ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΚΑΤΕΥΘΥΝΣΗ: ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

«Smart Grid Security»

Διπλωματική εργασία

Κατερίνα Κεπενέ- Τηλιακού Σταματία Κυριακή

Επιβλέπων: Ριζομυλιώτης Παναγιώτης

Σάμος, Μάρτιος 2016

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΚΑΤΕΥΘΥΝΣΗ: ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

«Smart Grid Security»

Διπλωματική εργασία

Κατερίνα Κεπενέ- Τηλιακού Σταματία Κυριακή

Επιβλέπων: Ριζομυλιώτης Παναγιώτης

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή στις 17 Μαρτίου 2016

....

Ριζομυλιώτης Π. Σκιάνης Χ. Καμπουράκης Γ.

Σάμος, Μάρτιος 2016

.....

Κεπενέ Κατερίνα

Διπλωματούχος Ασφάλειας Πληροφοριακών και Επικοινωνιακών Συστημάτων ΜΠΕΣ

.....

Τηλιακού Σταματία Κυριακή

Διπλωματούχος Ασφάλειας Πληροφοριακών και Επικοινωνιακών Συστημάτων ΜΠΕΣ

ΕΥΧΑΡΙΣΤΙΕΣ

Στο σημείο αυτό θα θέλαμε να ευχαριστήσουμε για την πολύτιμη βοήθεια του και άψογη συνεργασία του, τον καθηγητή μας κύριο Ριζομυλιώτη Παναγιώτη για τις γνώσεις και ιδέες που μοιράστηκε μαζί μας, με σκοπό να υλοποιηθεί η διπλωματική αυτή εργασία.

ΠΡΟΛΟΓΟΣ

Η διπλωματική εργασία έχει σαν αντικείμενο τη μελέτη της άσφαλειας των Έξυπνων Δικτύων Ηλεκτρικής Ενέργειας. Τα έξυπνα αυτά δίκτυα είναι μία υποδομή με τόσες πολλές νέες δυνατότητες που η ασφάλεια και η προστασία της αποτελούν ένα από τους σημαντικότερους στόχους που χρειάζονται προσοχή.

Η εργασία αυτή αποτελείται από έξι κεφάλαια. Στο πρώτο κεφάλαιο γίνεται μια εισαγωγή στα Έξυπνα Δίκτυα Ηλεκτρικής Ενέργειας. Στο δεύτερο κεφάλαιο γίνεται ανάλυση βασικών εννοιών του Έξυπνου Δικτύου και στις τεχνολογίες επικοινωνιών για εφαρμογές τους. Επίσης, το τρίτο κεφάλαιο αναφέρεται στα πρωτόκολλα ασφάλειας πληροφοριών και στις απαιτήσεις ασφάλειας.

Στο τέταρτο κεφάλαιο, γίνεται κατηγοριοποίηση των επιθέσεων στα Έξυπνα Δίκτυα Ηλεκτρικής Ενέργειας και το πέμπτο κάνει αναφορά σε θέματα κρυπτογραφίας.

Τέλος, στο έκτο κεφάλαιο γίνεται ανάλυση επικινδυνότητας με την μέθοδο CORAS.

Λέξεις Κλειδιά: “Έξυπνο δίκτυο, ασφάλεια, επιθέσεις, μέθοδος CORAS”

ABSTRACT

The objective of this diploma thesis is the study of Smart Grid security. The Smart Grid is an infrastructure with so many new features that security and protection are one of the most important tasks that need attention.

This diploma thesis consists of six chapters. The first chapter is an introduction to Smart Grid. The second chapter is an analysis of key concepts of Smart Grid and communications technologies for their applications. Also, the third chapter refers to the information security protocols and security requirements.

In the fourth chapter is the categorization of attacks on Smart Grid and the fifth refers to cryptography. Finally, the sixth chapter is risk analysis with CORAS method.

Keywords: “Smart Grid, security, attacks, CORAS method”

ΠΕΡΙΕΧΟΜΕΝΑ

«Smart Grid Security» 1
Διπλωματική εργασία 1
«Smart Grid Security» 3
Διπλωματική εργασία 3
ΕΥΧΑΡΙΣΤΙΕΣ 5
ΠΡΟΛΟΓΟΣ 6
ABSTRACT 7
ΠΕΡΙΕΧΟΜΕΝΑ 9
Πίνακας αντιστοίχησης συντομογραφιών 12
ΚΕΦΑΛΑΙΟ ΠΡΩΤΟ 15
1.1 Εισαγωγή 15
ΚΕΦΑΛΑΙΟ ΔΕΥΤΕΡΟ 16
2.1 Ορισμός Smart Grid 16
2.2 Πλεονεκτήματα Smart Grid 18
2.3 Τεχνολογίες του Smart Grid 21
2.4 Η αρχιτεκτονική ενός Smart Grid 22
2.5 Τεχνολογίες επικοινωνιών για εφαρμογές Smart Grid 23
2.5.1 Ασύρματες Τεχνολογίες 24
2.5.2 Ενσύρματες Τεχνολογίες (Wireline/Wired Technologies). 30
2.6 Έξυπνος Ψηφιακός Μετρητής (Smart Meter-SM) 32
2.6.1 Τηλεπικοινωνιακή υποδομή 33
2.7 Τα Συστήματα SCADA 33
2.8 Ενσωμάτωση SCADA σε Smart Grid 36
ΚΕΦΑΛΑΙΟ ΤΡΙΤΟ 38
3.1 Ασφάλεια και Smart Grid 38
3.2 Ο ιός Stuxnet 39
3.3. Πρωτόκολλα ασφάλειας πληροφοριών 40
3.4 Απαιτήσεις ασφάλειας των Smart Grid στον κυβερνοχώρο 42
3.5 Επιλογή απαιτήσεων ασφαλείας 46
ΚΕΦΑΛΑΙΟ ΤΕΤΑΡΤΟ 49

4.1 Επιτιθέμενοι. Ποιοι μπορεί να είναι; 49
4.2 Κίνητρα κακόβουλων επιθέσεων 49
4.3 Κατηγοριοποίηση επιθέσεων 51
4.4. Επιθέσεις σε SCADA και μέτρα αντιμετώπισης 54
4.5 Επιθέσεις Έξυπνου μετρητή και μέτρα αντιμετώπισης 55
4.6 Επιθέσεις Φυσικού επιπέδου και μέτρα αντιμετώπισης 58
4.7 Έγχυση Δεδομένων & επιθέσεις επανάληψης και μέτρα αντιμετώπισης 60
4.8 Βασισμένες στο δίκτυο επιθέσεις και μέτρα αντιμετώπισης 62
ΚΕΦΑΛΑΙΟ ΠΕΜΠΤΟ 64
5. Κρυπτογραφία και διαχείριση κλειδιών 64
5.1 Θέματα κρυπτογραφίας και διαχείρισης κλειδιών στα έξυπνα δίκτυα 64
5.1.1 Περιορισμοί 64
5.1.2 Γενικά Θέματα Κρυπτογραφίας 66
5.2 Λύσεις κρυπτογράφησης και διαχείρισης κλειδιών 74
5.2.1 Γενικά θέματα σχεδιασμού 74
5.2.2 Συστήματα Διαχείρισης Κλειδιών για Έξυπνα Δίκτυα. 79
ΚΕΦΑΛΑΙΟ ΕΚΤΟ 87
6. Πιστοποιητικά ασφάλειας για Έξυπνα Δίκτυα στην ΕΕ 87
6.1 Υφιστάμενη κατάσταση 87
6.2 Οι ανάγκες των ενδιαφερόμενων μερών σχετικά με την πιστοποίηση στα Έξυπνα Δίκτυα 88
6.3 Τα χαρακτηριστικά του «ιδανικού» μοντέλου πιστοποίησης ασφάλειας για έξυπνα δίκτυα. 91
6.4 Κυριότερα ζητήματα στην υφιστάμενη κατάσταση στην ΕΕ 92
6.5 Η εφοδιαστική αλυσίδα ενός Έξυπνου Δικτύου 93
6.5.1 Ανάλυση εφοδιαστικής αλυσίδας ενός Έξυπνου Δικτύου 94
6.5.2 Υιοθέτηση SG – AM για μοντέλο αλυσίδας εμπιστοσύνης. 95
6.5.3 Ορισμός των επιπέδων κινδύνων που ευθυγραμμίζονται με την SG-AM μεθοδολογία. . 96
6.5.3.1 Επίπεδα αντίκτυπου κινδύνου (Risk Impact Levels) 98
6.5.3.2 Κατηγορίες αντίκτυπου κινδύνου (Risk Impact Categories) 99
6.6 Αποτίμηση συμμόρφωσης και η συσχέτιση με τις δοκιμές 100
6.7 Περιγραφή σχημάτων πιστοποίησης που βασίζονται στο SG-AM 102
6.8 Κενά και προκλήσεις 106
6.9 Συστάσεις - προτάσεις 107
6.10 Σύνοψη 108

ΚΕΦΑΛΑΙΟ ΕΒΔΟΜΟ 110
7. Ανάλυση επικινδυνότητας για Smart Grid[32] 110
7.1 Αναγνώριση περιουσιακών στοιχείων και κινδύνων 111
7.1.1 . Προετοιμασία για την ανάλυση (βήμα 1) 111
7.1.2. Παρουσίαση του στόχου στον πελάτη (βήμα 2) 112
7.1.3 Καθορισμός του στόχου με χρήση διαγραμμάτων (βήμα 3). 113
7.1.4 Αποδοχή της περιγραφής του στόχου (βήμα 4) 118
7.1.5 Αναγνώριση κινδύνων με χρήση διαγραμμάτων απειλών (βήμα 5) 124
7.1.6 Υπολογισμός πιθανότητας κινδύνου (βήμα 6) 128
7.1.7 Αποτίμηση κινδύνου (βήμα 7) 133
7.1.8 Αντιμετώπιση κινδύνου (βήμα 8) 134
7.2 Απαιτήσεις ασφάλειας 138
7.3 Μέτρα ασφάλειας 139
7.4 Σύνοψη αποτελεσμάτων 148
Επίλογος 152
Βιβλιογραφία 153

Πίνακας αντιστοίχησης συντομογραφιών

ΑΡΚΤΙΚΟΛΕΞΟ	ΣΥΝΘΕΤΗ ΟΝΟΜΑΣΙΑ	ΣΥΝΤΟΜΗ ΕΠΕΞΗΓΗΣΗ
AMI	Advanced Metering Infrastructure	Προηγμένες υποδομές μέτρησης
AO	(Asset/System Optimization	Βελτιστοποίηση των περιουσιακών στοιχείων (εξοπλισμού) και του συστήματος
API	Application Program Interface	Διεπάφη εφαρμογής
CA	Certificate Authorities	Αρχές έκδοσης πιστοποιητικών
CEN	European Committee for Standardization	Ευρωπαϊκή Επιτροπή Τυποποίησης
CENELEC	European Committee for Electrotechnical Standardization	Ευρωπαϊκή Επιτροπή Ηλεκτροτεχνικής Τυποποίησης
CS	Customer Side Systems	Συστήματα εξυπηρέτησης καταναλωτή
DDOS	Distributed Denial of Service	Κατανεμημένη επίθεση άρνησης διαθεσιμότητας
DER	Distributed Energy Resources	Τεχνολογίες διεσπαρμένης παραγωγής
DMS	Distribution Management System/Distribution Automation	Διαχείριση του συστήματος διανομής/ διανομή αυτοματισμών
DOE	Department Of Energy	Υπουργείο Ενέργειας των ΗΠΑ
DR	Demand Response	Σύστημα διαχείρισης της ζήτησης

ECR	European Commission Research	Ευρωπαϊκή Επιτροπή Ενέργειας
EPRI	Electrical Power Research Institute	Ινστιτούτο Ερευνών Ηλεκτρικής Ενέργειας
ETSI	European Telecommunications Standards Institute	Ευρωπαϊκό Ινστιτούτο Τηλεπικοινωνιακών Προτύπων
FIPS	Federal Information Processing Standards	Ομοσπονδιακά πρότυπα επεξεργασίας πληροφοριών.
FTP	File Transfer Protocol	Δικτυακό πρωτόκολλο μεταφοράς αρχείων
FTPS	File Transfer Protocol Secure	Παραλλαγή του πρωτοκόλλου FTP που περιλαμβάνει μηχανισμούς ασφάλειας πληροφοριών
GPRS	General Packet Radio Service	Πρωτόκολλο μετάδοσης δεδομένων πάνω από δίκτυα κινητής τηλεφωνίας
HAN	Home Area Network	Οικιακό τοπικό δίκτυο
HSM	Hardware Security Module	Ηλεκτρονική μονάδα ασφάλειας υλικού
HTTP	Hyper-Text Transfer Protocol	Πρωτόκολλο μεταφοράς ιστοσελίδων – Βασικό πρωτόκολλο του διαδικτύου
HTTPS	Hyper-Text Transfer Protocol Secure	Παραλλαγή του HTTP που περιλαμβάνει μηχανισμούς ασφάλειας πληροφοριών
ICT	Information and Communications Technologies	Τεχνολογίες πληροφορικής και επικοινωνιών
IEC	International Electrotechnical Commission	Διεθνή Ηλεκτροτεχνική Επιτροπή
IEEE	Institute of Electrical and Electronics Engineers	Διεθνής σύνδεσμος ηλεκτρολόγων και ηλεκτρονικών μηχανικών
IP	Internet Protocol	Πρωτόκολλο διευθυνσιοδότησης στο Διαδίκτυο
IPS	Intrusion Prevention System	Μηχανισμός αποτροπής παραβιάσεων
ISO	International Organization for	Διεθνής οργανισμός τυποποίησης

	Standardization	
LAN	Local Area Network	Τοπικό Δίκτυο
NAN	Neighborhood Area Network	Γειτονικό Δίκτυο
NIST	National Institute of Standards and Technology	Αμερικανικό ινστιτούτο προτύπων και τεχνολογίας
MBWA	Mobile Broadband Wireless Access	Κινητή ασύρματη ευρυζωνική πρόσβαση
PLC	Power Line Communication	Πρότυπο μεταφοράς δεδομένο μέσω γραμμών μεταφοράς ΗΕ
RP	Relying Party	
SCADA	Supervisory Control And Data Acquisition	Σύστημα αυτομάτου ελέγχου βιομηχανικών διατάξεων
SEP	Smart Energy Profile	Έξυπνο Ενεργειακό Προφίλ
SG	Smart Grid	Έξυπνα δίκτυα
SGCG	Smart Grid Coordination Group	Ομάδα Συντονισμού Έξυπνου δικτύου
SM	Smart Meter	Μετρήτης που χρησιμοποιείται στα έξυπνα δίκτυα
SSH	Secure Shell	Πρωτόκολλο απομακρυσμένου ελέγχου πληροφοριακών συστημάτων UNIX
SSL	Secure Socket Layer	Ξεπερασμένη μέθοδος κρυπτογράφησης
SSN	Secondary Station Node	Δευτερογενής σταθμός κόμβου
TA	Transmission Enhancement Applications-	Εφαρμογές ενίσχυσης του συστήματος μεταφοράς
TCP	Transmition Control Protocol	Βασικό πρωτόκολλο στρώματος μεταφοράς στο Διαδίκτυο
TLS	Transport Layer Security	Απόγονος του SSL. Μέθοδος κρυπτογράφησης στο στρώμα μεταφοράς
USB	Universal Serial Bus	Πρότυπο σύνδεσης περιφερειακών διατάξεων σε υπολογιστικά συστήματα
WAN	Wide Area Network	Δίκτυο Ευρείας Περιοχής
MBWA	Mobile Broadband	Κινητή ασύρματη

	Wireless Access	ευρυζωνική πρόσβαση
WiMAX	Worldwide inter-operability for Microwave Access	Παγκόσμια διαλειτουργικότητα για πρόσβαση μικροκυμάτων
WMAN	Wireless Metropolitan Area Network	Ασύρματο Μητροπολιτικό Δίκτυο
WMN	Wireless Mesh Networks	Ασύρματα Δίκτυα Πλέγματος

ΚΕΦΑΛΑΙΟ ΠΡΩΤΟ

1.1 Εισαγωγή

Τα δίκτυα ηλεκτροδότησης είναι από τις πιο κρίσιμες υποδομές που κατασκεύασε ποτέ ο άνθρωπος. Λόγω του γεγονότος οτι πάνω τους στηρίζονται όλος ο τεχνολογικός πολιτισμός, η πρόοδος της κοινωνίας αλλά και η προσπάθεια για οικονομική ανάπτυξη και ευημερία.

Τα δίκτυα αυτά καταφέρνουν να ικανοποιούν τις ανάγκες του ανθρώπου καθώς αυτές με το πέρασμα του χρόνου γίνονται ολοένα και πιο σύνθετες. Στη σημερινή εποχή, πλέον, είναι απαραίτητα δίκτυα που αποσκοπούν στην πιο αποδοτική αξιοποίηση των ανανεώσιμων πηγών ενέργειας και στην προστασία του περιβάλλοντος. Ακόμα, δίκτυα που θα προσφέρουν μεγαλύτερη αξιοπιστία και ποιότητα ρεύματος αφού η αυξανόμενη ζήτηση για ηλεκτρική ενέργεια, μαζί με την πολύπλοκη φύση του δικτύου ηλεκτρικής ενέργειας, έχουν προκαλέσει σοβαρά προβλήματα στο ήδη καταπονημένο δίκτυο, όπως διακοπές ρεύματος, βυθίσεις τάσης και υπερφορτίσεις.

Το έξυπνο ενεργειακό δίκτυο έχει σαν σκοπό να αντιμετωπίσει τις παραπάνω ανησυχίες με αποδοτικό και δυναμικό τρόπο. Η μεγάλη πρόοδος η οποία έχει σημειωθεί τα τελευταία χρόνια στις τεχνολογίες πληροφοριών και επικοινωνιών (ICTs) επιτρέπει την μετατροπή των παραδοσιακών δικτύων ηλεκτρικής ενέργειας στο λεγόμενο έξυπνο ενεργειακό δίκτυο(Smart Grid) το οποίο εξασφαλίζει παραγωγικές αλληλεπιδράσεις μεταξύ των παρόχων ηλεκτρικής ενέργειας, των

καταναλωτών καθώς και άλλων οργανισμών που θα παρέχουν τις υπηρεσίες τους σε ένα τέτοιο δίκτυο.

Το Smart Grid (SG) είναι μία υποδομή με τόσες πολλές νέες δυνατότητες που αυτό έχει ώς αποτέλεσμα να αποκτήσει προφανώς ένα πολύ πιο κρίσιμο χαρακτήρα από ένα τυπικό δίκτυο ηλεκτροδότησης. Η ασφάλεια και η προστασία αυτής της υποδομής ,έναντι της πληθώρας κινδύνων που θα μπορούσαν να προκύψουν από την κακόβουλη αξιοποίηση των δυνατοτήτων που παρέχει, αποτελούν αναμφίβολα ένα από τους σημαντικότερους στόχους που χρήζουν προσοχής.

ΚΕΦΑΛΑΙΟ ΔΕΥΤΕΡΟ

2.1 Ορισμός Smart Grid

Δεν υπάρχει ένας ξεκάθαρος ορισμός του SG καθώς ο όρος αυτός είναι περισσότερο εμπορικός και όχι τεχνολογικός. Με βάση τη βιβλιογραφία δίνονται τέσσερις διαφορετικές προσεγγίσεις για τον ορισμό του SG. Πιο συγκεκριμένα, το SG παρουσιάζεται ως:

- *«Ένα εξελιγμένο ηλεκτρικό δίκτυο, του οποίου αναπόσπαστο κομμάτι είναι η αμφίδρομη επικοινωνία μεταξύ παραγωγού και καταναλωτή και τα ευφυή συστήματα μέτρησης και παρακολούθησης της λειτουργίας του».*

Πηγή: Ευρωπαϊκή Επιτροπή[2]

- *«Ένα ηλεκτρικό δίκτυο το οποίο με αποδοτικό τρόπο μπορεί να ενσωματώσει τη συμπεριφορά και τις δράσεις όλων των παραγόντων που βρίσκονται συνδεδεμένοι σε αυτό –παραγωγοί, καταναλωτές ή και καταναλωτές που παράγουν ενέργεια – ώστε να διασφαλίσει ένα οικονομικά αποδοτικό, βιώσιμο σύστημα ενέργειας με χαμηλές απώλειες και υψηλής ποιότητας υπηρεσία , σε ένα ασφαλές και αξιόπιστο δίκτυο».*

Πηγή: European Commission Task Force for Smart Grid[3]

- *«Μία ευφυής υποδομή παροχής ηλεκτρικής ενέργειας η οποία υποστηρίζεται από τις τελευταίες τεχνολογίες στον τομέα της επικοινωνίας, του υπολογισμού και της ηλεκτρονικής προκειμένου να ανταποκριθεί στις μελλοντικές απαιτήσεις της κοινωνίας σε ηλεκτρική ενέργεια».*

Πηγή:Electric Power Research Institute (ERPI)[1]

- «*Ένα εκσυγχρονισμένο ηλεκτρικό δίκτυο που χρησιμοποιεί τεχνολογίες πληροφορικής και επικοινωνιών για να συλλέξει και να επεξεργαστεί τις πληροφορίες σχετικά με τη συμπεριφορά των προμηθευτών και των καταναλωτών, με έναν αυτοματοποιημένο τρόπο, ώστε να βελτιώσει την αποδοτικότητα, την αξιοπιστία, την οικονομία και τη βιωσιμότητα της παραγωγής και της διανομής της ηλεκτρικής ενέργειας».*

Πηγή: U.S. Department of Energy το Smart Grid[3]

2.2 Πλεονεκτήματα Smart Grid

Το Σεπτέμβριο του 2011, το National Institute of Standards and Technology - NIST των ΗΠΑ και η Smart Grid Coordination Group - SGCG, ως αντιπρόσωπος τριών οργανισμών European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC) και το European Telecommunications Standards Institute (ETSI) εξέδωσαν κοινή ανακοίνωση για την αρχή της συνεργασία τους όσο αφορά την ανάπτυξη κοινών προτύπων για τη σχεδίαση και λειτουργία των SG με σκοπό να επιτευχθεί η μεταξύ τους δια-λειτουργικότητα. [4]

Σύμφωνα με αυτά τα πρότυπα γίνονται αντιληπτά και τα πλεονεκτήματα που θα παρέχει το ευφυές δίκτυο τα οποία είναι τα εξής :

- **Φιλοξενεί όλους τους δυνατούς τρόπους παραγωγής και αποθήκευσης.**

Η δυνατότητα για συνδέσεις τοποθέτησης και άμεσης λειτουργίας (plug and play) διαφορετικών πόρων πολλαπλασιάζει τις επιλογές για την παραγωγή και την αποθήκευση, όπως και αυτές των νέων τεχνολογιών που επιτρέπουν την αποτελεσματικότερη και καθαρότερη παραγωγή ηλεκτρικής ενέργειας.

- **Είναι επιτρεπτή η ενεργή συμμετοχή των καταναλωτών.**

Ο καταναλωτής έχει τη δυνατότητα της επιλογής και αυτο έχει ως αποτέλσμα να αυξάνεται η αλληλεπίδραση με το δίκτυο γεγονός που έχει αρκετά πλεονεκτήματα για αυτό αλλά και το περιβάλλον ενώ ταυτόχρονα μειώνεται και το κόστος της διανεμόμενης ηλεκτρικής ενέργειας.

- **Είναι επιτρεπτή η δημιουργία νέων προϊόντων, υπηρεσιών και αγορών.**

Η ανοικτή αγορά φανερώνει τυχόν σπατάλες και αναποτελεσματικότητα και βοηθά να εξαλειφθούν βγάζοντας τες έξω από το σύστημα. Επίσης, προσφέρει νέες επιλογές στον καταναλωτή και μειώνει τη συμφόρηση κατά τη μεταφορά της ενέργειας οδηγώντας σε πιο αποτελεσματικές αγορές ηλεκτρικής ενέργειας.

- **Βελτιστοποιεί τη χρήση του υπάρχοντος εξοπλισμού και έχει αποτελεσματικότερη λειτουργεία.**

Επιτυγχάνει την επιθυμητή λειτουργικότητα με το ελάχιστο δυνατό κόστος και επιτρέπει την πληρέστερη αξιοποίηση του υπάρχοντος εξοπλισμού. Ακόμα, ακολουθεί ένα πιο στοχευμένο και αποτελεσματικό πρόγραμμα συντήρησης του δικτύου που έχει σαν αποτέλεσμα λιγότερες αστοχίες στον εξοπλισμό και σε ασφαλέστερη λειτουργία.

- **Προβλέπει και ανταποκρίνεται αυτόνομα στις διαταραχές του συστήματος**

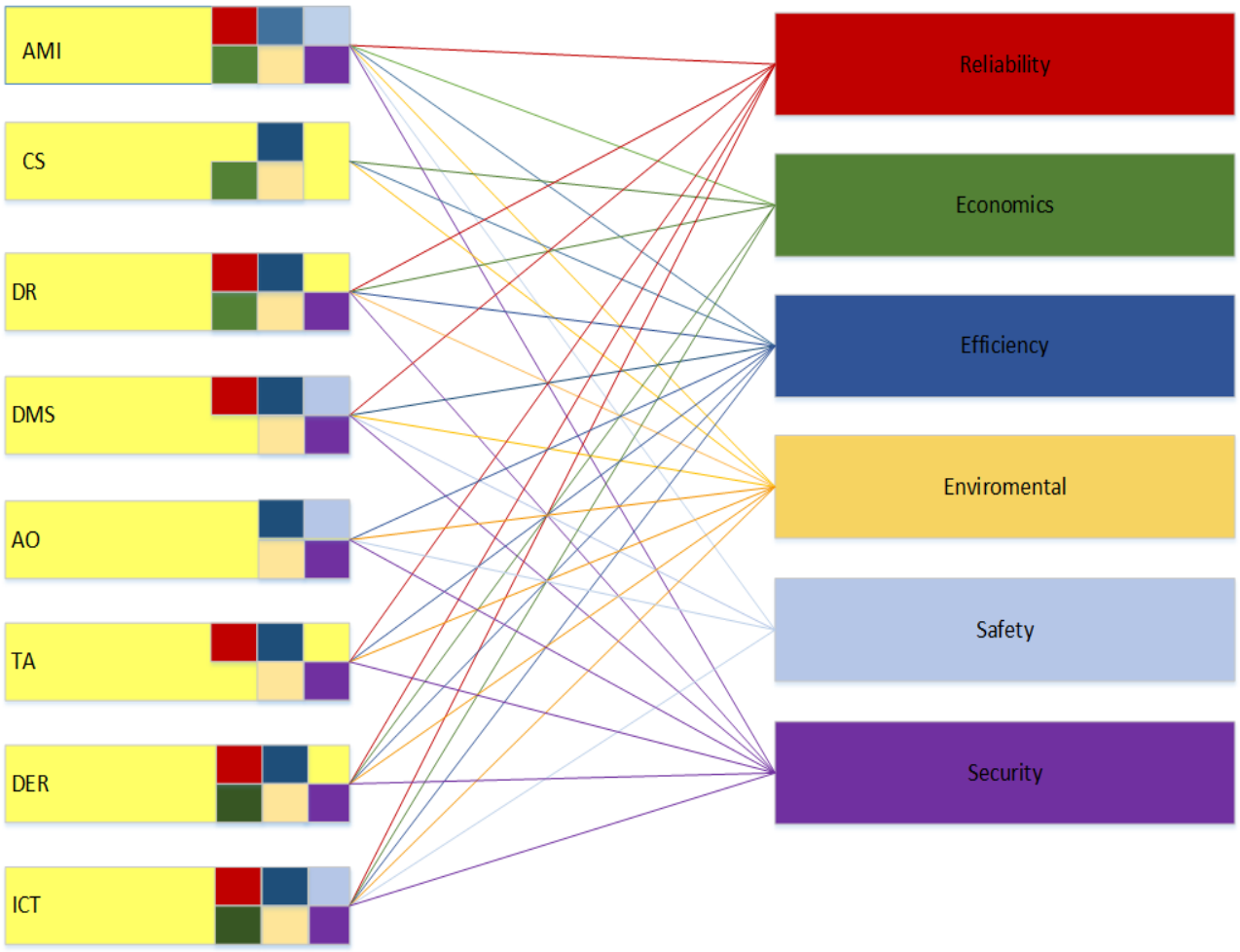
Το SG εκτελεί συνεχείς αυτοαξιολογήσεις για τον εντοπισμό και την ανάλυση της αίτιας του προβλήματος ώστε να μπορεί να ανταποκριθεί και να επαναφέρει ή να παρακάμψει το σφάλμα είτε σε ένα στοιχείο του δικτύου, είτε σε ένα τμήμα του.

Για να γίνουν αντιληπτές οι δυνατότητες των SG παρακάτω θα γίνει αναφορά σε ορισμένες εφαρμογές που τα συναντάει κανείς:

- Προηγμένες υποδομές μέτρησης (Advanced Metering Infrastructure-AMI)
- Συστήματα εξυπηρέτησης καταναλωτή (Customer Side Systems-CS)
- Σύστημα διαχείρισης της ζήτησης (Demand Response-DR)
- Διαχείριση του συστήματος διανομής/ διανομή αυτοματισμών (Distribution Management System/Distribution Automation-DMS)
- Εφαρμογές ενίσχυσης του συστήματος μεταφοράς (Transmission Enhancement Applications-TA)
- Βελτιστοποίηση των περιουσιακών στοιχείων (εξοπλισμού) και του συστήματος (Asset/System Optimization-AO)
- Τεχνολογίες διεσπαρμένης παραγωγής (Distributed Energy Resources-DER)
- Τεχνολογίες πληροφορικής και επικοινωνιών (Information and Communications Technologies-ICT)

Η ανάπτυξη αυτών των τεχνολογικών λύσεων αναμένεται να δημιουργήσουν βελτιώσεις στον τομέα της αξιοπιστίας, της οικονομίας, της αποτελεσματικότητας, του περιβάλλοντος, της προστασίας και της ασφάλειας.

Στην παρακάτω εικόνα 1 προσδιορίζονται οι σχέσεις μεταξύ των τεχνολογικών λύσεων και των βασικών τομέων-στόχων του SG. Οι πολλές διασυνδέσεις που υπάρχουν απεικονίζουν τη στενή σχέση μεταξύ των λύσεων που προσφέρει το SG, για να υπάρχουν τα μέγιστα δυνατά οφέλη σε όλους τους τομείς κατά τον σχεδιασμό και την εφαρμογή του.



Εικόνα 2: Σχέση τεχνολογικών λύσεων με τους βασικούς τομείς του Smart Grid [4]

2.3 Τεχνολογίες του Smart Grid

Σύμφωνα με το Υπουργείο Ενέργειας των ΗΠΑ (DOE-Department Of Energy) οι παρακάτω τεχνολογίες του SG είναι απαραίτητες ώστε να εξασφαλιστεί η αξιόπιστη, αποδοτική και καθαρή διανομή ηλεκτρικής ενέργειας [15]:

- **Η ενσωμάτωση αμφίδρομης επικοινωνίας.**

Αυτού του είδους η επικοινωνία επιτρέπει στους χειριστές να παρακολουθούν και να αλληλεπιδρούν με εξαρτήματα του έξυπνου δικτύου σε πραγματικό χρόνο με σκοπό την καλύτερη διαχείριση του των υπηρεσιών του δικτύου. Ένα παράδειγμα είναι, οι διακοπές ρεύματος που οι χειριστές αγνοούν μέχρι οι πελάτες τους να τους ειδοποιήσουν γι αυτές, συνήθως μέσω των τηλεφωνικών κλήσεων σε ένα κέντρο υποστήριξης πελατών. Σε ένα έξυπνο δίκτυο, οι επιχειρήσεις είναι σε θέση να ανιχνεύουν και να διαχειρίζονται το πρόβλημα χωρίς καμία ειδοποίηση από τους πελάτες, με αποτέλεσμα την ταχύτερη επίλυση των προβλημάτων και την μείωση του λειτουργικού κόστους.

- **Χρήση προηγμένων συσκευών.**

Αφορά συσκευές με ανοχή σε σφάλματα, συσκευές αποθήκευσης ηλεκτρικής ενέργειας, έξυπνες συσκευές και εξοπλισμό διάγνωσης σφαλμάτων. Ένα παράδειγμα είναι κατά την διάρκεια της ημέρας μπορεί να υπάρξει μία περίσσεια ηλεκτρική ενέργεια από μονάδες παραγωγής ηλιακής ενέργειας. Αυτή η περίσσεια θα μπορούσε να αποθηκεύεται σε συσκευές αποθήκευσης και να χρησιμοποιείται κατά την διάρκεια της νύχτας. Αντίστοιχα οι έξυπνες συσκευές θα μπορούσαν να προσφέρουν χρήσιμες πληροφορίες για την κατανάλωση ηλεκτρικής ενέργειας τόσο στους πελάτες όσο και στους παρόχους με απώτερο σκοπό την καλύτερη διαχείριση της ενέργειας.

- **Χρήση προηγμένων μεθόδων ελέγχου.**

Αυτές οι μέθοδοι επιτρέπουν την καλύτερη διαχείρηση των εξαρτημάτων του έξυπνου δικτύου. Για παράδειγμα, ένας χειριστής μπορεί να ανιχνεύσει ένα πρόβλημα σε κάποιο μηχάνημα από απόσταση και να το διορθώσει. Με αυτό τον τρόπο επιτυγχάνεται εξοικονόμηση χρόνου αλλά και κόστους.

- **Χρήση μεθόδων τηλεπισκόπησης και μέτρησης.**

Αυτές οι τεχνολογίες διασφαλίζουν την σταθερότητα και ασφαλή λειτουργία του δικτύου (smart meter-SM).

