διαχείρισης της ζήτησης αν αυτές δεν είναι διαχειρίσιμες από ευρύτερες αρχές (περιφερειακή οργανισμοί μεταφοράς ενέργειας ή ανεξάρτητες ρυθμιστικές αρχές).

Εξίσου σημαντικός είναι ο μηχανισμός αυτόματης προσθήκης ή απομάκρυνσης ενός μικρό-δικτύου ερμηνεύοντας μεταβλητές όπως ζήτηση, καιρικές συνθήκες, προβλέψεις για την κατανομή της ζήτησης στη διάρκεια της ημέρας. Τα παραπάνω θα καθορίσουν αν πρέπει για παράδειγμα ένα μικρό-δίκτυο να ενεργοποιηθεί ως συμπαραγωγός. Στη περίπτωση αυτή θα πρέπει να είναι πιστοποιημένο μέλος του ευρύτερου δικτύου και θα πρέπει να διαθέτει κεντρικό ελεγκτή με λειτουργίες μέτρησης, ελέγχου, προστασίας.

6.2.2. ΚΥΒΕΡΝΟ-ΑΣΦΑΛΕΙΑ ΜΙΚΡΟ-ΔΙΚΤΥΩΝ

Γνωρίζοντας πλέον ότι τα μικρό-δίκτυα θα ενεργοποιηθούν σε διαφορετικού τύπου οικοσυστήματα και για διαφορετικούς σκοπούς (πχ νοσοκομεία, στρατόπεδα, απομακρυσμένα χωριά) η εκτίμηση των κινδύνων ασφάλειας σε κάθε περίπτωση είναι διαφορετική. Για παράδειγμα, μία κοινότητα που είναι συνηθισμένη σε διακοπές ρεύματος είναι επίσης προετοιμασμένη να ανεχτεί τις επιπτώσεις κυβερνο-επιθέσεων. Επίσης μία κοινότητα που βασίζεται αποκλειστικά σε ανανεώσιμες πηγές ενέργειας γνωρίζει ότι οι πηγές αυτές είναι αναξιόπιστες και θα πρέπει να διαθέτει εφεδρικές πηγές σε περιπτώσεις ανάγκης. Από την άλλη μεριά οργανισμοί των οποίων η λειτουργία τους είναι σημαντική για το ευρύτερο κοινωνικό σύνολο (σχολεία, νοσοκομεία, στρατόπεδα) μπορούν να ανεχτούν μηδαμινές διακοπές ρεύματος. Στη περίπτωση αυτή οι υποδομές των οργανισμών αυτών ενισχύονται περισσότερο έτσι ώστε να εξασφαλιστεί ότι πάντα θα προμηθεύονται ενέργεια. Μερικά από τα μέτρα στις περιπτώσεις αυτές περιλαμβάνουν:

1. Ενσωμάτωση μηχανισμών ελέγχου των φορτίων
2. Οι τηλεπικοινωνιακές και ηλεκτρικές διασυνδέσεις πρέπει να είναι καλά οχυρωμένες και να υπάρχουν διαθέσιμες εναλλακτικές διαδρομές για να μειωθεί ο κίνδυνος καταστροφής τους σε περίπτωση φυσικής επίθεσης
3. Θα πρέπει να αποφευχθεί η χρήση ασύρματων ζεύξεων για ανταλλαγή σημάτων ελέγχου καθώς μπορεί να υπάρξει παρεμβολή στις ράδιο συχνότητες.
4. Όλη η κίνηση στο δίκτυο επικοινωνιών θα πρέπει να είναι κρυπτογραφημένη για να μην υποκλέπτεται πληροφορία από όσους παρακολουθούν τα πακέτα δεδομένων κίνησης σχετικά με τη παραγωγή στο δίκτυο.
5. Όλες οι τεχνολογίες που εφαρμόζονται στην ασφάλεια της κατανομής (υποδομή προχωρημένης μέτρησης - AMI, δίκτυα οικιστικών περιοχών - HAN)

Μία ακόμη σημαντική απειλή είναι το προσωπικό που ενώ εμπλέκεται στην απομακρυσμένη παραγωγή δεν αποτελεί προσωπικό ελεγχόμενο από τον οργανισμό διαχείρισης του δικτύου. Παρόλα αυτά η αλληλεπίδραση με αυτό το προσωπικό γεννά ορισμένους κινδύνους:

- Μέθοδοι και τρόποι με τους οποίους οι εταιρίες εμπορίας ενέργειας αλλά και οι λειτουργοί των μικρό-δικτύων θα επικοινωνήσουν με αυτό το προσωπικό πληροφορία σχετικά με τη κατάσταση της παραγωγής και δεδομένα ελέγχου.
- Μία εταιρία εμπορίας και ένα τοπικό δίκτυο μπορεί να συμφωνήσουν τα παραπάνω για μία σειρά περιπτώσεων όπως πότε απαιτείται αυτόνομη λειτουργία του τοπικού δικτύου και πότε μαζί με το γενικό δίκτυο. Αυτόματοι μεταγωγείς μπορούν να τοποθετηθούν στις ενώσεις των δύο δικτύων για να ελέγξουν τις εντολές ένθεν και ένθεν σε περιπτώσεις διακοπών ή άλλων περιπτώσεων.
- Σημαντικοί οργανισμοί όπως αυτοί που αναφέρθηκαν παραπάνω διαθέτουν ήδη μίνι συστήματα διανομής με μονή ή διπλή ηλεκτρική τροφοδοσία από τη τοποθεσία προς τη κεντρική παροχή ενέργειας η οποία διαθέτει μετρητές κατανάλωσης, λειτουργίες SCADA και άλλα μέτρα προστασίας.

6.2.3. ΚΑΤΑΝΕΜΗΜΕΝΟ ΣΥΣΤΗΜΑ ΕΞΥΠΝΟΥ ΕΛΕΓΧΟΥ

Το Κατανεμημένο Σύστημα Ελέγχου (ΚΣΕ) είναι ένα Πληροφοριακό Σύστημα που χρησιμοποιείται για τον έλεγχο, παρακολούθηση και λειτουργία του σταθμού παραγωγής.

Είναι υπεύθυνο για τον έλεγχο τον κατανεμημένων πόρων μέσα στον σταθμό παραγωγής. Επιπρόσθετα το ΚΣΕ είναι υπεύθυνο για την διαχείριση του ισοζυγίου των εφαρμογών του σταθμού παραγωγής και τον συντονισμό των διεργασιών σε αυτόν. Το ισοζύγιο των εφαρμογών του σταθμού παρακολουθεί όλες τις διεργασίες για την εύρυθμη λειτουργία τους. Η κάθε διεργασία συνδέεται με μία εφαρμογή του ΚΣΕ έτσι ώστε να ελέγχουν και να παρακολουθούν τις εκάστοτε παραγωγικές λειτουργίες.

Το ΚΣΕ δίκτυο αντιπροσωπεύει το δίκτυο ελέγχου και παρακολούθησης των λειτουργιών μέσα στον σταθμό παραγωγής. Κάθε απομακρυσμένη διεργασία ελέγχεται μέσω αισθητήρων από το κεντρικό σημείο ελέγχου του ΚΣΕ. Ενώ ελεγκτές προγραμματισμένης λογικής επιστρατεύονται για την εκτέλεση εντολών προς τις απομακρυσμένες διεργασίες.

Μία από αυτές τις διεργασίες είναι ο Έλεγχος Αυτόματης Παραγωγής η οποία χρησιμοποιείται για τον έλεγχο της παραγωγής εφόσον κρίνεται απαραίτητο η εξισορρόπηση του συνολικού συστήματος. Για παράδειγμα αν ένας παραγωγικός πόρος τεθεί ξαφνικά εκτός λειτουργίας τότε το σύστημα ελέγχου καλείται να μοιράσει ξανά το φορτίο ή να διακόψει τη παροχή σε ορισμένο αριθμό καταναλωτών για να αποφευχθεί η διακοπή σε μεγάλη μάζα πληθυσμού. Στη περίπτωση αυτή θα ενεργοποιηθεί ο Έλεγχος Αυτόματης Παραγωγής για την παραγωγή ενέργειας από άλλη κατανεμημένη πηγή ή εναλλακτικά να διαχειριστεί απομακρυσμένους διακόπτες κυκλωμάτων για τον τερματισμό της ροής ρεύματος σε συγκεκριμένες οικιστικές περιοχές.

Οι παραπάνω αποφάσεις και ενέργειες του συστήματος ελέγχου αποτελούν τους κύριους παράγοντες που λαμβάνονται υπόψη από την κυβερνοασφάλεια στον τομέα αυτό. Επομένως αν μία απειλή στην ασφάλεια του συστήματος στοχεύει στο να θέσει μεγάλο μέρος του φορτίου εκτός, θα επιχειρούσε να προκαλέσει μία κατάσταση κατά την οποία το σύστημα ελέγχου αναγκάζεται να ρίξει φορτίο εντός συστήματος. Ειδικά σε μεγάλα συστήματα παραγωγής (πχ σε χώρες όπως οι ΗΠΑ, Κίνα, κ.α.) το να ριχθεί φορτίο που θα καλύψει τη παραγωγή που προσφέρει ένας μεγάλος σταθμός που τίθεται εκτός θα ήταν αρκετά πολύπλοκο. Ωστόσο η κατανεμημένη διάταξη των σταθμών παραγωγής που διαθέτουν ΚΣΕ επιτρέπει την εκτέλεση της απειλής σε μία μόνο μονάδα παραγωγής. Επομένως ένα μόνο μέρος της παραγωγής επηρεάζεται και μειώνεται σημαντικά ο αριθμός των καταστάσεων πτώσης φορτίου. Έτσι μπορεί μεν να διακοπεί προσωρινά η παροχή σε λίγους όχι όμως στη πλειοψηφία αυξάνοντας έτσι την αξιοπιστία του συστήματος.

Αυτή είναι μία καλή πρακτική διαχείρισης κινδύνου λαμβάνοντας υπόψη τις επιπτώσεις μίας απειλής πτώσης φορτίου στο σύνολο της παραγωγικής μονάδας. Επομένως όσοι πόροι θεωρούνται ότι έχουν σημαντική βαρύτητα στο Έξυπνο Δίκτυο πρέπει να διασφαλιστούν από το ενδεχόμενο να αναγκαστούν να ρίξουν το φορτίο τους και από το να διαδώσουν την αποτυχία τους στο υπόλοιπο δίκτυο.

Ο πιο σημαντικός παράγοντας ο οποίος πρέπει να διασφαλιστεί από την εφαρμογή των μηχανισμών κυβερνο-ασφάλειας είναι η Εμπιστοσύνη. Μία εξωτερική απειλή μπορεί να ξεπεράσει τα εμπόδια ορισμένων ελέγχων ασφαλείας (πχ πολιτικές που εμποδίζουν τους χρήστες να χρησιμοποιήσουμε κύριες πηγές εντολών των συστημάτων ελέγχου). Στη καλύτερη περίπτωση θα προκαλέσει ένα συμβάν πτώσης φορτίου. Ωστόσο θα πρέπει να αποφευχθεί μία αλυσιδωτή αποτυχία στο σύστημα που θα μειώσει την εμπιστοσύνη προς αυτό. Οι πάροχοι ηλεκτρικής ενέργειας δεν θα μπορούν να πάρουν αποφάσεις βασισμένοι σε πληροφορίες που θα θεωρούνται αναξιόπιστες.