- **Χρήση βελτιωμένων διεπαφών και υποστήριξη λήψης αποφάσεων.**

Το έξυπνο δίκτυο επειδή χειρίζεται μεγάλη ποσότητα πληροφοριών, είναι ακατόρθωτο για έναν άνθρωπο να τις κατανοήσει σε μικρό χρονικό διάστημα. Έτσι, η χρήση της διεπαφής ανθρώπου-μηχανής (Human Machine Interface) απλοποιεί την πληροφορία για να μπορούν οι διαχειριστές να λαμβάνουν γρήγορα αποφάσεις.

- **Εφαρμογές της τεχνολογίας του SG**

Οι εφαρμογές αυτές θα παρέχουν στους καταναλωτές στατιστικά στοιχεία πραγματικού χρόνου όσον αφορά την χρήση και τιμολόγηση ηλεκτρικής ενέργειας, καθώς και συστάσεις για τη μείωση των λογαριασμών τους

2.4 Η αρχιτεκτονική ενός Smart Grid

Υπάρχουν αρκετοί τρόποι με τους οποίους μπορεί να γίνει περιγραφή ενός SG. Η παρακάτω αρχιτεκτονική σχεδίαση του SG έχει οριστεί αρχικά από Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (National Institute of Standards and Technology – NIST) η οποία έχει υιοθετηθεί από το Ινστιτούτο Ερευνών Ηλεκτρικής Ενέργειας (Electrical Power Research Institute – EPRI), την Ευρωπαϊκή Επιτροπή Ενέργειας (European Commission Research – ECR) καθώς και την Διεθνή Ηλεκτροτεχνική Επιτροπή (International Electrotechnical Commission – IEC). Η παρούσα αρχιτεκτονική αποτελεί τη βάση για την υλοποίηση της τελικής αρχιτεκτονικής του SG.

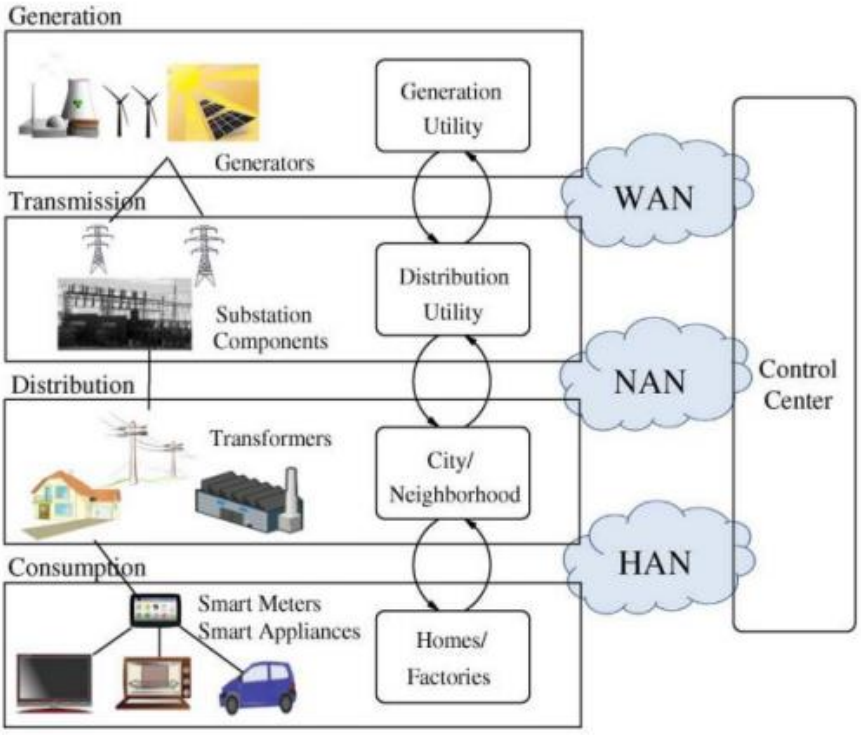
Πιο αναλυτικά, το SG διαχωρίζεται σε επίπεδα Παραγωγής, Μεταφοράς, Διανομής και Κατανάλωσης της ηλεκτρικής ενέργειας τα οποία μέσω δικτύων όπως :

• Οικιακό Δίκτυο (Home Area Network – HAN)

• Γειτονικό Δίκτυο (Neighborhood Area Network – NAN).

• Δίκτυο Ευρείας Περιοχής (Wide Area Network – WAN).

συνδέονται με ένα κέντρο ελέγχου[11][12] (Εικόνα 1.2).



Εικόνα 2.1 : Αρχιτεκτονική Smart Grid

.

Τέλος, το SG χωρίζεται σε δύο διαφορετικά δίκτυα:

• Micro Grid: όπου γίνεται η διανομή και η αποθήκευση ηλεκτρικής ενέργειας και εντοπίζουμε τα HAN και NAN δίκτυα.

• Macro Grid: γίνεται η παραγωγή και η μεταφορά ηλεκτρικής ενέργειας και εντοπίζουμε το WAN δίκτυο.

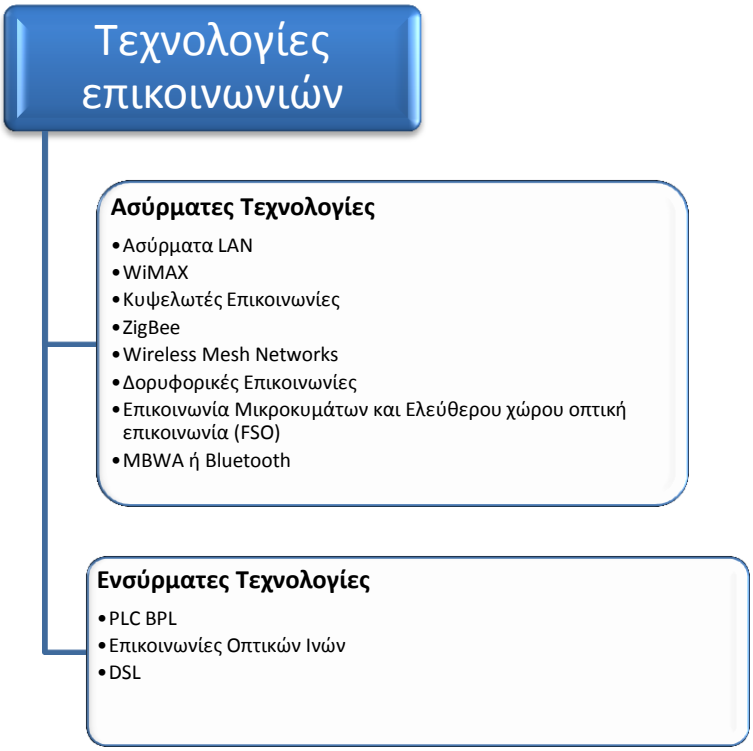
2.5 Τεχνολογίες επικοινωνιών για εφαρμογές Smart Grid

Ειναι δύσκολο να ορίσει κανείς τις απαιτήσεις ενός τηλεπικοινωνιακού δικτύου σε εφαρμογές που τώρα αναδύονται όπως τα SG. Οι δύο πιο σημαντικοί παράγοντες που χρειάζεται να ληφθούν υπόψη για να υπάρχει πιθανότητα επιτυχίας στο σύστημα είναι :

- η απόδοση του καναλιού (throughput),

- η καθυστέρηση καναλιού (latency).

Επίσης σημαντικοί, είναι η αξιοπιστία και η ασφάλεια. Η υιοθέτηση των διάφορων τεχνολογιών για τις επικοινωνίες των SG εξαρτάται από τα χαρακτηριστικά και τις απαιτήσεις του δικτύου (π.χ μικρές ή μεγάλες επιχειρήσεις, γεωγραφικές ανάγκες, στόχοι του έργου,εφαρμογές και οι υπηρεσίες).



Εικόνα 2.2 Κατηγοριοποίηση των υποψήφιων Τεχνολογιών Επικοινωνιών

2.5.1 Ασύρματες Τεχνολογίες

Τα ασύρματα δίκτυα συνήθως παρέχουν συνδέσεις μικρών αποστάσεων με συγκριτικά χαμηλούς ρυθμούς δεδομένων επειδή υφίστανται σημαντική εξασθένηση λόγω μετάδοσης και παρεμβολών από το περιβάλλον.

Η εφαρμογή ασύρματων τεχνολογιών έχει αρκετά πλεονεκτήματα όπως:

- μικρό κόστος εγκατάστασης,
- κινητικότητα,

- κάλυψη απομακρυσμένων περιοχών,
- γρήγορη εγκατάσταση κ.ά.

Ωστόσο, υπάρχουν και κάποιες κοινές ανησυχίες όπως:

- Οι ασύρματεςτεχνολογίες που λειτουργούν σε μη αδειοδοτημένο φάσμα συχνοτήτων είναι πιο ευάλωτες σε φαινόμενα θορύβου και παρεμβολής,
- Οι ασύρματες τεχνολογίες με αδειοδοτημένο φάσμα αντιμετωπίζουν λιγότερες παρεμβολές, αλλά είναι συγκριτικά μια δαπανηρή λύση
- η ασφάλεια για τα ασύρματα μέσα επικοινωνίας είναι μικρότερη.

Παρακάτω θα αναλυθούν ασύρματες τεχνολογίες που μπορούν να χρησιμοποιηθούν στις εφαρμογές των SG:

Ασύρματα Τοπικά Δίκτυα (Wireless LAN)

Τα ασύρματα τοπικά δίκτυα είναι βασισμένα στο πρότυπο IEEE 802.11. Παρέχουν εύρωστη, υψηλής ταχύτητας επικοινωνία σημείου-προς-σημείο (point-to-point) και σημείου-προς-πολλαπλά σημεία (point-to-multipoint). Στο πρότυπο αυτό υιοθετήθηκε τεχνολογία απλωμένου φάσματος που επιτρέπει να χρησιμοποιείται η ίδια ζώνη συχνοτήτων από πολλούς χρήστες με ελάχιστη παρεμβολή σε άλλους χρήστες. Το πρότυπο IEEE 802.11b, γνωστό επίσης και ως Wi-Fi, προσφέρει μέγιστο ρυθμό δεδομένων στα 11Mbps και λειτουργεί στη ζώνη συχνοτήτων 2.4GHz με διαμόρφωση DSSS. Η εφαρμογή ασύρματων LAN πλεονεκτεί σε σχέση με τα ενσύρματα γιατί:

- η εγκατάσταση είναι εύκολη
- πιο οικονομικά
- παρέχουν κινητικότητα των συσκευών.
- χρησιμοποιούνται σε διάφορες εφαρμογές (π.χ αυτοματισμό, προστασία υποσταθμών διανομής και στην απεικόνιση και τον έλεγχο των κατανεμημένωνενεργειακών πόρων (DERs)

WiMAX

Η τεχνολογία WiMAX (Worldwide inter-operability for Microwave Access) είναι μέρος της σειράς προτύπων 802.16 για δίκτυα WMAN (Wireless Metropolitan Area Network). Κύριος στόχος του WiMAX είναι να επιτύχει διαλειτουργικότητα σε

παγκόσμιο επίπεδο για μικροκυματική πρόσβαση. Το WiMAX παρέχει ρυθμούς δεδομένων μέχρι 70Mbps και απόσταση κάλυψης ως 48km γεγονός που τα καθιστά πιο κατάλληλα για επικοινωνίες μεγάλων αποστάσεων.

Κάποιες από τις εφαρμογές των SG που θα μπορούσε να χρησιμοποιηθεί το WiMAX είναι:

- Ασύρματα Αυτόματα Συστήματα Ανάγνωσης Μετρητών (WAMRS),
- Τιμολόγηση σε πραγματικό χρόνο (Real-time Pricing),
- Ανίχνευση και αποκατάσταση διακοπής λειτουργίας.

Τα πλεονεκτήματα της τεχνολογίας WiMAX είναι:

- μικρότερο κόστος ανάπτυξης και λειτουργίας,
- η ομαλή επικοινωνία,
- οι υψηλοί ρυθμοί μετάδοσης (ως τα 75Mbps),
- το επαρκές εύρος ζώνης
- η επεκτασιμότητα.

Τα αρνητικά του WiMAX είναι:

- το εύρος ζώνης διαμοιράζεται με τους χρήστες. Αυτό εξηγείται από το γεγονός ότι οι συχνότητες πάνω από 10GHz δεν μπορούν να διαδοθούν μέσω εμποδίων.
- παρουσιάζει ασυμμετρία των ταχυτήτων στις ζεύξεις ανόδου και καθόδου,
- το trade off μεταξύ απόστασης και ρυθμού μετάδοσης

Κυψελωτές Επικοινωνίες (Cellular network Communication)

Χρησιμοποιώντας την υπάρχουσα υποδομή επικοινωνιών, οι επιχειρήσεις αποφεύγουν σημαντικό κόστος και χρόνο που θα απαιτούνταν για τη δημιουργία μιας νέας και αποκλειστικής υποδομής. Οι 3G / 4G τεχνολογίες λειτουργούν στο φάσμα 824-894MHz/1900MHz, που είναι οι αδειοδοτημένες ζώνες συχνοτήτων. Η τοπολογία του δικτύου αποτελείται από κυψέλες, οι οποίες καλύπτουν μια ευρεία περιοχή και εξυπηρετούνται η καθεμία από τουλάχιστον ένα σταθμό βάσης.

Κάθε κυψέλη χρησιμοποιεί διαφορετικό σύνολο συχνοτήτων από τις γειτονικές της, ώστε να αποφεύγεται η παρεμβολή και να παρέχεται εγγυημένο εύρος ζώνης εντός των ορίων της.

Τα πλεονεκτήματα στα κυψελωτά δίκτυα είναι ότι:

- οι πάροχοι δε θα επιβαρυνθούν με κόστοςκατασκευής.
- παρέχεται επαρκές εύρος ζώνης για αρκετές από τις εφαρμογές,
- με την πανάπτυξη στις 3G / 4G τεχνολογίες, ο ρυθμός δεδομένων και η ποιότητα υπηρεσίας (QoS) βελτιώνονται πολύ γρήγορα.

Μερικές κρίσιμες εφαρμογές των έξυπνων δικτύων είναι ότι :

- χρειάζονται αδιάλειπτη διαθεσιμότητα επικοινωνιών.
- οι κυψελωτές επικοινωνίες είναι ακατάλληλες για εφαρμογές που σχετίζονται με πολλά δεδομένα και απαιτούν πολύ μεγάλο εύρος ζώνης.

ZigBee

Το ZigBee είναι μια αξιόπιστη, αποτελεσματική ως προς το κόστος, ασύρματη τεχνολογία επικοινωνιών, χαμηλή σε κατανάλωση ισχύος, ρυθμούς μετάδοσης δεδομένων,κόστος εφαρμογής και πολυπλοκότητα. Είναι ιδανική τεχνολογία για έξυπνο φωτισμό, παρακολούθηση της ενέργειας, οικιακό αυτοματισμό κλπ. Το ZigBee και το ZigBee Smart Energy Profile (SEP) έχουν αναγνωριστεί ως τα πιο κατάλληλα πρότυπα για εφαρμογές έξυπνου δικτύου στον οικιακό τομέα. Το ZigBee προσφέρει ρυθμούς δεδομένων 20-250Kbps και κάλυψη 10-100m.

Είναι ιδανικό για εφαρμογές έξυπνων δικτύων λόγω:

- της απλότητας,
- την κινητικότητα που παρέχει,
- την ευρωστία,
- τις χαμηλές απαιτήσεις εύρους ζώνης,
- τη λειτουργία του σε μη αδειοδοτημένο φάσμα
- την ευκολία εφαρμογής του.

Μερικά από τα αρνητικά του χαρακτηριστικά είναι :

- οι μικρές ικανότητες επεξεργασίας,
- το μικρό μέγεθος μνήμης,
- οι μικρές απαιτήσεις καθυστέρησης
- οι παρεμβολές από άλλες συσκευές που μοιράζονται το ίδιο μέσο μετάδοσης.

Ασύρματα Δίκτυα Πλέγματος (Wireless Mesh Networks – WMN)

Ένα δίκτυο πλέγματος είναι ένα ευέλικτο δίκτυο αποτελούμενο από μια ομάδα κόμβων, όπου νέοι κόμβοι μπορούν να ενταχθούν στην ομάδα και κάθε κόμβος μπορεί να δράσει ως ανεξάρτητος δρομολογητής. Τα WMN συχνά αποτελούνται από:

- πελάτες πλέγματος (φορητοί υπολογιστές, κινητά τηλέφωνα κτλπ),
- δρομολογητές πλέγματος που προωθούν την κίνηση από και προς τις πύλες, οι οποίες δεν είναι απαραίτητο να είναι συνδεδεμένες στο διαδίκτυο
- πύλες.

Τα δίκτυα αυτά είναι αξιόπιστα, προσφέρουν πλεονασμό και έχουν την ιδιότητα της αυτό-θεραπείας, δηλαδή επιτρέπει στα σήματα επικοινωνιών να βρίσκουν εναλλακτική διαδρομή μέσω των ενεργών κόμβων,σε περίπτωση που οποιοσδήποτε κόμβος εγκαταλείψει το δίκτυο.

Τα ασύρματα δίκτυα πλέγματος και τα δίκτυα χαμηλής ισχύος και χαμηλού ρυθμού (lowpower and low-rate, LPLR) παίζουν σημαντικό ρόλο στην επικοινωνιακή υποδομή των έξυπνων δικτύων. Τα WMN,είναι σχεδιασμένα για επικοινωνία σε επίπεδο κοινότητας και θεωρούνται μία από τις προβλεπόμενες προσεγγίσεις για να υποστηρίξουν τα έξυπνα δίκτυα.

Δορυφορικές επικοινωνίες

Οι δορυφορικές επικοινωνίες είναι μια καλή λύση για τον απομακρυσμένο έλεγχο και την παρακολούθηση, επειδή παρέχουν παγκόσμια κάλυψη και γρήγορη εγκατάσταση. Τέτοιου είδους επικοινωνία μπορεί εύκολα να εγκατασταθεί και απαιτεί μόνο την απόκτηση του απαραίτητου εξοπλισμού δορυφορικής επικοινωνίας. Οι δορυφόροι μπορούν να χρησιμοποιηθούν ως εφεδρικό σύστημα για τα υπάρχοντα

δίκτυα επικοινωνιών προκειμένου να εξασφαλιστεί η ασφαλής λειτουργία και η παράδοση της κρίσιμης κίνησης δεδομένων σε περιπτώσεις καταστροφών ή βλαβών του επίγειου συστήματος επικοινωνιών,

Μερικά απο τα μειονεκτήματα των δορυφορικών επικοινωνιών είναι :

- Ότι έχει σημαντικά υψηλότερη καθυστέρηση από αυτή ενός επίγειου συστήματος.
- Τα χαρακτηριστικά ενός δορυφορικού καναλιού ποικίλλουν ανάλογα με την επίδραση της εξασθένησης και τις καιρικές συνθήκες.

Mobile Broadband Wireless Access (MBWA)

Το πρότυπο 802.20 για MBWA μπορεί να χρησιμοποιηθεί σε εφαρμογές έξυπνων δικτύων, όπως ευρυζωνική επικοινωνία για plug-in ηλεκτρικά οχήματα, για απεικόνιση ή στα συστήματα SCADA. Παρέχει υψηλό εύρος ζώνης, μεγάλη κινητικότητα και χαμηλή καθυστέρηση (latency) στις αδειοδοτημένες ζώνες συχνοτήτων κάτω από τα 3.5GHz, χρησιμοποιώντας τα θετικά χαρακτηριστικά των IEEE 802.11 WLANs και IEEE 802.16 WMANs. Προσφέρει σε πραγματικό χρόνο μέγιστο ρυθμό δεδομένων από 1Mbps έως 20Mbps.

Ψηφιακή Τεχνολογία Μικροκυμάτων (Digital Microwave Technology)

Η τεχνολογία αυτή προσφέρει κάλυψη πολύ μεγάλων αποστάσεων, ως 60km.Μπορεί να χρησιμοποιηθεί στα έξυπνα δίκτυα για να υποστηρίξει επικοινωνία σημείου προς σημείο. Είναι επιρρεπής στις παρεμβολές λόγω πολλαπλών διαδρομών και λόγω ατμοσφαιρικών κατακρημνίσεων. Επίσης, η κρυπτογράφηση, για λόγους ασφαλείας, μπορεί να επιφέρει πρόσθετη καθυστέρηση καθώς χρειάζεται μεγαλύτερου μεγέθους μηνύματα.

Ελεύθερου χώρου οπτική επικοινωνία (Free-space optical communication)

Είναι μια τεχνολογία οπτικής επικοινωνίας, όπου χρησιμοποιεί το φως που μεταδίδεται στον ελεύθερο χώρο για τη μετάδοση δεδομένων από σημείο σε σημείο. Παρέχει υψηλούς ρυθμούς μετάδοσης και είναι ασφαλής. Παρέχει μεγάλες αποστάσεις σημείου-προς-σημείο επικοινωνίας σε απομακρυσμένες ή αγροτικές περιοχές και σε πυκνοκατοικημένες αστικές περιοχές, όπου οι λύσεις μικροκυμάτων δεν είναι πρακτικές από τη σκοπιά της παρεμβολής. Ωστόσο, τα χαρακτηριστικά και η

ποιότητα της επικοινωνίας επηρεάζεται σε μεγάλο βαθμό από τα εμπόδια (π.χ. από κτήρια και λόφους) και από περιβαλλοντικούς περιορισμούς (π.χ. βροχή).

Bluetooth

Το Bluetooth συμπεριλαμβάνεται στο πρότυπο IEEE 802.15.1 για τα ασύρματα προσωπικά δίκτυα.Είναι πρότυπο χαμηλής ισχύος και μικρού εύρους φάσματος. Ανάλογα με τη ρύθμιση παραμέτρων της επικοινωνίας, προσφέρει κάλυψη μεταξύ 1m-100m. Μπορεί να χρησιμοποιηθεί για τοπικές, online εφαρμογές απεικόνισης ως μέροστων συστημάτων αυτοματισμού των υποσταθμών.

2.5.2 Ενσύρματες Τεχνολογίες (Wireline/Wired Technologies).

Οι ενσύρματες τεχνολογίες γενικά προτιμούνται από τις επιχειρήσεις κοινής ωφέλειας, χρησιμοποιούνται για την κατασκευή επικοινωνιακών δικτύων και αφιερωμένα καλώδια που είναι διαφορετικά από τις ηλεκτρικές γραμμές. Ανάλογα με το μέσο μετάδοσης που χρησιμοποιείται, τα ενσύρματα δίκτυα περιλαμβάνουν τα SONET/SDH, Ethernet, DSL και ομοαξονικού καλωδίου δίκτυα πρόσβασης.

Οι τεχνολογίες οπτικών ινών και οπτικών δικτύων προσφέρουν πλατφόρμες που παρέχουν πολλαπλές υπηρεσίες, οι οποίες υποστηρίζουν εφαρμογές IP και Ethernet. Αυτό έχει ως αποτέλεσμα την απλότητας και την αποδοτικότητα του Ethernet όσο αφορά το κόστος. Η υιοθέτηση του IP με MPLS (MultiProtocol Label Switching) για την επίτευξη μεταφοράς πάνω από SONET/SDH στα υπάρχοντα δίκτυα μεταγωγής πακέτων (γνωστά ως carrier Ethernet) θα ενισχύσει την αξιοπιστία, την ποιότητα υπηρεσίας και την ασφάλεια για τις κρίσιμες εφαρμογές των έξυπνων δικτύων.

Τα Ethernet και Gigabit παθητικά οπτικά δίκτυα (EPON/GPON) χρησιμοποιούν οπτικές-ηλεκτρικές προσεγγίσεις για την παροχή επαρκούς χωρητικότητας για την παράδοση μεγάλων δεδομένων, καθώς και υψηλής ταχύτητας μετάδοση στα δίκτυα πρόσβασης. Εκμεταλλεύονται την πολυπλεξία διαίρεσης μήκους κύματος (Wavelength Division Multiplexing - WDM).

Powerline Communication (PLC)

Η τεχνική αυτή χρησιμοποιεί τις ηλεκτρικές γραμμές μεταφοράς ως επικοινωνιακό μέσο ώστε να παρέχει ένα δίκτυο επικοινωνιών όπως το Διαδίκτυο, αλλά ταυτόχρονα υποστηρίζει τις κλασσικές υπηρεσίες που σχετίζονται με τη διανομή ενέργειας.

Οι τεχνολογίες που χρησιμοποιούνται στο PLC είναι κυρίως στενού εύρους ζώνης που λειτουργούν σε χαμηλές συχνότητες και ευρυζωνικές που λειτουργούν σε υψηλές συχνότητες . Σε ένα τυπικό PLC δίκτυο, οι έξυπνοι μετρητές συνδέονται στο συγκεντρωτή δεδομένων μέσω ηλεκτρικών γραμμών μεταφοράς και τα δεδομένα μεταφέρονται στο κέντρο δεδομένων με τεχνολογίες κυψελωτών δικτύων. Η χρήση σε οικιακά δίκτυα (HAN) είναι η μεγαλύτερη εφαρμογή για την PLC τεχνολογία όπως και σε αστικές περιοχές για εφαρμογές όπως έξυπνες μετρήσεις, παρακολούθηση και έλεγχος.

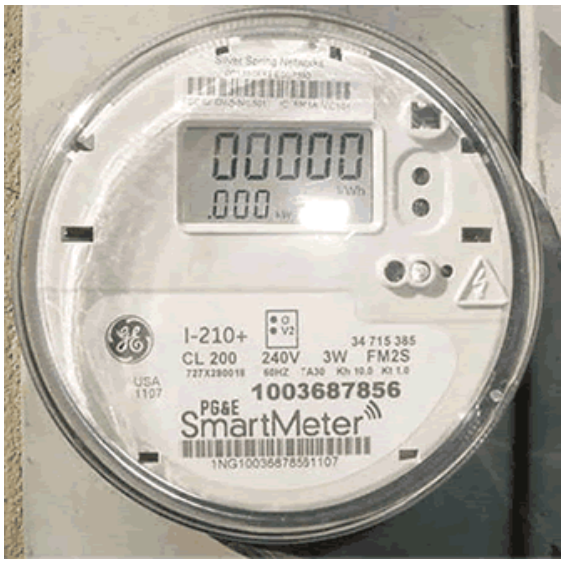
Παρόλα αυτά, το PLC αντιμετωπίζει προβλήματα εξασθένησης, θορύβου και παραμόρφωσης, που συναντώνται στις RF επικοινωνίες όταν υλοποιούνται μέσω των καλωδίων ηλεκτρικής ενέργειας.

Digital Subscriber Lines (DSL)

Είναι μία τεχνολογία υψηλής ταχύτητας μεταφοράς ψηφιακών δεδομένων που χρησιμοποιεί τα καλώδια του τηλεφωνικού δικτύου. Η ευρεία διαθεσιμότητα, το χαμηλό κόστος και η υψηλού εύρους μετάδοση δεδομένων αποτελούν τους πιο σημαντικούς λόγους που θέτουν το DSL στις πρώτες θέσεις των υποψήφιων τεχνολογιών για τους παρόχους ηλεκτρισμού στην εφαρμογή της ιδέας των έξυπνων δικτύων. Ωστόσο, η αξιοπιστία και ο πιθανός χρόνος μη-λειτουργίας της DSL τεχνολογίας πιθανόν να μην είναι αποδεκτοί για κρίσιμες εφαρμογές. Η εξάρτηση από την απόσταση και η έλλειψη προτυποποίησης μπορεί να προκαλέσουν επιπλέον προβλήματα.

2.6 Έξυπνος Ψηφιακός Μετρητής (Smart Meter-SM)

Αποτελεί μια ηλεκτρονική συσκευή μέτρησης με δυνατότητα επικοινωνίας με άλλες συσκευές. Η συσκευή μετράει την ενέργεια που χρησιμοποιείται και στέλνει τις πληροφορίες στο σύστημα και από κει καταλήγουν στον πελάτη, ενημερώνοντας τον για την εκάστοτε κατανάλωση του και το αντίστοιχο κόστος αυτής. Οι έξυπνοι μετρητές έχουν τη δυνατότητα αμφίδρομης επικοινωνίας. Αποτελούν ένα οικονομικό τρόπο για μέτρηση και παρακολούθηση της κατανάλωσης, που επιτρέπει στην καλύτερη ρύθμιση της παραγωγής βασιζόμενη σε ημερήσια δεδομένα πραγματικού χρόνου.



Εικόνα 2.3- Έξυπνος μετρητής

Οι Έξυπνοι Μετρητές ποικίλλουν στο σχεδιασμό ανάλογα με τις συγκεκριμένες συνθήκες στην αγορά, στα διαφορετικά κράτη μέλη, και τους διαφορετικούς τύπους μετρητών σε κάθε κτίριο. Η πλειοψηφία περιλαμβάνει τις ακόλουθες λειτουργίες :

- Ακριβής μέτρηση της ηλεκτρικής ενέργειας, του αερίου, του νερού ή της θερμότητας
- Μια δομή μετάδοσης δεδομένων

- Ένα περιβάλλον IT που ταιριάζει με τα υπόλοιπα στοιχεία
- Ένα σύστημα τιμολογίων κατάλληλο για τον καταναλωτή
- Τοπική προβολή των στοιχείων ενεργειακής χρήσης

2.6.1 Τηλεπικοινωνιακή υποδομή

- ✓ **Radio Frequency** : Ενσωματώνεται συσκεύη αποστολής σημάτων χαμηλού κόστους στον ήδη υπάρχων μετρητή και η πληροφορία λαμβάνεται από το Interface του μετρητή και γίνεται η μεταφορά στον transmitter. Αυτός με την σειρά του μεταφέρει την πληροφορία για αξιολόγηση στο Operation System.
- ✓ **Με GPRS** : Data transmission with packet switching μέσω κινητού τηλεφώνου. Παρέχει 24ωρη ανταλλάγη δεδομένων, συνεχή με υψηλές ταχύτητες επικοινωνίας. Κάθε μετρητής στο σύστημα έχει το δικό του GPRS module. Επειδή το GPRS είναι στο μετρητή αποφεύγονται εξωτερικές επιρροές και παρέχεται φυσική προστασία και ασφάλεια. Οι πληροφορίες κατανάλωσης των μετρητών που είναι φυσικά απομακρυσμένοι μεταξύ τους γίνεται με το υπάρχον GSM δίκτυο.
- ✓ **RS-485** : Μέσω του RS-485 γίνεται έλεγχος και καταγραφή ημερομηνίας και η ώρας μέσω ενός Real-Time Clock.
- ✓ **Wireless Network Σύνδεση** : Μπορεί να χρησιμοποιηθεί μεταξύ του host computer και του base station. Σε τοπικές εφαρμογές μπορούν να χρησιμοποιηθούν PSTN, PLC, IP network. H RF τεχνολογία είναι η πιο διαδεδομένη μορφή αποστολής σε AMR συστήματα.

2.7 Τα Συστήματα SCADA

Με τον όρο SCADA (Supervisory Control and Data Acquisition- Εποπτικός Έλεγχος και Συλλογή Δεδομένων) εννοούμε:

« *Τα συστήματα εκείνα, που επιτρέπουν στο χειριστή μιας κατανεμημένης στο χώρο διεργασίας να συλλέγει πληροφορίες από διάφορα σημεία σε ένα κεντρικό υπολογιστή,*

από τον οποίο μπορεί επίσης να εκτελεί χειρισμούς ή να στέλνει εντολές ελέγχου έχοντας εποπτεία της διαδικασίας ».

Τα SCADA χρησιμοποιούνται κυρίως:

- Στη βιομηχανία για την αυτοματοποίηση της παραγωγής και των σχετικών με αυτή διαδικασιών.
- Στα δίκτυα των επιχειρήσεων και οργανισμών κοινής ωφελείας (δίκτυα - μεταφοράς και διανομής ηλεκτρικής ενέργειας, νερού ή φυσικού αερίου, δίκτυα αποχέτευσης)
- Στα συστήματα αυτοματισμού πολυώροφων κτιρίων (π.χ. νοσοκομεία, ξενοδοχεία) ή άλλων μεγάλων εγκαταστάσεων (π.χ. αεροδρόμια),
- Στα σιδηροδρομικά δίκτυα
- Στη γεωργία (δίκτυα άρδευσης, αυτοματοποίηση μεγάλων γεωργικών μονάδων).

Σε ένα σύστημα SCADA σημαντικό ρόλο παίζει το λογισμικό του κέντρου ελέγχου. Η ποιότητα του λογισμικού αυτού είναι καθοριστικής σημασίας για την καλή λειτουργία ολόκληρου του συστήματος. Όταν το λογισμικό του κέντρου ελέγχου είναι απαλλαγμένο από σφάλματα και δυσλειτουργίες, ανταποκρίνεται σωστά και αξιόπιστα σε οτιδήποτε μπορεί να συμβεί κατά τη λειτουργία του συστήματος, είναι εύχρηστο, ευέλικτο και μπορεί να δεχτεί όλες τις απαιτούμενες επεκτάσεις. Αντίθετα, όταν το λογισμικό του κέντρου ελέγχου δεν έχει τα παραπάνω χαρακτηριστικά, τότε το σύστημα SCADA αδυνατεί να καλύψει τις ανάγκες, για τις οποίες σχεδιάστηκε. Επιπλέον, τυχόν ελλείψεις ή αστοχίες στις συσκευές πεδίου, τους τοπικούς ελεγκτές ή το σύστημα επικοινωνίας μπορούν να διορθωθούν σχετικά εύκολα με απομάκρυνση των βαθμίδων, που δεν λειτουργούν ικανοποιητικά και αντικατάστασή τους από άλλες, διαφορετικής τεχνολογίας ή ανώτερης ποιότητας.

Η αντικατάσταση αυτή δεν συνιστά αλλαγή συστήματος SCADA, υπό την προϋπόθεση φυσικά ότι το υπάρχον κέντρο ελέγχου υποστηρίζει τις νέες βαθμίδες. Αντίθετα, αν το κέντρο ελέγχου δεν λειτουργεί ικανοποιητικά τότε μιλάμε για προμήθεια νέου συστήματος. Έτσι, ο όρος SCADA χρησιμοποιείται συχνά στην πράξη

με μια ειδικότερη έννοια και σημαίνει απλώς το λογισμικό του κέντρου ελέγχου και όχι ολόκληρο το σύστημα.