Τέτοιες αποφάσεις θα πρέπει να λαμβάνονται με αυτόματο τρόπο καθώς το δίκτυο γίνεται περισσότερο νοήμον. Αυτό θα βοηθήσει την αξιόπιστη διαδικασία λήψης αποφάσεων για τη διαχείριση μίας αποτυχίας στην παραγωγή που θα έχει ανιχνευθεί και θα πρέπει να καθοδηγήσει την ζήτηση παραγωγής από ένα κατανεμημένο πόρο ή τη πτώση του φορτίου προς μικρό μέρος του πληθυσμού για τη προστασία της πλειοψηφίας. Επομένως στα σημεία αυτά αλληλεπίδρασης μεταξύ κεντρικού ελέγχου και κατανεμημένων πόρων θα πρέπει να

εντοπιστούν οι διάφοροι τύπο κινδύνων και να ληφθούν μέτρα που θα προστατεύουν την λήψη αποφάσεων με αυτοματοποιημένο τρόπο.

7. ΕΦΟΔΙΑΣΤΙΚΗ ΑΛΥΣΙΔΑ ΣΤΟ GRID (LOGISTICS)

7.1. ΔΙΑΧΕΙΡΙΣΗ ΑΠΟΘΗΚΕΥΣΗΣ & ΑΣΦΑΛΕΙΑ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Η αποθήκευση ενέργειας είναι μία πρακτική που εφαρμόζεται σχεδόν σε κάθε συσκευή της σύγχρονης τεχνολογικής ζωής. Η αποθήκευση παίρνει διάφορες μορφές: από τις παραδοσιακές τράπεζες φορτίου σε υποσταθμούς, δεξαμενές νερού υδροηλεκτρικών εργοστασίων, σε πιο ευέλικτες μορφές χημικών λύσεων όπως αυτές των μπαταριών. Η ανάπτυξη της τελευταίας μορφής αποθήκευσης έχει περισσότερες προοπτικές, για παράδειγμα στη χρήση τους σε ηλεκτροκίνητα οχήματα. Επιπλέον μεγαλύτερης κλίμακας συστήματα μπαταριών μπορούν να μεταφέρονται όπου είναι απαραίτητα και να προσφέρουν από 500 KW έως και 2.8 MWh σε ορισμένες περιπτώσεις.

Συστήματα αποθήκευσης ενέργειας βασισμένα σε χημικές λύσεις (μπαταρίες) εισάγουν και ένα νέο πλαίσιο συντονισμού αυτού του είδους των πόρων με το Έξυπνο Δίκτυο:

1. Ένα μεγάλο πλήθος τοπικών πόρων αποθήκευσης εισάγονται στο σύστημα και πρέπει να υπάρξει ένας συντονισμός με το πλησιέστερο σύστημα διανομής της αποθηκευμένης ενέργειας.
2. Ηλεκτροκίνητα αυτοκίνητα θα χρησιμοποιούν το συνολικό δίκτυο ως βασική πηγή ενέργειας και άμεσης τροφοδοσίας.
3. Οι μηχανισμοί ελέγχου και επικοινωνίας των συστημάτων αποθήκευσης πρέπει να ενημερώνουν για τα εναπομείναντα επίπεδα αποθηκευμένης ενέργειας καθώς επίσης να προβλέπουν πόση ενέργεια θα χρειαστούν από το δίκτυο για την επανατροφοδοσία τους.
4. Ο κάθε πόρος αποθήκευσης ενέργειας πρέπει να μπορεί να επικοινωνεί με το δίκτυο επικοινωνίας του δικτύου και να ταυτοποιείται σε αυτό για να θεωρείται τερματική οντότητα του ευρύτερου δικτύου.

Επομένως οι αποθηκευτικοί πόροι είναι επίσης κρίσιμοι για την Κυβερνο Ασφάλεια του δικτύου. Αν κάποιος καταφέρει να ελέγξει τους παραπάνω μηχανισμούς του αποθηκευτικού πόρου μπορεί να ελέγχει και την αλληλεπίδραση με τον ευρύτερο δίκτυο προκαλώντας παραπληροφόρηση και λήψη επικίνδυνων ή ανεπαρκών αποφάσεων. Επομένως πρέπει να υπάρχει μία τυποποιημένη επικοινωνία του κάθε αποθηκευτικού πόρου με το Δίκτυο προκειμένου ο κάθε πάροχος να βασίζεται σε αυτοματοποιημένα κριτήρια αξιοποίησης ή όχι ενός πόρου.

7.2. ΠΑΡΟΧΗ ΕΝΕΡΓΕΙΑΣ ΑΠΟ ΗΛΕΚΤΡΟΚΙΝΗΤΑ ΟΧΗΜΑΤΑ

Επιπλέον η αξιοποίηση του Δικτύου για την τροφοδοσία ηλεκτροκίνητων αυτοκινήτων αλλά και το αντίστροφο, οδήγησε σε ένα γενικότερο ορισμό ενός συστήματος διαχείρισης διανυσμάτων μπαταριών. Ένα τέτοιο σύστημα πρέπει να κατέχει τα παρακάτω χαρακτηριστικά:

1. Εκτίμηση της κατάστασης χρέωσης
2. Παρακολούθηση της κατάστασης υγείας του κάθε επιμέρους κελιού και του ευρύτερου διανύσματος μπαταριών
3. Έλεγχος θερμοκρασίας
4. Έλεγχος φόρτισης / απόφόρτισης της ισχύος
5. Κατανομή ισχύος στα κελιά
6. Καταγραφή δεδομένων στο ημερολόγιο

Αυτά τα δεδομένα πρέπει να είναι διαθέσιμα σε κάθε πάροχο που πρέπει να επικοινωνήσει με ηλεκτροκίνητα οχήματα για τη λήψη ενέργειας από αυτά. Επιπλέον η διαδικασία φόρτισης εξισορροπεί τα παραπάνω δεδομένα με δεδομένα που χρησιμοποιούνται στη

διαπραγμάτευση ζήτησης, τιμής και άλλων σχετικών συμβάντων. Οι πάροχοι προσομοιώνουν τον έλεγχο κατανεμημένης παραγωγής καθώς φροντίζουν να λαμβάνουν πληροφορίες και να στέλνουν παρόμοια σήματα σε πραγματικό χρόνο. Ο έλεγχος της ασφάλειας αυτής της αλληλεπίδρασης είναι σημαντικός καθώς οι παραπάνω πόροι θα πρέπει να αμειφτούν για την προσφορά ενέργειας τη δεδομένη χρονική στιγμή. Ο έλεγχος της ασφάλειας επίσης θα πρέπει να φροντίζει ώστε εξωτερικοί εισβολείς δεν στέλνουν εσφαλμένα σήματα (πχ με τροποποιημένη την ημέρα ή ώρα). Έλεγχοι ασφάλειας στη περίπτωση αυτοί θα μπορούσαν να είναι:

1. Προστασία του συστήματος επιλογής οχήματος πίσω από ένα τείχο προστασίας (firewall)
2. Εφαρμογή μηχανισμού ταυτοποίησης των οχημάτων πριν την επιλογή τους ως πόροι προσφοράς ενέργειας
3. Έλεγχος για παρουσία στο δίκτυο κακόβουλων οχημάτων
4. Εφαρμογή μέτρων στη πρόσβαση των δεδομένων των οχημάτων, των οδηγών κα
5. το κάθε όχημα θα πρέπει να προστατεύεται με παρόμοια μέτρα όπως αυτά που προστατεύουν τους κατόχους και χρήστες οικιακών δικτύων.

7.3. ΔΙΑΧΕΙΡΙΣΗΣ ΑΣΦΑΛΕΙΑΣ ΤΩΝ ΠΟΡΩΝ ΑΠΟΘΗΚΕΥΣΗΣ ΕΝΕΡΓΕΙΑΣ

Ένα από τα πιο σημαντικά μέτρα που πρέπει να λαμβάνονται για την ορθή αλληλεπίδραση αποθηκευτικού χώρου και Δικτύου είναι ο έλεγχος των αποδεκτών ορίων ισχύος που μπορεί να δεχτεί το δίκτυο από μία συσκευή. Οποιαδήποτε αυξημένη προσφορά εκτός ορίων δεν γίνεται αποδεκτή και θεωρείται πληροφορία από κακόβουλη ή εσφαλμένη πηγή. Με τον τρόπο αυτό αποφεύγονται οι αλυσιδωτές αρνητικές αντιδράσεις στο δίκτυο. Επιπρόσθετα, το σύστημα διαθέτει μηχανισμό επιλογής των κατάλληλων πόρων αξιολογώντας τη κάθε λεπτομέρεια των σημάτων που δέχεται από αυτούς.

Ένα άλλο σημαντικό μέτρο είναι η λήψη μετρήσεων σε τακτικά διαστήματα μέσα στην ημέρα από τους αποθηκευτικούς πόρους ή τα ηλεκτροκίνητα οχήματα. Για παράδειγμα τα οχήματα περνούν το 90% του χρόνου της ημέρας σε κατάσταση παρκαρίσματος. Η λήψη δεδομένων αξιολογεί και αυτό το παράγοντα για την ανίχνευση πιθανών απειλών. Είναι επίσης απαραίτητο η εφαρμογή ενός προγράμματος κρυπτογράφησης για τη πιστοποίηση του κάθε αποθηκευτικού πόρου. Ο μηχανισμός αυτός θα επιτρέπει την πιστοποίηση της γνησιότητας του κλειδιού που θα διαθέτει ο κάθε πόρος και το ταίριασμα του με το ιδιωτικό κλειδί του δικτύου. Εναλλακτικά, ο κάθε πόρος αποθήκευσης ενέργειας μπορεί να έχει το δικό του ιδιωτικό κλειδί για να επιτρέπει την ανταλλαγή δεδομένων και υπηρεσιών με σταθμούς φόρτισης, στάθμευσης, πληρωμής των αντίστοιχων λογαριασμών τους και άλλων.

Η αξιοποίηση των πόρων αποθήκευσης ενέργειας είναι μία σημαντική προοπτική όμως είναι ταυτόχρονα και αρκετά πολύπλοκη. Πράγματι περιλαμβάνει περισσότερες απαιτήσεις επικοινωνίας και συντονισμού σε σχέση με την υλοποίηση του συμβατού Έξυπνου Δικτύου. Από την άλλη αποτελεί μία προοπτική που θα αντισταθμίσει τα μειονεκτήματα των εναλλακτικών πηγών ενέργειας (ηλιακή, αιολική κ.α.). Αρκεί να οριστεί το συνολικό πλαίσιο της εφοδιαστικής αλυσίδας και της διαχείρισης των κατανεμημένων πόρων αποθήκευσης.

8. ΔΙΑΧΕΙΡΙΣΗ ΚΙΝΔΥΝΩΝ

8.1. ΤΑΞΙΝΟΜΗΣΗ ΚΙΝΔΥΝΩΝ & ΑΠΕΙΛΩΝ

Αναμφισβήτητα το επίκεντρο της ασφάλειας στο Έξυπνο Δίκτυο Ενέργειας είναι ο εντοπισμός απειλών και η άμεση αντιμετώπιση τους. Αυτό γιατί όσο αυξάνει ο αριθμός των υπολογιστικών και δικτυακών διασυνδέσεων στο Έξυπνο Δίκτυο τόσο θα αυξάνει και η επίδραση των συμβάντων ασφαλείας στη λειτουργία και αξιοπιστία του Δικτύου. Η χρήση δικτυακών υποδομών βασισμένων στο πρωτόκολλο του ίντερνετ (IP) είναι πολύ χρήσιμο για την ανάπτυξη του Δικτύου Ενέργειας. Από την άλλη γεννάει απειλές που πρέπει να αντιμετωπιστούν με την εφαρμογή των κατάλληλων μέτρων ασφαλείας. Για τη καλύτερη δυνατή διαχείριση των κινδύνων οι πάροχοι διαβλέπουν μια αυξανόμενη ανάγκη για την ανάπτυξη λύσεων ασφαλείας καθώς και σχετικών πρωτοκόλλων για την προστασία των λειτουργικών τους δικτύων που διατρέχουν πάνω από το πρωτόκολλο IP.

Σε αυτό το πλαίσιο λειτουργίας των υποδομών του Δικτύου είναι ξεκάθαρο ότι μία απειλή προσπαθεί να εκμεταλλευτεί μία αδυναμία του λειτουργικού δικτύου και να προκαλέσει αστάθεια. Τέτοιου είδους απειλές θα πρέπει να αναλυθούν και να περιοριστούν έχοντας υπόψη δύο κύριες κατηγορίες [2], [4], [5], [6], [9], [13] & [20]:

- Κακόβουλες απειλές, και είναι αυτές που επιδιώκουν να προκαλέσουν σφάλμα
- Μη κακόβουλες απειλές, είναι αυτές που προκαλούν σφάλμα χωρίς τη θέληση τους

8.1.1. ΚΑΚΟΒΟΥΛΕΣ ΑΠΕΙΛΕΣ

Οι κακόβουλες απειλές στοχεύουν στο να εκμεταλλευτούν πληροφόρηση μέσα στο λειτουργικό περιβάλλον έτσι ώστε οι πάροχοι να υποπέσουν σε σφάλματα. Η πιο τυπική απειλή είναι η δημιουργία παραπλανητικής πληροφόρησης που αναγκάζει ένα πάροχο να λάβει μία εσφαλμένη απόφαση. Για παράδειγμα, αν το πληροφοριακό σύστημα του παρόχου έχει τη «πληροφορία» για σφάλμα σε μία γραμμή τότε θα διακόψει τη τροφοδοσία της. Και το αντίστροφο, η εσφαλμένη πληροφόρηση ότι η τροφοδοσία μίας γραμμής έχει διακοπεί μπορεί να προκαλέσει θανάσιμα ατυχήματα σε όσους εξακολουθούν να δουλεύουν σε αυτή.

Η πιθανότητα επίδρασης μίας κακόβουλης απειλής είναι χαμηλή καθώς οι πάροχοι διαθέτουν τους μηχανισμούς διακοπής τροφοδοσίας και επικοινωνίας με το δίκτυο. Τείχος προστασίας και περιορισμοί στα σημεία πρόσβασης φροντίζουν για την εξουσιοδοτημένη πρόσβαση σε τοίχοι και υπηρεσίες του δικτύου λειτουργίας. Το δίκτυο λειτουργίας φιλοξενεί πίσω από τη πύλη προστασίας λειτουργίες υποσταθμών και τερματικές συσκευές. Το SCADA (δίκτυο εποπτικού ελέγχου και λήψης δεδομένων) δρα ως ένα δίκτυο απομονωμένο από το λειτουργικό δίκτυο μέσω σημείων πρόσβασης και τειχών προστασίας. Επιπλέον λίστες δικαιωμάτων πρόσβασης μέσα σε κάθε σημείο πρόσβασης ελέγχουν τη ροή της πληροφορίας και εμποδίζουν μη εξουσιοδοτημένα δεδομένα να μπουν σε ή να βγουν από κάποιο από τα παραπάνω δίκτυα. Συγκεκριμένες πύλες και υπηρεσίες ανοίγουν ανάμεσα στα δίκτυα για την ασφαλή επικοινωνία τους. Οι κανόνες που ορίζουν ποιες πόρτες επιτρέπεται να ανοίξουν ή ποιες υπηρεσίες επιτρέπεται να είναι ενεργές ενδέχεται να υπάρχουν σε κάθε τείχος προστασίας.

8.1.1.1. ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ

Στην συνέχεια περιγράφονται οι ενέργειες που εντάσσονται στα μέτρα προστασία από τις κακόβουλες απειλές.

«Επιθεώρηση με μνήμη»: η λειτουργία αυτή ενός τοίχους προστασίας ταυτοποιεί την κίνηση προς τα έξω με τη κίνηση προς τα μέσα στη διάρκεια μίας συναλλαγής δημιουργώντας μία ενιαία ροή διασύνδεσης. Εφόσον το τοίχος προστασίας επιτρέπει κίνηση προς τα έξω σε μία συσκευή τότε στην ίδια διασύνδεση επιτρέπει και κίνηση προς τα μέσα. Η

ασφάλεια της πρόσβασης στη ροή αυτή προς τα έξω και προς τα μέσα παρακολουθείται σε όλη τη διάρκεια της συναλλαγής για να πιστοποιείται η κατάσταση της.

Η παραβίαση της ασφάλειας συστημάτων μέσα σε εταιρικά δίκτυα έχει να κάνει με τη συμπεριφορά των εσωτερικών χρηστών. Για παράδειγμα, οι χρήστες ενδεχομένως να αποθηκεύσουν στον υπολογιστή τους κακόβουλα προγράμματα από ιστοσελίδες που έχουν ήδη μολυνθεί. Το μολυσμένο αρχείο μπορεί να αναπαράγει επιπλέον αρχεία ή προγράμματα μολύνοντας τη τοπική συσκευή.

Επιπλέον η παραβίαση της ασφάλειας συστημάτων μέσα σε εταιρικά δίκτυα γεννά τον κίνδυνο του ελέγχου λειτουργικών συστημάτων και υπολογιστών στο ίδιο δίκτυο. Ο έλεγχος του λειτουργικού συστήματος είναι σημαντική απειλή γιατί δίνει την δυνατότητα στους διακινητές παράνομου λογισμικού να δημιουργούν στο δίκτυο ψεύτικα αποτυπώματα και εκμεταλλεύονται τη ταυτότητα του προσβλημένου υπολογιστή.

Επιπλέον ο εισβολέας εντοπίζει αδυναμίες του λειτουργικού συστήματος και τις εκμεταλλεύεται για να δημιουργήσει κερκόπορτες. Για παράδειγμα εντοπίζει αν από το λειτουργικό σύστημα λείπει μία αναβάθμιση και αναγκάζει τον υπολογιστή να προχωρήσει στην εγκατάσταση του από παραπλανητική ιστοσελίδα. Έχοντας πρόσβαση σε ένα τέτοιο υπολογιστή ο εισβολέας διερευνά την ύπαρξη πρόσβασης σε ευαίσθητα συστήματα όπως το SCADA, οι διαδικασίες και η παραγωγή. Ένας εισβολέας μπορεί να διατηρεί ταυτόχρονα πρόσβαση σε συστήματα διαφορετικών εταιριών με απώτερο σκοπό το κέρδος πουλώντας τα δεδομένα στη μαύρη αγορά. Επομένως η διαρροή εμπιστευτικών πληροφοριών τα οποία αφορούν τη λειτουργία του δικτύου, των παρόχων, των προμηθευτών και των πελατών είναι μία πολύ σοβαρή απειλή.

«αναστολέας ιστοσελίδων και εφαρμογών» (web blockers): Ο βασικός τρόπος εμπόδισης της εισβολής κακόβουλου λογισμικού στο σύστημα είναι η απαγόρευση της πρόσβασης των χρηστών σε σημεία στα οποία ενέχεται να εκτελέσουν ή να αποθηκεύσουν τοπικά κακόβουλο λογισμικό. Αυτό απαιτεί την εφαρμογή συγκεκριμένων πολιτικών στο τείχος προστασίας του δικτύου για τον έλεγχο του τι επιτρέπεται να κατεβάσουν από το ίντερνετ και τι όχι. Επιπλέον μέτρο είναι ο ορισμός μίας «λευκής» λίστας εφαρμογών που επιτρέπεται να εκτελεστεί στο δίκτυο και οποιαδήποτε άλλη εφαρμογή αποκλείεται αυτομάτως.

«διακομιστής μεσολάβησης» (proxy servers): οι διακομιστές αυτοί ελέγχουν το περιεχόμενο απομακρυσμένων ιστοσελίδων στο οποίο επιτρέπεται να έχουν πρόσβαση οι χρήστες. Οι διακομιστές ορίζουν φίλτρα περιορισμού όσο το δυνατόν περισσότερων σελίδων από τις εκατομμύρια που ορίζονται καθημερινά στον κυβερνοχώρο. Οι εταιρίες δημιουργούν τα δικά τους φίλτρα ή ζητούν την επίβλεψη τους από παρόχους ανάλογων υπηρεσιών.

«Σύστημα ανίχνευσης εισβολής» (intrusion detection system –IDS): ένα σύστημα IDS δρα στη δεύτερη ζώνη άμυνας του δικτύου καθώς νέες εισβολές ενδέχεται να μην εντοπιστούν από τη πρώτη ζώνη που περιλαμβάνει τα παραπάνω μέτρα (διακομιστές και αναστολείς περιεχομένου σελίδων και εφαρμογών). Το σύστημα IDS καταγράφει την κίνηση στο δίκτυο και ειδικότερα σε θύρες του δικτύου στις οποίες συνήθως δεν δημιουργείται επιχειρησιακή κίνηση. Στις περιπτώσεις αυτές ή σε περιπτώσεις στις οποίες ανιχνεύσει πακέτα δεδομένων που αντιστοιχούν σε κακόβουλο λογισμικό τότε αναπαράγει ειδοποιήσεις προς τους διαχειριστές. Είναι πιθανό να δημιουργηθούν και εσφαλμένες προειδοποιήσεις ελέγχοντας κάθε πιθανό σενάριο εισβολής. Οι περιπτώσεις αυτές φιλτράρονται με πιο αποτελεσματικό τρόπο αν υπάρχει συνεργασία ανάμεσα στα εργαλεία εντοπισμού κακόβουλου λογισμικού (όπως αυτά παραπάνω) και του συστήματος ανίχνευσης εισβολής. Διασταυρώνουν την γνώση που έχουν για την ύπαρξη ή όχι κακόβουλου λογισμικού για να υπολογιστεί η πιθανότητα ύπαρξης απειλής με μεγαλύτερη ακρίβεια.

Σύστημα διαχείρισης των αναβαθμίσεων ασφαλείας, εξυπηρετητών, λειτουργικών συστημάτων και εφαρμογών: το σύστημα αυτό ενημερώνει για τη τρέχουσα κατάσταση των αναβαθμίσεων, την έκδοση νέων αναβαθμίσεων και τον προγραμματισμό της εγκατάστασης τους. Οι αναβαθμίσεις αυτές προκύπτουν όταν οι κατασκευαστές λογισμικού, λειτουργικών συστημάτων και εφαρμογών ανακαλύψουν κενά ασφαλείας τα οποία πρέπει άμεσα να αντιμετωπιστούν μέσω ειδικών εκδόσεων στο πρόγραμμα τους. Επομένως οι εκδόσεις αυτές αναγκαστικά είναι επακόλουθες των απειλών κακόβουλου λογισμικού ή κενών ασφαλείας που έχουν προηγουμένως εντοπιστεί. Αποτελεί ευθύνη των κατασκευαστών λογισμικού να ενημερώνουν για κενά ασφαλείας καθώς επίσης ευθύνη των διαχειριστών να προβαίνουν στην έγκαιρη και έγκυρη εγκατάσταση τους.