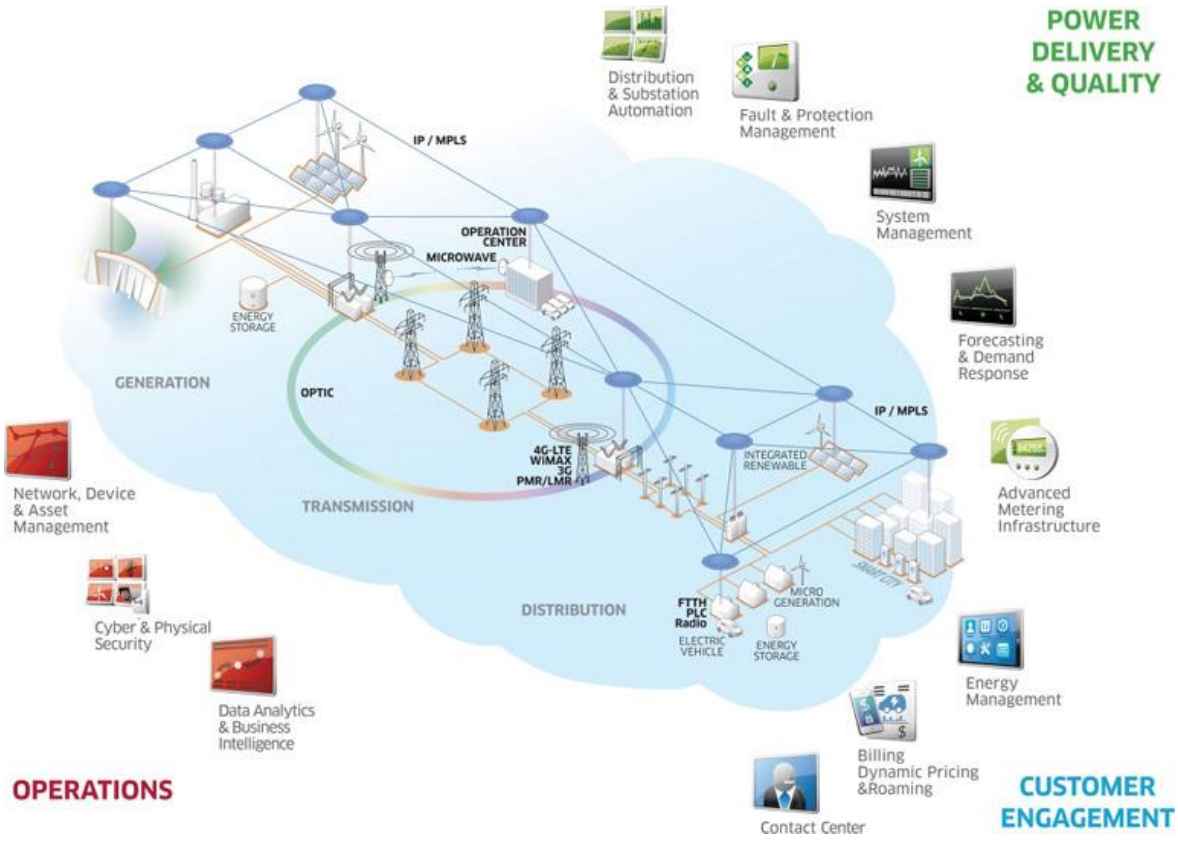
Το κέντρο ελέγχου ενός συστήματος SCADA είναι ένα εξαιρετικά πολύπλοκο πρόγραμμα. Διαχειρίζεται σωστά έναν όγκο πληροφοριών πραγματικού χρόνου και τις δρομολογεί με τέτοιο τρόπο ώστε ο κάθε χρήστης του συστήματος και η κάθε μηχανή, που συνδέεται σε αυτό, να έχει την πληροφορία που χρειάζεται τη στιγμή και στη μορφή που θέλει. Ακόμα, οι ανάγκες της επιχείρισης όσο και οι διαθέσιμες τεχνολογικές λύσεις μεταβάλλονται με την πάροδο του χρόνου και το λογισμικό του κέντρου ελέγχου πρέπει να προσαρμόζεται εύκολα και ομαλά στις καινούργιες κάθε φορά συνθήκες.

Οι απαιτήσεις από το λογισμικό των SCADA είναι πολλές φορές τόσο πολύπλοκες και διαφορετικές μεταξύ τους, που να είναι αδύνατον να καλυφθούν από τις δυνατότητες ενός μόνου εργαλείου, όσο πλούσιο και αν είναι αυτό. Είναι πολύ σημαντικό ένα πρόγραμμα SCADA να μπορεί να συνεργάζεται με άλλα προγράμματα και να ενσωματώνει στις εφαρμογές του εξειδικευμένο λογισμικό άλλων κατασκευαστών όποτε χρειαστεί.

Η αγορά ζητά κέντρα ελέγχου ανοιχτής αρχιτεκτονικής, βασισμένα σε καθιερωμένα διεθνή πρότυπα, τα οποία επιτέπουν τη συνένωση και τη συνεργασία ανεξάρτητων μεταξύ τους προϊόντων υλικού ή λογισμικού, τα οποία ενδεχομένως προέρχονται από διαφορετικούς κατασκευαστές. Η σύνδεση των διαφορετικών αυτών κομματιών και η ενσωμάτωσή τους σε ένα ολοκληρωμένο σύστημα πραγματοποιείται με τη βοήθεια ειδικών τεχνολογιών, που περιγράφονται συνολικά με τον όρο «τεχνολογίες ολοκλήρωσης» (integration technologies). Στις επόμενες ενότητες θα γνωρίσουμε κάποιες βασικές τέτοιες τεχνολογίες.

2.8 Ενσωμάτωση SCADA σε Smart Grid

Η ενσωμάτωση SCADA στο Smart Grid, δεν είναι δύσκολη. Συνδέονται μεταξύ τους με ηλεκτρικά δίκτυα και δίκτυα δεδομένων. Επιτρέπει την κεντρική και κατανεμημένη ομαδοποίηση των πληροφοριών και κάνει έλεγχο ολόκληρης της χρησιμότητας του ηλεκτρικού δικτύου της συσκευής όπως απεικονίζεται στην εικόνα παρακάτω.



Εικόνα 2.4 SCADA/Smart Grid Integration (Source: http://www2.alcatel-lucent.com)

Το σύστημα SCADA παρέχει στον καταναλωτή, μέσω της διασύνδεσης των συστημάτων διαχείρισης ενέργειας, να μπορέσει να διαχειρίζεται τη δική του χρήση ενέργειας και να έχει και τον έλεγχο του κόστους της. Επιτρέπει το δίκτυο να διορθώνει μόνο του κάποια προβήματα με άμεση ανταπόκριση σε διακοπές, σε ζητήματα ποιότητας της ηλεκτρικής ενέργειας, καθώς και τα προβλήματα του συστήματος. Είναι ανεκτικό τόσο σε σωματικές όσο και σε επιθέσεις στον

κυβερνοχώρο, και βελτιστοποιεί τα περιουσιακά στοιχεία του δικτύου με την παρακολούθηση και τη βελτιστοποίηση τους, ελαχιστοποιώντας ταυτόχρονα το κόστος συντήρησης και λειτουργίας. Επιπλέον, επιτρέπει ανταγωνιστικές αγορές ενέργειας και μετριάζει την επέκταση που συχνά προκύπτει στην προσπάθεια να εξασφαλίσει εγγυήση τιμών.

Για να παρέχει επαρκώς και να γίνεται η διαχείριση των προϊόντων και των υπηρεσιών που καθίστασται δυνατό από το Smart Grid, είναι απαραίτητη η ευφυΐα και ο ελέγχος που πρέπει να υπάρχουν σε όλο το μήκος της αλυσίδας εφοδιασμού. Αυτό περιλαμβάνει την παραγωγή και μεταφορά ηλεκτρικής ενέργειας από την έναρξη μέχρι την παράδοση των τελικών σημείων στην πλευρά του μετρητή του πελάτη και περιλαμβάνει τόσο σταθερές όσο και κινητές συσκευές στην αρχιτεκτονική.

Οι ψηφιακές επικοινωνίες σε ένα Smart Grid εμφανίζονται προοδευτικά σε ποικιλία συσκευών, τεχνολογιών, καθώς και τα πρωτόκολλα που περιλαμβάνουν ενσύρματο και ασύρματο τηλέφωνο, φωνή και αποστολή δεδομένων ραδιοφώνου, οπτικών ινών, μεταφορά γραμμής ισχύος, και τηλεόραση. Το DCS(Decision Control Software) επιτρέπει τη δυναμική διαχείριση του δικτύου, που περιλαμβάνει την παρακολούθηση ενός σημαντικού αριθμού σημείων ελέγχου. Για να είναι πλήρως αποτελεσματικό και λειτουργικό, η παρακολούθηση γίνεται για κάθε γραμμή ηλεκτρικής ενέργειας και κομμάτι του εξοπλισμού στο σύστημα διανομής, επιτρέποντας στους πελάτες να παρακολουθούν και να ελέγχουν τις δικές τους συσκευές και την χρήση. Αυτό οδηγεί σε σημαντικούς όγκους δεδομένων που πρέπει να οργανώνονται, να αναλυθούν, και να χρησιμοποιηθούν τόσο για χειροκίνητη όσο και για αυτοματοποιημένη απόφαση του λογισμικού που έρχεται σε δύο βασικές κατηγορίες: αποκεντρωμένη και back office.

ΚΕΦΑΛΑΙΟ ΤΡΙΤΟ

3.1 Ασφάλεια και Smart Grid

Μέχρι στιγμής έχει γίνει λόγος για τα SG όσο αφορά την αποδοτικότητα, την αξιοπιστία, την βελτιστοποίηση της διαδικασίας παραγωγής και την εξοικονόμιση ηλεκτρικής ενέργειας κι όχι όσο αφορά την ασφάλεια. Όπως αναφέρθηκε παραπάνω, σε ένα SG διακινούνται τεράστιοι όγκοι δεδομένων, οι οποίοι αφορούν μοτίβα κατανάλωσης των πελατών, με στόχο την καλύτερη πρόβλεψη ζήτησης για τον ισοζυγισμό της παραγωγής ώστε ο πελάτης, με κάποιες κατευθυντήριες γραμμές και εισηγήσεις σχετικά με το πότε είναι πιο οικονομικά για τον ίδιο, να προγραμματίσει ορισμένες δουλειές του πιο ενεργειακά δαπανηρές.

Αρκεί μόνο να σκεφτεί κανείς πόση πληροφορία μπορεί να εξάγει κανείς για τους ενοίκους ενός σπιτιού ή τους υπαλλήλους μιας εταιρείας, μόνο και μόνο μελετώντας τα καθημερινά αυτά μοτίβα κατανάλωσης, ώστε να αντιληφθεί πόσο σημαντικό ρόλο έχει η ασφάλεια ενός Έξυπνου δικτύου. Επίσης, υπάρχει το ενδεχόμενο μιας παρείσφρησης στο δίκτυο ενός κακόβουλου χρήστη, ο οποίος εκμεταλλευόμενος την απουσία κρυπτογράφησης της πληροφορίας στο AMI δίκτυο ή της απουσίας αυθεντικοποίησης πριν να επιτραπεί η αποστολή πληροφορίας, καταφέρνει να προσποιηθεί πως είναι το κέντρο ελέγχου που αποστέλλει πληροφορία προς το μετρητή. Έτσι, θα είναι σε θέση να διαβάσει τα δεδομένα που αποστέλλονται ή να αποστείλει ψευδή μηνύματα προς τον μετρητή

Ακόμα ένας κίνδυνος είναι οι ενημερώσεις του λογισμικού στα κέντρα ελέγχου και τα επιμέρους τμήματα του δικτύου. Η δυνατότητα ενημέρωσης της έκδοσης ενός λογισμικού επιτρέπει την εμπλούτιση του λογισμικού ακόμα και μετά την κυκλοφορία του πράγμα το οποίο καθιστά τον χρήστη προετοιμασμένο ώστε να αντιμετωπίσει τις νέες απειλές. Όμως, αυτό μπορεί να αποτελέσει μια από τις σημαντικότερες αδυναμίες του δικτύου αφού ένας κακόβουλος χρήστης ο οποίος ανεβάζει στο δίκτυο μια «ενημέρωση» ενός συγκεκριμένου λογισμικού, η οποία είναι ένα επιβλαβές λογισμικό και θέτει σε κίνδυνο ολόκληρο το δίκτυο. Ένα τέτοιο παράδειγμα είναι, ο ιός Stuxnet ο

οποίος δημιουργήθηκε το 2010 για να επιμολύνει SCADA συστήματακατασκευασμένα από τη SIEMENS στο Ιράν

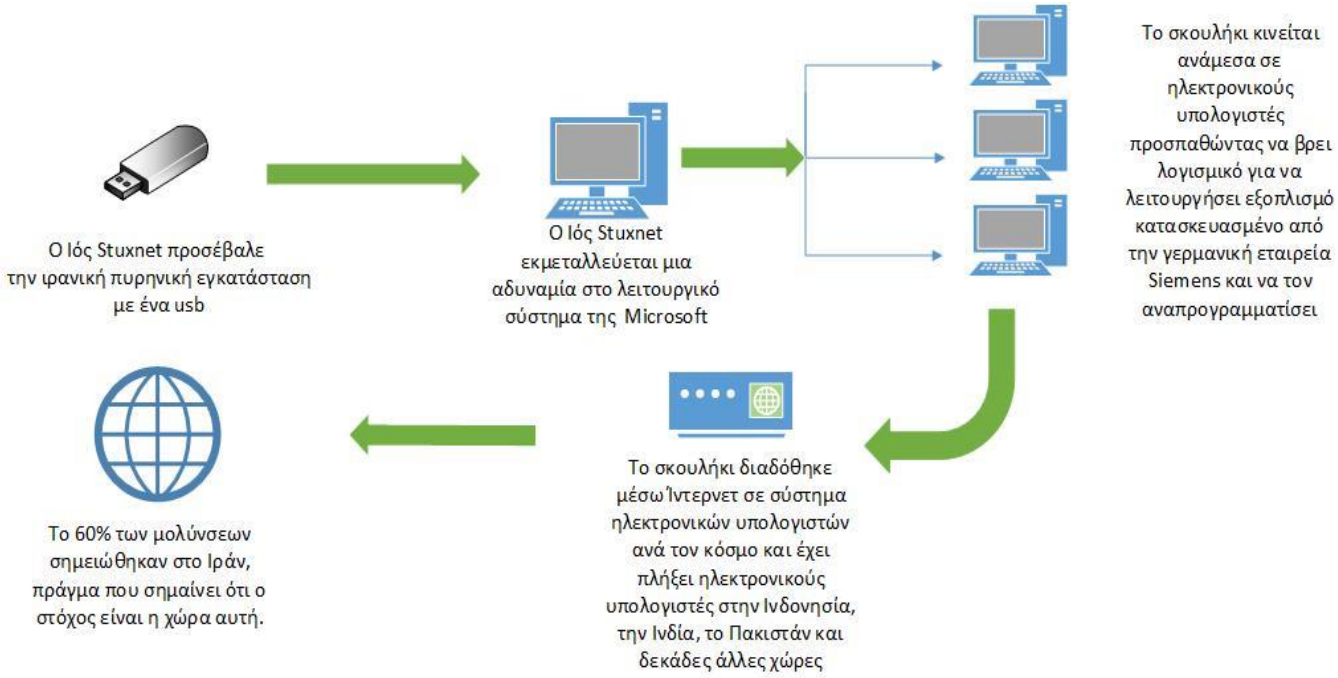
3.2 Ο ιός Stuxnet

Ο ιός Stuxnet είναι ένα από τα ισχυρότερα όπλα κυβερνοπολέμου που έχει κατασκευαστεί ποτέ και για πρώτη φορά αποδεικνύει στην πράξη αυτό που εδώ και χρόνια φοβούνταν οι ειδικοί των υπολογιστών: ότι ένας ιός κάποια στιγμή θα είναι σε θέση να πλήξει ζωτικές υποδομές μιας χώρας, όπως σταθμούς ενέργειας, διυλιστήρια και δίκτυα ενέργειας, και είτε να τα αποδιοργανώσει, είτε ακόμα και να τα θέσει υπό τον έλεγχό του. Έκανε την εμφάνισή του τον Ιούνιο του 2010, χτυπώντας αρχεία τραπεζών, δεδομένα σταθμών παραγωγής ενέργειας, συστήματα ελέγχου κυκλοφορίας και εργοστάσια σε ολόκληρο τον κόσμο.

Τα μηχανήματα των εργοστασίων συνήθως δεν ελέγχονται άμεσα από υπολογιστές,. Ο βιομηχανικός εξοπλισμός είναι συχνά αυτοματοποιημένος και ελέγχεται από ένα ξεχωριστό σύστημα υπολογιστών με το δικό του λογισμικό, χωρίς καν την ανθρώπινη επέμβαση. Τα συστήματα αυτά συνήθως χρησιμοποιούν τη δική τους γλώσσα προγραμματισμού και όχι τις συνήθεις για Windows, Mac ή Linux, πράγμα που κάνει δύσκολη τη ζωή των κακόβουλων χρηστών. Για αυτό το λόγο, άλλωστε, χρειάζονται ειδικού τύπου ιοί για να διεισδύσουν σε τέτοια συστήματα και ο Stuxnet εκμεταλλεύτηκε το γεγονός ότι καμιά φορά ένας προσωπικός υπολογιστής που "τρέχει" Windows, μπορεί να εποπτεύει ένα βιομηχανικό σύστημα.

Βασικός στόχος του ιού Stuxnet ήταν οι εγκαταστάσεις εμπλουτισμού ουρανίου του Ιράν. Ο ιός κατάφερε να διεισδύσει στους ηλεκτρονικούς υπολογιστές που ελέγχουν τα συστήματα φυγοκέντρισης στις πυρηνικές εγκαταστάσεις της Νατάνζ, προκαλώντας δυσλειτουργίες και υλικές ζημιές. Σύμφωνα με τους εμπειρογνώμονες, ο ιός παρεμβαλλόταν στο σύστημα μετάδοσης εντολών προς τους φυγοκεντριστές που χρησιμοποιούνται για τον εμπλουτισμό ουρανίου ώστε να αλλάξει την ταχύτητά τους με αποτέλεσμα να επηρεαστεί η παραγωγή του ουρανίου.

Πιο συγκεκριμένα, διαδίδονταν μέσω usb και αξιοποιούσε τέσσερις άγνωστες ευπάθειες των Windows με σκοπό να μολύνει τους υπολογιστές των θυμάτων, ενώ παράλληλα διέθετε και ένα rootkit, το οποίο ήταν εγκεκριμένο από πιστοποιητικό ασφάλειας, πιθανότατα κλεμμένο από τις εταιρείες Realtek Semicon ductors και JMicron. Ο ιός είχε σχεδιαστεί ώστε να μολύνει τα συστήματα εποπτικού ελέγχου και συλλογής δεδομένων (SCADA) της Siemens, που χρησιμοποιούνται για τον έλεγχο και την παρακολούθηση συγκεκριμένων βιομηχανικών διεργασιών.



Εικόνα 3. Ιός Stuxnet

3.3. Πρωτόκολλα ασφάλειας πληροφοριών

Οι ανάγκες ασφάλειας των μεταδιδόμενων πληροφοριών ώθησαν στην ανάπτυξη των σχετικών πρωτοκόλλων όπου είναι σχεδιασμένα να παρέχουν ταυτόχρονα εμπιστευτικότητα και ακεραιότητα των δεδομένων καθώς και

πιστοποίηση της ταυτότητας των συστημάτων που επικοινωνούν. Παρακάτω γίνεται ανάλυση αυτών.

1. **Ipsec**

Είναι ένα πρωτόκολλο ασφάλειας πληροφοριών που λειτουργεί στο στρώμα διαδικτύου της συλλογής πρωτοκόλλων του Διαδικτύου. Αναλαμβάνει την προστασία των πακέτων IP που αποστέλλονται μεταξύ δύο κόμβων . Η παρακάτω διαδικασία εγγυάται την τήρηση των προδιαγραφών εμπιστευτικότητας, ακεραιότητας και πιστοποίησης που παρέχει το πρωτόκολλο.

- Προβλέπει την αμοιβαία ταυτοποίηση των δύο οντοτήτων που επικοινωνούν μέσω της σύνδεσης.
- Ανταλλάσσονται τα κλειδιά κρυπτογράφησης που θα χρησιμοποιηθούν στη συγκεκριμένη σύνδεση και συμφωνείται ο αλγόριθμος κρυπτογράφησης.
- Τέλος, κάθε πακέτο IP ενθυλακώνεται σε ένα πακέτο IPsec. Εισάγεται μία τιμή επαλήθευσης της ακεραιότητας, και μετά γίνεται κρυπτογράφηση και αποστολή [16].

2. **Transport Layer Security (TLS)**

Χρησιμοποιείται στις ασφαλείς εκδόσεις δημοφιλών πρωτοκόλλων όπως τα HTTPS και FTPS. Το TLS προέρχεται από το πρωτόκολλο SSL (Secure Socket Layer) και εγγυάται εμπιστευτικότητα, ακεραιότητα και πιστοποίηση. Το πρωτόκολλο TLS λειτουργεί ενδιάμεσα στο στρώμα μεταφοράς και το στρώμα εφαρμογής της συλλογής πρωτοκόλλων του Διαδικτύου. Η πιστοποίηση των οντοτήτων που επικοινωνούν γίνεται με χρήση πιστοποιητικών X.509 που εκδίδονται από ανεξάρτητες αρχές και περιέχουν το δημόσιο κλειδί κρυπτογράφησης που χρησιμοποιεί κάθε οντότητα. Ακολούθως, αποκαθίσταται η σύνδεση με ασύμμετρη κρυπτογράφηση κατά την οποία συμφωνείται ο αλγόριθμος συμμετρικής κρυπτογράφησης και το τυχαίο συμμετρικό κλειδί που θα χρησιμοποιηθούν στη συνέχεια. Από το σημείο -και μετά, η επικοινωνία πραγματοποιείται με συμμετρική κρυπτογράφηση των πακέτων TCP στα οποία έχει προστεθεί μια τιμη ελέγχου της ακεραιότητας των δεδομένων.[16]

3.4 Απαιτήσεις ασφάλειας των Smart Grid στον κυβερνοχώρο

Οι απαιτήσεις ασφάλειας στον κυβερνοχώρο όσο αφορά την υποδομή των SG μπορούν να κατηγοριοποιηθούν ως εξής:

- απαιτήσεις ασφάλειας στον κυβερνοχώρο,
- τυπικές κυβερνοεπιθέσεις,
- αντίμετρα [18] [19][20]

Παρακάτω αναφέρεται η κύρια πηγή των κινδύνων για την ασφάλεια των πληροφοριών που προσδιορίζονται σε έξι τρωτά σημεία του έξυπνου δικτύου και τονίζουν τα σημεία εισόδου του εισβολέα στην υποδομή του έξυπνου δικτύου:

1) το σταθμό παραγωγής ενέργειας,

2) το Δίκτυο διανομής ηλεκτρικής ενέργειας,

3) τα εξελιγμένα συστήματα μέτρησης,

4) Ηλεκτρικά οχήματα,

5) Εσωτερικοί χρήστες του Διαδικτύου, και

6) Λειτουργικά Δίκτυα των συστημάτων μεταφοράς ηλεκτρικής ενέργειας [21][12].

Σύμφωνα με το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST), οι τρεις βασικές απαιτήσεις ασφάλειας στον κυβερνοχώρο για τα SG είναι: η διαθεσιμότητα, η ακεραιότητα, και η εμπιστευτικότητα.

Οι λειτουργίες των συστημάτων ενέργειας διαχειρίζονται την αξιοπιστία των δικτύων ενέργειας όπου η διαθεσιμότητα της είναι η πρωταρχική απαίτηση ενώ η ακεραιότητα των πληροφοριών θεωρείται δευτερεύουσα αλλά ταυτόχρονα και συνεχώς αυξανόμενης κρισιμότητας. Εξίσου σημαντική είναι η εμπιστευτικότητα των πληροφοριών των πελατών όσο αφορά τα προσωπικά δεδομένα των καταναλωτών.

Παρότι δίνεται έμφαση στα τυχαία και περιστασιακά προβλήματα ασφάλειας (πχ φυσικές κατάστροφές, ανθρώπινα ή τεχνικά λάθη), οι τεχνολογίες διαχείρησης συστημάτων ενέργειας μπορούν να χρησιμοποιηθούν και να επεκταθούν ώστε να παρέχουν και πρόσθετα μέτρα ασφάλειας.

Η διαθεσιμότητα είναι ο πιο σημαντικός στόχος ασφάλειας για αξιόπιστα συστήματα ενέργειας. Η χρονική καθυστέρηση που σχετίζεται με την διαθεσιμότητα ποικίλει ανάλογα με το είδος του εξοπλισμού και της πληροφορίας. Η ακεραιότητα των συστημάτων ενέργειας διαβεβαιώνει ότι:

- τα δεδομένα δεν έχουν διαφοροποιηθεί από μη εξουσιοδοτημένη πρόσβαση,
- η αυθεντικότητα της πηγής των δεδομένων, οι χρονοσφραγίδες των δεδομένων και η ποιότητα των δεδομένων είναι γνωστές και γνήσιες
- Η εμπιστευτικότητα είναι το λιγότερο κρίσιμο σημείο αξιοπιστίας των συστημάτων ενέργειας. Παρόλα αυτά, η κρισιμότητα της εμπιστευτικότητας ολοένα και αυξάνεται και ειδικά με την αυξανόμενη ύπαρξη πληροφοριών καταναλωτών στο διαδίκτυο. [17]

	Ενδεχόμενα αντίκτυπα επιπέδων		
	Χαμηλά	**Μέτρια**	**Υψηλά**
Εμπιστευτικότητα Διαφύλαξη εξουσιοδοτημένων περιορισμών στη πρόσβαση της πληροφορία και της γνωστοποίησης, περιλαμβάνει μέσα για την προστασία της ιδιωτικής ζωής και των περιουσιακών πληροφοριών	Η μη εξουσιοδοτημένη αποκάλυψη πληροφοριών αναμένεται να έχει **περιορισμένες** αρνητικές επιπτώσεις σχετικά με τις οργανωτικές πράξεις,το ενεργητικό του οργανισμού, ή τους ιδιώτες.	Η μη εξουσιοδοτημένη αποκάλυψη πληροφοριών αναμένεται να έχει **σοβαρές** αρνητικές επιπτώσεις σχετικά με τις οργανωτικές πράξεις,το ενεργητικό του οργανισμού, ή τους ιδιώτες.	Η μη εξουσιοδοτημένη αποκάλυψη πληροφοριών αναμένεται να έχει **σοβαρές ή καταστροφικές** επιπτώσεις σχετικά με τις οργανωτικές πράξεις,το ενεργητικό του οργανισμού, ή τους ιδιώτες.
Ακεραιότητα Η φύλαξη κατά της ανάρμοστης τροποποίησης της πληροφορίας ή της καταστροφής της, περιλαμβάνει τη διασφάλιση πληροφοριών και τη μη άρνηση αναγνωρίσης και αυθεντικότητας.	Η μη εξουσιοδοτημένη τροποποίηση ή καταστροφή πληροφοριών αναμένεται να έχει **περιορισμένες** αρνητικές επιπτώσεις σχετικά με τις οργανωτικές πράξεις,το ενεργητικού του οργανισμού, ή τους ιδιώτες.	Η μη εξουσιοδοτημένη τροποποίηση ή καταστροφή πληροφοριών αναμένεται να έχει **σοβαρές** αρνητικές επιπτώσεις σχετικά με τις οργανωτικές πράξεις,του ενεργητικού του οργανισμού, ή τους ιδιώτες.	Η μη εξουσιοδοτημένη τροποποίηση ή καταστροφή πληροφοριών αναμένεται να έχει **σοβαρές ή καταστροφικές** επιπτώσεις σχετικά με τις οργανωτικές πράξεις,του ενεργητικού του οργανισμού, ή τους ιδιώτες.
Διαθεσιμότητα Εξασφαλίζει την έγκαιρη και αξιόπιστη πρόσβαση στην πληροφορία και την χρήση της	Η διακοπή της πρόσβασης ή της χρήσης της πληροφορίας ή σε ένα πληροφοριακό σύστημα αναμένεται να έχει **περιορισμένη** αρνητική επίδραση στις οργανωτικές πράξεις, το ενεργητικό του οργανισμού, ή τους ιδιώτες.	Η διακοπή της πρόσβασης ή της χρήσης της πληροφορίας ή σε ένα πληροφοριακό σύστημα αναμένεται να έχει **σοβαρή** αρνητική επίδραση στις οργανωτικές πράξεις, το ενεργητικό του οργανισμού, ή τους ιδιώτες.	Η διακοπή της πρόσβασης ή της χρήσης της πληροφορίας ή σε ένα πληροφοριακό σύστημα αναμένεται να έχει **σοβαρή ή καταστροφική** επίδραση στις οργανωτικές πράξεις, το ενεργητικό του οργανισμού, ή τους ιδιώτες.

Πίνακας 2- Impact Levels Definitions [17]

ΛΟΓΙΚΗ ΔΙΕΠΑΦΗ	ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ	ΑΚΕΡΑΙΟΤΗΤΑ	ΔΙΑΘΕΣΙΜΟΤΗΤΑ
1	L	H	H
2	L	H	M
3	L	H	H
4	L	H	M
5	L	H	H
6	L	H	M
7	H	H	L
8	H	H	L
9	H	H	M
10	L	H	M
11	L	M	M
12	L	M	M
13	H	H	L
14	H	H	H
15	L	M	M
16	H	M	L
17	L	H	M
18	M	H	L
19	L	H	M
20	L	H	M
21	L	H	M
22	H	H	H

Πίνακας 3 -SG Impact Levels [17]

Καθένα από τα Impact Level βασίζονται από τα κενά ασφάλειας που θα επέλθουν στις λειτουργίες και στα περουσιακά στοιχεία του οργανισμού ή στα μεμωνομένα άτομα-καταναλωτές.

ΑΞΙΟΠΙΣΤΙΑ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ ΙΣΧΥΟΣ: είναι η διατήρηση της ροής ενέργειας προς τους καταναλωτές, τις επιχειρήσεις και τις βιομηχανίες. Για δεκαετίες, η βιομηχανία συστημάτων ενέργειας έχει αναπτύξη εκτεταμένα συστήματα και εξοπλισμό για να αποφύγει ή να περιορίσει τις προσωρίνες διακοπές λειτουργίας των συστημάτων. Στην πραγματικότητα, οι λειτουργίες των συστημάτων ενέργειας έχουν οριστεί ως οι μεγαλύτερες και πολυπλοκότερες μηχανές στον κόσμο.

ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ ΚΑΙ ΙΔΙΩΤΙΚΟΤΗΤΑ ΤΩΝ ΠΕΛΑΤΩΝ :Λόγω του ότι τα SG φτάνουν μέχρι σπίτια και τις επιχειρήσεις και λόγω του ότι όλο και περισσότεροι πελάτες συμμετέχουν στην διαχείριση της ενέργειας τους, η εμπιστευτικότητα και η ιδιωτικότητα των δεδομένων τους είναι ένα σημαντικό θέμα. Αντίθετα με την αξιοπιστία των συστημάτων ενέργειας, η ιδιωτικότητα των πελατών είναι ένα καινούργιο πεδίο.

Τα impact levels που παρουσιάζονται στον παραπάνω πίνακα δείχνουν τις επιπτώσεις σε εθνικό δίκτυο ενέργειας ειδικά από την άποψη της σταθερότητας και της αξιοπιστίας. Συνεπώς, η επίπτωση της εμπιστευτικότητας είναι χαμηλή σε αυτές τις κατηγορίες λογικών διεπαφών 1 έως 6 .Αντίθετα, στις κατηγορίες 7,8,13,14,16 και 22 έχουν υψηλή επίπτωση εμπιστευτικότητας λόγω του τύπου δεδομένων που χρειάζεται να προστατεύονται (π.χ δεδομένα χρήσης ηλεκτρικής ενέργειας του πελάτη)

3.5 Επιλογή απαιτήσεων ασφαλείας

Οι λειτουργίες των συστημάτων ενέργειας θέτουν πολλές προκλήσεις ασφάλειας που είναι διαφορετικές από τις περισσότερες άλλου είδους βιομηχανίες. Σε πολλές περιπτώσεις ο υπάρχων εξοπλισμός στα βιομηχανικά συστήματα ελέγχου που χρησιμοποιούνται στις λειτουργίες των συστημάτων ενέργειας μπορεί να μην είναι δυνατόν να ενσωματώσουν όλες τις απαίτησεις που θα αναφερθούν παρότι χρήζουν της προστασίας που προσφέρουν οι απαίτησεις αυτές.

Για παράδειγμα, το διαδίκτυο είναι διαφορετικό περιβάλλον από τις λειτουργίες του δικτύου ενέργειας. Συγκεκριμένα, υπάρχουν αυστηρές απαιτήσεις απόδοσης και αξιοπιστίας που απαιτούνται από τα συστήματα ενέργειας.Πιο αναλυτικά:

- Η λειτουργία των συστημάτων ενέργειας πρέπει να είναι συνεχόμενη 24*7 με υψηλή διαθεσιμότητα ανεξάρτητα από οποιονδήποτε συμβιβασμό στην ασφάλεια ή στην εφαρμογή των μέτρων ασφαλείας που επιβραδύνουν την λειτουργεία των συστημάτων ενέργειας.
- Αυτά τα συστήματα ενέργειας πρέπει να είναι σε θέση να συνεχίζουν να λειτουργούν με τον καλύτερο δυνάτο τρόπο κατά την διάρκεια οποιασδήποτε επίθεσης ασφάλειας.