Πολιτικές ελεγχόμενης πρόσβασης: οι πολιτικές αυτές περιορίζουν τη πρόσβαση προς έξω και προς τα μέσα σε ένα εξυπηρετητή μόνο σε συγκεκριμένες θύρες και υπηρεσίες του και οι οποίες είναι οι πλέον απαραίτητες. Καθώς ο εξυπηρετητής θα επικοινωνήσει με άλλους υπολογιστές στο δίκτυο για την εύρυθμη εκτέλεση μίας κοινής υπηρεσίας και αυτές οι διασυνδέσεις ελέγχονται μέσω συγκεκριμένων πολιτικών (για παράδειγμα κανόνες ορίζουν από ποιές διευθύνσεις και θύρες θα γίνεται η επικοινωνία μεταξύ τους). Λίστες δικαιωμάτων ελέγχουν την πρόσβαση των χρηστών σε υπηρεσίες των διαφόρων εξυπηρετητών του δικτύου. Ο έλεγχος γίνεται με τη συνδρομή του εξυπηρετητή καταλόγου ο οποίος ελέγχει αν ο χρήστης έχει τις απαραίτητες διαπιστεύσεις για να επικοινωνήσει μία συγκεκριμένη θύρα. Οι έλεγχοι αυτοί γίνονται σε συνεργασία του μεταγωγέα δικτύου με τον εξυπηρετητή καταλόγου. Επιπλέον παρεμβαίνει το σύστημα ανίχνευσης εισβολών για τον εντοπισμό μη συνηθισμένων πακέτων δεδομένων με βάση τους κανόνες που έχουν οριστεί.

Ο τρόπος λειτουργίας των μεταγωγέων δικτύου (switches) και του ελέγχου της πρόσβασης σε αυτό ονομάζεται διαμερισμός (segmentation). Ο διαμερισμός απομονώνει σταθμούς εργασίας χρηστών από εξυπηρετητές και εφαρμογές. Αυτό επιτρέπει τον ορισμό συγκεκριμένης κίνησης δεδομένων από το ένα διαμέρισμα στο άλλο και η κίνηση αυτή ελέγχεται από τον μεταγωγέα. Όλα τα παραπάνω μέτρα σίγουρα δεν μπορούν να αποκλείσουν εκατό τοις εκατό οποιαδήποτε απειλή, ωστόσο καθιστά τη λειτουργία του δικτύου πιο αξιόπιστη και οχυρωμένη για να αντιμετωπίσει επιθέσεις.

8.1.2. ΚΑΚΟΒΟΥΛΕΣ ΑΠΕΙΛΕΣ ΣΤΑ ΣΥΣΤΗΜΑΤΑ ΕΛΕΓΧΟΥ

Οι κύριε απειλές μέσα στα συστήματα ελέγχου είναι επιμέρους δίκτυα μέσα σε αυτή την υποδομή με δυνατότητα πρόσβασης στο ίντερνετ σε καθημερινή βάση. Εφόσον τα επιμέρους δίκτυα εκτίθενται στον κυβερνοχώρο, για παράδειγμα μέσω ξεχωριστών σημείων πρόσβασης, αυξάνουν τη πιθανότητα κάποιας απειλής. Μπορεί το τείχος προστασίας του οργανισμού να ελέγχει την κίνηση από ένα κεντρικό σημείο ωστόσο χρειάζεται να ελέγχουν επιμέρους συσκευές – μεταγωγείς του δικτύου για το πώς έχουν καταμεριστεί για να διαχωρίζουν την εξωτερική από την εσωτερική κίνηση. Επιπλέον ζήτημα είναι πως ελέγχεται η εξωτερική κίνηση: για παράδειγμα αν επιτρέπεται μέσω του συγκεκριμένου υποδικτύου η αποθήκευση ενός απομακρυσμένου αρχείου σε φορητό μέσο αποθήκευσης (USB) και το αρχείο αυτό μεταφερθεί κατόπιν σε υπολογιστή του Συστήματος Ελέγχου χωρίς προηγουμένως να φιλτραριστεί αποτελεί σίγουρα ένα κίνδυνο. Επιπλέον το φορητό μέσο αποθήκευσης ενδεχομένως να περιλαμβάνει προσωπικά αρχεία του χειριστή τα οποία επίσης δεν θα έχουν ελεγχθεί.

Ένας άλλος παράγοντας που γεννά κινδύνους είναι το γεγονός ότι οι ενημερώσεις ασφαλείας για συστήματα ελέγχου παράγονται με βραδύτερους ρυθμούς και σε λιγότερες εκδόσεις θεωρώντας τα ασφαλή και ότι προσβάλλονται σε χαμηλό βαθμό από κακόβουλο λογισμικό.

Επίσης υπάρχουν οι λεγόμενες «προγραμματισμένες» απειλές οι οποίες δοκιμάζουν να εκμεταλλευτούν μια σειρά από αδυναμίες και να εκτελέσουν την απειλή τους ως μία σειρά εντολών και σε μία εκτενή περίοδο του χρόνου έτσι ώστε να μην ανιχνευτούν από συμβατικά συστήματα ασφαλείας. Και αν αυτές αντιμετωπίζονται πλέον με πιο σύγχρονα συστήματα ασφαλείας

8.1.2.1. ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ

Για τη μείωση της επικινδυνότητας των παραπάνω παραγόντων θα πρέπει να προσδιοριστούν τα διανύσματα απειλών τα οποία σχετίζονται με συστήματα ελέγχου. Αυτά περιλαμβάνουν:

- Φορητά μέσα αποθήκευσης
- Σημεία πρόσβασης στο δίκτυο
- Σημείο πρόσβασης προμηθευτή ή κατασκευαστή
- Σημείο πρόσβασης μέσω μόντεμ
- Σημείο απομακρυσμένης πρόσβασης
- Σημείο φυσικής πρόσβασης

Ένα ερώτημα που γεννάται σε σχέση με τα παραπάνω διανύσματα απειλών είναι πώς μπορεί να εμποδιστεί η χρήση τους. Εναλλακτικά, αν ορισμένα από αυτά είναι απαραίτητο να χρησιμοποιηθούν το ερώτημα είναι πως θα εντοπιστεί η απειλή και θα υπάρξει άμεση ειδοποίηση. Για να απαντηθεί το ερώτημα το πρόβλημα μεταφέρεται σε ένα παραπάνω επίπεδο: ποιοι είναι οι κίνδυνοι για το σύστημα ελέγχου και τι μέτρα λαμβάνονται σε αυτό για την αντιμετώπιση τους.

Ένα σημαντικό μέτρο προς αυτή τη κατεύθυνση είναι η ενοποίηση των δικτύων των εμπλεκόμενων οργανισμών, λειτουργικών, παραγωγικών μονάδων και των δικτύων κεντρικής διαχείρισης. Τα δίκτυα αυτά ποτέ δεν θα λειτουργούν ως μία ενιαία οντότητα ωστόσο ανοίγοντας ειδικές θύρες και υπηρεσίες για να επιτρέπεται η απευθείας επικοινωνία ανάμεσα τους θα επιτυγχάνεται ισοδύναμο αποτέλεσμα. Η νέα αυτή υποδομή θα χρειαστεί τους κατάλληλους δρομολογητές, μεταγωγείς και άλλες τηλεπικοινωνιακές συσκευές. Οι νέες τεχνολογίες θα πρέπει να προσαρμοστούν στις απαιτήσεις των συστημάτων ελέγχου του έξυπνου δικτύου και να λάβουν υπόψη τα παραπάνω δεδομένα για να θωρακιστούν από παρόμοιου τύπου απειλές.

8.1.3. ΜΗ-ΚΑΚΟΒΟΥΛΕΣ ΑΠΕΙΛΕΣ ΣΤΑ ΣΥΣΤΗΜΑΤΑ ΕΛΕΓΧΟΥ

Οι μη κακόβουλες απειλές αποτελούν κίνδυνο για τα συστήματα ελέγχου επειδή μπορεί να προκαλέσουν μία καταστροφή ή παρενέργεια εξαιτίας κάποιου ατυχήματος. Πολλές φορές βέβαια πίσω από μία μη κακόβουλη απειλή υποβόσκει μία κακόβουλη επιχείρηση. Για παράδειγμα, μία κακόβουλη ενέργεια μπορεί να παρουσιάσει παραπλανητική πληροφορία στην οθόνη του χειριστή προκαλώντας λανθασμένες εντολές διαχείρισης της πληροφορίας. Κλειδί στην αντιμετώπιση μη κακόβουλων περιπτώσεων είναι η μείωση των λαθών από τους χειριστές και η συνεκτικότητα των διεργασιών και διαδικασιών κατά την εκτέλεση τους. Ο υπολογισμός τυχόν αποκλίσεων στο αποτέλεσμα μίας διεργασίας ανάμεσα στις διαφορετικές εκτελέσεις δημιουργεί αυτόματα κανόνες που προσδιορίζουν μία πηγή λάθους και δεν επιτρέπουν στον χειριστή να λάβει σχετικές αποφάσεις για περαιτέρω ενέργειες.

8.1.3.1. ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ

Ένα από τα μέτρα που προτείνονται στην περίπτωση αυτή είναι η εφαρμογή προτύπων αξιόπιστης εφαρμογής των απαιτούμενων διαδικασιών.

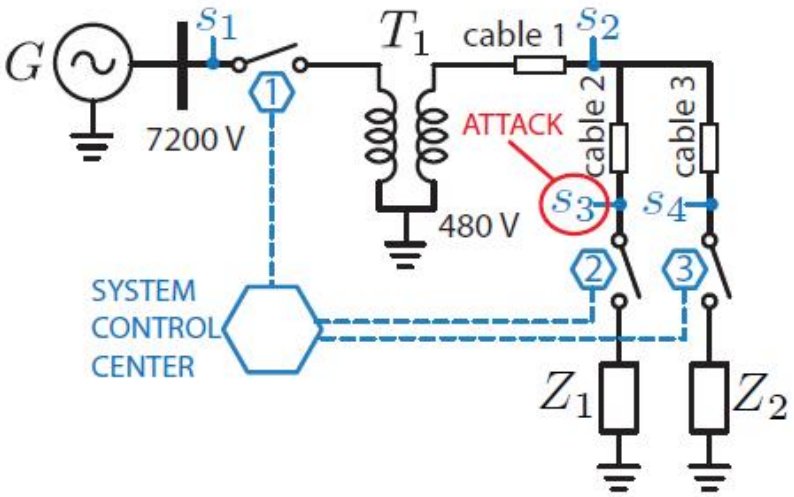
- Το πρότυπο συμμόρφωσης διαβεβαιώνει ότι τα συστήματα, και οι άνθρωποι εκτελούν τις διαδικασίες με συνεκτικό τρόπο και σύμφωνα με τους κανόνες που έχουν προσδιοριστεί από τη διαχείριση του Δικτύου.
- Το πρότυπο αντιμετώπισης εκτάκτων περιπτώσεων πιστοποιεί ότι οι χειριστές του δικτύου μεταφοράς ενέργειας έχουν σχεδιάσει, υλοποιούν και συντηρούν ένα σύνολο πλάνων για πτώση φορτίου. Τα πλάνα αυτά κατευθύνουν τον χειριστή στο να αποφασίσει πότε είναι απαραίτητη η πτώση φορτίου και ποιες ενέργειες πρέπει να εκτελέσει για την πραγματοποίηση του. Σε περίπτωση που δεν τηρηθεί το παραπάνω πρωτόκολλο τότε όχι μόνο παραβιάζεται το πρότυπο αλλά και καταγράφεται ως μη κακόβουλη απειλή.

- Σε άλλες περιπτώσεις σφάλματος το πρότυπο ασφαλείας μπορεί να απαιτεί ότι το σύστημα ελέγχου ενημερώνει αλλά και περιμένει επιβεβαίωση του συμβάντος από πολλαπλά συστήματα προτού αποφασίσει να εκτελέσει μία προβλεπόμενη ακολουθία ενεργειών. Ασφαλώς ο χρόνος αντιμετώπισης του συμβάντος παίζει σημαντικό ρόλο καθώς σε μία επείγουσα κατάσταση στην οποία πρέπει να εκτελεστούν ενέργειες σε πολύ σύντομο διάστημα πρέπει να διασφαλιστεί ότι θα έχουν συλλεχθεί όλα τα δεδομένα σε πολύ μικρότερο χρόνο.