- Η λειτουργία των συστημάτων ενέργειας πρέπει να μπορεί να ανακάμψει άμεσα μετά απο μία επίθεση ασφάλειας
- Ο ελεγχος των μέτρων ασφαλείας δεν πρέπει να επηρεαζει την λειτουργεία των συστημάτων ενέργειας.
- Η διαχείρηση, η παρακολούθηση και ο έλεγχος ολοένα και θα επεκτείνονται πέρα από τα παραδοσικά, φυσικά και ασφαλή περιβάλλοντα των μονάδων ενέργειας και θα μεταφέρονται σε εξωτερικά περιβάλλοντα όπου η μονάδα ενέργειας έχει μικρή ή καθόλου επιρροή και έλεγχο.

Δεν υπάρχει ένα μοναδικό σύνολο απαιτήσεων της κυβερνοασφάλειας που θέτει κάθε μία από τις κατηγορίες λογικών διεπαφών του SG. Αυτό μπορεί να χρησιμοποιηθεί ως βάση για τους οργανισμούς όταν αναπτύσσουν την στρατηγική κυνερνοασφάλειας όταν παρουσιάζουν την εκτίμηση επικινδυνότητας και όταν επιλέγουν και τροποποιούν τις απαιτήσεις ασφάλειας για εφαρμοφές πληροφοριακών συστημάτων smart grid. Επιπρόσθετα κριτήρια πρέπει να χρησιμοποιούνται στον καθορισμό των απαιτήσεων κυβερνοασφάλειας πριν επιλεγούν και εφαρμοστούν τα μέτρα ασφάλειας. Αυτά τα επιπλεόν κριτήρια πρέπει:

- Να λαμβάνουν υπόψη τα χαρακτηριστικά των διεπαφών του συστήματος,
- Να περιλαμβάνουν περιορισμούς που προκύπτουν από τις τεχνολογίες των μηχανημάτων και του δικτύου,
- Να λαμβάνει υπόψη τα υφισταμενα μέρη- συσκευές του συστήματος, τις διάφορες οργανωτικές δομές, το κανονιστικό-νομικό πλαίσιο και κριτήρια που αφορούν τα κόστη.

Οι παρακάτω απαιτήσεις ασφάλειας έχουν προκύψει από διάφορες πηγές :

- NIST SP 800-53, DHS Catalog, NERC CIPs και NRC Regulatory Guidance. Αφού επιλεχθούν οι απαιτήσεις ασφάλειας, τροποποιούνται όπως απαιτείται. Ο στόχος είναι να αναπτυχθεί ένα σύνολο απαιτήσεων ασφαλείας που ανταποκρίνονται στις ανάγκες του ηλεκτρικού τομέα. Κάθε απαίτηση τοποθετείται σε μία απο τις τρεις κατηγορίες:
- Διακυβέρνηση, Κίνδυνος και Συμμόρφωση (GRC)
- Κοινές τεχνικές
- Μεμονωμένες τεχνικές

Ο σκοπός των GRC απαιτήσεων είναι να απευθύνονται στο επίπεδο του οργανισμού. Οι GRC απαιτήσεις καθότι πλαισιόνονται από τις πολιτικές, διεργασίες και από τις διαδικασίες συμμόρφωσης ενδέχεται να περιλαμβάνουν τεχνικές έννοιες (implications). Ενδέχεται να είναι απαραίτητο να αυξηθούν οι GRC απαιτήσεις σε επίπεδο οργανισμού για διαφορετικούς τύπους οργανωτικών δομών ασφάλειας, για συγκεκριμένες κατηγορίες λογικών διεπαφών και για πληροφοριακά συστήματα SG.

Οι κοινές τεχνικές απαιτήσεις εφαρμόζονται σε όλες τις κατηγορίες λογικών διεπαφών ενώ οι μεμονωμένες εφαρμόζονται σε μία ή περισσότερες κατηγορίες των λογικών διεπαφών. Οι μεμονώμενες και οι κοινές τεχνικές απαιτήσεις πρέπει να υπάρχουν σε κάθε σύστημα SG και όχι απαραίτητα σε κάθε μέρος του συστήματος επείδη ο σκοπός είναι η ασφάλεια σε επίπεδο συστήματος.

Κάθε οργανισμός πρέπει να αναπτύσσει μία αρχιτεκτονική ασφάλειας για κάθε πληροφοριακό σύστημα SG και να τοποθετεί απαιτήσεις ασφάλειας σε κάθε συσκευή – μέρος του συστήματος. Κάποιες απαιτήσεις ασφάλειας μπορεί να βρίσκονται σε περισσότερες από μία συσκευές χωρίς να σημαίνει ότι όλες οι απαιτήσεις πρέπει να βρίσκονται σε όλες τις συσκευές [17] .

ΚΕΦΑΛΑΙΟ ΤΕΤΑΡΤΟ

4.1 Επιτιθέμενοι. Ποιοι μπορεί να είναι;

Επιτιθέμενοι μπορούν να αξοιποιήσουν διάφορα τρωτά σημεία με διαφορετικά κίνητρα και εμπειρογνωμοσύνη ο καθένας και να προκαλέσουν διαφορετικού μεγέθους βλάβη στο δίκτυο. Οι επιτιθέμενοι θα μπορούσαν να είναι παιδιά, ελίτ χάκερ, τρομοκράτες, εργαζόμενοι, ανταγωνιστές, ή ακόμα και πελάτες. Μπορεί κανείς να τοποθετήσει σε ομάδες τους επιτιθέμενους ως εξής: [15]

1) Μη κακόβουλοι εισβολείς που βλέπουν την ασφάλεια και τη λειτουργία του συστήματος ως ένα παζλ που πρέπει να σπάσουν. Αυτού του είδους επιτιθέμενοι συνήθως οδηγούνται από διανοητική πρόκληση και περιέργεια.

2) Οι καταναλωτές οδηγούνται από εκδίκηση απέναντι στους άλλους καταναλωτές ώστε να βρούν τρόπους να διαχειριστούν και να κλείσουν το ρεύμα στο σπίτι τους

3) Οι τρομοκράτες που βλέπουν το έξυπνο δίκτυο ως ένα ελκυστικό στόχο που επηρεάζει εκατομμύρια ανθρώπους ώστε η τρομοκρατία τους να γίνει ορατή

4) Οι εργαζόμενοι που είναι δυσαρεστημένοι σχετικά με τη χρησιμότητα / πελάτες ή κακώς εκπαιδευμένοι εργαζόμενοι που προκαλούν ακούσια λάθη.

5) Οι ανταγωνιστές επιτίθενται ο ένας στον άλλο για χάρη του κέρδους.

4.2 Κίνητρα κακόβουλων επιθέσεων

Υποκλοπή προσωπικών δεδομένων κατανάλωσης Ηλεκτρικής ενέργειας

Οι ευφυείς μετρητές μετρούν σε πραγματικό χρόνο την κατανάλωση ισχύος και αποστέλλουν χρήσιμα στοιχεία στο κέντρο ελέγχου του διαχειριστή του δικτύου Ηλεκτρικής Ενέργειας. Τα δεδομένα κατανάλωσης ισχύος αποτελούν προσωπικά δεδομένα, μέσω της επεξεργασίας των οποίων μπορούν προκύπτουν σημαντικές πληροφορίες για την προσωπική ζωή των καταναλωτών. Είναι πολύ εύκολο από τη μέτρηση της κατανάλωσης Ηλεκτρικής Ενέργειας να εξακριβωθεί ποιές συσκευές λειτουργούν, σε ποιές ώρες και με ποιό προγραμματισμό[17].

Μπορούν να εξαχθούν πληροφορίες σχετικά με το πρόγραμμα κάθε καταναλωτή, τον τρόπο ζωής του, τις συνήθειές του, ακόμα και το πότε βρίσκεται στην οικία του. Τέτοιες πληροφορίες είναι περιζήτητες από εταιρίες διαφημίσεων και στοχευμένου marketing ώστε να παράγουν εξατομικευμένες διαφημίσεις στους καταναλωτές προσαρμοσμένες στον τρόπο ζωής τους. Η υψηλή διεισδυτικότητα αυτού του είδους marketing θα ωθήσει πολλές εταιρίες να προσφέρουν αδρές αμοιβές για να λαμβάνουν τέτοιου είδους πληροφορίες. Οι αμοιβές αυτές θα αποτελέσουν σημαντικό κίνητρο για κακόβουλους χρήστες να επιτεθούν είτε στους ευφυείς μετρητές είτε στη ψηφιακή πλατφόρμα όπου γίνεται η διαχείριση του λογαριασμού κάθε καταναλωτή και των συνδεδεμένων ηλεκτρικών συσκευών.

Κλοπή ρεύματος – Απάτη

Η κλοπή ρεύματος είναι ένα απο τα πιο σημαντικά προβλήματα στα δίκτυα ηλεκτρικής ενέργειας καθώς μπορεί η ζημιά να είναι πολύ μεγάλη για τους προμηθευτές και αυτός είναι ένας από τους λόγους ανάπτυξης του SG. Η υποδομή των ευφυών μετρητών επιτρέπει στους προμηθευτές ηλεκτρικής ενέργειας να συγκρίνουν τα δεδομένα κατανάλωσης με τα δεδομένα διάθεσης της ανά περιοχή και καταναλωτή. Με αυτό τον τρόπο επιλύεται σε μεγάλο βαθμό το πρόβλημα της διαπίστωσης της κλοπής ηλεκτρικής ενέργειας. Το ολοένα και αυξανόμενο κόστος ηλεκτρικής ενέργειας θα ωθήσει αρκετούς καταναλωτές να αναζητήσουν νέους τρόπους κλοπής ρεύματος.

Οι προσπάθειες αυτές θα έχουν ως κύριο στόχο τους ευφυείς μετρητές με σκοπό την παραβίασή τους και την αποστολή εσφαλμένων στοιχείων στο διαχειριστή του δικτύου ηλεκτρικής ενέργειας. Οι κακόβουλοι καταναλωτές θα μπορούν να αποστέλλουν ψευδή δεδομένα που θα είναι σε θέση να τους εμφανίζουν μέχρι και ως ιδιώτες παραγωγούς ηλεκτρικής ενέργειας.

Πρόσβαση στο δίκτυο της εταιρίας ΗΕ

Ένας επίδοξος εισβολέας που στοχεύει το εσωτερικό δίκτυο του διαχειριστή του δικτύου ηλεκτρικής ενέργειας μπορεί να επιχειρήσει να χρησιμοποιήσει τον ίδιο

τον ευφυή μετρητή και τη σύνδεσή του με το κέντρο διαχείρισης δεδομένων ώστε να αποκτήσει πρόσβαση. Αυτή η παραβίαση του μετρητή αποκοπεί σε μεγαλύτερη επίθεση εναντίον δικτυακών στόχων του διαχειριστή του δικτύου ηλεκτρικής ενέργειας.

4.3 Κατηγοριοποίηση επιθέσεων

Πολλές επιθέσεις διαφορετικών κατηγοριών μπορεί να διαπράττονται εις βάρος ολόκληρου του SG ή κατά συγκεκριμένων μερών. Το πρώτο βήμα για την προστασία από τέτοιου είδους επιθέσεις είναι η αναγνώριση και η κατάλληλη ανίχνευση. Παρακάτω γίνεται κατηγοροποίηση διαφόρων τύπων επιθέσεων και αντιμέτρων που υπάρχουν έναντι του SG. Οι πέντε κατηγορίες κυβερνοεπιθέσεων των έξυπνων δικτύων και τα αντίμετρα που θα αναλυθούν είναι τα εξής:

1. Εποπτικού Ελέγχου και Συλλογής Δεδομένων (SCADA)

   επιθέσεις,

2. Έξυπνου μετρητή (SM) επιθέσεις,

3. Φυσικού επιπέδου επιθέσεις,

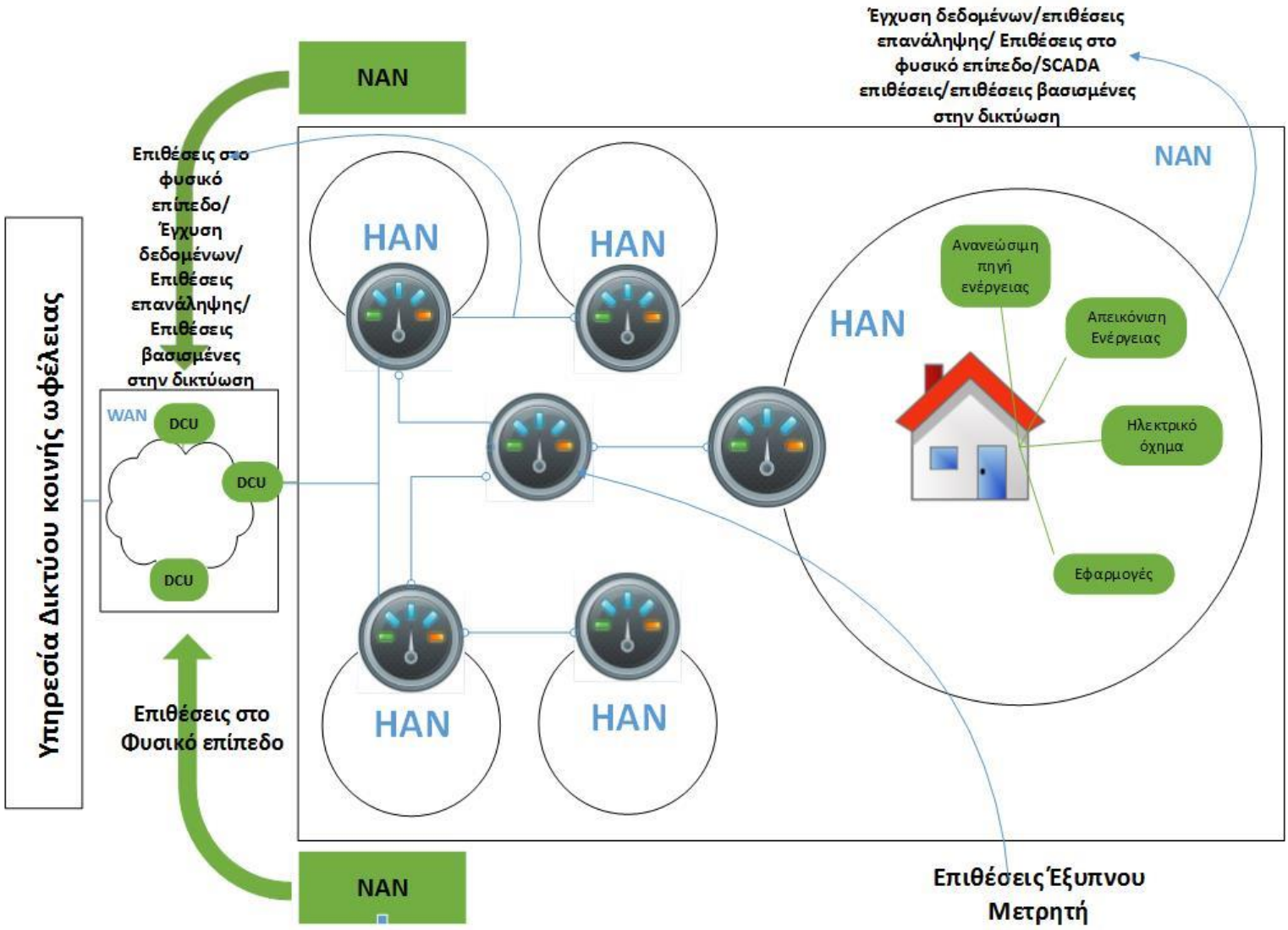
4. Έγχυσης δεδομένων και επιθέσεις επανάληψης,

5. Βασισμένες στο δίκτυο επιθέσεις.

ΤΥΠΟΙ ΕΠΙΘΕΣΕΩΝ ΜΕ ΠΕΡΙΓΡΑΦΗ		
ΤΥΠΟΣ ΕΠΙΘΕΣΗΣ	ΠΟΙΑ ΙΔΙΟΤΗΤΑ ΑΣΦΑΛΕΙΑΣ ΕΠΗΡΕΑΖΕΤΑΙ	ΤΟΠΟΘΕΣΙΑ ΘΥΜΑΤΟΣ
SCADA	Εμπιστευτικότητα, άρνηση της υπηρεσίας(DoS), ακεραιότητα	Οικιακό δίκτυο
ΕΞΥΠΝΟΣ ΜΕΤΡΗΤΗΣ (SM)	Εμπιστευτικότητα,ακεραιότητα, διαθεσιμότητα, μη αποποίηση	Οικιακό &Γειτονικό Δίκτυο
ΦΥΣΙΚΟ ΕΠΙΠΕΔΟ	Ακεραιότητα των δεδομένων, άρνηση της υπηρεσίας(DoS), εμπιστευτικότητα	Οικιακό, Γειτονικό & Ευρείας Περιοχής Δίκτυο
ΕΓΧΥΣΗΣ ΔΕΔΟΜΕΝΩΝ & ΕΠΑΝΑΛΗΨΗΣ	Εμπιστευτικότητα	Οικιακό, Γειτονικό & Ευρείας Περιοχής Δίκτυο
ΒΑΣΙΣΜΕΝΕΣ ΣΤΟ ΔΙΚΤΥΟ	Διαθεσιμότητα, εμπιστευτικότητα	Οικιακό, Γειτονικό & Ευρείας Περιοχής Δίκτυο

Πίνακας 1- Τύποι επιθέσεων με περιγραφή

Στον παραπάνω Πίνακα 1, γίνεται μια επισκόπηση των ιδιοτήτων ασφαλείας που επηρεάζονται από τις διάφορες SG επιθέσεις, και η θέση δικτύου εφόσον οι εν λόγω επιθέσεις παρέχονται.



Εικόνα 4-SG αρχιτεκτονική επικοινωνίας με απεικονιζόμενες επιθέσεις

4.4. Επιθέσεις σε SCADA και μέτρα αντιμετώπισης

Η ενσωμάτωση του δικτύου ηλεκτρικής ενέργειας με υπολογιστικές συσκευές και δίκτυα είχε μια βαθιά επίδραση στην ασφάλεια του έξυπνου δικτύου. Τα τρωτά σημεία στο δίκτυο ηλεκτρικής ενέργειας είναι μια γνωστή ανησυχία [12]. Η ενσωμάτωση των συσκευών του δικτύου ηλεκτρικής ενέργειας με backend διακομιστές και κατά κανόνα το Διαδίκτυο, έχει οδηγήσει στην έκθεση του έξυπνου δικτύου σε ένα ευρύ φάσμα επιθέσεων στον κυβερνοχώρο. Ένα τέτοιο σύστημα το οποίο έχει λάβει προσοχή είναι το SCADA.

Οι κυριότερες επιθέσεις που μπορεί να στοχεύουν κρίσιμους πόρους υποδομών του έξυπνου δικτύου μέσω του SCADA μπορούν να συνοψιστούν ως εξής [12]:

1. **<u>Αδυναμίες πλατφόρμας</u>**

Τα γνωστά κενά ασφάλειας στα υπάρχουσα εταιρικά και back-end δίκτυα και τους υπολογιστικούς πόρους είναι εκμεταλλεύσιμα για να στοχεύσουν συσκευές του έξυπνου δικτύου. Εάν δεν έχει εγκατασταθεί μια τροποίηση του λειτουργικού συστήματος, ο αντίπαλος μπορεί να θέσει σε κίνδυνο το υπολογιστικό σύστημα του έξυπνου δικτύου, να εξαπολύσει μια επίθεση εναντίον συσκευών του SCADA. Ομοίως, εφαρμογές που είναι ευάλωτες, και δεν έχουν ένα front-end πρόγραμμα προστασίας ή σύστημα ανίχνευσης εισβολών, θα παρέχουν την ιδανική πλατφόρμα στον αντίπαλο για να επιτεθεί στο SG. Άλλα πιθανά τρωτά σημεία περιλαμβάνουν επιθέσεις που βασίζονται στο λογισμικό, οι οποίες εκμεταλλεύονται τις αδυναμίες των προγραμμάτων που εκτελούνται με τους πόρους του συστήματος SCADA.

Μερικά παραδείγματα περιλαμβάνουν Denial of Service, όπου η έμφυτη ικανότητα του λογισμικού να ζητά συνεχώς πόρους τεχνικού εξοπλισμού για εκτέλεση προγραμμάτων, αξιοποιούνται πέρα των δυνατοτήτων του συστήματος. Επίσης, ένα μεγάλο σύνολο αιτημάτων για κατανομή των πόρων στους τελικούς διακομιστές, μπορεί να οδηγήσει σε Denial of Service, εναντίον νόμιμων χρηστών, επηρεάζοντας πάντοτε την εμπιστοσύνη των καταναλωτών σχετικά με τον πάροχο του δικτύου.

2. **<u>Αδυναμίες πολιτικής</u>**

Σε γενικές γραμμές, ασθενείς πολιτικές που μπορεί να ορίζονται από διαχειριστές ασφάλειας υπήρξαν μια βασική αιτία ανησυχίας. Μια παρόμοια απειλή υφίσταται για

πληροφοριακά συστήματα τα οποία διασυνδέονται με SCADA συσκευές του SG . Εάν ένας αδύναμος κωδικός πρόσβασης οδηγεί στην αποκάλυψη ενός συστήματος από έναν εισβολέα, ο διαχειριστής της πολιτικής είναι υπεύθυνος. Είναι, ως εκ τούτου, επιτακτική ανάγκη η θέσπιση ισχυρών πολιτικών ασφαλείας προκειμένου να διασφαλιστεί ότι οι εκμεταλλεύσιμες αδυναμίες λόγω αδύναμων πολιτικών, είναι ανύπαρκτες.

3. <u>Αδυναμίες δικτύου</u>

Οι συσκευές του επιπέδου δικτύου αποτελούν μια σημαντική απειλή στην υποδομή του SG. Μια συσκευή δικτύου διαμορφωμένη με βάση αδύναμες πολιτικές ασφαλείας μπορεί να οδηγήσει σε αποκάλυψη του έξυπνου δικτύου μέσω διαδικτυακών κενών εισόδου και εξόδου, οι οποίες συνδέουν τις συσκευές SCADA με το κεντρικό δίκτυο της υποδομής του έξυπνου δικτύου. Παραποίηση των IP πακέτων στο επίπεδο της συσκευής δικτύου, μέσω πλαστογράφησης της πηγής/διεύθυνσης προορισμού, αλλοίωση packet flag, και επαναφορά απομακρυσμένων δεδομένων, είναι μερικά παραδείγματα για το πως συσκευές επιπέδου δικτύου μπορούν να αποτελέσουν σοβαρή απειλή για το έξυπνο δίκτυο.

4.5 Επιθέσεις Έξυπνου μετρητή και μέτρα αντιμετώπισης

Ο SM είναι ένα κεντρικό σημείο σύνδεσης ανάμεσα στο σπίτι ενός χρήστη και στον πάροχο του δικτύου. Επιπλέον, οι μέτρησεις της χρήσης ηλεκτρικής ενέργειας από ένα νοικοκυριό παρακολουθούνται και ακολούθως μεταβιβάζονται στο κέντρο δεδομένων της εταιρίας κοινής ωφέλειας, σε τακτική βάση από το SM. Ως εκ τούτου, η ασφάλεια του SM είναι υψίστης σημασίας για τη συνολική ασφάλεια του έξυπνου δικτύου. Μια περίληψη των επιθέσεων του SM εναντίον των τεσσάρων βασικών πυλώνων της ασφάλειας πληροφοριών περιγράφονται παρακάτω [22]:

1. Εμπιστευτικότητα

Επιθέσεις με στόχο το απόρρητο αποτελούν απόπειρες για να κλέψουν πληροφορίες οι οποίες πρέπει να κρατούνται μυστικές ή να μοιράζονται μόνο μεταξύ έμπιστων ομάδων. Παραδείγματα τέτοιων επιθέσεων είναι: η ανάγνωση μνήμης της

συσκευής, η τροποποίηση του προγράμματος ελέγχου ενός SM, πλαστογράφηση/σκάλισμα του ωφέλιμου φορτίου και επιθέσεις αναπαραγωγής μηνυμάτων. Έχουν προταθεί αρκετά μέτρα πρόληψης για να μειωθεί η επίδραση της παραβίασης του απορρήτου των δεδομένων μέσα σε ένα SM.

Αυτά περιλαμβάνουν: την αντικατάσταση μυστικών κλειδιών που μοιράζεται το SM με μια μονάδα συγκέντρωσης δεδομένων σε ένα γειτονικό δίκτυο, αναδιαμόρφωση/επαναφορά συσκευής για την αφαίρεση των χαρακτηριστικών των κακόβουλων επιθέσεων, συμπεριλαμβανομένης της επαναφοράς του μυστικού κλειδιού και αντικαθιστώντας την πραγματική συσκευή.

Η ιδιωτικότητα των δεδομένων του χρήστη εμπνέει βαθύτατη ανυσηχία μέσα στο έξυπνο δίκτυο. Το πρότυπο της χρήσης ηλεκτρικής ενέργειας ενός δεδομένου νοικοκυριού μπορεί να οδηγήσει στην αποκάλυψη διαφορων ευαίσθητων παραμέτρων: καταναλωτικές συνήθειες (πάντα προς πώληση σε ανεπιθύμητους φορείς και επιχειρήσεις μάρκετινγκ), είτε ο καταναλωτής είναι σπίτι είτε ταξιδεύει [23]. Τέτοιες πληροφορίες μπορούν να εκθέσουν πληροφορίες σε ανταγωνιστές του παρόχου υπηρεσιών κοινής ωφέλειας [24].

2. Ακεραιότητα

Μια επίθεση εναντίον της ακεραιότητας ενός SM λαμβάνει χώρα όταν νόμιμα δεδομένα του SM παραποιούνται, αντικαθισταται ή διαγράφονται πριν τη μετάδοσή τους στη μονάδα συγκέντρωσης δεδομένων ενός δικτύου της γειτονιάς. Τα δεδομένα παραποιούνται από τον αντίπαλο είτε σε τοπικό επίπεδο, δηλαδή εντός των πόρων ή της μνήμης του υπολογιστή του θύματος, ή εξ αποστάσεως μέσω πλαστογράφησης/έγχυσης/διαγραφής μηνυμάτων. Ο αντίπαλος μπορεί να χορηγήσει πλασματικά δεδομένα μέσα στο SM κανάλι επικοινωνίας είτε για να απεικονίσει αυξημένη κατανάλωση ηλεκτρικής ενέργειας ενός νοικοκυριού, είτε να τη μειώσει.

Επιθέσεις επανάληψης μηνυμάτων μπορούν να ξεκινήσουν με μία από τις δύο προθέσεις. Ο πάροχος κοινής ωφέλειας μπορεί να λάβει τις ίδιες ενδείξεις SM από ένα νοικοκυριό, όπως και οι προηγούμενες. Κατά συνέπεια, η αυξημένη χρήση ηλεκτρικής ενέργειας ενός νοικοκυριού μπορεί να περάσει αδήλωτη. Ομοίως, μια πλασματική επίθεση για τη μείωση των δεδομένων αναφερόμενης ηλεκτρικής ενέργειας από ένα νοικοκυριό μπορεί να ωφελήσει τους τελικούς χρήστες, με το κόστος της απώλειας για τον πάροχο κοινής ωφέλειας. Υπάρχουν διάφορες τεχνικές για τη μείωση της επίδρασης των επιθέσεων ακεραιότητας SM. Η πιο κοινή προσέγγιση είναι για τη

δημιουργία και διατήρηση μυστικών κλειδιών λογικού μήκους (με βάση τις τρέχουσες τεχνολογικές τάσεις) μεταξύ του αποστολέα και του παραλήπτη των δεδομένων της χρήσης ηλεκτρικής ενέργειας. Μια τέτοια προσέγγιση θα βοηθήσει στην εξακρίβωση ότι ένας κώδικας πιστοποίησης μηνύματος (message authentication code – MAC) θα επιβεβαιώσει την ακεραιότητα του μηνύματος στο άκρο του παραλήπτη.

3. Διαθεσιμότητα

Ένας SM είναι επίσης ευάλωτος σε επιθέσεις εναντίον της συνεχόμενης διαθεσιμότητας του. Μερικά κοινά παραδείγματα τέτοιων επιθέσεων είναι: η απενεργοποίηση της συσκευής, παρεμβολές στο κανάλι επικοινωνίας, Denial-of-Service κατά του DNS server στο εταιρικό δίκτυο, και πλαστογράφηση. Λαμβάνοντας υπόψη την κατάσταση της ασφάλειας ZigBee, να απενεργοποιηθεί σε ένα SM, είναι δυνατόν να γίνει αίτημα απενεργοποίησης ώστε ο SM να κλείσει. Φυσικά, αυτό έχει ως συνέπεια να μην υπάρχει ηλεκτρική ενέργεια και στα νοικοκυριά μέχρι να γίνει επανεκκίνηση του SM. Ηλεκτρονικές παρεμβολές σε κανάλια επικοινωνίας θα έχουν παρόμοιες συνέπειες όπως και η προηγούμενη επίθεση.

Εάν τροποποιηθούν τα μυστικά κλειδιά που αποθηκεύονται εντός του SM θα αποτραπεί η αποκρυπτογράφηση των ασφαλούς μηνυμάτων που μεταδίδονται από τους μετρητές στις μονάδες δεδομένων του συμπυκνωτή και στους end-servers. Και για τα τρία σενάρια,η διαθεσιμότητα του έξυπνου μετρητή επηρεάζεται.

Αντίμετρα κατά των επιθέσεων αυτών περιλαμβάνουν:

- αντικατάσταση παραβιασμένων ή παραποιημένων SM,
- αλλαγή στη συχνότητα του καναλιού για τη μετάδοση του μηνύματος,
- ενημέρωση των μυστικών κλειδιών,
- να γίνει επιτρεπτή η λειτουργία ασφαλείας του προτύπου ZigBee.

4. Non- Repudiation

Οι επιθέσεις αυτές είναι προσπάθειες από τον επιτιθέμενο για να αρνηθεί οποιαδήποτε πράξη. Για παράδειγμα, ένας συμβιβασμένος SM μπορεί να μεταδώσει μια εσφαλμένη ανάγνωση στον πάροχο του δικτύου και να ισχυρίζονται ότι δεν το

έχουν πράξει. Αν ο έξυπνος μετρητή χρησιμοποιεί ένα μυστικό κλειδί για την κρυπτογράφηση των δεδομένων, η μη άρνηση αναγνώρισης επιβάλλεται εκ φύσεως, καθώς κανένας άλλος φορέας αναμένεται να διαθέτει αντίγραφο του ίδιου μυστικού κλειδιού. Αντιθέτως, η έλλειψη ενός μηχανισμού που βασίζεται στο μυστικό κλειδί θα επιβαρύνει τον προσδιορισμό μιας τέτοιας επίθεσης.

Μια κοινή αιτία για τις επιθέσεις εναντίον του SM [25] είναι η χειραγώγηση της διαμόρφωσης του μετρητή. Ο μετρητής πρέπει να είναι αρκετά ασφαλής για να αντέχει τις επιθέσεις που βασίζονται στο υλικό και στο λογισμικό, οι οποίες προσπαθούν να τροποποίησουν την διαμόρφωση του. Η ανάπτυξη μεγάλης κλίμακας SM (Αριθμός έξυπνων μετρητών = Αριθμός Νοικοκυριών), σε μια μητροπολιτική πόλη, απαιτούν αρκετή ασφάλεια, για να αποτρέψει μια μεγάλης κλίμακας καταστροφή μέσω τέτοιων επιθέσεων.

4.6 Επιθέσεις Φυσικού επιπέδου και μέτρα αντιμετώπισης

Παρακάτω γίνεται μία λεπτομερής ανάλυση των επιθέσεων στο φυσικό επίπεδο [26][27]:

1. **Eavesdropping**

Η επίθεση αποτελείται από την λήψη πακέτων από το δίκτυο, τα οποία διαβιβάζονται μέσω υπολογιστών και στην συνέχεια την ανάγνωση του περιεχομένου τους σε αναζήτηση ευαίσθητων πληροφοριών. Η επίθεση μπορεί να γίνει με την χρήση εργαλείων, τα οποία ονομάζονται «sniffers». Αυτά τα εργαλεία συλλέγουν πακέτα που διακινούνται σε κάποιο δίκτυο και ανάλογα με την ποιότητά τους, αναλύουν τα δεδομένα που έχουν συλλεχθεί.

Για παράδειγμα σε ένα ενσύρματο τοπικό δίκτυο συνήθως χρησιμοποιείται μία συσκευή, η οποία ονομάζεται Ethernet hub, με σκοπό την σύνδεση πολλών συσκευών Ethernet μαζί ώστε αυτές να ενεργούν ως ένα ενιαίο τμήμα του δικτύου. Η μέθοδος Eavesdropping στο τοπικό αυτό δίκτυο γίνεται ευκολότερη γιατί η

συσκευή Hub αναμεταδίδει όλη την κίνηση πληροφορίας που παίρνει από την μία της θύρα σε όλες τις άλλες θύρες. Έτσι ο εισβολέας χρησιμοποιώντας έναν αναλυτή πρωτοκόλλων, μπορεί να παρακολουθεί την κίνηση του τοπικού δικτύου ανακαλύπτοντας ευαίσθητες πληροφορίες [OWASP].

Η βασική διαφορά της τεχνικής με την τεχνική "Man in the middle" είναι ότι στην πρώτη ο παραλήπτης λαμβάνει όλα τα μηνύματα που στέλνονται από τον αποστολέα, χωρίς να έχει παραποιηθεί το περιεχόμενό τους, δηλαδή ο εισβολέας απλά υποκλέπτει την συνομιλία μεταξύ των δύο χωρίς βέβαια αυτοί να το γνωρίζουν. Αντίθετα στην τεχνική "Man in the middle" ο εισβολέας προσποιείται πως είναι ο παραλήπτης, λαμβάνει όλα τα μηνύματα που στέλνονται από την αποστολέα και τα παραποιεί [SCA].

2. Jamming

Ο κύριος στόχος αυτής της επίθεσης είναι να αποτρέψει τους SM να επικοινωνούν με τον πάροχο του δικτύου, μέσω παρεμβολών του ασύρματου μέσου, με σήματα θορύβου. Τέτοιες επιθέσεις μπορούν να ταξινομηθούν σε δύο τύπους:

i)Προληπτική παρεμβολή: όπου οι jammer μπορούν να εκπέμπουν σήματα θορύβου συνεχώς για να εμποδίσει εντελώς ένα ασύρματο κανάλι, και

ii) αντιδραστική παρεμβολή: όπου οι jammer**,** πρώτα κρυφακούν στο κανάλι και ξεκινάνε επίθεση μόνο όταν τα σήματα ανιχνεύονται στο κανάλι.

Αυτή η επίθεση έχει σαν αποτέλεσμα, ο SM μπορεί να επηρεάζεται με δύο τρόπους: (i) το κανάλι θα επισημανθεί ως "Απασχολημένο" για κάθε αίσθηση μεταφοράς που έγινε από έναν θεμιτό SM

(ii) ο SM μπορεί να εμποδίζεται να λαμβάνει πακέτα.

2. Έγχυση Αιτημάτων/ Περιορισμένη Πρόσβαση

Ο κύριος στόχος αυτής της επίθεσης είναι να διακόψει τις εργασίες ρουτίνας στο επίπεδο MAC του SM. Ο εισβολέας εμποδίζει τους SM να αρχίσει τις νόμιμες MAC ενέργειες ή προκαλεί πακέτο σύγκρουσης.

Αυτή η επίθεση επισημαίνεται ως εξής:

(i) είναι παρόμοια με την αντιδραστική παρεμβολή όπου η επίθεση ξεκίνησε με την πρόθεση να εμποδίσει το κανάλι επικοινωνίας,

(ii) στοχεύει σε ένα κανάλι πρόσβασης πολλών χρηστών,

(iii) ο εισβολέας θέτει το χρονικό του περιθώριο "υποχώρησης" πολύ μικρό έτσι ώστε το κανάλι δίνει προτεραιότητα πρόσβασης στον "αντίπαλο" κάθε φορά που θέλει να επικοινωνήσει, και αρνείται την πρόσβαση στους νόμιμους SM του δικτυου.

4.Επιθέσεις έγχυσης

Σε αντίθεση με τις δύο προηγούμενες επιθέσεις που βασίζονται σε ψευδείς σήματα, αυτή η επίθεση εισάγει μορφοποιημένα μηνύματα στο ασύρματο δίκτυο. Αυτή η επίθεση μπορεί να αναδείχθεί ως εξής:

(i) ο αντίπαλος μιμείται είτε ένα νόμιμο αποστολέα ή δέκτη για να πάρει τη μη εξουσιοδοτημένη πρόσβαση σε ένα ασύρματο δίκτυο,

(ii) αυτή η επίθεση είναι παρόμοια με TCP-SYN flooding επίθεση όπου, οι πόροι του θύματος κατακλύζονται από την επεξεργασία των πλασματικών μηνύματα που έλαβε.

Μια τέτοια επίθεση μπορεί να προληφθεί μέσω των κατάλληλων μηχανισμών ασφαλείας , για να εξασφαλίσει το μήνυμα πιστοποίηση.

4.7 Έγχυση Δεδομένων & επιθέσεις επανάληψης και μέτρα αντιμετώπισης

Μια άλλη κατηγορία των κακόβουλων επιθέσεων SM είναι η έγχυση των δεδομένων και οι επιθέσεις επανάληψεις. Ψευδείς επιθέσεις έγχυσης δεδομένων συμβαίνουν όταν εγχέονται παραποιημένα στοιχεία στο μετρητή ή σε γειτονικές περιοχές μέτρησης τα οποία παρατηρούνται από το χειριστή του δικτύου. Τέτοιες επιθέσεις στοχεύουν στην υποδομή του SM, ιδιαίτερα στη μέτρηση και στην παρακολούθηση των υποσυστημάτων με στόχο το χειρισμό του μετρητή και των διανυσματικών μετρήσεων, έτσι ώστε να παραπλανηθεί η λειτουργία και ο έλεγχος του

φορέα παροχής της χρησιμότητας [28]. Η προτεινόμενη τεχνική ανίχνευσης για μια τέτοια επίθεση είναι μια εκτίμηση σχετικά με την κατάσταση του συστήματος από τις παρατηρούμενες μετρήσεις και με υπολογισμούς μεταξύ της παρατηρούμενης και της εκτιμώμενης μέτρησης. Τα επαναλαμβανόμενα μηνύματα επίθεσης συμβαίνουν όταν ο εισβολέας αποκτά ένα υπερυψωμένο προνόμιο στο SM και επομένως μπορεί να προκαλέσει έγχυση στα σήματα ελέγχου του συστήματος. Για να ξεκινήσει μια τέτοια επίθεση ο αντίπαλος πρέπει:

(α) να προβεί στη σύλληψη και την ανάλυση των δεδομένων που διαβιβάζονται μεταξύ συσκευών και SM για να αποκτήσει τα χαρακτηριστικά του πελάτη στη χρήσης ενέργειας, και

(β) στην κατασκευή και έγχυση ψευδών σημάτων ελέγχου στο σύστημα.

Ο στόχος της επαναλαμβανόμενης επίθεσης είναι: (α) να κλέψει ενέργεια και να την επαναδρομολογήσει σε άλλη θέση, και (β) να προκαλέσει σωματική/φυσική βλάβη στο σύστημα. Το γνωστό παράδειγμα μιας τέτοιας επίθεσης είναι ο ιός Stuxnet που έχει γίνει αναφορά σε προηγούμενο κεφάλαιο. Οι οικιακές συσκευές αντιμετωπίζονται ως αμετάβλητα συστήματα γραμμικού χρόνου, και ο SM είναι υπεύθυνος για το έργο της παρατήρησης των οικιακών συσκευών.

Η εκτίμηση μιας κατάστασης βασίζεται στα φίλτρα Kalman τα οποία χρησιμοποιούνται για τη δοκιμή της ελάχιστης διακύμανσης που παρατηρείται στις πραγματικές αναγνώσεις της συσκευής σε σύγκριση με τις αναμενόμενες αναγνώσεις. Μια συσκευή ανίχνευσης επιβεβαιώνει μια ανώμαλη δραστηριότητα που μπορεί να επηρεάσει το έξυπνο δίκτυο. Το σύστημα δεν είναι προσαρμόσιμο μόνο σε ένα νοικοκυριό, αλλά και για μια ομάδα νοικοκυριών σε μια γειτονιά. Η επαναλαμβανόμενη επίθεση ορίζεται απλά ως η τροποποίηση στο σήμα ελέγχου που μεταδίδεται από μια συσκευή ενός καταναλωτή στον SM. Η εκτίμηση της κατάστασης γίνεται σε κεντρικό επίπεδο από το κέντρο ελέγχου του συστήματος. Ο στόχος της εκτίμησης είναι να ανακτήσει την πλήρη κατάσταση του συστήματος. Μετά την έγχυση των δεδομένων, η κατάσταση δεν παραμένει ίδια.

4.8 Βασισμένες στο δίκτυο επιθέσεις και μέτρα αντιμετώπισης

1. Man in the middle επίθεσεις

Η Man in the middle είναι μία επίθεση για παραβίαση της ασφάλειας ενόςσυστήματος. Ο επιτιθέμενος παρεμποδίζει την επικοινωνία μεταξύ δύο μερών και ελέγχει τη ροή επικοινωνίας. Αυτό έχει ως αποτέλεσμα να είναι σε θέση μπορεί να αποσπάσει ή να αλλοιώσει τις πληροφορίες που στέλνονται από έναν από τους αρχικούς συμμετέχοντες.

Πιο συγκεκριμένα, ο επιτιθέμενος προσποιείται πως είναι κάποιος από τους δύο συμμετέχοντες με σκοπό να λαμβάνει μηνύματα από την μεταξύ τους επικοινωνία. Έτσι μπορεί να μετατρέπει το περιεχόμενό τους και να στείλει ψευδή μηνύματα στον παραλήπτη.

Ένα παράδειγμα είναι όταν ο παραλήπτης είναι κάποιος χειριστής σε κέντρο ελέγχου μιας εταιρίας παροχής ηλεκτρισμού. Ο επιτιθέμενος μπορεί να του στείλει ψευδή δεδομένα και να τον αναγκάσει να ανοίξει κάποιον διακόπτη όταν δεν απαιτείται ή να τον κάνει να πιστεύει ότι όλα είναι υπό έλεγχο στο δίκτυο ώστε να μην αναλάβει δράση όταν απαιτείται κάποια ενέργεια.

Μια τεχνική άμυνας για τον εντοπισμό αυτών επιθέσεων στο SG βασίζεται στα σχόλια που ελήφθησαν από μεμονωμένους κόμβους στο δίκτυο. Μέσω της υποστήριξης του αναγκαίου πρωτόκολλου επικοινωνίας, κάθε κόμβος οφείλει να επικοινωνεί με το κέντρο συγχώνευσης για να μεταφέρουν τις ατομικές παρατηρήσεις τους. Οι εκ προθέσεως επιθέσεις μπορούν να απευθύνονται μόνο σε ένα συγκεκριμένο υποσύνολο κόμβων του SG, και ως εκ τούτου σχόλια από όλους τους κόμβους είναι απαραίτητα για την ακριβής ανίχνευση αυτών των επιθέσεων. Προβλέπεται ένα θεωρητικό παιχνίδι όπου, ο επιτιθέμενος αντιμετωπίζεται ως ένας παίκτης και ο αμυντικός ως άλλος. Με βάση την ιδέα ότι ο επιτιθέμενος έχει την πρόθεση να θέσει σε κίνδυνο τους πιο κρίσιμους κόμβους, η στρατηγική άμυνας είναι να εξασφαλίζουν

έγκαιρα τις τοπικές παρατήρησεις από τους επιμέρους κρίσιμους κόμβους. Επίσης, η επακόλουθη επικοινωνία των ευρημάτων στο κέντρο συγχώνευσης, είναι απαραίτητη.

2. **Επιθέσεις Άρνησης Υπηρεσιών (Denial Of Service DoS attacks)**

Οι επιθέσεις DoS είναι από τα σημαντικότερα προβλημάτα ασφαλείας του έξυπνου δικτύου. Βασικός σκοπός τους είναι η διακοπή υπηρεσιών προσπαθώντας να περιορίσουν την πρόσβαση σε μία μηχανή ή σε μια υπηρεσία αντί να υπονομεύσουν την ίδια την υπηρεσία. Πετυχαίνουν τον στόχο τους στέλνοντας μία μεγάλη ροή πακέτων, τα οποία πλημμυρίζουν κάποιο δίκτυο ή εκμεταλλεύονται όλη την διαθέσιμη χωρητικότητα με αποτέλεσμα να μην είναι επιτρεπτή η πρόσβαση σε αυτό από τους νόμιμους χρήστες. Οι επιθέσεις DoS είναι δύσκολο να ανιχνευτούν, και αυτό τις καθιστά πολύ επικίνδυνες.

Οι επιτιθέμενοι χρησιμοποιούν παραποιημένες διευθύνσεις IP προκειμένου να κρύψουν την ταυτότητά τους πίσω από άλλες μηχανές που έχουν θέσει υπό τον έλεγχό τους. Επιπλέον οι ροές των πακέτων DoS δεν παρουσιάζουν κοινά χαρακτηριστικά με αποτέλεσμα να καθιστούν ιδιαίτερα δύσκολη την ανίχνευσή τους και ακόμα πιο δύσκολη τη διαφοροποίηση των πακέτων επίθεσης από τα νόμιμα πακέτα.

Ωστόσο υπάρχουν και οι Κατανεμημένες επιθέσεις Άρνησης Εξυπηρέτησης (Distributed Denial of Service Attacks DDoS). Χωρίς καμία ή με μικρή προειδοποίηση, μία επίθεση DDoS μπορεί εύκολα να εξαντλήσει τους υπολογιστικούς και επικοινωνιακούς πόρους του θύματός της μέσα σε σύντομο χρονικό διάστημα. Η επίδραση των επιθέσεων αυτών είναι πιο σοβαρή, καθώς αυτές οι επιθέσεις χρησιμοποιούν πολλούς υπολογιστές για να πραγματοποιήσουν.

ΚΕΦΑΛΑΙΟ ΠΕΜΠΤΟ

5. Κρυπτογραφία και διαχείριση κλειδιών

5.1 Θέματα κρυπτογραφίας και διαχείρισης κλειδιών στα έξυπνα δίκτυα

5.1.1 Περιορισμοί

Περιορισμοί λόγω υπολογιστικής ισχύος

Κάποιες συσκευές Έξυπνου Δικτύου ειδικά οικιακές ή αστικοί μετρητές πιθανόν να έχουν περιορισμένη υπολογιστική ισχύ και δυνατότητα αποθήκευσης κρυπτογραφικών υλικών. Η άφιξη των ημιαγωγών χαμηλού κόστους που περιλαμβάνουν χαμηλού κόστους ενσωματωμένους επεξεργαστές με εσωτερικές δυνατότητες κρυπτογράφησης, θα βοηθήσει σε αυτού του είδους τους περιορισμούς εάν η εφοδιαστική αλυσίδα απορροφήσει αυτή την τεχνολογία και την ευθυγραμμίσει με συστήματα διαχείρισης κρυπτογραφικών κλειδιών για τις λειτουργίες των Έξυπνων Δικτύων. Αναμένεται ότι μελλοντικά οι περισσότερες συσκευές που θα συνδέονται σε Έξυπνα Δίκτυα θα διαθέτουν βασικές κρυπτογραφικές δυνατότητες και θα υποστηρίζουν συμμετρικούς αλγόριθμους για κρυπτογράφηση. Η κρυπτογράφηση δημόσιου κλειδιού μπορεί να υποστηρίζεται είτε στο λογισμικό είτε στον εξοπλισμό με την βοήθεια κάποιου βοηθητικού επεξεργαστή. Η χρήση εξοπλισμού χαμηλού κόστους με ενσωματωμένη υποστήριξη κρυπτογράφησης είναι απαραίτητη αλλά όχι και απόλυτα επαρκής για να πετύχουμε ακεραιότητα , διαθεσιμότητα και εμπιστευτικότητα υψηλού επιπέδου στα Έξυπνα Δίκτυα. Μία αξιόπιστη και απρόσκοπτη εφαρμογή κρυπτογράφησης που είναι κατάλληλη για έξυπνα δίκτυα θα ήταν επωφελής για όλα τα ενδιαφερόμενα μέρη σε εφαρμογές έξυπνων δικτύων.

Εύρος ζώνης καναλιού

Τα έξυπνα δίκτυα περιλαμβάνουν επικοινωνίες μέσω ποικίλων καναλιών με διάφορα εύρη ζώνης. Η κρυπτογράφηση από μόνη της δεν μπορεί γενικά να επηρεάσει το εύρος ζώνης του καναλιού καθώς οι συμμετρικοί αλγόριθμοι παράγουν σχεδόν τον ίδιο αριθμό bits με αυτό του μη κρυπτογραφημένου μηνύματος. Όμως η κρυπτογράφηση επηρεάζει αρνητικά τους αλγόριθμους συμπίεσης δεδομένων καθώς τα κρυπτογραφημένα δεδομένα είναι ομοιόμορφα τυχαία και άρα δεν μπορούν να συμπιεστούν. Οι αλγόριθμοι συμπίεσης μπορούν να εφαρμοστούν πριν από την κρυπτογράφηση κάτι που πρέπει να ληφθεί υπόψη στο σχεδιασμό του δικτύου.

Η προστασία της ακεραιότητας των δεδομένων όπως αυτή παρέχεται από μια CMAC κωδικοποίηση (Cipher Based Message Authentication Code) προσθέτει ένα συγκεκριμένο επιπλέον φορτίο σε κάθε μήνυμα από 64 έως 96 bits. Σε αργά κανάλια που συνήθως ανταλλάσουν μηνύματα μικρού μεγέθους αυτό το επιπλέον φορτίο μπορεί να επιφέρει σημαντική καθυστέρηση αν δεν αυξηθεί σημαντικά το εύρος ζώνης του καναλιού.

Επίσης, τα κανάλια μικρού εύρους ζώνης είναι πολύ αργά στην συχνή ανταλλαγή μεγάλων πιστοποιητικών. Εάν η αρχική ανταλλαγή πιστοποιητικού δεν είναι time critical και χρησιμοποιείται για εγκαθίδρυση διαμοιραζόμενου συμμετρικού κλειδιού ή για κλειδιά που χρησιμοποιούνται για μεγάλη χρονική διάρκεια ,όπως στο IKE πρωτόκολλο (Internet Key Exchange) , η ανταλλαγή πιστοποιητικών μπορεί να είναι πρακτική ακόμα και μέσω αργών καναλιών. Όμως αν η ανταλλαγή κλειδιών που βασίζεται σε πιστοποιητικά είναι time critical , πρωτόκολλα όπως το IKE που ανταλλάσουν πολλαπλά μηνύματα πριν τη φάση του pre-shared κλειδιού, μπορεί να κοστίσουν πάρα πολύ ακόμα κι αν το μέγεθος του πιστοποιητικού είναι πολύ μικρό.

Συνδεσιμότητα

Τα συστήματα με υποδομή δημόσιου κλειδιού που βασίζονται σε peer-to-peer μοντέλο εγκαθίδρυσης κλειδιού όπου κάθε μέλος πρέπει να επικοινωνεί με οποιοδήποτε άλλο μέλος, μπορεί να μην είναι συμβατά από πλευράς ασφάλειας με τα μέρη ενός έξυπνου δικτύου. Κάποιες συσκευές είναι πιθανό να μην μπορούν να συνδεθούν με εξυπηρετητές κλειδιών (Key servers) , αρχές έκδοσης πιστοποιητικών (Certificate Authorities CA) και OCSP (Online Certificate Status Protocol)

εξυπηρετητές. Σε πολλές περιπτώσεις οι συνδέσεις μεταξύ των συσκευών ενός έξυπνου δικτύου μπορεί να έχουν πολύ μεγαλύτερη διάρκεια ίσως και μόνιμη , απ' ότι οι τυπικές συνδέσεις μέσω διαδικτύου.

5.1.2 Γενικά Θέματα Κρυπτογραφίας

Εντροπία

Κάποιες συσκευές μπορεί να μην έχουν πρόσβαση σε επαρκείς πόρους εντροπίας για να αποδώσουν την κατάλληλη τυχαιότητα παραγωγής κρυπτογραφικών κλειδιών και άλλων κρυπτογραφικών διαδικασιών. Αυτό είναι ένα θεμελιώδες ζήτημα και έχει αντίκτυπο στα συστήματα διαχείρισης κλειδιών που πρέπει να σχεδιαστούν και να λειτουργήσουν σε Έξυπνα Δίκτυα.

Σύνθεση κωδικού (Cipher Suite)

Μια δομή κωδικού που θα είναι επαρκώς ασφαλής για μεγάλες εφαρμογές έξυπνων δικτύων θα καθιστούσε δυνατή την δια - λειτουργικότητα του δικτύου. Οι FIPS, NIST SP's NSA Suite B Cryptography στρατηγικές, παρέχουν ασφαλείς βασικές μεθόδους για επίτευξη δια - λειτουργικότητας. Το προφίλ της συσκευής και η αξία των δεδομένων κατέχουν σημαντικό ρόλο στην επιλογή δομής και πολυπλοκότητας κωδικού.

Θέματα διαχείρισης κλειδιών

Όλα τα πρωτόκολλα ασφάλειας βασίζονται σε ασφαλή συσχέτιση (SA). Μια ασφαλής συσχέτιση μπορεί να είναι αυθεντικοποιημένη ή μη – αυθεντικοποιημένη. Η εγκαθίδρυση αυθεντικοποιημένης SA προϋποθέτει ότι τουλάχιστον το ένα μέρος διαθέτει κάποιο είδος διαπιστευτηρίων που μπορούν να επιβεβαιώσουν την ταυτότητα ή τα χαρακτηριστικά του σε άλλους. Γενικά συνηθίζονται δύο είδη διαπιστευτηρίων: τα μυστικά κλειδιά που μοιράζονται μεταξύ των οντοτήτων του δικτύου και πιστοποιητικά δημόσιου κλειδιού. Τα πιστοποιητικά δημόσιου κλειδιού χρησιμοποιούνται για να συνδέσουν τα ονόματα των χρηστών ή των συσκευών με δημόσιο κλειδί με κάποιο μοντέλο πιστοποίησης μέσω τρίτου όπως το PKI.

Ο εφοδιασμός των συσκευών με μυστικά κλειδιά μπορεί να έχει σημαντικό κόστος , ενώ η χρήση ψηφιακών πιστοποιητικών δεν παρουσιάζει ευπάθειες ασφάλειας. Αυτό συμβαίνει διότι με τα συμμετρικά κλειδιά, τα κλειδιά πρέπει να μεταφερθούν από τη συσκευή που τα παράγει και να αποθηκευτούν τουλάχιστον σε άλλη μια συσκευή και τυπικά για κάθε ζεύγος επικοινωνούντων συσκευών απαιτείται ένα διαφορετικό κλειδί. Στη διαδικασία διαμοιρασμού κλειδιών πρέπει να διασφαλιστεί ότι κάθε συσκευή λαβαίνει το σωστό κλειδί, διαδικασία που είναι επιρρεπής σε ανθρώπινο λάθος και εκτεθειμένη σε κακόβουλους. Υπάρχουν hardware λύσεις για ασφαλή μεταφορά και παράδοση κλειδιών αλλά αυτό μπορεί να απαιτεί μεγάλη λειτουργική επιφόρτιση και το κόστος τους είναι απαγορευτικό , ιδιαιτέρως στα μικρά συστήματα. Αυτό το κόστος μπορεί να πολλαπλασιαστεί αν κάθε συσκευή πρέπει να έχει διάφορες και ανεξάρτητες συσχετίσεις ασφάλειας (SA) που καθεμία απαιτεί διαφορετικό κλειδί. Τεχνικές όπως αυτές που χρησιμοποιεί το Kerberos μπορεί να εξαλείψει μεγάλο μέρος της μη – αυτόματης διαδικασίας και του κόστους συσχέτισης, αλλά δεν μπορεί να παρέχει μεγάλο βαθμό διαθεσιμότητας όταν διακόπτεται η επικοινωνία του δικτύου ή παροχή ενέργειας καθώς καμία πλευρά δεν έχει πρόσβαση στο κέντρο διαμοιρασμού κλειδιών (KDC).

Η απόδοση ψηφιακών πιστοποιητικών μπορεί να είναι πολύ καλύτερη από άποψη κόστους. Κάθε συσκευή τυπικά χρειάζεται ένα πιστοποιητικό για εγκαθίδρυση κλειδιού, και μια εγκαθίδρυση ιδιωτικού κλειδιού που γίνεται μια φορά. Κάποια προϊόντα παράγουν, αποθηκεύουν και χρησιμοποιούν ιδιωτικό κλειδί σε FIPS -140 hardware security module (HSM). Σε τέτοια συστήματα είναι προφανές ότι παρέχεται μεγαλύτερος βαθμός ασφάλειας με μικρότερο λειτουργικό κόστος. Βέβαια και η λειτουργία του PKI μηχανισμού για παραγωγή και διαχείριση πιστοποιητικών δημιουργεί ένα επιπρόσθετο φόρτο και τυπικά δεν είναι κατάλληλη για μικρά ή μεσαίου μεγέθους συστήματα. Μια λύση που βασίζεται σε PKI μπορεί να έχει υψηλό κόστος εγκατάστασης αλλά απαιτεί μόνο ένα πιστοποιητικό ανά συσκευή και είναι καταλληλότερη για μεγάλα συστήματα.

Θέματα υποδομής δημόσιου κλειδιού – Public Key Infrastructure

Τα θέματα που σχετίζονται με την υποδομή δημόσιου κλειδιού χωρίζονται σε δύο κατηγορίες: η πολυπλοκότητα της λειτουργίας της και το γεγονός ότι οι PKI

πολιτικές δεν είναι διεθνώς κατανοητές. Βασικό πλεονέκτημα είναι η μεγάλη ευελιξία που προφέρει μια τέτοια υποδομή. Η PKI αποτελεί ένα πλαίσιο που επιτρέπει στον κάθε οργανισμό να ορίζει τις πολιτικές του και τις πολιτικές πιστοποιητικών του (certificate policy Object Identifiers CP OIDs), να αποφασίζει τον τρόπο αξιολόγησης των αιτημάτων πιστοποιητικών, το πώς προστατεύονται τα ιδιωτικά κλειδιά, πώς δομείται η CA ιεραρχία και την διάρκεια ισχύος των πιστοποιητικών. Αυτή η ευελιξία την καθιστά ακριβή λύση καθώς οι ενδιαφερόμενοι οργανισμοί πρέπει να εξετάσουν κάθε ένα από αυτά τα ζητήματα και να τα αποτιμήσουν σε σχέση με τις λειτουργικές τους απαιτήσεις για να καθορίσουν τα ακριβή χαρακτηριστικά της PKI λύσης που θα υιοθετήσουν. Όταν ένας οργανισμός με PKI υποδομή αποφασίσει να συνεργαστεί με άλλους οργανισμούς πρέπει να καταβληθεί προσπάθεια για να αναλυθούν οι PKI λύσεις που έχουν οι οργανισμοί και να γίνουν οι απαραίτητες προσαρμογές και αντιστοιχήσεις για να μπορεί να επιτευχθεί συμβατότητα στις PKI υποδομές τους.

Ένα άλλο θέμα είναι η ανάγκη για ανάκληση πιστοποιητικών και η επαλήθευση της ισχύος των πιστοποιητικών πριν αυτά γίνου αποδεκτά από κάποια οντότητα του συστήματος που πρέπει να αυθεντικοποιηθεί. Αυτό τυπικά το πετυχαίνει ένα αξιόπιστο τρίτο μέρος που εκτελεί την αυθεντικοποίηση , ελέγχει τις λίστες ανάκλησης πιστοποιητικών ή ελέγχει την κατάσταση των πιστοποιητικών μέσω online server. Αυτό απαιτεί συνδεσιμότητα με κάποιον server και ενδεχομένως να προκύπτουν θέματα διαθεσιμότητας .

Επίσης υπάρχει το ζήτημα της έμπιστης διαχείρισης. Οι PKI μέθοδοι συχνά δέχονται κριτικές για το γεγονός ότι απαιτούν μόνο one-way authentication. Συνήθως όμως κάθε οργανισμός διαμορφώνει τους δικούς του συνδυασμούς αυθεντικοποίησης όταν υπάρχει ανάγκη για δια-τμηματικές λειτουργίες. Στα έξυπνα δίκτυα κάθε οργανισμός κοινής ωφέλειας διαθέτει την δική του υποδομή PKI. Οι οργανισμοί που χρειάζεται να συνεργάζονται μπορούν να ανταλλάσουν υπογραφές στα απαραίτητα πιστοποιητικά ασφάλειας. Επιπλέον θα ήταν πιθανό όλοι οι οργανισμοί κοινής ωφέλειας να ιδρύσουν μια ή περισσότερες γέφυρες CAs έτσι ώστε κάθε οργανισμός να χρειάζεται μόνο να ανταλλάσει υπογραφές μόνο με την «γέφυρα». Όλες οι υπογραφές πιστοποιητικών θα πρέπει να περιορίζονται σε συγκεκριμένες εφαρμογές ή σενάρια χρήσης.

PKI θέματα υψηλής διαθεσιμότητας

Το προφανές μειονέκτημα στο PKI ότι πρέπει να αυθεντικοποιεί τα πιστοποιητικά μέσω on line server δεν θα έπρεπε να θεωρείται μεγάλο ζήτημα. Οι κόμβοι δικτύου όσο είναι συνδεδεμένοι μπορούν περιοδικά να αποκτούν δηλώσεις με τις καταστάσεις των πιστοποιητικών και να τις χρησιμοποιούν ετεροχρονισμένα όταν αυθεντικοποιούνται με άλλο κόμβο. Γενικά με αυτή τη μέθοδο ο κόμβος μπορεί να δείχνει την κατάσταση του πιστοποιητικού του μαζί με το πιστοποιητικό στη διαδικασία της αυθεντικοποίησης. Το TLS υποστηρίζει αυτή τη λειτουργικότητα. Με αυτό τον τρόπο επιτυγχάνεται πολύ υψηλή διαθεσιμότητα ακόμα και αν οι κόμβοι είναι εκτός δικτύου.

Οι μέθοδοι συμμετρικού κλειδιού για την εγκαθίδρυση ασφαλών συσχετίσεων μπορούν να χωριστούν σε δυο γενικές κατηγορίες : σε server based διαπιστευτηρίων και σε προκαθορισμένων διαπιστευτηρίων. Στα server based συστήματα όπως το Kerberos ή RADIUS η συνδεσιμότητα στον εξυπηρετητή ασφάλειας είναι απαραίτητη για την εγκαθίδρυση ασφαλών συσχετίσεων. Μερικές φορές υπάρχουν διπλοί τέτοιοι εξυπηρετητές για να εξασφαλιστεί ότι τουλάχιστον ένας από αυτούς θα είναι διαθέσιμος. Όμως ανάλογα με το μέγεθος του δικτύου είναι πιθανό αυτό να μην αποτελεί μια υλοποιήσιμη λύση που να διασφαλίζει ότι απαραίτητες συσχετίσεις θα εγκαθιδρύονται πάντα ακόμα και σε διακοπές του συστήματος. Η αναπαραγωγή των εξυπηρετητών ασφάλειας προσθέτει επιπλέον ευπάθειες. Καθώς είναι αδύνατο να διασφαλιστεί ότι κάθε κόμβος θα έχει ανά πάσα στιγμή πρόσβαση σε ένα εξυπηρετητή ασφάλειας , αυτή η λύση δεν είναι κατάλληλη για περιπτώσεις που απαιτείται υψηλή διαθεσιμότητα.

Η λύση με τα προκαθορισμένα διαπιστευτήρια απαιτεί κάθε συσκευή να έχει προμηθευτεί με τα μυστικά κλειδιά όλων των οντοτήτων με τα οποία θα χρειαστεί να αυθεντικοποιηθεί . Αυτή η λύση πιθανόν να είναι πολύ «ακριβή», εκτεθειμένη σε ανθρώπινο λάθος και επιφορτισμένη με σημαντικές ευπάθειες λόγω της αναπαραγωγής τόσου μεγάλου πλήθους κλειδιών.

Τα ψηφιακά πιστοποιητικά έχουν το πλεονέκτημα ότι ο πρώτος κόμβος μπορεί να εγκαθιδρύσει μια αυθεντικοποιημένη συσχέτιση ασφάλειας με κάθε άλλο κόμβο που έχει σχέση εμπιστοσύνης με αυτόν που διανέμει τα πιστοποιητικά. Αυτή η σχέση εμπιστοσύνης μπορεί να είναι άμεση ή αποτέλεσμα αλυσίδας πιστοποιητικών.

Στην περίπτωση που μια αλυσίδα πιστοποιητικών χρειάζεται να δημιουργήσει σχέση ασφάλειας, οι συσκευές συνήθως τηρούν διαφόρων τύπων πιστοποιητικά. Η συσκευή χρειάζεται μια σειρά πιστοποιητικών που θα ξεκινάει με το σταθερό έμπιστο μέρος TA(Trust Anchor) και θα ολοκληρώνεται με το δικό της πιστοποιητικό. Η συσκευή είναι πιθανό να συντηρεί μια ή περισσότερες σειρές πιστοποιητικών που θα ξεκινούν με το TA και θα καταλήγουν με τον απομακρυσμένο TA ή CA. Η συσκευή μπορεί να τηρεί την τρέχουσα κατάσταση του δικού της πιστοποιητικού. Σε ένα σύστημα που κάθε κόμβος τηρεί τέτοια δεδομένα είναι πιθανό ότι όλοι οι κόμβοι που μπορεί να καταστούν έμπιστοι μπορούν να αυθεντικοποιηθούν αμοιβαία ακόμα και χωρίς καμία υποδομή του δικτύου.

Με την χρήση του PKI είναι απαραίτητη η ύπαρξη του έμπιστου τρίτου μέρους Relying Party (RP) που θα επιβεβαιώνει την κατάσταση των πιστοποιητικών. Κανονικά το RP ελέγχει τη λίστα ανάκλησης πιστοποιητικών CRL ή ενημερώνεται για το πιστοποιητικό από έναν OCSP (Online Certificate Status Protocol) εξυπηρετητή. Υπάρχει μια μέθοδος που προτάθηκε στο RFC 4366,αλλά δεν εφαρμόστηκε ευρέως και χρησιμοποιεί την τεχνική OCSP stapling. Με αυτή την τεχνική μια συσκευή λαβαίνει μια απάντηση OCSP για το δικό της πιστοποιητικό και την στέλνει στο RP. Τυπικά οι OCSP απαντήσεις αποθηκεύονται για ένα προκαθορισμένο χρόνο περίπου όπως και οι CRLs. Επομένως είναι πιθανό οι συσκευές να λαβαίνουν OCSP απαντήσεις για τα δικά τους πιστοποιητικά όταν έχουν πρόσβαση στους πόρους του δικτύου και να τις διαβιβάζουν στο RP σε μεταγενέστερο χρόνο. Μια συνήθης στρατηγική είναι οι συσκευές να ζητούν OCSP απαντήσεις σε ημερήσια βάση και να τις αποθηκεύουν. Μια άλλη προσέγγιση είναι οι συσκευές να ζητούν OCSP απάντηση μόνο όταν τους ζητηθεί επιβεβαίωση.