Με λίγα λόγια η τυποποίηση των διαδικασιών εκτέλεσης προγραμματισμένων λειτουργιών και αντιμετώπισης εκτάκτων περιπτώσεων βοηθάει σημαντικά στο να αποφευχθούν αποκλίσεις εξαιτίας κακόβουλων (ή μη) ενεργειών. Κάθε απόκλιση προκαλεί προειδοποίηση την οποία μπορούν να επεξεργαστούν στο κέντρο λειτουργιών ασφαλείας σε συνάρτηση με άλλες τυχόν προειδοποιήσεις. Ο έλεγχος μίας μη κακόβουλης απειλής εμποδίζει τη γέννηση κακόβουλων κινδύνων στη πηγή τους.

Στο (Kundur et al., 2010) προτείνεται μία μεθοδολογική προσέγγιση της ανάλυσης των επιπτώσεων των επιθέσεων μέσω του κυβερνοχώρου στο Έξυπνο Δίκτυο. Η προσέγγιση αυτή προσπαθεί να ποσοτικοποιήσει και να κατηγοριοποιήσει τις επιπτώσεις των επιθέσεων έτσι ώστε να μπορεί να εντάξει και το βαθμό επίπτωσης στην παραγωγή ενέργειας. Το τελευταίο αποτελεί σημαντικό παράγοντα στην εκτίμηση αδυναμιών στο Δίκτυο. Η προσέγγιση των Kundur et al. (2010) βασίζεται στην εφαρμογή θεωρίας γράφων και δυναμικού προγραμματισμού (μοντελοποίησης) για τον ορισμό σχέσεων μεταξύ των φυσικών συστημάτων ενέργειας στον ευρύτερο κυβερνο χώρο. Οι σχέσεις αυτές αλλάζουν δυναμικά κατάσταση μέσα στον χρόνο κάτι που καθιστά απαραίτητο τη χρήση μοντελοποίησης.

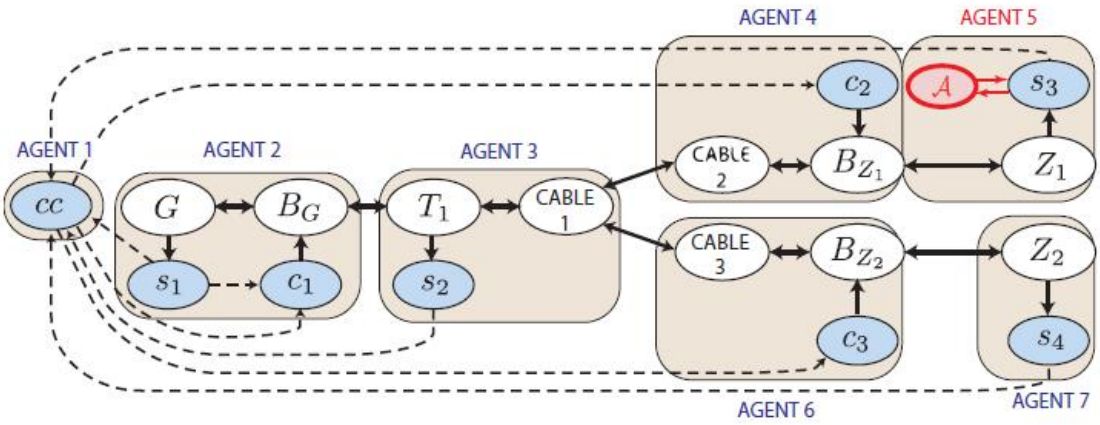
Η διατύπωση δυναμικών συστημάτων βασισμένα σε γραφήματα καθοδηγεί την ανάλυση των επιπτώσεων των διαφόρων κυβερνο επιθέσεων καθώς συσχετίζουν μία κυβερνο επίθεση σε φυσικές επιπτώσεις στο ίδιο το δίκτυο. Επιπλέον οι ακμές του γραφήματος συμβολίζουν σήματα ελέγχου που επιτρέπουν τη διασύνδεση φυσικών και κυβερνο-συστημάτων. Η διασύνδεση αυτή ορίζεται ως μία ακμή η οποία ενεργοποιείται όταν δημιουργείται μία τιμή από τον αντίστοιχο αισθητήρα του φυσικού δικτύου και πρέπει να τη μεταδώσει στον κυβερνοχώρο.



Εικόνα 20, διάγραμμα στο οποίο απεικονίζεται επίθεση αλλοίωσης του αισθητήρα s3 με σκοπό τη παραποίηση των αποφάσεων διαχείρισης φορτίων από το κέντρο ελέγχου [9]

Στο παράδειγμα της εικόνας 20 αποτυπώνεται η μοντελοποίηση μίας κυβερνο επίθεσης. Τυπικά σκοπός μίας τέτοιας επίθεσης είναι να μοχλεύσει έναν από τους αισθητήρες με σκοπό να αλλοιώσει τις μετρήσεις του και συνεπώς τη λήψη αποφάσεων σχετικά με τη

μετάδοση φορτίων ενέργειας. Όπως φαίνεται και σε ένα επιπρόσθετο παράδειγμα, η προσέγγιση αυτή καταφέρνει να αποτυπώσει μία ενιαία άποψη για τη κατάσταση στο φυσικό και το κυβερνο-δίκτυο τη στιγμή της επίθεσης. Οι κόμβοι αποτελούνται από γεννήτριες G, διασπαστές των κυκλωμάτων Bi, ένα μετασχηματιστή T, φορτία/δυναμικά υβρίδια Zi του ηλεκτρολογικού δικτύου, κέντρο ελέγχου cc, αισθητήρες si, και κέντρα εκτέλεσης εντολών ci, στον κυβερνοχώρο. Οι ακμές αναπαριστούν εξαρτήσεις μεταξύ καταστάσεων κατά την δυναμική μοντελοποίηση. Στο παράδειγμα της εικόνας 21, ο εισβολέας επιτίθεται στον αισθητήρα s3.



Εικόνα 21, γράφημα απεικόνισης του ηλεκτρολογικού δικτύου και κυβερνο χώρου [9]

Ο Skopik στο (Skopik et al., 2012) εντοπίζει επίσης μία σειρά από αδυναμίες στις συσκευές και στην επικοινωνία μεταξύ τους, στη διαχείριση των μυστικών κλειδιών, στην αναβάθμιση του λειτουργικού συστήματος των συσκευών, ευπάθειες στους μετρητές και άλλες συσκευές, και ευπάθειες στις εφαρμογές.

Ευπάθειες στους μικροελεγκτές εντοπίζονται καθώς ο σχεδιασμός τους ισοσταθμίζει το κόστος (με σκοπό να είναι όσο το δυνατότερο πιο φθηνοί) με την ασφάλεια. Αυτό κάνει το σύστημα κρυπτογράφησης πιο ευπαθές καθώς τα κλειδιά αλλάζουν περιοδικά και είναι πιο εύκολο να αναγνωριστούν. Αδύναμες υλοποιήσεις των γεννητριών τυχαίων αριθμών οδηγούν στην δημιουργία εύκολα προβλέψιμων αριθμών το οποίο πάλι επηρεάζει το σύστημα κρυπτογράφησης. Σύγχρονες τεχνολογίες όπως η ράδιο επικοινωνία σε κοντινό χώρο (Near Field Radio Communication) και η οποία έχει δοκιμαστεί για την ασφάλεια της δεν μπορεί να χρησιμοποιηθεί σε φθηνές συσκευές εξαιτίας των περιορισμών στη κατανάλωση ενέργειας.

Το μεγαλύτερο μέρος των σύγχρονων μετρητών δεν μπορεί να ανταποκριθεί στην ενσωμάτωση πολύπλοκων τεχνικών διαχείρισης κλειδιών και ούτε υπάρχει σχεδιασμός προστασίας τους μέσα στη συσκευή. Πολύπλοκες αρχιτεκτονικές οι οποίες περιλαμβάνουν μετρητές, κόμβους συσσώρευσης ισχύος, και εξυπηρετητές υποστήριξης απαιτούν ενιαίο τρόπο διαχείρισης κλειδιών μεταξύ τους. Η διανομή των κλειδιών με απομακρυσμένο τρόπο όπως στη περίπτωση της PKI τεχνικής μετρά τις αντοχές των συσκευών αυτών γιατί απαιτεί μεγάλη υπολογιστική απόδοση. Επιπλέον όλη αυτή τη διαχείριση του μηχανισμού διάδοσης και εγκατάστασης κλειδιών θα τη χειριστούν άνθρωποι, επομένως και αυτοί πρέπει να περάσουν από διαδικασίες ελέγχου.

Μία άλλη πρόκληση για τον σχεδιασμό των συσκευών είναι η ασφάλεια του λειτουργικού τους συστήματος. Θα πρέπει να υπάρχει βασική μέριμνα ασφάλειας της μνήμης της συσκευής και του κώδικα εκτέλεσης σε αυτή το οποίο πάλι έρχεται σε σύγκρουση με την απαιτούμενη ισχύ σε επεξεργασία και κατανάλωση ενέργειας.

Σε επίπεδο δικτύου θα πρέπει να εξεταστεί ένας ορθολογικός σχεδιασμός των εκάστοτε τοπολογιών και της διασύνδεσης μεταξύ τους. Απαιτείται τακτική εκτέλεση δοκιμών διείσδυσης (penetration testing), αξιολόγηση από εξωτερικούς, επίσημους φορείς, και η διαθεσιμότητα ισχυρών μηχανισμών ταυτοποίησης, εξουσιοδότησης χρηστών και κρυπτογράφησης. Ένα ιεραρχικό μοντέλο σχεδιασμού στο οποίο είναι διακριτά τα όρια μεταξύ των επιπέδων λειτουργίας βοηθά στην ελαχιστοποίηση και την απομόνωση των εισβολών. Με τον ίδιο τρόπο θα πρέπει να καθιερωθούν μηχανισμοί άμεσης απομόνωσης/αφαίρεσης από το δίκτυο των συσκευών που έχουν αλλοιωθεί από εισβολείς. Για τις ίδιες τις συσκευές απαιτείται ένας πιο ορθολογικός σχεδιασμός λαμβάνοντας υπόψη ότι επόμενες γενιές πρωτοκόλλων και μηχανισμών ασφάλειας, ενημέρωσης του λειτουργικού τους απαιτούν μεγαλύτερη υπολογιστική ισχύ και κατανάλωση.

8.2. ΠΡΟΛΗΠΤΙΚΑ ΜΕΤΡΑ ΜΕΙΩΣΗΣ ΑΡΝΗΤΙΚΩΝ ΕΠΙΔΟΣΕΩΝ Ή ΠΙΘΑΝΟΤΗΤΑ ΑΠΕΙΛΗΣ

8.2.1. ΕΓΚΑΙΡΗ ΑΝΑΛΥΣΗ ΣΥΜΒΑΝΤΟΣ

Ο προσδιορισμός ενός συμβάντος, είτε ως κακόβουλη ή μη κακόβουλη απειλή, είναι απαραίτητος για την ενίσχυση της αξιοπιστίας του δικτύου. Τυπικά συμβάντα που σχετίζονται με κακόβουλες απειλές είναι διαχειρίσιμα από το προσωπικό που είναι υπεύθυνο για τη κυβερνο-ασφάλεια, ενώ μη κακόβουλα περιστατικά είναι αντιμετωπίσιμα από τους χειριστές του κέντρου ελέγχου. Η ανταλλαγή τεχνογνωσίας και εκπαίδευση καθώς και η σύγκληση των διαδικασιών των δύο τομέων είναι απαραίτητα για την αποτελεσματικότερη αντιμετώπιση ποικίλλων απειλών. Για παράδειγμα, το προσωπικό στο τομέα της κυβερνο-ασφάλειας θα εκπαιδευτεί στον προσδιορισμό διαφορετικού τύπου συμβάντων ενώ το προσωπικό του κέντρου ελέγχου θα εκπαιδευτεί στη διαχείριση προειδοποιητικών μηνυμάτων που συσχετίζονται. Η κατανόηση προειδοποιητικών μηνυμάτων για επιθέσεις άρνησης υπηρεσίας θα βοηθήσει για την καλύτερη δυνατή αντίληψη των επιπρόσθετων επιδράσεων που ακολουθούν στα υπόλοιπα συστήματα [3], [4], [5], [7], [9], [13] & [15].