Για μια ολοκληρωμένη ασφαλή λύση, τα ψηφιακά πιστοποιητικά πρέπει να μεταφέρουν όχι μόνο τα διαπιστευτήρια αυθεντικοποίησης αλλά και διαπιστευτήρια εξουσιοδότησης. Αυτό μπορεί να γίνει με διάφορους τρόπους. Υπάρχουν πολλές παράμετροι του πιστοποιητικού που μπορεί να χρησιμοποιηθούν για να κωδικοποιήσουν πληροφορία εξουσιοδότησης. Το καταλληλότερο είναι το Certification Policy (CP) πεδίο που δείχνει στο RP αν είναι εφικτή η εφαρμογή ενός πιστοποιητικού για κάποιο συγκεκριμένο σκοπό.

Γενικά οι οργανισμοί πρέπει να αξιολογούν τα πλεονεκτήματα του να υποστηρίζουν μόνο μια ομάδα πιστοποιητικών με βάση το ότι τα πιστοποιητικά πρέπει να ανανεώνονται κάθε φορά που αλλάζουν οι εξουσιοδοτήσεις μιας οντότητας. Λαβαίνοντας υπόψη ότι οι συσκευές ενός Έξυπνου Δικτύου δεν πρόκειται να αλλάζουν συχνά εξουσιοδοτήσεις, το να τοποθετηθούν τα διαπιστευτήρια εξουσιοδότησης μαζί με αυτά της αυθεντικοποίησης δεν δημιουργεί σοβαρό πρόβλημα.

Με κατάλληλες σειρές πιστοποιητικών, πρόσφατες απαντήσεις OCSP και διαπιστευτήρια εξουσιοδότησης είναι δυνατόν να παρέχονται υψηλής αξιοπιστίας συστήματα που να επιτρέπουν δύο οντότητες να αυθεντικοποιούνται για εξουσιοδοτημένες υπηρεσίες ακόμα κι αν μεγάλο μέρος των πόρων του δικτύου είναι μη διαθέσιμο.

Hardware Security Module and PKI

Είναι δυνατό να παράγονται και να αποθηκεύονται τα μυστικά ή ιδιωτικά κλειδιά που χρησιμοποιούνται σε μια PKI υποδομή , σε ένα HSM. Ένα εύλογο ερώτημα είναι αν αυτές οι συσκευές ανεβάζουν το ήδη επιβαρυμένο κόστος οντοτήτων του Έξυπνου Δικτύου όπως οι Sensor Nodes. Πρόσφατα η αγορά των έξυπνων καρτών κατέβασε τα κόστος των chip που μπορούν να αποθηκεύσουν με ασφάλεια κλειδιά. Αυτά τα chip κοστίζουν ελάχιστα όταν αγοραστούν σε μεγάλες ποσότητες. Και όχι μόνο παρέχουν πλεονεκτήματα στην ασφάλεια αλλά επιπλέον τα chip μπορούν να ελαφρύνουν λειτουργικά την CPU της συσκευής που τοποθετούνται στις διαδικασίες της κρυπτογράφησης. Έτσι η υπολογιστική ισχύς του επεξεργαστή δεν θα είναι πια εμπόδιο για την υιοθέτηση PKI μεθόδων κρυπτογράφησης για νέες συσκευές (όχι για τα legacy συστήματα). Συνήθως η κρυπτογράφηση δημόσιου κλειδιού απαιτείται μόνο στην φάση εγκαθίδρυσης ασφαλούς συσχέτισης. Στη συνέχεια της επικοινωνίας προτιμούνται οι μέθοδοι συμμετρικής κρυπτογράφησης.

Διαχείριση Εμπιστοσύνης

Υπάρχουν διάφορα μοντέλα high- level trust management: strictly hierarchy (τα αυστηρά ιεραρχικά), full mesh (δικτυωτά), federated(συνενωμένα). Όταν διάφοροι οργανισμοί προσπαθούν να παρέχουν υψηλή δικτυακή συνδεσιμότητα που επεκτείνεται στους πόρους διαφόρων υπηρεσιών ή πρακτόρων ,το αυστηρά ιεραρχικό

μοντέλο πολύ γρήγορα καταστρατηγείται γιατί είναι τυπικά πολύ δύσκολο όλοι οι εμπλεκόμενοι να συμφωνήσουν στο τι αποκαλούν έμπιστο και σύμφωνα με ποια πολιτική το έμπιστο μέρος θα λειτουργεί. Το αυστηρά ιεραρχικό μοντέλο βασίζεται στην απόλυτη ασφάλεια της κεντρικής έμπιστης «διαδρομής» και τυχόν παραβίαση της κεντρικής δομής καταστρέφει την ασφάλεια όλου του συστήματος. Το mesh model ενδέχεται να είναι πού ακριβό. Στην πραγματικότητα το federal μοντέλο συνδυάζει τα καλύτερα χαρακτηριστικά του mesh και του hierarchy μαζί. Ο όρος PKI federation αναφέρεται σε ένα σύστημα που ελέγχει μόνο του τα δικά του PKI μέρη και τις πολιτικές και αποφασίζει από μόνο του τις εσωτερικές του δομές , συνήθως αλλά όχι πάντα ιεραρχικές. Το σύστημα αποφασίζει πότε και πως θα αυθεντικοποιηθεί με τη μέθοδο cross-sign με άλλα συστήματα. Μια τέτοια προσέγγιση είναι η μόνη λογική λύση για μεγάλα διατμηματικά συστήματα. Στην πραγματικότητα η δραστηριότητα του cross-signing με πολλές άλλες περιοχές μπορεί να επιφέρει σημαντικό επιπλέον φορτίο. Οι οργανισμοί κοινής ωφέλειας θα επιδίωκαν να δημιουργηθούν τοπικές κοινοπραξίες που θα παρέχουν υπηρεσίες γέφυρας για τους οργανισμούς μέλη της, που θα μειώνουν το επιπλέον φορτίο.

Οι μικρές εταιρείες κοινής ωφέλειας θα μπορούσαν λόγο κόστους να έχουν outsourcing PKI. Αυτό διαφέρει από έναν δημόσιο PKI πάροχο που παρέχει πιστοποιητικά (Internet model). Ένα τέτοιο πιστοποιητικό κυρίως αποδεικνύει ότι είσαι ο νόμιμος ιδιοκτήτης του domain name που υπάρχει στο πιστοποιητικό σου. Για τα έξυπνα δίκτυα αυτό δεν είναι αρκετό. Τα πιστοποιητικά πρέπει να χρησιμοποιούνται για απόδειξη ιδιοκτησίας όπως χρησιμοποιούνται και για διαπιστευτήρια εξουσιοδότησης.

Ανάγκη για ένα μοντέλο πολιτικής.

Μία πολιτική πιστοποιητικών (certificate policy CP) είναι ένα κείμενο που περιγράφει τους κανόνες που διέπουν τη διανομή πιστοποιητικών. Ένα τέτοιο κείμενο περιλαμβάνει απαιτήσεις για όλους τους PKI εμπλεκόμενους, ακόμα και για αυτούς που εμπίπτουν στον RP. Επίσης περιλαμβάνει νομικούς όρους όπως τα όρια ευθύνης που αποδέχεται το PKI. Ο RFC 3647 παρέχει ένα πρότυπο CP το οποίο χρησιμοποιούν οι περισσότεροι PKI.

Κάθε πιστοποιητικό περιλαμβάνει certificate policy extension που αντανακλά στη CP που το διέπει. Αυτή η επέκταση περιλαμβάνει ένα παγκοσμίως μοναδικό

OBJECT ID που μπορεί να χρησιμοποιηθεί από ένα RP για να ανατρέξει στο κείμενο της πολιτικής. Έτσι μπορεί να αντλήσει πληροφορίες για το πιστοποιητικό όπως το επίπεδο βεβαιότητας το πώς ελέγχθηκε το πώς προστατεύονται τα ιδιωτικά κλειδιά και το αν θα πρέπει να ζητήσει πρόσφατες πληροφορίες για την κατάσταση του πιστοποιητικού.

Το OBJECT ID της CP δείχνει την συμβατότητα του πιστοποιητικού για μια συγκεκριμένη χρήση. Ένα PKI μπορεί να χρησιμοποιεί διαφορετικά CP OBJECT IDS για διαφορετικού τύπου συσκευές. Το RP μπορεί να ρυθμιστεί με τα αποδεκτά CP OIDS και έτσι να μην χρειάζεται να ανακτήσει και να διαβάσει το CP κείμενο.

Διάρκεια ζωής πιστοποιητικών.

Η λύση έκδοσης πιστοποιητικών με διάρκεια ζωής 50 έτη και άνω μπορεί να φαίνεται βολική αλλά όμως μπορεί να φέρει σημαντικές επιπλοκές στο μέλλον. Τα ανακλημένα πιστοποιητικά πρέπει να παραμένουν στις CR λίστες μέχρι τη λήξη τους. Αυτό μπορεί να δημιουργήσει πολύ μεγάλες λίστες το οποίο είναι πρόβλημα για συσκευές που περιλαμβάνονται σε έξυνα δίκτυα και διαθέτουν περιορισμένους πόρους.

Η διάρκεια ζωής των πιστοποιητικών πρέπει να διαμορφωθεί ανάλογα με τους κινδύνους του συστήματος. Προτείνεται να μην υπερβαίνει το ανώτατο όριο των 10 ετών. Μία επερχόμενη ημερομηνία λήξης θα έπρεπε να θέτει μία ένδειξη στο σύστημα που θα προκαλεί την αντικατάσταση του πιστοποιητικού, κάτι το οποίο θα μπορούσε να μειώσει την επιβάρυνση της αποθήκευσης μεγάλου αριθμού ανακλημένων πιστοποιητικών.

Smart Grid System – Specific Encryption and Key Management Issues

Στα συστήματα που έχουν κρυπτογράφηση πρέπει να υπάρχει σύστημα διαχείρισης κλειδιών, που να παρέχει προστασία στα κρυπτογραφικό υλικό και ποικιλομορφία στα κλειδιά. Κάθε συσκευή πρέπει να διαθέτει μοναδικά διαπιστευτήρια έτσι ώστε το σπάσιμο μιας συσκευής να μην συνεπάγεται το σπάσιμο όλων. Το σύστημα διαχείρισης κλειδιών KMS (Key Management System) ,πρέπει να υποστηρίζει περιοδική ανακύκλωση κλειδιών και ανάκληση.

Υπάρχουν πραγματικές περιπτώσεις στις οποίες μια μεγάλη υποδομή μετρητών χρησιμοποιεί το ίδιο συμμετρικό κλειδί παντού ακόμα και σε διαφορετικά μέρη. Προκειμένου να διαμοιράζονται υπηρεσίες δικτύου γειτονικές εταιρείες πιθανόν να μοιράζονται και να χρησιμοποιούν το ίδιο κλειδί στα δίκτυα μετρήσεων τους. Έτσι διακινδυνεύοντας την ασφάλεια ενός μετρητή, κινδυνεύει η ασφάλεια των μετρητών και των δύο δικτύων.

5.2 Λύσεις κρυπτογράφησης και διαχείρισης κλειδιών

Η ασφαλής διαχείριση κλειδιών είναι απαραίτητη για μια αποτελεσματική χρήση κρυπτογράφησης σε μια υποδομή Έξυπνου Δικτύου. Στην οδηγία του NIST SP 800-57 για την διαχείριση κλειδιών, προτείνονται βέλτιστες πρακτικές για προγραμματιστές και διαχειριστές για ασφαλή διαχείριση κλειδιών. Αυτές οι συστάσεις είναι εφαρμόσιμες τόσος σε υποδομές Έξυπνων Δικτύων όσο και σε οποιοδήποτε άλλο σύστημα χρησιμοποιεί κρυπτογράφηση , και αποτελούν σημείο αναφοράς για την διαχείριση κλειδιών σε Έξυπνα Δίκτυα.

5.2.1 Γενικά θέματα σχεδιασμού.

Επιλογή και χρήση τεχνικών κρυπτογράφησης.

Ο σχεδιασμός κρυπτογραφικών αλγορίθμων και πρωτοκόλλων που λειτουργούν σωστά και δεν έχουν μη δοκιμασμένες ροές , είναι γενικά δύσκολο. Στην κοινότητα της κρυπτογραφίας έχει συμφωνηθεί ότι οι αλγόριθμοι και τα πρωτόκολλα που είναι γνωστά και δημοσιευμένα και δοκιμασμένα στον χρόνο, είναι λιγότερο πιθανό να περιέχουν άγνωστες και μη δοκιμασμένες ροές απ’ ότι αυτά που παραμένουν μυστικά, διότι η δημοσίευση τους ενεργοποιεί τον εξαντλητικό έλεγχο από ολόκληρη την κοινότητα. Γι’ αυτό προτιμώνται οι προτεινόμενες από τον NIST τεχνικές και οι FIPS εγκεκριμένες. Παρόλα αυτά οι μοναδικές απαιτήσεις που παρουσιάζουν κάποια τμήματα των Έξυπνων Δικτύων μπορεί να οδηγήσουν σε πραγματική ανάγκη για χρήση τεχνικών και πρωτοκόλλων πέραν αυτών.

Οι γενικές αναφορές είναι ότι αυτές οι επιπλέον τεχνικές που δεν περιλαμβάνονται στις λίστες των NIST και FIPS, δεν έχουν υποστεί ελέγχους και

αναλύσεις ανάλογα με τις καθιερωμένες διαδικασίες του FIPS και τις προτεινόμενες τεχνικές από τον NIST. Κατ' ελάχιστον αυτές οι τεχνικές θα πρέπει να έχουν τεθεί σε ένα δημόσιο διάλογο, να έχουν ελεγχθεί και σχολιαστεί από κάποια κοινότητα κρυπτογράφων και θα έχουν αναπτυχθεί με αναγνωρισμένα πρότυπα. Επιπλέον θα πρέπει να δημιουργηθεί κάποιο σενάριο για τη χρήση του μέσα στους περιορισμούς που υπάρχουν από του πόρους και από την μοναδική φύση της κάθε εφαρμογής.

Δυνατότητα αναβάθμισης κρυπτογραφικών μεθόδων

Τα θέματα που προκύπτουν προς εξέταση όταν σχεδιάζεται η δυνατότητα αναβάθμισης των μεθόδων κρυπτογράφησης είναι τα εξής:

- Ο εξοπλισμός των Έξυπνων Δικτύων συνήθως απαιτείται να έχει ένα μέσο όρο ζωής τα 20 έτη, το οποίο είναι πολύ μεγαλύτερο από αυτό των πληροφοριακών και τηλεπικοινωνιακών συστημάτων.
- Λόγω των απαιτήσεων για αξιοπιστία στα ηλεκτρικά δίκτυα, οι δοκιμές είναι συνήθως σχολαστικές και διαρκούν πολύ καιρό.
- Η αντικατάσταση των ήδη εγκατεστημένων συσκευών μπορεί να διαρκέσει και να κοστίσει περισσότερο από ότι πολλά πληροφοριακά και τηλεπικοινωνιακά συστήματα.

Σε αυτά τα θέματα πρέπει να δοθεί μεγάλη προσοχή στη φάση του σχεδιασμού κάθε συσκευής και συστήματος για Έξυπνα Δίκτυα.

Συνήθως οι αποτυχίες στα συστήματα κρυπτογράφησης συμβαίνουν για τους παρακάτω λόγους:

- Λάθη στην εφαρμογή. Για παράδειγμα μια «φτωχή» τροφοδοσία της γεννήτριας ψευδοτυχαίων αριθμών, χαμηλοί πόροι εντροπίας, λάθος σε κώδικα αλγόριθμου ή πρωτόκολλου, λάθη και ευπάθειες στο API (Application Program Interface) που οδηγούν σε σοβαρές διαρροές ασφάλειας.
- Υπολογιστικά λάθη. Ο συνδυασμός αλγορίθμων κρυπτογράφησης χωρίς επαρκή ανάλυση οδηγεί σε λιγότερο ασφαλή συστήματα.
- Μη ασφαλείς αλγόριθμοι. Η πιθανότητα οι βασικοί σύγχρονοι αλγόριθμοι κρυπτογράφησης, να καταστούν απόλυτα ανασφαλείς είναι χαμηλή, αλλά

είναι υπαρκτή. Πιθανότερο όμως είναι ότι θα εφευρεθούν τρόποι που θα μειώνουν την υπολογιστική ισχύ των αλγόριθμων.

Υπάρχουν επίσης κάποια θέματα που αφορούν τον σχεδιασμό των συστημάτων των Έξυπνων Δικτύων και αφορούν τους κινδύνους.

- Συστήνεται η χρήση εγκεκριμένων και διεξοδικά ελεγμένων κρυπτογραφικών αλγορίθμων. Ο τομέας ασφάλειας του NIST (Computer Security Division) έχει δημοσιεύσει πληθώρα τέτοιων μηχανισμών καθώς και οδηγίες εφαρμογής τους.
- Οι αλγόριθμοι που έχουν δημοσιευτεί στην κοινότητα κρυπτογραφίας και έχουν ωριμάσει, θα πρέπει να προτιμώνται σε σχέση με αυτούς που βασίζονται σε μια κλειστού τύπου ανάπτυξη.
- Πρέπει να προτιμώνται οι επικυρωμένες κρυπτογραφικές εφαρμογές.
- Κρυπτογραφικές διαδικασίες (software και hardware) που μπορεί να υποστηρίξουν ευελιξία στο μήκος του κλειδιού διατηρώντας την απαραίτητη απόδοση, θα πρέπει να προτιμώνται σε σχέση με αυτούς που δεν παρέχουν αυτή την ευελιξία.
- Η παροχή κρυπτογραφικού σχεδιασμού που ξεπερνά τις τρέχουσες απαιτήσεις ασφάλειας προκειμένου να αποφευχθεί αργότερα μια αναβάθμιση.
- Οι κρυπτογραφικοί αλγόριθμοι συχνά χρησιμοποιούνται μέσα στα πρωτόκολλα επικοινωνιών. Για να είναι εφικτή πιθανή μελλοντική αλλαγή στου κρυπτογραφικούς αλγόριθμους χωρίς να διακόπτεται η τρέχουσα λειτουργία, η λύση είναι να σχεδιάζονται πρωτόκολλα που επιτρέπουν εναλλακτικούς κρυπτογραφικούς αλγόριθμους.
- Θα υπάρχουν περιπτώσεις που κυρίως λόγω κόστους ή άλλους τεχνικούς περιορισμούς κάποια κρυπτογραφικά συστήματα να μην είναι αναβαθμίσιμα. Σε τέτοιες περιπτώσεις καλό είναι να υπάρχει βεβαιότητα ότι υπάρχει τρόπος για αντιμετώπιση αυτών των συστημάτων ή συσκευών ως λιγότερο έμπιστα μέσα στην υποδομή.

Γεννήτρια τυχαίων αριθμών

Τυχαίοι ή ψευδοτυχαίοι αριθμοί συχνά χρησιμοποιούνται σε κρυπτογραφικούς αλγόριθμους. Μία αποτυχία της γεννήτριας τυχαίων αριθμών μπορεί να θέσει σε

κίνδυνο τον κρυπτογραφικό αλγόριθμο ή πρωτόκολλο και επομένως την συσκευή ή το σύστημα.

Πολλές συσκευές Έξυπνων Δικτύων μπορεί να διαθέτουν περιορισμένο βαθμό εντροπίας έτσι ώστε να λειτουργούν σαν πραγματική πηγή τυχαίων αριθμών. Ο σχεδιασμός μιας ασφαλούς γεννήτριας τυχαίων αριθμών με χαμηλή εντροπία είναι δύσκολη. Επομένως απαιτείται η χρήση καλά σχεδιασμένης και ασφαλώς τροφοδοτούμενης γεννήτριας ψευδοτυχαίων αριθμών. Σε κάποιες περιπτώσεις οι συσκευές Έξυπνων Δικτύων μπορεί να χρειάζονται επιπλέον εξοπλισμό για να μπορούν να παρέχουν καλή πηγή τυχαίων αριθμών που θα τροφοδοτεί την γεννήτρια.

Υπάρχουν διάφορες εξουσιοδοτημένες πηγές για πληροφορίες σε αλγόριθμους που παράγουν τυχαίους αριθμούς. Μια από αυτές είναι η οδηγία του NIST SP 800-90.

Τοπική λειτουργική αυτονομία

Είναι σημαντικό να μπορούν να υποστηριχθούν κρυπτογραφικές διαδικασίες ακόμα κι όταν η σύνδεση με άλλες συσκευές είναι αδύνατη. Για παράδειγμα σε μια διακοπή του δικτύου, οι τεχνικοί μπορεί να πρέπει να αυθεντικοποιηθούν σε συσκευές υποσταθμών που χρειάζονται επισκευή ακόμα κι αν η σύνδεση στο κέντρο ελέγχου είναι αδύνατη. Η διαδικασίες αυθεντικοποίησης και εξουσιοδότησης πρέπει να μπορούν να λειτουργούν τοπικά με αυτόνομο τρόπο στους υποσταθμούς.

Διαθεσιμότητα

Η διαθεσιμότητα για κάποια έξυπνα δίκτυα μπορεί να είναι σημαντικότερη από την ασφάλεια. Η άρνηση εγκαθίδρυσης σύνδεσης λόγω ληγμένου πιστοποιητικού ή κλειδιού μπορεί να διακόψουν πολύ σημαντικές επικοινωνίες.

Φυσική Ασφάλεια

Η προστασία των κρίσιμων παραμέτρων ασφάλειας CSPs ,όπως τα κλειδιά και τα δεδομένα αυθεντικοποίησης, είναι απαραίτητη για την διατήρηση της ασφάλειας που παρέχεται από την κρυπτογράφηση. Για την προστασία έναντι της μη εξουσιοδοτημένης πρόσβασης, τροποποίησης ή αντικατάστασης αυτών των δεδομένων , οι κρυπτογραφικές διαδικασίες μπορεί να περιέχουν χαρακτηριστικά που παρέχουν φυσική ασφάλεια. Κάποιες τέτοιες μέθοδοι είναι multichip standalone, multichip embedded και single – chip συσκευές. Συγκεκριμένα παραδείγματα τέτοιων

τύπων συσκευών που παρέχουν κρυπτογραφικές υπηρεσίες και φυσική ασφάλεια είναι οι Tamper Resistant Security Modules (TRSMs), Hardware Security Modules, Security Authentication Module cards (SAM cards) , οι οποίοι έχουν αναγνωριστεί ως FIPS 140-2 κρυπτογραφικές διαδικασίες.

Η φυσική ασφάλεια είναι η ικανότητα που έχει μια διαδικασία να μπορεί να προστατεύεται από μη εξουσιοδοτημένη πρόσβαση στις CSPs και από παραποίηση. Μια κρυπτογραφική διαδικασία που εφαρμόζεται σε ένα λογισμικό και τρέχει σε ένα απροστάτευτο σύστημα, συνήθως δεν έχει την δυνατότητα να προστατευτεί από φυσική επίθεση. Οι firmware κρυπτογραφικές διαδικασίες, είναι μικρά προγράμματα που ελέγχουν εσωτερικά μια διαδικασία. Αυτές οι διαδικασίες συνήθως σχεδιάζονται να παρέχουν μια σειρά από μέτρα προστασίας της φυσικής ασφάλειας.

Για να καθοριστεί ο βαθμός προστασίας φυσικής ασφάλειας που απαιτείται για μια συσκευή, είναι απαραίτητο να ληφθεί υπόψη το περιβάλλον λειτουργίας της και η αξία και ευαισθησία των δεδομένων που τηρούνται στη συσκευή και επομένως πρόκειται για διοικητική απόφαση. Για παράδειγμα μπορεί να αποφασιστεί ότι για μια διαδικασία που προστατεύει δεδομένων χαμηλής αξίας και τρέχει σε περιβάλλον με φυσικούς ελέγχους και προστασία, δεν απαιτείται επιπλέον φυσική προστασία και μπορεί να εφαρμοστεί σε λογισμικό που τρέχει σε υπολογιστή γενικής χρήσης. Στο ίδιο περιβάλλον, για δεδομένα υψηλής αξίας θα απαιτούνταν ισχυρή φυσική προστασία.

Σε μη προστατευόμενα ή μερικώς προστατευόμενα περιβάλλοντα, οι κρυπτογραφικές διαδικασίες διαθέτουν επιπλέον φυσική προστασία. Ακόμα και στο επίπεδο του καταναλωτή οι συσκευές που επεξεργάζονται και περιέχουν ευαίσθητα δεδομένα συνήθως περιέχουν φυσική ασφάλεια. Οι μετρητές των έξυπνων δικτύων συχνά επεξεργάζονται πληροφορία και παρέχουν λειτουργικότητα που κάποιες φορές μπορεί να είναι ευαίσθητες ή μεγάλης αξίας. Σε αυτές τις περιπτώσεις είναι διοικητική ευθύνη να καθοριστούν τα μέτρα και ο βαθμός της φυσικής ασφάλειας.

5.2.2 Συστήματα Διαχείρισης Κλειδιών για Έξυπνα Δίκτυα.

Υποδομή Δημόσιου Κλειδιού

Τα πιστοποιητικά εκδίδονται με χρονική ισχύ που καθορίζεται στο X509 πιστοποιητικό με δύο πεδία “not Before” και “not After”.Είναι σημαντικό τα πιστοποιητικά να θεωρούνται έγκυρα μόνο όταν χρησιμοποιούνται εντός χρονικής ισχύος. Εάν διαπιστωθεί ότι το πιστοποιητικό έχει εκδοθεί για μια οντότητα που δεν θεωρείται πλέον έμπιστη (πχ κλεμμένη συσκευή) ,το πιστοποιητικό πρέπει να ανακληθεί. Οι λίστες ανακλημένων πιστοποιητικών χρησιμοποιούνται για να αποθηκεύουν τον μοναδικό αριθμό και την ημερομηνία ανάκλησης των πιστοποιητικών. Relying Party (RP) είναι μια οντότητα του δικτύου που βασίζει τις ενέργειες της στην πληροφορία των πιστοποιητικών και για να αποφασίσει αν δέχεται ένα πιστοποιητικό ελέγχει τουλάχιστον τα εξής:

- Αν το πιστοποιητικό εκδόθηκε από έμπιστη πηγή.
- Αν είναι εντός χρονικής ισχύος.
- Ότι το πιστοποιητικό δε βρίσκεται σε κάποια επίσημη λίστα ανάκλησης πιστοποιητικών.

Ορθή χρήση Ανάκλησης και Λήξης πιστοποιητικών

Όταν ένα πιστοποιητικό δεν είναι πλέον έγκυρο, προστίθεται στη λίστα ανάκλησης πιστοποιητικών. Αυτές οι λίστες (CRLs) γίνονται ολοένα και μεγαλύτερες καθώς προστίθενται συνεχώς μη έγκυρα πιστοποιητικά. Για αυτό το λόγο οι διαχειριστές της υποδομής δημόσιου κλειδιού ορίζουν ένα κατάλληλο χρονικό όριο ισχύος των πιστοποιητικών και έτσι όταν για κάποιο πιστοποιητικό που έχει ανακληθεί , έχει λήξει η ισχύς του , δεν χρειάζεται να βρίσκεται σε CRL. Έτσι διατηρείται ένα λογικό μέγεθος των CRLs.

Οι διαχειριστές πρέπει να ισορροπήσουν την διάρκεια της χρονική ισχύος των πιστοποιητικών, με το λειτουργικό φόρτο που αυξάνεται όσο μικραίνει η χρονική ισχύς και με το εύχρηστο μέγεθος των CRLs.

Όταν εκδίδονται πιστοποιητικά για εργαζόμενους που το επίπεδο ευθύνης τους μπορεί να μεταβάλλεται συχνά, τότε είναι καλύτερα η ισχύς των πιστοποιητικών να είναι σχετικά μικρή (πχ. 1-2 έτη). Έτσι όταν θα χρειαστεί να ανακληθεί το πιστοποιητικό του εργαζόμενου για να εκδοθεί νέο, το ανακλημένο πιστοποιητικό χρειάζεται να μείνει στην CRL μόνο μέχρι την λήξη του.

Όταν εκδίδονται πιστοποιητικά για συσκευές που πρόκειται να διαρκέσουν για πολλά χρόνια και αυτές οι συσκευές βρίσκονται σε ασφαλές περιβάλλον, δεν απαιτείται μικρή χρονική ισχύς γιατί υπάρχει μικρή πιθανότητα ανάκλησης τους και επομένως δεν θα επιβαρύνουν το μέγεθος της CRL.

Ένα δίλημμα που προκύπτει είναι αν ένα Relying Party σε ένα Έξυπνο Δίκτυο πρέπει ή όχι να δέχεται ένα πιστοποιητικό (συσκευής ή χρήστη) που έχει λήξει η χρονική ισχύς του. Στην περίπτωση που απορριφθεί η αίτηση αυθεντικοποίησης λόγω λήξης του πιστοποιητικού μπορεί να προκληθεί μεγάλη δυσλειτουργία στο σύστημα. Λαμβάνοντας υπόψη ότι οι συσκευές των Έξυπνων Δικτύων εγκαθίστανται με την προοπτική να λειτουργούν για πολλά χρόνια (10 -15 έτη), η αντικατάσταση τους δεν θα συμβαίνει συχνά ,εκτός από μη προγραμματισμένα γεγονότα. Τα πιστοποιητικά αυτών των συσκευών μπορεί να βρεθούν σε CRL μόνο όταν οι συσκευές αντικαθίστανται ή όταν πρέπει να καταργηθούν τα κλειδιά τους. Αν σε τέτοιες συσκευές δεν γίνεται αντικατάσταση του πιστοποιητικού πριν τη λήξη του, η συσκευή δεν θα μπορεί να επικοινωνεί με το δίκτυο. Γι' αυτό η αντικατάσταση των πιστοποιητικών πρέπει να προγραμματίζεται 1 χρόνο περίπου πριν από τη λήξη τους για να υπάρχει το χρονικό περιθώριο σε περίπτωση αποτυχίας και να αποφευχθεί ο κίνδυνος να μείνει η συσκευή εκτός δικτύου.

Λόγω του μεγέθους και της εμβέλειας των Έξυπνων Δικτύων, υπάρχουν κι άλλες μέθοδοι για διατήρηση εύχρηστων CRLs. Μια από αυτές είναι ο διαχωρισμός της CRL σε μικρότερες με βάση κάποιες συγκεκριμένες παραμέτρους των πιστοποιητικών όπως η τοποθεσία της συσκευής, ο τύπος της συσκευής ή το έτος έκδοσης τους.

Υψηλή Διαθεσιμότητα και Δια - λειτουργικότητα των Πιστοποιητικών και των CRLs

Η αυθεντικοποίηση που βασίζεται σε πιστοποιητικά προσφέρει πολλά πλεονεκτήματα ανάλογα με την υψηλή διαθεσιμότητα και δια - λειτουργικότητα που παρέχει. Με αυτό το είδος αυθεντικοποίησης δύο οντότητες που δεν έχουν ρυθμιστεί να αναγνωρίζει και να εμπιστεύεται η μια την άλλη, μπορούν να επικοινωνήσουν και να αποφασίσουν αν είναι εξουσιοδοτημένες για πρόσβαση σε τοπικούς πόρους ή για να συμμετέχουν στο δίκτυο. Με την τεχνική cross – signing ή bridging αυτές οι δύο οντότητες μπορεί να προέρχονται από διαφορετικούς οργανισμούς . Παρ' όλα αυτά αν οι CRLs βρίσκονται σε κεντρικούς servers και κάποια στιγμή δεν είναι διαθέσιμες στα Relying Parties τότε δεν θα είναι εφικτό να αυθεντικοποιηθούν. Αυτό μπορεί να συμβεί για διάφορους λόγους. Οι CRLs μπορούν να αποθηκεύονται και να χρησιμοποιούνται από τα RP για κάποια χρονική περίοδο που καθορίζεται από την πολιτική που εφαρμόζει το σύστημα. Επίσης οι CRLs μπορούν να περιορίζονται σε μικρές γεωγραφικές περιοχές, όπως για παράδειγμα όλες οι συσκευές ενός υποσταθμού και οι οντότητες που πρόκειται να επικοινωνούν με αυτές. Αυτές οι CRLs μπορούν να αποθηκεύονται σε ένα υποσταθμό και έτσι να είναι εύκολα προσβάσιμες από όλες τις συσκευές του υποσταθμού. Μια άλλη εναλλακτική λύση που μπορεί να προσφέρει πολύ υψηλή διαθεσιμότητα, είναι ότι κάθε οντότητα περιοδικά ανακτά την κατάσταση του δικού της πιστοποιητικού και την κουβαλά, οπότε όταν χρειάζεται να αυθεντικοποιηθεί σε ένα RP υποβάλει το πιστοποιητικό του και την πρόσφατη κατάσταση του. Αν το RP δεν έχει διαθέσιμη άλλη πηγή για να αντλήσει την κατάσταση του πιστοποιητικού και αν αυτό που του υποβάλει είναι πρόσφατο τότε το RP αποδέχεται την κατάσταση του πιστοποιητικού ως έγκυρη.

Άλλα θέματα σχετικά με την κατάσταση των πιστοποιητικών

Τα μέρη ενός έξυπνου δικτύου μπορεί να διαθέτουν πιστοποιητικά που έχουν εκδοθεί από τους κατασκευαστές τους. Αυτά τα πιστοποιητικά αποδεικνύουν ποιός είναι ο κατασκευαστής, το μοντέλο και ο σειριακός αριθμό της συσκευής. Σε αυτή την περίπτωση η εταιρεία που χρησιμοποιεί την συσκευή θα πρέπει να εκδώσει επιπλέον πιστοποιητικό που περιέχει ειδικές παραμέτρους για την λειτουργία της συσκευής στο σύστημα. Αυτά τα πιστοποιητικά μπορεί να είναι είτε νέα αναγνωριστικά πιστοποιητικά που περιέχουν αυτά τα επιπλέον χαρακτηριστικά , είτε ξεχωριστά

πιστοποιητικά με αυτά τα χαρακτηριστικά. Για πιστοποιητικά που αφορούν χρήστες η δεύτερη λύση είναι καταλληλότερη γιατί παρέχει μεγαλύτερη ευελιξία. Όταν πρόκειται για συσκευές τα νέα αναγνωριστικά πιστοποιητικά είναι μια λύση που κοστίζει λιγότερο και συνήθως αυτή προτιμάται.

Standardized Trust Management μηχανισμοί μπορεί να περιέχουν cross – sign διαδικασίες, περιορισμούς για τα cross - signed πιστοποιητικά, απαιτήσεις για τοπικούς bridge παρόχους καθώς και εγκεκριμένες μεθόδους για έκδοση προσωρινών πιστοποιητικών σε οντότητες σε έκτακτες περιπτώσεις. Ιδανικά η έκδοση προσωρινών πιστοποιητικών δεν θα έπρεπε να χρειάζεται. Παρ' όλα αυτά συμβαίνει μετά από κάποιο πολύ σοβαρό περιστατικό (π.χ. φυσική καταστροφή) να πρέπει να σταλούν πόροι από προέλευση που μέχρι τότε δεν είχε προβλεφθεί. Σε αυτές τις περιπτώσεις υπάρχουν δύο επιλογές. Η μια είναι να βεβαιώνεται εκ των προτέρων ότι όλα τα πιθανά μέρη είναι έμπιστα. Αυτό συνεπάγεται μεγάλο κίνδυνο και μεγάλο λειτουργικό φόρτο. Η άλλη είναι να υπάρχουν μέσα για γρήγορη έκδοση προσωρινών διαπιστευτηρίων στους πόρους που προέρχονται από απομακρυσμένες πηγές. Αυτή η μέθοδος μπορεί να βασίζεται στα υφιστάμενα διαπιστευτήρια των πόρων ίσως με την μορφή έκδοσης πιστοποιητικού χαρακτηριστικών.

Η προτυποποίηση των πολιτικών έκδοσης πιστοποιητικών για τα έξυπνα Δίκτυα θα πρέπει να στοχεύει στην δια - λειτουργικότητα. Παρόμοια πρότυπα έχουν υιοθετήσει με επιτυχία και άλλοι χώροι (π.χ. υγεία). Ιδανικά αυτά τα πρότυπα θα καθορίζουν όλους τους πιθανούς ρόλους των υποκείμενων των πιστοποιητικών, όλες τις κατηγορίες των συσκευών και ειδικές απαιτήσεις για τα μέρη της PKI υποδομής για κάθε επίπεδο διασφάλισης που παρέχεται.

Έμπιστες Αρχές (Trust Roots)

Ένας τυπικός web browser στέλνει μεγάλο αριθμό πιστοποιητικών. Μπορεί να μην είναι όλες οι αρχές έκδοσης πιστοποιητικών κατάλληλες για να είναι trust roots για ένα σύστημα σε Έξυπνο Δίκτυο. Απ' την άλλη με την ύπαρξη τρίτων έμπιστων μερών που παρέχουν υπηρεσίες δεδομένων και διαχείρισης ,ίσως δεν είναι σκόπιμο για την εταιρεία κοινής ωφέλειας να είναι η μόνη έμπιστη αρχή.

Επιπλέον υπάρχει και το ερώτημα του ποιός εκδίδει τα πιστοποιητικά και του πώς το σύστημα μπορεί να γνωρίζει ότι η οντότητα που αυθεντικοποιείται είναι και ο

πραγματικός κάτοχος του πιστοποιητικού. Στο Internet η μέθοδος που ακολουθείται είναι πιστοποιητικά υψηλού επιπέδου (top level) που είναι η βάση εμπιστοσύνης. Αυτή η εμπιστοσύνη μπορεί να επεκταθεί σε δευτερογενείς οργανισμούς έκδοσης πιστοποιητικών. Η ερώτηση είναι το πώς επιλέγεται ένας οργανισμός να είναι trust root οργανισμός και πώς επιβεβαιώνεται ξ ταυτότητα των πιστοποιητικών τους.

Single Sign On

Οι συσκευές των Έξυπνων Δικτύων όπως οι ασύρματες συσκευές είναι συσκευές χαμηλής υπολογιστικής ισχύος με ασύρματη διεπαφή και συχνά συνδέονται στα backhaul δίκτυα με συνδέσεις χαμηλού εύρους ζώνης. Αυτές οι συσκευές τυπικά διαθέτουν 4 έως 12 kb μνήμης RAM και 64 έως 256 επιπρόσθετη μνήμη. Τα χαρακτηριστικά της σύνδεσης μπορεί να ποικίλουν ανάλογα με τα ράδιο - ασύρματα χαρακτηριστικά. Για παράδειγμα το σύστημα μέτρησης μπορεί περιοδικά να «ξυπνά» και να συγχρονίζεται στο δίκτυο , αντί να μένει συνέχεια ενεργό. Μια άλλη απαίτηση για τις συσκευές είναι η υποστήριξη multi – hop δικτύων με χρήση τοπολογίας πλέγματος (mesh).

Μπορεί να χρησιμοποιηθούν και προηγμένοι μετρητές για άλλους σκοπούς εκτός από την μέτρηση κατανάλωσης. Για λόγους ασφάλειας κάθε τέτοιος μετρητής πρέπει να αυθεντικοποιείται και πρέπει να μπορεί να διατηρεί την ακεραιότητα των δεδομένων που μεταφέρει στο σύστημα. Σε αυτές τις περιπτώσεις το επιπλέον φορτίο που δημιουργείται επηρεάζει την απόδοση, κάτι που πρέπει να ληφθεί υπόψη λόγο της χαμηλής υπολογιστικής ισχύος των συσκευών.

Από πλευράς διαχείρισης κλειδών, η βελτιστοποίηση του αριθμού των ανταλλαγών που πραγματοποιούνται πρέπει να ληφθεί υπόψη για κάθε επίπεδο και πρωτόκολλο που χρησιμοποιείται στα από τα τμήματα ενός Έξυπνου Δικτύου. Αυτό μπορεί να επιτευχθεί με την εφαρμογή την Single Sing On μεθόδου στα τμήματα του έξυπνου Δικτύου , όπου με μια εκτέλεση της διαδικασίας αυθεντικοποίησης μπορούν να παραχθούν κλειδιά για διάφορα πρωτόκολλα μέσα στο ίδιο επίπεδο επικοινωνίας ή μεταξύ διαφορετικών επιπέδων επικοινωνίας. Σε ένα τυπικό σενάριο, ένας έξυπνος μετρητής αυθεντικοποιείται στο δίκτυο με κρυπτογράφηση δημόσιου κλειδιού που παράγει ένα βασικό κλειδί από το οποίο προκύπτουν κρυπτογραφικά κλειδιά για προστασία κάθε εφαρμογής. Το πλεονέκτημα αυτού του σχήματος είναι ότι η

υπολογιστική διαδικασία απαιτείται μόνο μια φορά για την παραγωγή του βασικού κλειδιού (root key).

Διαχείριση συμμετρικών κλειδιών

Στα περιβάλλοντα που χρησιμοποιούν συμμετρικό κλειδί, χρησιμοποιείται το ίδιο κλειδί για κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων. Έτσι το ίδιο κλειδί πρέπει να μοιράζεται στις οντότητες που πρέπει να επικοινωνούν. Υπάρχουν πλεονεκτήματα και μειονεκτήματα σε αυτή τη μέθοδο κρυπτογράφησης. Τα συστήματα συμμετρικής κρυπτογράφησης σε σχέση με τα δημόσιου κλειδιού, διαχειρίζονται αποτελεσματικότερα μεγάλο όγκο δεδομένων. Τα συμμετρικά κλειδιά έχουν συνήθως μικρότερη διάρκεια ζωής από τα δημόσια κλειδιά λόγω του όγκου των δεδομένων που κρυπτογραφούνται με τη χρήση του ίδιου κλειδιού. Μειώνοντας τον όγκο των δεδομένων που κρυπτογραφούνται με το ίδιο συμμετρικό κλειδί , μειώνεται και ο κίνδυνος εύρεσης του κλειδιού αλλά και των αρχικών δεδομένων. Εδώ τίθενται σημαντικά θέματα για την διαχείριση των συμμετρικών κλειδιών. Κάποιες αρχικές θεωρήσεις σχετικά με την διαχείριση κλειδιών περιλαμβάνουν την παραγωγή κλειδιού, τον διαμοιρασμό κλειδιού και την ευελιξία των κλειδιών δηλαδή να μπορούν να αντικατασταθούν γρήγορα όταν πρέπει να κρυπτογραφηθούν διαφορετικά δεδομένα.

Η προστασία των συμμετρικών κλειδιών είναι πολύ σημαντική σε αυτού του είδους τα συστήματα και είναι και η μεγαλύτερη πρόκληση στα συστήματα διαχείρισης συμμετρικού κλειδιού. Η παραγωγή του συμμετρικού κλειδιού μπορεί να γίνει με δύο τρόπους, είτε τοπικά στη συσκευή , είτε απομακρυσμένα. Στην πρώτη περίπτωση ο αλγόριθμος Diffie Hellman είναι μια επιλογή για την παραγωγή κλειδιών. Σε αυτή την περίπτωση δεν συμμετέχουν εξωτερικοί παράγοντες στην παραγωγή κλειδιών αλλά μόνο πληροφορία που ξέρουν τα δύο μέρη που θέλουν να επικοινωνήσουν. Ωστόσο η τοπική παραγωγή κλειδιού δεν είναι πάντα εφικτή λόγω τεχνικών περιορισμών των συσκευών.

Στην περίπτωση της απομακρυσμένης έκδοσης συμμετρικού κλειδιού, το κλειδί παράγεται σε κάποια συσκευή και μεταφέρεται σε μια ή περισσότερες άλλες οντότητες. Η τοποθέτηση του συμμετρικού κλειδιού στις συσκευές που θα το χρησιμοποιήσουν μπορεί να γίνει με διάφορους τρόπους όπως η προ - αποθήκευση των κλειδιών ή ο ηλεκτρονικός διαμοιρασμός κλειδιών. Στην προ - αποθήκευση τα συμμετρικά κλειδιά τοποθετούνται χειροκίνητα στη συσκευή πριν από την χρήση του

κλειδιού. Αυτό μπορεί να γίνει είτε στην κατασκευή είτε στην εγκατάσταση της συσκευής. Τα κλειδιά που μοιράζονται ηλεκτρονικά πρέπει να προστατεύονται στην διακίνηση τους μέσα στο δίκτυο. Αυτό μπορεί να γίνει κρυπτογραφώντας το συμμετρικό κλειδί κατά την αποστολή του έτσι ώστε μόνο η συσκευή που θα το λάβει να μπορεί να το αποκρυπτογραφήσει.

Η λύση της απομακρυσμένης παραγωγής κλειδιών έχει μεγαλύτερη πολυπλοκότητα λόγω των κινδύνων που υπάρχουν στον διαμοιρασμό του κλειδιού. Στην απομακρυσμένη παραγωγή και διαμοιρασμό κλειδιού η ιδέα του Perfect Forward Secrecy (PFS) μπορεί να υιοθετηθεί για την πλειοψηφία των συσκευών.Η PFS βασίζεται στη χρήση ενός κλειδιού που δεν έχει προηγουμένως ξαναχρησιμοποιηθεί. Στην απομακρυσμένη έκδοση κλειδιών η PFS μπορεί να επιτευχθεί λόγω του ότι η συσκευή που παράγει τα κλειδιά μπορεί να τηρεί ιστορικότητα όλων των προηγούμενων χρησιμοποιημένων κλειδιών.

Η προετοιμασία των συμμετρικών κλειδιών που θα χρησιμοποιηθούν πρέπει να λάβει υπόψη και τον οργανισμό του οποίου οι συσκευές λαμβάνουν το συμμετρικό κλειδί και το σύνολο των κλειδιών για τις συσκευές που πρέπει να παρέχουν ευελιξία κλειδιού. Επομένως η διαχείριση των συμμετρικών κλειδιών από τον οργανισμό είναι πολύ σημαντική για την διατήρηση του ελέγχου των κλειδιών όταν διαμοιράζονται.

Ένα άλλο θέμα σχετικό με τον φυσικό διαμοιρασμό των κλειδιών, είναι η μέθοδος για την εγκαθίδρυση σχέσης εμπιστοσύνης μεταξύ της συσκευής που θα λάβει το κλειδί και της συσκευής key loader, μια συσκευή που χρησιμοποιείται για την μεταφορά του κλειδιού απευθείας στην συσκευή. Είναι απαραίτητο οι διαχειριστές του συστήματος να ορίζουν το πώς επιτυγχάνεται αυτή η σχέση εμπιστοσύνης.

Στην περίπτωση του ηλεκτρονικού διαμοιρασμού των συμμετρικών κλειδιών, όπου τα κλειδιά παράγονται από έναν εξωτερικό εξυπηρετητή κλειδιών, το θέμα της εμπιστοσύνης και της προστασίας του κλειδιού κατά την μεταφορά, είναι πολύ σημαντικά για την επιτυχή εφαρμογή αυτής της μεθόδου. Για να περιοριστεί ο κίνδυνος του να διαρρεύσει το κλειδί, η μεταφορά του μπορεί να γίνει κρυπτογραφώντας το κείμενο του κλειδιού με ένα κλειδί κρυπτογράφησης κλειδιών (KEK Key Encryption Key). Ένα κλειδί KEK μπορεί να δημιουργηθεί χρησιμοποιώντας το δημόσιο κλειδί που κατέχει η συσκευή για την οποία προορίζεται το συμμετρικό κλειδί. Έτσι μόνο αυτή η συσκευή μπορεί να αποκρυπτογραφήσει το

κρυπτογραφημένο συμμετρικό κλειδί, με την χρήση του αντίστοιχου ιδιωτικού κλειδιού.

Στα συστήματα που ακολουθούν κρυπτογράφηση συμμετρικού κλειδιού με ηλεκτρονικό διαμοιρασμό κλειδιών, πρέπει να υπάρχει συνεργασία μεταξύ του παραγωγού κλειδιού και του καταναλωτή κλειδιού. Αυτό συνεπάγεται διαχειριστικό κόστος για τον παραγωγό του κλειδιού. Κάποιοι από τα θέματα που αφορούν τους παραγωγούς κλειδιών, είναι το να γνωρίζουν ακριβώς ποιές ομάδες συσκευών λαμβάνουν το ίδιο συμμετρικό κλειδί, οι κίνδυνοι που υπάρχουν στο κανάλι μετάδοσης του κλειδιού, ο προγραμματισμός της αποστολής κλειδιού έτσι ώστε ο καταναλωτής του κλειδιού να έχει το σωστό κλειδί στον σωστό χρόνο και το πώς αντιδρά σε περιπτώσεις διακινδύνευσης ή διαρροής του κλειδιού. Υπάρχουν και πλεονεκτήματα στην απομακρυσμένη παραγωγή κλειδιού, καθότι πολλές από τις συσκευές των Έξυπνων Δικτύων δεν διαθέτουν τους κατάλληλους πόρους για την διαδικασία παραγωγής κλειδιού τοπικά.

Η ευελιξία του συμμετρικού κλειδιού είναι σημαντική όταν το κλειδί τίθεται σε κίνδυνο και έχει άμεση σχέση με την προετοιμασία του κλειδιού. Στην περίπτωση που το κλειδί κινδυνεύει ,η ευελιξία του κλειδιού επιτρέπει στην συσκευή που το χρησιμοποιεί να το αλλάξει χωρίς να διακοπεί η επικοινωνία της συσκευής με το άλλο μέρος. Όμως η ευελιξία του κλειδιού πρέπει να είναι παράγοντας της συνολικής διαχείρισης κλειδιών και να προδιαγράφεται από τις διαδικασίες σχεδιασμού και διαμοιρασμού των κλειδιών. Το πακέτο διαμοιρασμού κλειδιών πρέπει να περιλαμβάνει αρκετό υλικό που θα παρέχει λειτουργικά κλειδιά αλλά και ανάκαμψη σε περιπτώσεις κινδύνου.

Η λήψη τελικών αποφάσεων για την διαχείριση των συμμετρικών κλειδιών, πρέπει να βασίζεται σε αποτίμηση των κινδύνων και να λαμβάνει υπόψη παράγοντες όπως η συχνότητα κατανάλωσης κλειδιών, ο όγκος των δεδομένων που κρυπτογραφούνται από το κλειδί, η ασφάλεια και η ισχύς του καναλιού διαμοιρασμού, ο αριθμός των κλειδιών που απαιτούνται και ο τρόπος που θα επιλεχθεί για τον διαμοιρασμό των κλειδιών.

ΚΕΦΑΛΑΙΟ ΕΚΤΟ

6. Πιστοποιητικά ασφάλειας για Έξυπνα Δίκτυα στην ΕΕ

Η λειτουργία των Έξυπνων Δικτύων απαιτεί αυτοματισμό και συνεργασία διαφόρων οντοτήτων και περιβαλλόντων. Τα διάφορα μέρη χρειάζεται να ανταλλάσουν πληροφορίες για να βεβαιώσουν ότι έχουν ληφθεί οι σωστές αποφάσεις σχετικά με την διανομή ενέργειας. Παρότι ο εξοπλισμός στα Έξυπνα Δίκτυα υπάρχει για να διευκολύνει την ανταλλαγή δεδομένων με έξυπνες αυτόματες και απομακρυσμένου ελέγχου συσκευές, οι πρακτικές παραγωγής και συντήρησης των συσκευών είναι οι ίδιες με αυτές των κοινών δικτύων. Έτσι προκύπτει ένα κενό καθώς τα επίπεδα της ασφάλειας δεν ακολουθούν την αυξανόμενη αυτοματοποίηση και τις πολλαπλές διασυνδέσεις των Έξυπνων Δικτύων.

Γι' αυτό τον λόγο τα πιστοποιητικά κυβερνοασφάλειας των Έξυπνων Δικτύων έχουν γίνει δημοφιλή ως μέσο αναβάθμισης της ασφάλειας που προσφέρουν αυτά τα πολύπλοκα συστήματα στους χρήστες. Τα πιστοποιητικά ασφάλειας στα Έξυπνα Δίκτυα παρέχουν μεγάλο πλεονέκτημα τόσο στους προμηθευτές όσο και στους παρόχους υπηρεσιών.

Η στρατηγική κυβερνοασφάλειας της Ευρωπαϊκής Ένωσης3 αναγνωρίζει ότι είναι κοινή ευθύνη όλων των ενδιαφερόμενων μερών να προστατεύονται στα πλαίσια της αυξανόμενης εξάρτησης από τις τεχνολογίες πληροφορικής και επικοινωνιών.

Στην Ευρωπαϊκή Ένωση υπάρχει ανάγκη για περισσότερο οργανωμένο και εναρμονισμένο πλαίσιο για πρακτικές πιστοποιητικών Έξυπνων Δικτύων για να υποστηριχθεί η δημιουργία αλυσίδας εμπιστοσύνης στη διανομή ενέργειας μέσω των δικτύων.

6.1 Υφιστάμενη κατάσταση

Κόστος: οι ανομοιόμορφες διεθνείς πολιτικές, η έλλειψη πόρων και ο μεγάλος αριθμός εμπλεκόμενων μερών είναι κάποιοι από τους λόγους που καθιστούν τα υπάρχοντα σχήματα πιστοποιητικών αρκετά ακριβά.

Έλλειψη ενιαίας προσέγγισης: οι ενδιαφερόμενοι αντιμετωπίζουν μια κατακερματισμένη κατάσταση στην οποία υπάρχουν πολλές διαφορετικές προσεγγίσεις για την κυβερνοασφάλεια στα Έξυπνα Δίκτυα.

Κύκλος ζωής: η διαδικασία πιστοποίησης κάποιες φορές διαρκεί περισσότερο από όσο διάστημα χρειάζεται μια νέα ευπάθεια να εμφανιστεί στον κυβερνοχώρο.

Νομικό πλαίσιο: υπάρχουν λίγες νομικές διατυπώσεις που αφορούν στην ασφάλεια στα έξυπνα δίκτυα και αφήνοντας έτσι πολλά περιθώρια για παρερμηνείες

Κοινά κριτήρια:

- Είναι το επικρατέστερο σχήμα πιστοποιητικών στην αγορά.
- Θα ήταν μη ρεαλιστικό να υπάρχουν κοινά κριτήρια πιστοποιητικών σε όλη την εφοδιαστική αλυσίδα των Έξυπνων Δικτύων.
- Για να εφαρμοστεί σε περιβάλλον Έξυπνου Δικτύου θα πρέπει να επεκταθεί και να περιλαμβάνει ειδικά προφίλ προστασίας για Έξυπνα Δίκτυα παρόμοια με αυτά που χρησιμοποιεί η βιομηχανία Έξυπνων Καρτών.

Περιβάλλον πιστοποιητικών: η πιστοποίηση των προϊόντων γίνεται στα εργαστήρια και όχι σε συνθήκες λειτουργικού περιβάλλοντος. Ένα προϊόν μπορεί να πιστοποιηθεί αλλά αυτό δεν σημαίνει απαραίτητα ότι όταν βγει στην παραγωγή έχει παραμετροποιηθεί σωστά, ότι δουλεύει σωστά και ότι δεν θα επηρεάσει την λειτουργία ολόκληρου του δικτύου.

Εκπαίδευση: δεν υπάρχει ούτε σε διεθνές ούτε σε Ευρωπαϊκό επίπεδο δραστηριοποίηση για κατάρτιση ειδικών σε θέματα πιστοποίησης ασφάλειας σε Έξυπνα Δίκτυα.

6.2 Οι ανάγκες των ενδιαφερόμενων μερών σχετικά με την πιστοποίηση στα Έξυπνα Δίκτυα

Επίλυση ζητημάτων εμπιστοσύνης μεταξύ των εμπλεκόμενων μερών στην ΕΕ αναφορικά με τα Έξυπνα Δίκτυα

Αυτό σχετίζεται με τα διαφορετικά εθνικά κανονιστικά πλαίσια και την ποικιλομορφία της φύσης των Έξυπνων Δικτύων που δημιουργούν ασάφεια σχετικά με την ευθύνη και την λογοδοσία. Επιπλέον οι εφοδιαστικές αλυσίδες των χρησιμοποιούμενων μερών και συστημάτων είναι πολύ, μεγάλες αδιαφανείς και πολύπλοκες. Αυτό θέτει ζητήματα εμπιστοσύνης μεταξύ των ενδιαφερόμενων στη ΕΕ γιατί δεν μπορούν να προβλεφθούν όλοι οι σχετικοί κίνδυνοι.

Δημιουργία κοινού μοντέλου αναφοράς για ασφάλεια Έξυπνων Δικτύων στην ΕΕ

Τα μέλη της ΕΕ τείνουν να καθορίζουν τις δικές τους απαιτήσεις ασφάλειας και να δημιουργούν τα δικά τους μοντέλα για να πιστοποιήσουν τα προϊόντα τους. Αυτό δημιουργεί κατακερματισμό στην αγορά αν δεν υπάρχει πλαίσιο συνεργασίας. Η δημιουργία τέτοιων μοντέλων βασικά γίνεται από αρχές πιστοποίησης. Πάραυτα ακόμα δεν υπάρχει ούτε ενιαία προστασία ούτε ενιαίο μοντέλο πιστοποίησης για Έξυπνα Δίκτυα στην ΕΕ[30].

Καθιέρωση κοινής βάσης για το ελάχιστο σύνολο ελεγχόμενων μέτρων για Έξυπνα Δίκτυα στην ΕΕ.

Υπάρχει ανάγκη για Ευρωπαϊκό σύνολο απαιτήσεων που να μπορούν να χρησιμοποιηθούν για ενίσχυση της κυβερνοασφάλειας στα Έξυπνα Δίκτυα. Είναι σημαντικό να υπάρχει ένα κοινό επίπεδο ασφάλειας με κοινή βάση σε όλη την ΕΕ καθώς διευκολύνει την διαμόρφωση κοινής διεπαφής για την συνεργασία των μελών της.

Καθορισμός αποδεκτής μεθόδου για τα επίπεδα ασφάλειας για διαφορετικές κρίσιμες εκδοχές του δικτύου.

Η πιστοποίηση όλων των μερών ενός έξυπνου δικτύου πιθανόν να είναι ανέφικτη και δεν αποτελεί ένδειξη για την ασφάλεια ολόκληρου του δικτύου. Χρειάζεται να καθοριστεί η κρισιμότητα του κάθε μέρους του δικτύου και να εφαρμοστούν τεχνικές ασφάλειας που να βασίζονται σε αυτή. Για παράδειγμα ένα μέρος του δικτύου που είναι εκτεθειμένο σε ανοικτό περιβάλλον έχει μεγάλη επίδραση στην ασφάλεια του δικτύου. Είναι λοιπόν σκόπιμο να επενδυθεί περισσότερος χρόνος και χρήμα για την ασφάλεια και πιστοποίηση των κρίσιμων μερών του δικτύου.

Πιθανόν οι κρίσιμες υποδομές να μην μπορούν να πιστοποιηθούν με κοινές μεθόδους των παραδοσιακών πληροφοριακών συστημάτων. Επιπλέον ένα πιστοποιημένο προϊόν δεν συνεπάγεται και ένα ασφαλές προϊόν καθότι δεν μπορούν να ληφθούν υπόψη όλοι οι πιθανοί κίνδυνοι. Η πρόκληση στα έξυπνα δίκτυα είναι η αντιμετώπιση των ευπαθειών και των απειλών που αυξάνονται με ολοένα και μεγαλύτερο ρυθμό εξαιτίας της πολυπλοκότητας των συστημάτων και της μεγάλης αλληλεξάρτησης μεταξύ των μερών τους. Με την πιστοποίηση μπορούν να περιοριστούν οι πιθανότητες κίνδυνων σε περιβάλλοντα Έξυπνων Δικτύων. Χρειάζεται προσοχή σε μια τέτοια προσέγγιση πιστοποίησης όπου διατηρείται η ευελιξία και υπάρχει ένα ελάχιστο αποδεκτό επίπεδο κινδύνου ανάλογα με την κρισιμότητα του αντικειμένου, καθότι αυτή η κρισιμότητα μπορεί να διαφοροποιείται για κάθε ενδιαφερόμενο ή για κάθε μέλος της ΕΕ.

Καθιέρωση εναρμονισμένης προσέγγισης στην ΕΕ για τα μέρη, τα συστήματα και την λειτουργική ασφάλεια των Έξυπνων Δικτύων , για να αυξηθεί η εμπιστοσύνη.

Αυξάνοντας το επίπεδο της ασφάλειας και περιορίζοντας τους κινδύνους τα πρότυπα πιστοποίησης θα αυξήσουν την εμπιστοσύνη των τελικών χρηστών για τα έξυπνα δίκτυα και συσκευές και θα βοηθήσουν στην αποδοχή τους από το κοινό.

Έκδοση Ευρωπαϊκής οδηγίας για εναρμονισμένη προσέγγιση που να διευκολύνει τη νομοθεσία σε εθνικό επίπεδο

Υπάρχει ανάγκη για μια εναρμονισμένη προσέγγιση που θα λαμβάνει υπόψη τα διαφορετικά επίπεδα οικονομικής ανάπτυξης και είδη αγορών και να διευκολύνει την νομοθεσία.

Προώθηση δημόσιας και ιδιωτικής αλληλεπίδρασης στην ΕΕ σχετικά με την ασφάλεια στα Έξυπνα Δίκτυα.

Είναι σημαντικό να διασφαλίζεται ότι κάθε αποδεκτό μοντέλο επιφέρει την αλληλεπίδραση μεταξύ δημόσιων και ιδιωτικών μελών στην ΕΕ, για να εξασφαλιστεί η ευρύτερη αποδοχή του[31].

Καθιέρωση κοινής ευθύνης στον περιορισμό των κινδύνων μεταξύ των ενδιαφερόμενων μερών στην ΕΕ.

Η Στρατηγική Κυβερνοασφάλειας της ΕΕ δίνει προτεραιότητα στην ανάγκη δημιουργίας βιομηχανικών και τεχνικών πόρων για κυβερνοασφάλεια.

Μείωση του κόστους πιστοποίησης Έξυπνων Δικτύων στην ΕΕ.

Η προσπάθεια που χρειάζεται να καταβληθεί για να διασφαλιστεί ότι η ασφάλεια διατηρείται σε όλα τα μέλη της ΕΕ, είναι μεγάλη λόγω ων διαφορετικών ειδών Έξυπνων Δικτύων στα κράτη μέλη της ΕΕ. Με διαφορετικές προσεγγίσεις για τα πιστοποιητικά και τις απαιτήσεις ασφάλειας ανά κράτος, αυξάνεται το κόστος συμμόρφωσης με τα Ευρωπαϊκά πρότυπα.

6.3 Τα χαρακτηριστικά του «ιδανικού» μοντέλου πιστοποίησης ασφάλειας για έξυπνα δίκτυα.

1. Παρέχει μια ολιστική προσέγγιση για να διασφαλίσει την εμπιστοσύνη στην εφοδιαστική αλυσίδα του Έξυπνου Δικτύου. Έτσι θα υπάρχει σαφήνεια στο μέρος της ευθύνης που αναλογεί σε κάθε αντικείμενο του δικτύου.
2. Χρησιμοποιεί ένα κοινό Ευρωπαϊκό μοντέλο αναφοράς για ασφάλεια SG όπως το SG-AM που είναι ευρέως αποδεκτό από τους Ευρωπαϊκούς Οργανισμούς Προτυποποίησης και τις Αρχές Πιστοποίησης. Υπάρχει η πεποίθηση ότι η M/490 τυποποίηση είναι μια πολλά υποσχόμενη πρωτοβουλία για την εναρμόνιση και διαλειτουργικότητας της αγοράς.
3. Έχει κοινό σύνολο απαιτήσεων που περιγράφονται στα προφίλ που αναγνωρίζουν τα εμπλεκόμενα μέρη έτσι ώστε η αποδοχή σε ένα κράτος μέλος να είναι έγκυρη και στα άλλα μέλη.
4. Χρησιμοποιεί διεθνώς ισοδύναμα επίπεδα ασφάλειας και κινδύνων που συνάδουν με τα επίπεδα που καθορίζονται από αποδεκτές στην ΕΕ προσεγγίσεις.
5. Περιλαμβάνει υποστήριξη για τα αντικείμενα τα συστήματα και τις λειτουργίες των SG , έτσι ώστε να υπάρχει ένα πλαίσιο που περιγράφει την ασφάλεια σε ένα ολοκληρωμένο Έξυπνο Δίκτυο.
6. Περιλαμβάνει ελέγχους συμμόρφωσης, λειτουργικότητας και διαλειτουργικότητας.

7. Διευκολύνει την δημόσια και ιδιωτική αλληλεπίδραση και προβλέπει την ύπαρξη συντονιστικού πλαισίου σαν διεπαφή μεταξύ ιδιωτικών και δημόσιων φορέων.
8. Δεν αποτελεί εντολή της ΕΕ αλλά ένα πλαίσιο λειτουργίας που αποτελεί οδηγό εφαρμογής και υποστηρίζει την νομοθεσία σε εθνικό επίπεδο.
9. Βελτιώνει την ωριμότητα σχετικά με την ασφάλεια στα SG στην ΕΕ, με πρωτοβουλίες που αποτελούν οδηγό για τη λήψη κατάλληλων μέτρων ασφάλειας.

6.4 Κυριότερα ζητήματα στην υφιστάμενη κατάσταση στην ΕΕ

Στην Ευρώπη μόνο κάποια κράτη μέλη έχουν αναπτύξει εξειδικευμένες απαιτήσεις ασφάλειας για Έξυπνα Δίκτυα για να εξυπηρετήσουν τα εξειδικευμένες τοπικές ανάγκες των SG και των νομικών απαιτήσεων που σχετίζονται με την ενέργεια.

Η έλλειψη απαιτήσεων ασφάλειας και πρωτοβουλιών οφείλεται στο γεγονός ότι δεν υπάρχει ξεκάθαρη εικόνα του πλήθους των δημοσίως γνωστών περιστατικών ασφάλειας στον χώρο. Συνεπώς δεν υπάρχει αναγνώριση της αναγκαιότητας για βελτίωση της κυβερνοασφάλειας με ένα κοινό πλαίσιο συνεργασίας. Στην πραγματικότητα οι ιδιωτικές επιχειρήσεις δεν αποκαλύπτουν τα περιστατικά ασφάλειας που τους προκύπτουν για προστασία της φήμης τους. Τα συγκεκριμένα περιστατικά δεν είναι εύκολο να ανιχνευθούν μετά την πραγματοποίηση τους οπότε δεν είναι εφικτή η διεξαγωγή έρευνας.

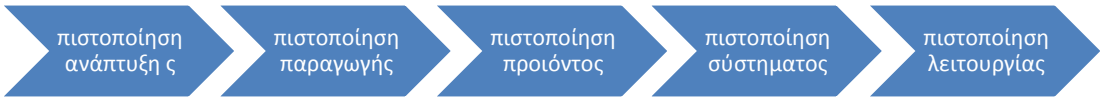
Παρότι υπάρχουν οργανισμοί που υποστηρίζουν την πιστοποίηση σε Ευρωπαϊκό επίπεδο όπως EA και SOG-IS, δεν υπάρχει νομοθεσία που να επιβάλει την ύπαρξη Ευρωπαϊκού μοντέλου πιστοποίησης για Έξυπνα Δίκτυα. Τα κοινά κριτήρια υιοθετήθηκαν από σχεδόν όλες τις χώρες παρότι σε πολλές περιπτώσεις αντικαταστάθηκαν με προσεγγίσεις που κάλυπταν τις τοπικές ανάγκες. Αυτό αποδεικνύει και την διαφορετικότητα στα χαρακτηριστικά της κάθε χώρας.