8.2.2. ΑΠΟΜΟΝΩΣΗ ΣΥΜΒΑΝΤΟΣ

Ένα συμβάν πρέπει άμεσα να απομονωθεί είτε πρόκειται για κακόβουλη απειλή ή μη κακόβουλο κίνδυνο. Ο σκοπός της απομόνωσης του συμβάντος είναι ο τερματισμός της απειλής και η συνέχιση της λειτουργίας του συστήματος. Μία ανάλυση της αιτίας που προκάλεσε τον κίνδυνο θα βοηθήσει στο τι προκάλεσε την απειλή και γιατί. Απαντώντας σε αυτά τα ερωτήματα είναι χρήσιμο στο να προσδιοριστούν ενέργειες αντιμετώπισης της απειλής σε μόνιμη βάση.

Μία επίθεση άρνησης της υπηρεσίας ενός μεταγωγέα στο δίκτυο ελέγχου θα έχει σαν αποτέλεσμα τα συστήματα που λειτουργούν σε αυτό το δίκτυο να μην μπορούν να λειτουργήσουν. Το πρόβλημα γίνεται ακόμη δυσχερέστερο αν αφορά τον βασικό μεταγωγέα του δικτύου ο οποίος μεσολαβεί σε όλες τις IP επικοινωνίες μηνυμάτων. Επιπλέον κάποια από τα συστήματα εξαρτώνται από άλλα συστήματα για να μπορέσουν να λειτουργήσουν. Εφόσον η πληροφορία δεν φθάνει στον πίνακα ελέγχουν δεν μπορούν οι χειριστές να έχουν εικόνα της επίθεσης και ποια μέρη της πληροφορίας έχουν επηρεαστεί. Οι υπεύθυνοι ασφαλείας θα πρέπει να αφαιρέσουν όλες τις φυσικές διασυνδέσεις προς τον μεταγωγέα ή την πύλη του δικτύου. Η τακτική αυτή θα καθαρίσει το δίκτυο από τα πακέτα που μεταδίδονταν στη διάρκεια της επίθεσης και θα δώσει χρόνο στον ειδικό της ασφάλειας να επαναπρογραμματίσει τη συσκευή, και να της αλλάξει IP διεύθυνση για να μην είναι πλέον στόχος.

Κατόπιν παραμένει το πρόβλημα εντοπισμού της πηγής από την οποία εκπέμπονται τα κακόβουλα δεδομένα. Λογισμικό παρακολούθησης των πακέτων που μεταδίδονται στο δίκτυο είναι χρήσιμο για τον εντοπισμό ύποπτων επικοινωνιών. Οι ροές αυτές θα διακοπούν αναζητώντας κατόπιν τα κακόβουλα αρχεία που προκαλούν τις επικίνδυνες ροές. Σχετικές στρατηγικές αντιμετώπισης προβλέπουν τη διαγραφή κακόβουλων αρχείων ή ακόμη και την επανεγκατάσταση του συστήματος για την εκκένωση του από προηγούμενα αρχεία. Η τελική

ανάλυση της αίτιας πηγής του προβλήματος θα προβάλει τις αδυναμίες στην ασφάλεια του δικτύου όπως για παράδειγμα η απουσία μέτρων προστασίας από κακόβολο κώδικα σε κάθε σταθμό εργασίας ή και το γεγονός ότι επιτρέπεται η χρήση φορητών μέσων αποθήκευσης. Επομένως οι στρατηγικές αντιμετώπισης αυτών των κινδύνων περιλαμβάνουν πολιτικές απαγόρευσης της χρήσης φορητών μέσων στους σταθμούς εργασίας ή η εγκατάσταση ανιχνευτών κακόβουλου κώδικα σε κάθε σταθμό εργασίας. Και βέβαια η μη επανάληψη παρόμοιων συμβάντων μετά την ενεργοποίηση των παραπάνω μέτρων και πολιτικών αυξάνει την αξιοπιστία του συστήματος [3], [4], [5], [7], [9], [13] & [15].

8.3. ΜΕΤΡΑ ΑΝΑΚΑΜΨΗΣ ΑΠΟ ΚΑΤΑΣΤΡΟΦΕΣ

Τυπικά το Έξυπνο Δίκτυο δεν εφαρμόζει κεντρική διαχείριση αλλά την κατανέμει σε περιφέρειες έτσι ώστε μία μεγάλη απειλή να απειλήσει μόνο μία περιφέρεια και απομονωμένα από τις άλλες. Για να μπορέσει μία επίθεση να απειλήσει όλες τις περιφέρειες θα πρέπει να είναι πολύ καλά ορχηστρωμένη. Η επίθεση αυτή θα πρέπει να χτυπήσει ταυτόχρονα όλα τα συστήματα ελέγχου των περιφερειακών δικτύων. Ενώ η παρακολούθηση των υποδικτύων βοηθά στην άμεση αντιμετώπιση του ζητήματος και την αποφυγή πρόωρου τερματισμού του συστήματος και των επιμέρους διασυνδέσεων, υπάρχει η πιθανότητα πρόκλησης εμποδίων στις παραγωγικές μονάδες ή στο δίκτυο μετρητών μίας περιοχής της πόλης. Έτσι θα δημιουργηθεί η εικόνα ενός μη ασταθούς συστήματος στη περιφέρεια του και μπορεί να επηρεάσει όλη τη βιομηχανική αλυσίδα.

Οι διαχειριστές του Δικτύου γνωρίζουν ότι θα συμβούν αμέτρητα συμβάντα που θα θέτουν σε κίνδυνο τη αδιάλειπτη λειτουργία του. Οι διαχειριστές θα πρέπει να έχουν προετοιμάσει πλάνα αντιμετώπισης απρόοπτων και να τα δοκιμάζουν τακτικά έτσι ώστε να είναι πανέτοιμοι για να αντιμετωπίσουν πραγματικές καταστάσεις. Οι παραδοσιακοί πάροχοι έχουν εμπειρία σε βάθος για τέτοιου είδους συμβάντα. Καθώς δίνουν έμφαση στην αξιοπιστία συνήθως διατηρούν περισσότερα από ένα εναλλακτικά συστήματα. Για παράδειγμα αν συμβεί πτώση φορτίου σε μία περιφέρεια ο πάροχος της γνωρίζει από πού να προμηθευτεί άμεσα φορτίο για να καλύψει την απώλεια.

Μία κυβερνο-καταστροφή για το Δίκτυο θεωρείται η πτώση φορτίου σε μία ή περισσότερες περιφέρειες και δεν υπάρχει αρκετό φορτίο για να καλύψει την απώλεια. Η παραβίαση του δικτύου και η απενεργοποίηση οικιακών μετρητών μπορεί να προκαλέσει ένα συμβάν μετάπτωσης φορτίου. Αυτός που πραγματοποιεί την επίθεση σκοπεύει στο να αποκτήσει πρόσβαση στην δικτυακή υποδομή των οικιακών μετρητών προκαλώντας μία αλυσιδωτή αντίδραση μετάπτωσης φορτίου. Επιπλέον στρεσάρει το δίκτυο διανομής γιατί μπορεί να προκαλέσει αυτόματη ενεργοποίηση των μετρητών και μεγάλη ζήτηση για φορτίο σε πολύ μικρό χρονικό διάστημα. Βέβαια αυτό μπορεί να συμβεί σε μία συγκεκριμένη περιοχή και στο καλύτερο δυνατό σενάριο δεν θα επηρεάσει ολόκληρο το δίκτυο. Στο χειρότερο δε σενάριο θα καταφέρει ο εισβολέας να προκαλέσει μία ενορχηστρωμένη επίθεση σε διαφορετικά υποδίκτυα και να συμβεί πτώση φορτίου σε πολλές περιοχές αν όχι σε όλο το δίκτυο. Ακόμη και σε ένα καθολικό μπλακ άουτ το σύστημα θα επανέρθει αλλά μετά από μεγάλο χρονικό διάστημα.

Οι πάροχοι έχουν την ευθύνη επαναφοράς του συστήματος σε καθεστώς πλήρους λειτουργίας σε περίπτωση απώλειας φορτίου. Ένα πλάνο επαναφοράς μεταφράζεται σε μία σειρά διαδικασιών έκτακτης ανάγκης. Οι πάροχοι διατηρούν επίσης ένα πλάνο μηδενικής αφετηρίας (blanc start capability) το οποίο ενεργοποιείται όταν χαθεί ολόκληρο το φορτίο. Επιπλέον ένα τέτοιο συμβάν προκαλεί και ένα πλάνο αντιμετώπισης της απειλής προκαλώντας να ερμηνεύσει και τη πηγή του προβλήματος για να μη συμβεί ξανά. Μόνο έτσι μπορεί να αποτραπεί το ίδιο συμβάν να μη συμβεί ξανά. Για παράδειγμα αν παρθεί η απόφαση να επανακτηθεί η λειτουργία του συστήματος πριν εντοπιστεί η αιτία του προβλήματος αυτό θα ξανασυμβεί.

Η διαχείριση τέτοιων συμβάντων επιβάλει την εκτίμηση του μέτρου επίπτωσης. Αν ένας σταθμός παραγωγής τεθεί εκτός η επίπτωση μπορεί να εκτιμηθεί ως χαμηλή. Αν όμως δύο ή

περισσότεροι σταθμοί τεθούν εκτός τότε η επίπτωση θεωρείται μεσαίου επιπέδου. Για τον υπολογισμό της επίπτωσης ανά σημαντικό πόρο του Δικτύου είναι χρήσιμη η εφαρμογή της μεθοδολογίας εκτίμησης κινδύνων (Risk Based Assessment Methodology - RBAM).

9. ΣΥΜΠΕΡΑΣΜΑΤΑ

Το Έξυπνο Δίκτυο παραθέτει νέες προκλήσεις για την Ασφάλεια. Φαίνεται από τα παραπάνω ότι οι τυπικές λύσεις Ασφάλειας που εφαρμόζονται σε παραδοσιακά ΙΤ δίκτυα δεν μπορούν να εφαρμοστούν αποτελεσματικά σε Δίκτυα Ηλεκτρισμού. Οι στόχοι της Ασφάλειας είναι διαφορετικοί στο κάθε τομέα με την έννοια ότι ασφάλεια ΙΤ δικτύων στοχεύει στην εφαρμογή τριών αρχών: εμπιστευτικότητα, ακεραιότητα, και διαθεσιμότητα ενώ η ασφάλεια σε δίκτυα Ηλεκτρισμού συμβολίζει την ανθρώπινη ασφάλεια, προστασία των γραμμών ηλεκτρισμού και του εξοπλισμού, και λειτουργία του συστήματος, πέρα από την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα.

Επιπλέον, η αρχιτεκτονική ασφάλειας στα ΙΤ δίκτυα είναι διαφορετική από τα άλλα δίκτυα καθώς η ασφάλεια πετυχαίνεται παρέχοντας προστασία στο κέντρο του δικτύου ενώ στα δίκτυα ηλεκτρισμού η ασφάλεια πετυχαίνεται στο κέντρο του δικτύου και στα άκρα του. Καθώς επίσης η τοπολογία είναι διαφορετική τα ΙΤ δίκτυα χρησιμοποιούν ένα συγκεκριμένο σύνολο λειτουργικών συστημάτων και πρωτοκόλλων ενώ τα δίκτυα ηλεκτρισμού χρησιμοποιούν πολλαπλά λειτουργικά συστήματα και πρωτόκολλα εξειδικευμένα στους προμηθευτές. Επιπλέον οι μετρικές Ποιότητας Υπηρεσιών είναι διαφορετικές με την έννοια ότι στα ΙΤ δίκτυα είναι αποδεκτό να επανεκινηθούν οι συσκευές σε περίπτωση αποτυχίας ή αναβάθμισης ενώ στα άλλα δίκτυα η υπηρεσία πρέπει να είναι διαθέσιμη 24/7.

Οι παραπάνω διαφορές απαιτούν την εφαρμογή νέων λύσεων ασφαλείας στο Έξυπνο Δίκτυο Ηλεκτρισμού.

1. Αυστηρή ταυτοποίηση: η αναγνώριση χρηστών, εξοπλισμού και απαιτεί αυστηρούς μηχανισμούς ταυτοποίησης. Οι οργανισμοί θα πρέπει να υλοποιήσουν μία Πολιτική Άρνησης έτσι ώστε πρόσβαση στο δίκτυο θα πρέπει να δοθεί σε όσους έχουν σαφή δικαιώματα πρόσβασης
2. Προστασία από κακόβουλα προγράμματα σε Ενσωματωμένα και Γενικού Σκοπού Συστήματα. Μέσω μηχανισμών κλειδιών για την επικύρωση λογισμικού τα Ενσωματωμένα Συστήματα πρέπει να επικυρώνουν τη γνησιότητα προγραμμάτων πριν την εγκατάστασης τους. Ενώ τα Γενικού Σκοπού Συστήματα επιδέχεται να χρησιμοποιήσουν προγράμματα τρίτων. Για το λόγο αυτό θα πρέπει να έχουν προηγουμένως εξασφαλίσει αντιικά προγράμματα και προγράμματα παρεμπόδισης εισβολών.
3. Σύστημα παρεμπόδισης εισβολών στο δίκτυο όπως και Σύστημα ανίχνευσης εισβολών στο σύστημα είναι τεχνολογίες σε επίπεδο εξυπηρετητή που θα παρέχουν προστασία από έξω προς τα μέσα και το αντίστροφο.
4. Εκτίμηση των ευπαθειών πρέπει να εκτελεστεί ετήσια για να διασφαλιστεί ότι τα στοιχεία τα οποία έχουν διεπαφή με τη περίμετρο είναι ασφαλή.
5. Εκπαίδευση των χρηστών για την χρήση δικτυακών εργαλείων και εφαρμογών θα βοηθήσει στην αποφυγή σχετικών αδυναμιών.
6. Οι συσκευές πρέπει να γνωρίζουν τις πηγές και τους προορισμούς των επικοινωνιών στις οποίες εμπλέκονται. Αυτό διασφαλίζεται με τη χρήση αμοιβαίων τεχνικών ταυτοποίησης οι οποίες χρησιμοποιούν Ασφάλεια σε Επίπεδο Μεταφοράς (TLS) ή Ασφάλεια στο Επίπεδο του ίντερνετ πρωτοκόλλου (IPSec).
7. Οι συσκευές θα πρέπει να υποστηρίζουν αρχιτεκτονικές εικονικών δικτύων (VPN) για ασφαλή επικοινωνία
8. Οι συσκευές θα πρέπει να χρησιμοποιούν την Υποδομή Δημόσιου Κλειδιού (PKI) για ασφαλή επικοινωνία. Θα πρέπει να ληφθούν υπόψη οι περιορισμοί σε κρυπτογραφία και διαχείριση κλειδιών: οι τρέχουσες συσκευές δεν διαθέτουν επαρκή ισχύ και χώρο αποθήκευσης για να εκτελέσουν πιο πολύπλοκες τεχνικές κρυπτογράφησης και ταυτοποίησης.

9. Από όλα τα δεδομένα που μεταφέρονται οι διάφοροι πόροι πρέπει να κρατήσουν μόνο τα δεδομένα που χρειάζονται για να πετύχουν τους στόχους τους.
10. Οι μηχανικοί ασφάλειας IT δικτύων και του συστήματος ελέγχου πρέπει να εμπλακούν εξίσου στην ασφάλεια του Έξυπνου Δικτύου.
11. Η ασφάλεια πρέπει να είναι μέρος του Σχεδιασμού του Δικτύου, διαφορετικά θα αποτελεί ευθύνη μόνο του κατασκευαστή και οι όποιες ευπάθειες θα θεωρηθούν ασυμβατότητες.
12. Οι πάροχοι θα πρέπει να λάβουν σοβαρά υπόψη την απασχόληση εταιριών τηλεπικοινωνιών. Οι εταιρίες αυτές μπορούν να βοηθήσουν στη διαχείριση της επικοινωνίας και ζητημάτων ασφαλείας στη μεταφορά δεδομένων.
13. Ένα συμπαγές πρωτόκολλο ταυτοποίησης είναι απαραίτητο για την επικοινωνία μεταξύ των εμπλεκόμενων μερών στο Έξυπνο Δίκτυο.

Τίθενται επίσης η ανάγκη επέκτασης της έρευνας ως προς την υλοποίηση ενός πλήρους και κατανοητού πλαισίου μοντελοποίησης κινδύνων και κυβερνο-ασφάλειας (Govindarasu et al, 2012). Όπως αναφέρθηκε παραπάνω θα πρέπει η δυναμική του φυσικού συστήματος να συσχετίζεται με τα λειτουργικά μέρη του δικτύου ελέγχου που λειτουργεί στον κυβερνο-χώρο. Τα μοντέλα αυτά θα επιτρέψουν τον ποσοτικό ορισμό των επιπτώσεων των κυβερνο επιθέσεων όσον αφορά την απώλεια φορτίου, παραβίαση της σταθερότητας, καταστροφή εξοπλισμού και οικονομικές απώλειες.

Είναι επίσης ορατή η ανάγκη υλοποίησης εξειδικευμένων αλγορίθμων οι οποίοι καλούνται να προστατέψουν το Δίκτυο από διαφόρων μορφών κυβερνο-επιθέσεις (άρνηση εξυπηρέτησης, εισβολή στο δίκτυο, εκτέλεση κακόβουλων προγραμμάτων, απομονωμένες και καλά ενορχηστρωμένες επιθέσεις). Τα μέτρα που θα ληφθούν θα πρέπει να υπολογίσουν επιθέσεις από το εξωτερικό της περιμέτρου, το εσωτερικό δίκτυο και λειτουργικά σφάλματα. Θα πρέπει επίσης να θεωρήσουν στη χειρότερη περίπτωση ότι σκοπός των κακόβουλων επιθέσεων είναι η πρόκληση καταστροφή και ότι ο εισβολέας έχει γνώση κυβερνο-ασφάλειας αλλά και γνώση του τρόπου λειτουργίας των στοιχείων του δικτύου.

Τέτοιοι αλγόριθμοι μπορεί να είναι (Govindarasu et al., 2012):

1. Αλγόριθμοι μετρίασης του κινδύνου κυβερνο-επιθέσεων: μέσω συσχέτισης σε πραγματικό χρόνο μαζικών ροών δεδομένων και καταγραφών δεδομένων (data logs) τα οποία παρέχονται από τους υποσταθμούς και κέντρων ελέγχων. Απαιτεί παρακολούθηση, καταγραφή και ανάλυση σε πραγματικό χρόνο.
2. Αλγόριθμοι μοντελοποίησης του τρόπου παρακολούθηση, προστασίας και ελέγχου κυβερνο επιθέσεων: ανάλυση της σταθερότητας σε περίπτωση επιθέσεων (πχ τι συμβαίνει σε περίπτωση άρνησης εξυπηρέτησης και έχει ως συνέπεια τη καθυστερημένη ή και καθόλου άφιξη σημάτων ελέγχου, επιθέσεις αποστολής αντιγράφων των γνήσιων σημάτων κλπ) και του βαθμού αντοχής. Σημαντικές λειτουργίες του Δικτύου (Αυτόματος Έλεγχος Παραγωγής, έλεγχος Τάσης, και λειτουργίες προστασίας) απαιτούν μοντελοποίηση και ανάλυση του τρόπου αντιμετώπισης αυτών των επιθέσεων.
3. Αλγόριθμοι φυσικής και κυβερνο άμυνας οι οποίοι εμποδίζουν, ανιχνεύουν, και αντέχουν σε κυβερνο επιθέσεις στο Δίκτυο. Οι αλγόριθμοι αυτοί συνδυάζουν τεχνικές κυβερνο άμυνας (επαναδρομολόγηση, διαμερισμός δικτύου) με τις τεχνικές άμυνας στη παραγωγή ενέργειας (μεταβολή ρυθμού παραγωγής, άμεση διανομή ενέργειας αν ζητηθεί, πτώση φορτίου και ελεγχόμενος διαχωρισμός του δικτύου).
4. Μοντελοποίηση συντονισμένων κυβερνο επιθέσεων: λαμβάνονται υπόψη οι χρονικές και χωροταξικές πλευρές των επιθέσεων και οι απαιτήσει για τον ελάχιστο βαθμό αξιοπιστίας του συστήματος.
5. Ένα πλαίσιο επίγνωσης της κατάστασης του συστήματος σε πραγματικό χρόνο: το πλαίσιο αυτό πρέπει να συσχετίζεται με μία αρχιτεκτονική ασφάλειας για άμεση διαθεσιμότητα πληροφορίας όπως ειδοποιήσεις ασφαλείας και μέτρα αντιμετώπισης, εργαλεία εκτέλεσης ανάλυσης του κινδύνου σε πραγματικό χρόνο (καταγραφή

ύποπτων ενεργειών, εισβολών και του βαθμού σοβαρότητας τους) και να παρέχει δυνατότητες γραφικής απεικόνισης και ελέγχου στους χειριστές και τους διαχειριστές.

Επιπρόσθετα τονίζεται η ανάγκη εφαρμογής προτύπων και πολιτικών επιπλέον των εργαλείων και πρακτικών που ακολουθούνται ως τώρα (Govindarasu et al., 2012):

Τα υπάρχοντα πρότυπα όπως το CIP του ινστιτούτου NERC θα πρέπει να εμπλουτιστούν με νέα πρότυπα για να εγγυηθούν επαρκή ασφάλεια απέναντι σε απειλές οι οποίες συνεχώς εξελίσσονται. Τα τωρινά πρότυπα λαμβάνουν υπόψη το στόχο της αποφυγής δημιουργίας κινδύνων για τα κεντρικοποιημένα υποσυστήματα του δικτύου ενώ ανέχονται την δυσκολία εξυπηρέτησης τοπικών δικτύων και μετρητών. Ωστόσο η δυσαρέσκεια των πελατών και η παραβίαση της ιδιωτικότητας τους είναι σημαντική παράγοντες οι οποίοι μπορεί να επιβραδύνουν την εξέλιξη του δικτύου. Για το λόγο αυτό θα πρέπει να καθιερωθούν περισσότερο τυποποιημένες μέθοδοι συλλογής και χρήσης δεδομένων ακόμη και σε τοπικό επίπεδο.

Επιπλέον έμφαση δίνεται στην ενίσχυση του λογισμικού που είναι υπεύθυνο για την εφαρμογή ελέγχων στο δίκτυο. Ειδικά εφόσον το λογισμικό αυτό και οι συνοδευτικές συσκευές είναι προϊόντα τρίτων θα πρέπει να επιλεχθούν όσα διαθέτουν επαρκή χαρακτηριστικά όσον αφορά την ασφάλεια. Για παράδειγμα, στην τεχνολογία λογισμικού έχουν καθιερωθεί πρότυπα με κοινά κριτήρια αξιολόγησης της ποιότητας του λογισμικού. Τέτοια πρότυπα μπορούν να ενσωματωθούν και στη ποιοτική αξιολόγηση των προγραμμάτων που εκτελούνται στο Δίκτυο (Govindarasu et al., 2012).

Ένας επιπλέον σημαντικός παράγοντας της ενίσχυσης της ασφάλειας του δικτύου είναι η σύναψη συμπράξεων δημοσίου ιδιωτικού τομέα (ΣΔΙΤ) στον τομέα της ενέργειας. Οι συμπράξεις αυτές ενδυναμώνουν τις καθημερινές λειτουργίες στο δίκτυο και την ανταλλαγή πληροφοριών για αναδυόμενων απειλών. Η σύμπραξη από μόνη της δεν είναι αρκετή αν δεν συνοδεύεται από νέες προσεγγίσεις ανταλλαγής πληροφοριών σχετικά με απειλές. Οι απαιτήσεις ασφάλειας για μελλοντικές προσεγγίσεις συγκεντρώνονται στον πίνακα 6:

	Ασφάλεια Πληροφοριών	Ασφάλεια Υποδομών	Ασφάλεια Εφαρμογών
Ανάγκες	• Προστασία Πληροφοριών o Εμπιστευτικότητα o Ακεραιότητα o Διαθεσιμότητα o Ταυτοποίηση o Μη -απάρνηση	• Προστασία Υποδομής o Δρομολογητές o Εξυπηρετητές διαχείρισης ονομασίας τομέων (DNS) o Σύνδεσμοι o Πρωτόκολλα ίντερνετ	• Εφαρμογές ελέγχου παραγωγής • Εφαρμογές ελέγχου μεταφοράς • Εφαρμογές ελέγχου διανομής • Αγορές ενέργειας πραγματικού χρόνου

Μέσα	• Κρυπτογράφηση/αποκρυπτογράφηση • Ψηφιακή υπογραφή • Κωδικοί ταυτοποίησης μηνυμάτων • Υποδομή Δημόσιου Κλειδιού	• Τοίχοι προστασίας • Ανίχνευση εισβολής • Ασφαλή πρωτόκολλα • Πρωτόκολλα ταυτοποίησης • Κατηγοριοποίηση επίθεσης • Εξυπηρετητές ασφάλειας	• Αλγόριθμοι ελέγχου ανεκτικοί σε επιθέσεις • Αλγόριθμοι μοντελοποίησης o Ανωμαλιών o Ανοχή εισβολής o Περιορισμός κακόβουλων δεδομένων • Μοντελοποίηση κινδύνων και μετρίαση

Πίνακας 6,απαιτήσεις ασφάλειας για μελλοντικά πρότυπα και πολιτικές [6]

Επομένως η ανάπτυξη ισχυρών τεχνικών μοντελοποίησης κινδύνων απαιτούνται για να ποσοτικοποιηθούν κίνδυνοι από πλευράς φυσικής και κυβερνο ασφάλειας. Βελτιωμένα μέτρα μετρίασης των κινδύνων απαιτούνται επίσης δίνοντας έμφαση στους τομείς των υποδομών και των εφαρμογών. Ειδικά, αλγόριθμοι ελέγχου της ανεκτικότητας σε επιθέσεις, καταγραφής και προστασίας θα πρέπει να υλοποιηθούν εκμεταλλευόμενοι τη γνώση του συστήματος που έχει συσσωρευθεί. Τέλος, πληροφορία που να αφορά κινδύνους θα πρέπει να είναι διαθέσιμη σε χειριστές και διαχειριστές μέσω της υλοποίησης μίας υποδομής αντίληψης της τρέχουσας κατάστασης και σε πραγματικό χρόνο. Η υποδομή αυτή θα πρέπει να διασυνδέεται με υποσυστήματα παρακολούθησης και άμεσης ανταπόκρισης κατά την εμφάνιση μίας απειλής.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Baumeister, T., 2010.*Literature Review on Smart Grid Cyber Security*. Honolulu: UniversityofHawai.

[2] Skopik, F., Maa, Z., Bleiera, T. and Grüneisb, H., 2012.A Survey on Threats and Vulnerabilities in Smart Metering Infrastructures. *International Journal of Smart Grid and Clean Energy*, July Issue, 2012, p.7.

[3] Fouda, M., Fadlullah, Z. Md., Kato, N., Lu, R. and Shen, X., 2011. A Lightweight Message Authentication Scheme for Smart Grid Communications, *IEEE TRANSACTIONS ON SMART GRID*, 2(4), p.11.

[4] Aloul, F., Al-Alia, A. R., Al-Dalkya, R., Al-Mardinia, M. and El-Hajjb W., 2012. Smart Grid Security: Threats, Vulnerabilities and Solutions. *International Journal of Smart Grid and Clean Energy*, June Issue, 2012, p.6.

[5] Ericsson, G. N., 2010. Cyber Security and Power System Communication—Essential Parts of a Smart Grid Infrastructure, *IEEE TRANSACTIONS ON POWER DELIVERY*, 25(3), p.7.

[6] Govindarasu, M., Hahn, A. and Sauer, P., 2012. *Cyber-Physical Systems Security for Smart Grid*. Iowa: Iowa State University.

[7] Khurana, H., Bobba, R., Yardley, T., Agarwal, P. and Heine, E., 2010. Design Principles for Power Grid Cyber-Infrastructure Authentication Protocols. In: System Sciences (HICSS), *43rd Hawaii International Conference on*. Honolulu. 5-8 January 2010. Urbana-Champaign: University of Illinois.

[8] Depeng, L., Aung, Z., Williams, J.R. and Sanchez, A., 2012. Efficient authentication scheme for data aggregation in smart grid with fault tolerance and fault diagnosis. In: Innovative Smart Grid Technologies (ISGT), *2012 IEEE PES*. Washington. 16-20 January 2012. Abu Dhabi: Masdar Inst. of Sci. & Technol.

[9] Kundur, D., Feng, X., Liu, S., Zourntos, T. and Butler-Purry, K.L., 2010.Towards a Framework for Cyber Attack Impact Analysis of the Electric Smart Grid. In: Smart Grid Communications (SmartGridComm), *2010 First IEEE International Conference on*. Gaithersburg. 4-6 October 2010. Texas: Texas A&M University.

[10] Mutrty, M. S. R., 2010*. Energy Management Systems (EMS)*. [online] USAID SARI/Energy Available at: <http://www.sari-energy.org/PageFiles/What_We_Do/activities/CEB_Power_Systems_Simulation_Training,_Colombo,_Sri_Lanka/Course_ppts/Lecture_49_EMS.pdf> http://www.sari-energy.org/PageFiles/What_We_Do/activities/CEB_Power_Systems_Simulation_Training,_Colombo,_Sri_Lanka/Course_ppts/Lecture_49_EMS.pdf> [Accessed 18 July 2013].

[11] Kursawe, K., Danezis, G. and Kohlweiss, M., 2011.Privacy-friendly aggregation for the smart-grid. In: Fischer-Hübner, S. and Hooper, N., *PETS'11 Proceedings of the 11th international conference on Privacy enhancing technologies*. Bremen. 12-15 June 2012. Heidelberg: Springer-Verlag Berlin.

[12] Mo, Y., Kim, T.H.J., Brancik, K., Dickinson, D., Lee, H., Perrig, A. and Sinopoli, B., 2010. Cyber–Physical Security of a Smart Grid Infrastructure. *Proceedings of the IEEE*, 100(1), pp.195-209.

[13] NISTIR, 2010.*Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements*. (National Institute of Standards and Technology Interagency Report 7628, vol. 1) DC: U.S. Department of Commerce.

[14] Oh, S. and Kwak, J., 1012. Mutual Authentication and Key establishment mechanism using DCU certificate in Smart Grid. *Applied Mathematics & Information Sciences*, January Issue, 2012, p.8.

[15] Cavoukian, A., 2009. *Smart Privacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation*. Ontario: Information and Privacy Commissioner

[16] Cheung, H., Hamlyn, A. and Yang, C., 2011. Network Security Authentication of Power System Operations, *ECEN 689: Cyber Security of the Class Presentation* [online via internal VLE] Texas A&M University. Available at: <http://www.comm.toronto.edu/~dkundur/course_info/smart-grid-sec/presentations/Qin%20Yan.ppt.pdf> [Accessed 10 July 2013].

[17] NSTB, 2009.*Study of Security Attributes of Smart Grid Systems – Current Cyber Security Issues*. (NL/EXT-09-15500) Idaho: U.S. Department of Energy Office of Electricity Delivery and Energy Reliability.

[18] Wu, Z. and Zhou, C. 2011. Fault-Tolerant and Scalable Key Management for Smart Grid.*Smart Grid,IEEE Transactions on*, 2(2), pp.375-381.

[19] Giacomoni, A. M., Amin, S.M. and Wollenberg, B. F., 2011. Reconfigurable interdependent infrastructure systems: Advances in distributed sensing, modeling, and control. In: IEEE, *American Control Conference (ACC)*, San Francisco, 29 June-1 July 2011.

[20] McDaniel, P. and McLaughlin, S., 2009. Security and Privacy Challenges in the Smart Grid. *Security & Privacy, IEEE*, 7(3), pp.75-77.

[21] Li, Q. and Cao, G., 2011. Multicast Authentication in the Smart Grid With One-Time Signature. Smart Grid, *IEEE Transactions on*, 2(4), pp.686-696.

[22] Niu, W., 2011. Smart Grid Privacy via Anonymization of Smart Metering Data, *ECEN 689: Cyber Security of the Class Presentation* [online via internal VLE] Texas A&M University. Available at: <http://www.comm.utoronto.ca/~dkundur/course_info/smart-grid-sec/presentations/Wei%20Niu.ppt.pdf> [Accessed 10 July 2013].

[23] Pearson, I.L.G., 2011. Smart grid cyber security for Europe. *Energy Policy*, 39(9), pp.5211–5218.

[24] Sorebo, G. and Echols, M. 2012. *Smart Grid Security*. London-New York: CRC Press.

[25] Brunschwiler, Cyrill., 2013. Advanced Metering Infrastructure Architecture and Components. Compass Security Blog, [blog] 28 February. Available at: <http://blog.csnc.ch/tag/home-area-network/> [Accessed 10 July 2013].

[26] Giacomoni, A. M., Amin, S.M. and Wollenberg, B. F., 2010. Smart Grid Distribution Systems Vulnerabilities and Security Needs. Security Technology, [blog] 27 July. Available at: <http://tli.umn.edu/blog/security-technology/smart-grid-distribution-systems-vulnerabilities-and-security-needs/> [Accessed 10 July 2013].

[27] CA and U.S. Department of Defense, 2002. Complex Interactive Networks/Systems Initiative: Final Summary Report: Overview and Summary Report for Joint EPRI and U.S. Department of Defense University Research Initiative. Washington DC: EPRI.

[28] Athreya, A. and Shankar, R. 2012. Smart Grid Security. [pdf] Carnegie Mellon University Silicon Valley. Available at: <http://wnss.sv.cmu.edu/courses/14814/s12/files/adHawks_14814s12_22.pdf> [Accessed 10 July 2013].