6.5 Η εφοδιαστική αλυσίδα ενός Έξυπνου Δικτύου

Για να μπορεί να χτιστεί εμπιστοσύνη σχετικά με την ασφάλεια των SG πρέπει οι εμπλεκόμενοι να είναι έμπιστοι. Η πιστοποίηση είναι ένα τυπικό μέσο για να χτιστεί αυτή η εμπιστοσύνη. Παρακάτω φαίνεται μια τυπική εφοδιαστική αλυσίδα Έξυπνου Δικτύου.

Σχήμα 6.1: Εφοδιαστική αλυσίδα SG

Είναι σημαντικό να σημειώσουμε ότι ένα μοναδικό πιστοποιητικό που θα καλύπτει όλες τις φάσεις της αλυσίδας θα ήταν ιδιαίτερα πολύπλοκο και απαιτεί συνεργασία πολλών παραγόντων. Για να είναι έμπιστη η αλυσίδα αυτή θα πρέπει κάθε φάση να ακολουθεί συγκεκριμένους κανόνες ασφάλειας δημιουργώντας έτσι ένα ασφαλές περιβάλλον όπου μπορεί να θεωρηθεί ότι ένα σύστημα μπορεί να λειτουργεί με ασφαλή τρόπο. Ωστόσο αν κάποια φάση της αλυσίδας τεθεί σε κίνδυνο τότε όλη η αλυσίδα μπορεί να επηρεαστεί.



Σχήμα 6.2: Πιστοποίηση εφοδιαστικής αλυσίδας SG

Η αλυσίδα μπορεί να είναι έμπιστη μόνο αν το μοντέλο πιστοποίησης είναι αποδεκτό και θεωρείται έμπιστο από τους ενδιαφερόμενους. Σε εθνικό επίπεδο τα έμπιστα μοντέλα συνήθως βασίζονται σε οδηγίες όπως ISO/IEC 17067, που χρησιμοποιούνται για μοντέλα πιστοποίησης προϊόντων. Αυτό επιτρέπει στο αντικείμενο που εφαρμόζει

το μοντέλο να λαβαίνει επίσημη αναγνώριση από τον αρμόδιο εθνικό οργανισμό. Αυτός ο οργανισμός με τη σειρά του αναγνωρίζεται από κάποιον διεθνή οργανισμό αναγνώρισης εμπιστοσύνης και έτσι δημιουργείται μια αλυσίδα εμπιστοσύνης.

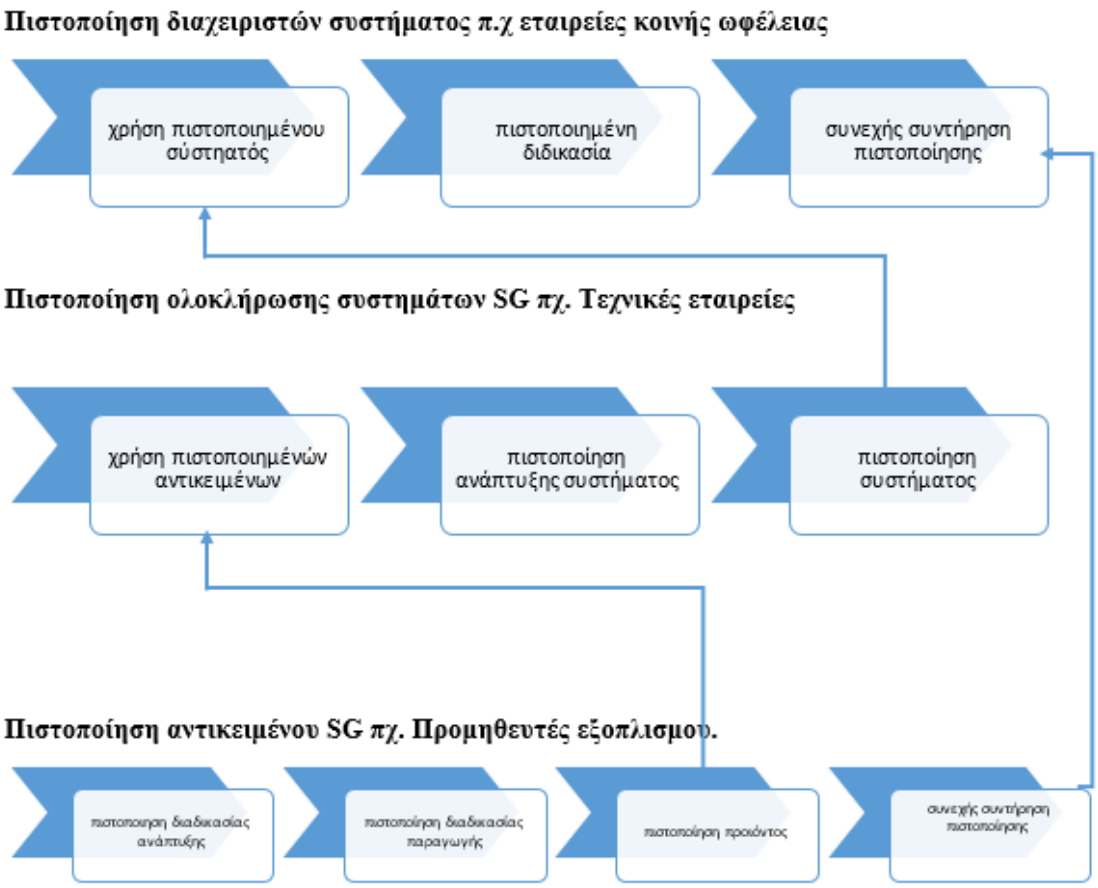
6.5.1 Ανάλυση εφοδιαστικής αλυσίδας ενός Έξυπνου Δικτύου

Στο παρακάτω σχήμα (6.3) απεικονίζεται μια πλήρης εφοδιαστική αλυσίδα ενός συστήματος σε περιβάλλον Έξυπνου Δικτύου που βασίζεται στην ανάλυση των εμπλεκόμενων στην ανάπτυξη, παραγωγή, ολοκλήρωση και λειτουργία και το μοντέλο που περιγράφεται από το πρότυπο IEC 62443.

Σύμφωνα με αυτό το μοντέλο η πιστοποίηση γίνεται σε τρία επίπεδα:

- Πιστοποίηση λειτουργίας του SG.
- Πιστοποίηση ολοκλήρωσης SG.
- Πιστοποίηση μερών του SG.

Ένα SG μπορεί να έχει μεγάλη σχεδιαστική πολυπλοκότητα δυσκολεύοντας την πιστοποίηση των ICT αντικειμένων. Ένα Έξυπνο Δίκτυο απλώνεται σε μια μεγάλη γεωγραφική περιοχή και υπάρχουν πολλαπλές διασυνδέσεις σε διαφορετικά μέρη του συστήματος. Ένα Έξυπνο Δίκτυο μπορεί να επικοινωνεί με ένα οικιακό δίκτυο αυτοματισμού (HAN) , αποκεντρωμένες πηγές ενέργειας (DER), η εμπορικό σύστημα ενέργειας. Αυτές οι διασυνδέσεις μπορούν να συμβούν σε διάφορα μέρη του συστήματος και να ανταλλάσουν χαμηλού ή υψηλού επιπέδου δεδομένα με μέρη που έχουν διαφορετικά επίπεδα εμπιστοσύνης. Αυτές οι αλληλεπιδράσεις δεν θα πρέπει να επηρεάζουν την αλυσίδα εμπιστοσύνης και είναι θεωρητικά εφικτό καθώς υπάρχουν οδηγίες και βέλτιστες πρακτικές για διασυνδέσεις με τρίτα μέρη που εφαρμόζονται αντίστοιχα με τα NIST IR7628 και ISO27002 πρότυπα.



Σχήμα 6.3: **Αλυσίδα εμπιστοσύνης Έξυπνου Δικτύου**

Οι απειλές συνεχώς εξελίσσονται και οι ευπάθειες στον εξοπλισμό και στο λογισμικό είναι καθημερινά ζητήματα. Έτσι προκύπτει ανάγκη για συνεχόμενη συντήρηση και αναβάθμιση των πιστοποιήσεων. Αυτή η ανάγκη αναγνωρίζεται από τους ενδιαφερόμενους και ο κύκλος ζωής των πιστοποιητικών πρέπει να το λαβαίνει υπόψη.

6.5.2 Υιοθέτηση SG – AM για μοντέλο αλυσίδας εμπιστοσύνης.

Το SG-AM πλαίσιο στοχεύει στην υποστήριξη του σχεδιασμού των περιπτώσεων χρήσης για έξυπνα δίκτυα. Η υποστήριξη επιτυγχάνεται ακολουθώντας μια αρχιτεκτονική προσέγγιση που επιτρέπει την αναπαράσταση των σημείων αλληλεπίδρασης τόσο για τα υφιστάμενα έξυπνα δίκτυα όσο και για αυτά του εγγύς μέλλοντος.

Το SG- AM μοντέλο μπορεί να εφαρμοστεί για μεμονωμένα και αλληλεπιδρώντα μέρη της περιοχής του δικτύου και παρέχει γνώση του πώς μια σειρά από επίπεδα ασφάλειας μπορούν να παρέχουν μια διαβαθμισμένη προσέγγιση για την ασφάλεια στα Έξυπνα Δίκτυα. Επίσης αποτυπώνει το πώς πρότυπα ασφάλειας πιθανόν αλληλεπικαλύπτουν ή συμπληρώνουν το ένα το άλλο.

Το SG-AM αναγνωρίζει την ανάγκη για διαφορετικά πρότυπα πιστοποίησης για SG. Στο σχήμα 6 απεικονίζεται το SG-AM μοντέλο σε συνδυασμό με την αλυσίδα εμπιστοσύνης του σχήματος 5 που μπορεί να χρησιμοποιηθεί για αντιστοίχηση διαφορετικών μοντέλων κατάλληλα για πιστοποίηση ασφάλειας στα Έξυπνα Δίκτυα.

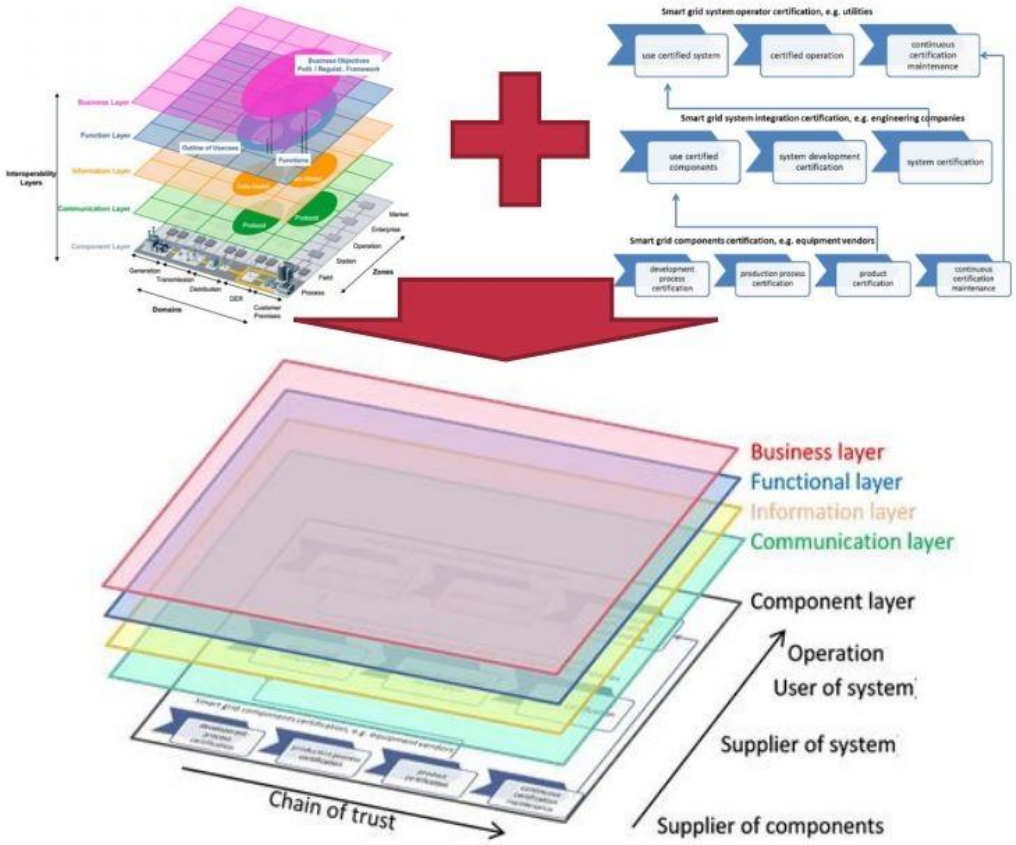
Το επίπεδο ασφάλειας που καλύπτεται από τα μεμονωμένα πιστοποιητικά μπορεί να σχετιστεί με τη θέση του πιστοποιητικού στην αλυσίδα και στο SG-AM μοντέλο, και το ρόλο που κατέχει στην αλυσίδα του SG. Έτσι το μοντέλο μπορεί να χρησιμοποιηθεί για να αναδείξει τις εξαρτήσεις, το πώς τα πιστοποιητικά σχετίζονται μεταξύ τους στο SG και παρέχει ένα τρόπο να εκτιμηθεί η επίδραση του επιπέδου ασφάλειας που χρησιμοποιείται σε ένα αντικείμενο του δικτύου.

Το σχήμα 6.4 παρακάτω είναι μια γραφική αναπαράσταση του πώς η αλυσίδα εμπιστοσύνης που περιγράφηκε μπορεί να εφαρμοστεί σε SG-AM περιπτώσεις χρήσης. Στο σχήμα φαίνεται ότι η πλήρης αλυσίδα θα πρέπει να εφαρμόζεται σε κάθε επίπεδο για ένα πλήρως πιστοποιημένο Έξυπνο Δίκτυο. Το SM-AM δεν περιγράφει ένα πλήρες πρότυπο Έξυπνου Δικτύου, αλλά παρέχει μια μέθοδο για τη δημιουργία κοινού μοντέλου αναφοράς για περιπτώσεις χρήσης Έξυπνων Δικτύων.

6.5.3 Ορισμός των επιπέδων κινδύνων που ευθυγραμμίζονται με την SG-AM μεθοδολογία.

Προκειμένου να ελαχιστοποιηθεί το κόστος των πιστοποιητικών, πρέπει να ληφθεί υπόψη η κρισιμότητα του αντικειμένου προς πιστοποίηση. Μία προσέγγιση που βασίζεται στους κινδύνους μπορεί να βοηθήσει σε στοχευμένες προσπάθειες πιστοποιητικών σε περιπτώσεις χρήσεις Έξυπνων Δικτύων και επομένως αναδεικνύει το κατάλληλο επίπεδο ασφάλειας. Επιπλέον μια Ευρωπαϊκή προσέγγιση για τα

επίπεδα ασφάλειας θα βοηθήσει για ένα κοινό μοντέλο αναφοράς για όλα τα κράτη μέλη. Παρακάτω περιγράφεται το πώς το M/490 SG-IS πλαίσιο απαντά στο «τί θα πιστοποιηθεί;».

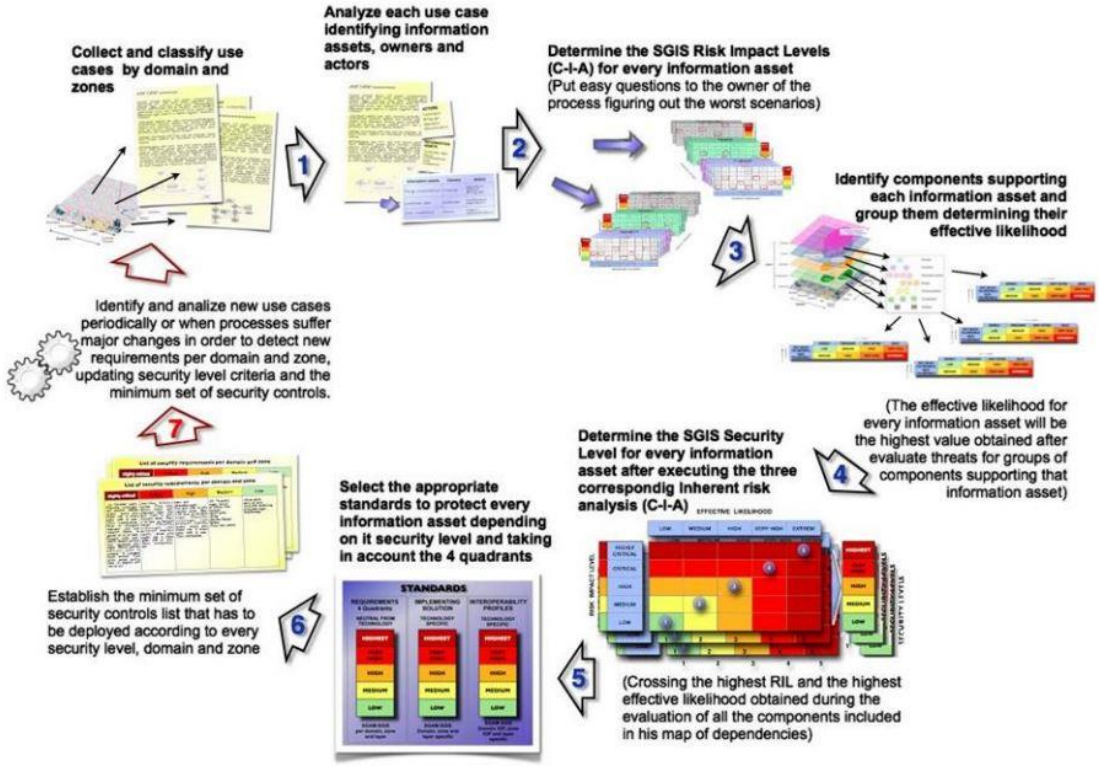


Σχήμα 6.4 [29] : Μοντέλο αλυσίδας εμπιστοσύνης

Το 2012 η ομάδα εργασίας Smart Grid Information Security (SG-IS) του Smart Grid Coordination Group (SG-CG) ανέπτυξε μια μεθοδολογία που βοηθά στον καθορισμό των απαιτήσεων ασφάλειας μέσω μιας προσέγγισης που βασίζεται στις περιπτώσεις χρήσης. Το SG-IS εργαλείο παρέχει τα ενδιαφερόμενα μέρη των περιπτώσεων χρήσης των SG , έναν εύκολο και πραγματικό τρόπο για αναγνώριση των αναγκών ασφάλειας και εντοπίζει κενά στα προτεινόμενα πρότυπα των περιπτώσεων χρήσης προκειμένου να τεθούν οι απαιτήσεις ασφάλειας όπως χρειάζεται. Το 2014 μετονομάστηκε σε SG-

IS πλαίσιο λειτουργίας. Το μοντέλο που χρησιμοποιείται από το SG-IS βασίζεται στο πλαίσιο SG-AM και επομένων είναι εύχρηστο για παρουσίαση αποτίμησης κινδύνων σε SG-AM περιπτώσεις χρήσης. Αποτελεί μια χρήσιμη μεθοδολογία για καθορισμό των επιπέδων κινδύνου σε μια αλυσίδα εμπιστοσύνης.

Το SG-IS πλαίσιο περιγράφει λεπτομερώς πώς να εκτιμηθεί η αξία των περιπτώσεων χρήσης, παραθέτει τις σχετικές κατηγορίες αγαθών και αναγνωρίζει ένα μοντέλο για καθορισμό του Risk Impact Level (PIL) για συγκεκριμένο αγαθό σε μια περίπτωση χρήσης. Το ακόλουθο σχήμα 6.5 περιγράφει συνοπτικά πώς η μεθοδολογία εφαρμόζεται.



Σχήμα 6.5 [29] : Μεθοδολογία για καθορισμό απαιτήσεων ασφάλειας

6.5.3.1 Επίπεδα αντίκτυπου κινδύνου (Risk Impact Levels)

Ο αντίκτυπος του κινδύνου καθορίζεται αναλύοντας το πώς τα περιστατικά ασφάλειας που σχετίζονται με ένα συγκεκριμένο πληροφοριακό αγαθό, επηρεάζει τις διαδικασίες που αυτό εμπλέκεται. Διαφορετικά περιστατικά παράγουν διαφορετικής εμβέλειας αντίκτυπο και ο μεγαλύτερος αντίκτυπος που αναγνωρίζεται σε όλα τα πιθανά

σενάρια, καθορίζει το RIL του αγαθού που αναλύεται. Τα αποτελέσματα αποτυπώνονται σε μια κλίμακα από το 1 έως το 5 , όπου 1 είναι το χαμηλότερο και 5 το υψηλότερο επίπεδο αντίκτυπου κινδύνου.

6.5.3.2 Κατηγορίες αντίκτυπου κινδύνου (Risk Impact Categories)

Η SG-IS Impact Analysis μεθοδολογία αναγνωρίζει 6 διαφορετικές κατηγορίες οι οποίες αποτιμώνται ανεξάρτητα με τη χρήση της κλίμακας RIL.

Το SG-IS πλαίσιο παρέχει τρόπο να αναγνωρίζονται οι απαιτήσεις ασφάλειας για συγκεκριμένα σενάρια χρήσης και αγαθά των Έξυπνων Δικτύων. Έτσι ο ιδιοκτήτης του αγαθού θα αποφασίσει το επίπεδο ασφάλειας, με βάση τη μεθοδολογία που προτείνεται.

Impact categories/ Impact level	Λειτουργία (Διαθεσιμότητα)				Νομικά θέματα		Άνθρωπος	Φήμη	Οικονομικά
	Παροχή ενέργειας	Ροή ενέργειας	Πληθυσμός	Υποδομές	Προστασία δεδομένων	Άλλοι νομικοί κανονισμοί			
5	Τοπικά δίκτυα από 10GW	από 10GW/h	Από 50% σε 1 χώρα ή 25% σε περισσότερες χώρες	Διεθνείς και κρίσιμες υποδομές	-	Κλείσιμο εταιρείας	Άμεση και έμμεση απώλεια ζωής	Μόνιμη απώλεια εμπιστοσύνης παντού	>50% EBITDA
4	Εθνικά δίκτυα από 1GW μέχρι 10GW	από 1GW/h μέχρι 10GW/h	Από 25% έως 50%	Εθνικές κρίσιμες υποδομές	-	Προσωρινή διακοπή δραστηριότητας	Άμεση απώλεια ζωής	Μόνιμη απώλεια εμπιστοσύνης σε χώρα	<50% EBITDA
3	Αστικά δίκτυα από 100MW μέχρι 1GW	από 100MW/h μέχρι 1GW/h	Από 10% έως 25%	Σημαντικές κρίσιμες υποδομές	Διαρροή ή τροποποίηση ευαίσθητων δεδομένων	Πρόστιμο από το 10% του EBITDA	Έμμεση απώλεια ζωής	Προσωρινή απώλεια εμπιστοσύνης σε χώρα	<33% EBITDA
2	Δίκτυα σε γειτονιά από 1MW μέχρι 100MW	από 1MW/h μέχρι 100MW/h	Από 2% έως 10%	Complimentary υποδομές	Διαρροή ή τροποποίηση προσωπικών δεδομένων	Πρόστιμο μέχρι το 10% του EBITDA	Σοβαρός τραυματισμός ή αναπηρία	Προσωρινή και τοπική απώλεια εμπιστοσύνης	<10% EBITDA
1	Οικιακά δίκτυα κάτω από 1MW	Λιγότερο από 1MW/h	Λιγότερο από 2%	Καμία complimentary υποδομή	Δεν υπάρχουν προσωπικά ή ευαίσθητα δεδομένα	Προειδοποιήσεις	Μικρά περιστατικά	Μικρής διάρκειας και εμβέλειας	<1% EBITDA

Σχήμα 6.6 : Αποτίμηση αντίκτυπου κινδύνου σε SG διαδικασία για κάποιο συγκεκριμένο αγαθό.

Και το SG-AM μοντέλο και το SG-IS πλαίσιο είναι αναγνωρισμένα από τα μέλη της ΕΕ σαν αποδεκτές προσεγγίσεις στην περιγραφή των Έξυπνων Δικτύων και των σχετικών επιπέδων κινδύνων και παρέχουν μια καλή βάση για Ευρωπαϊκό πλαίσιο λειτουργίας που συνεισφέρει στην εναρμόνιση των πρακτικών πιστοποίησης των Έξυπνων Δικτύων στην ΕΕ.

Συνδυάζοντας τα SG-AM και SG-IS, μπορεί να χτιστεί μια αλυσίδα εμπιστοσύνης για μια περίπτωση χρήσης συγκεκριμένη χώρας με το απαιτούμενο επίπεδο ασφάλειας. Με αυτό τον τρόπο η χώρα μέλος μπορεί περιγράψει την δική της περίπτωση χρήσης και την αποτίμηση κινδύνου που βασίζονται σε αποδεκτές από την ΕΕ μεθοδολογίες.

Με αυτό τον τρόπο αντιμετωπίζονται οι παρακάτω ανάγκες:

- Κοινό μοντέλο αναφοράς ασφάλειας για SG στην ΕΕ.
- Κοινά αποδεκτή μέθοδος για τα επίπεδα ασφάλειας για διαφορετικές κρίσιμες πτυχές των Έξυπνων Δικτύων.

6.6 Αποτίμηση συμμόρφωσης και η συσχέτιση με τις δοκιμές

Για να είναι δυνατή η πιστοποίηση ασφάλειας ενός Έξυπνου Δίκτυο , οι ιδιοκτήτες των αγαθών πρέπει να αποδείξουν ότι οι απαιτήσεις ασφάλειας ικανοποιούνται. Αυτή η απόδειξη συνήθως προκύπτει από την αποτίμηση ή δοκιμή της συμμόρφωσης με τις συγκεκριμένες απαιτήσεις.

Την αποτίμηση της συμμόρφωσης μπορεί να αναλάβει ο προμηθευτής του προϊόντος ή της υπηρεσίας, ο αγοραστής ή άλλοι που μπορεί να έχουν συμφέρον όπως για παράδειγμα ασφαλιστικές εταιρείες. Όταν αναφερόμαστε στην αποτίμηση συμμόρφωσης αναφερόμαστε στα εμπλεκόμενα μέρη ως εξής:

- Πρώτο μέρος : αυτός (πρόσωπο ή οργανισμός) που παρέχει το προϊόν.
- Δεύτερο μέρος: αυτός που θα χρησιμοποιήσει το προϊόν.
- Τρίτο μέρος: κάποιος ανεξάρτητος από τα προηγούμενα 2 μέρη που έχει κάποιου είδους ενδιαφέρον για το προϊόν.

Το $1^{ο}$ μέρος θεωρείται το λιγότερο αξιόπιστο για την αποτίμηση συμμόρφωσης. Επομένως ανάλογα με το μέγεθος του κινδύνου της μη – συμμόρφωσης πρέπει να γίνει

η επιλογή το ποιος επιτρέπεται να διενεργήσει την αποτίμηση. Μια προσέγγιση που βασίζεται στο SG-IS πλαίσιο λειτουργίας μπορεί να βοηθήσει στην εκτίμηση του κινδύνου για συγκεκριμένο σενάριο και του σχετικού επιπέδου επιβεβαίωσης.

Παρακάτω παρουσιάζονται οι συνηθέστερες διαδικασίες αποτίμησης συμμόρφωσης.

- **Επιθεώρηση** είναι ο έλεγχος του σχεδιασμού ενός προϊόντος, του προϊόντος, της διαδικασίας ή της εγκατάστασης του και ο καθορισμός της συμμόρφωσης του με συγκεκριμένες απαιτήσεις.
- **Πιστοποίηση** από κάποιον οργανισμό πιστοποίησης επίσημα καθιερώνει ότι το αντικείμενο ικανοποιεί τις απαιτήσεις κάποιου πρότυπου.
- Η **αναγνώριση** παρέχει ανεξάρτητη επικύρωση της ικανότητας ενός οργανισμού να παρέχει εξειδικευμένες υπηρεσίες αποτίμησης συμμόρφωσης.
- Οι **δοκιμές** είναι ο καθορισμός των χαρακτηριστικών του προϊόντος απέναντι στις απαιτήσεις του πρότυπου. Υπάρχουν 3 διαφορετικές κατηγορίες δοκιμών: οι δοκιμές συμμόρφωσης, οι δοκιμές λειτουργικότητας και οι δοκιμές διαλειτουργικότητας. Σχετικά με τη ασφάλεια στα Έξυπνα Δίκτυα και τα 3 είδη δοκιμών χρειάζονται. Οι δοκιμές συμμόρφωσης πρέπει να γίνονται για να επιβεβαιωθεί ότι το αντικείμενο ικανοποιεί τις απαιτήσεις που θέτει η ΕΕ και οι χρήστες. Οι δοκιμές λειτουργικότητας χρειάζονται για να επιβεβαιωθεί η εφαρμογή και η λειτουργία των απαιτούμενων μέτρων ασφάλειας. Οι δοκιμές διαλειτουργικότητας χρειάζονται για να επιβεβαιωθεί η ασφαλής αλληλεπίδραση του αντικειμένου με άλλα αντικείμενα του δικτύου.
- Δοκιμές σε βάθος (penetration test) που επικεντρώνουν στη εξερεύνηση πιθανών ροών με αδυναμίες που μπορεί να υποβαθμίσουν την ασφάλεια του συστήματος.

Διαφορετικές τεχνικές αποτίμησης συμμόρφωσης μπορούν να συνδυαστούν με τα επίπεδα αντίκτυπου κινδύνου. Με αυτό τον τρόπο είναι πιθανό να μειωθεί το κόστος της πιστοποίησης αφού τα λιγότερο κρίσιμα μέρη μπορεί να μην αποτελέσουν αντικείμενο πιστοποίησης αλλά να χρησιμοποιηθούν οικονομικότερες λύσεις για την αποτίμηση συμμόρφωσης τους.

6.7 Περιγραφή σχημάτων πιστοποίησης που βασίζονται στο SG-AM

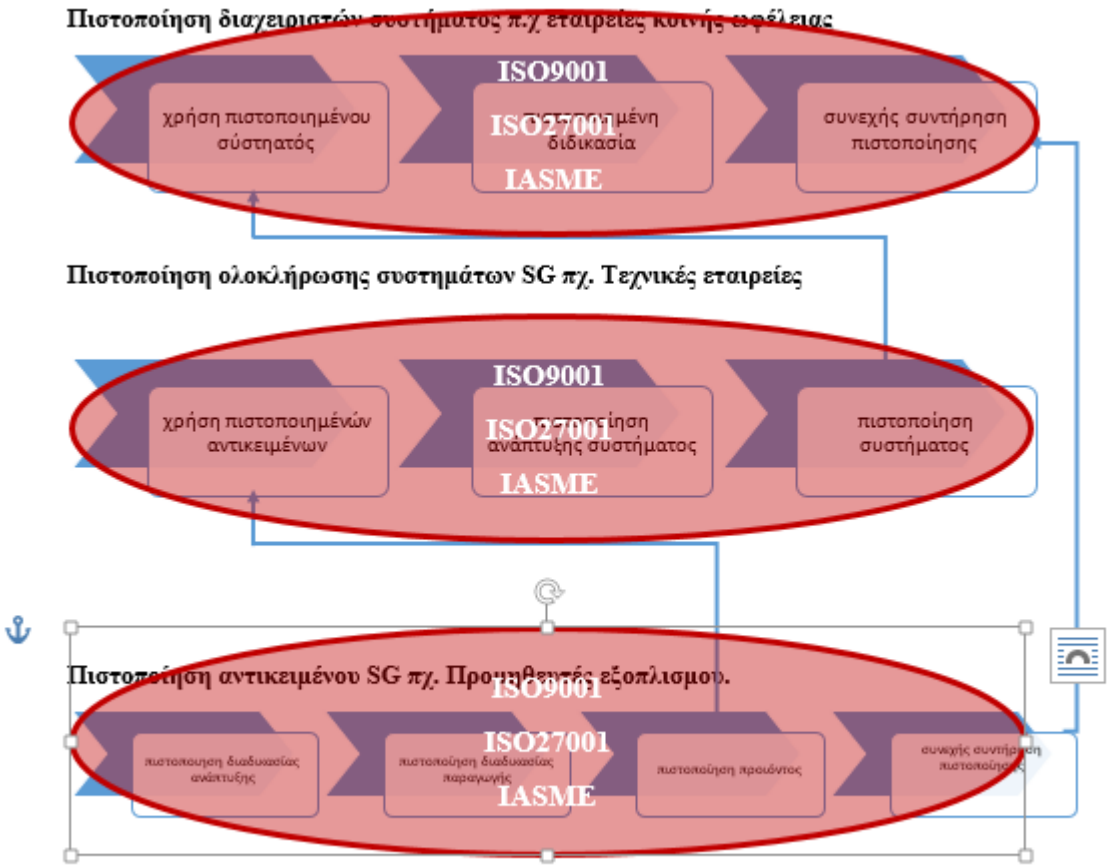
Δεν είναι εφικτό να υπάρχει ακριβής αντιστοίχηση των σχημάτων πιστοποίησης με το μοντέλο SG-AM. Οι περιοχές στο αρχικό SG-AM μοντέλο έχουν αντικατασταθεί από τις φάσεις του κύκλου ζωής του προϊόντος (ανάπτυξη, παραγωγή, λειτουργία, συντήρηση). Οι ζώνες του SG-AM έχουν αντικατασταθεί από τις φάσεις ιδιοκτησίας του προϊόντος (παραγωγή, ολοκλήρωση, αποδοχή, λειτουργία). Έτσι το SG-AM μπορεί να αποτελέσει οδηγό για το που πρέπει να τοποθετηθεί το σχήμα πιστοποίησης μέσα στην αλυσίδα εμπιστοσύνης του Έξυπνου Δικτύου. Τα επίπεδα που περιγράφονται στο SG-AM και διατηρούνται ίδια είναι:

- Επιχειρηματικό επίπεδο.
- Λειτουργικό επίπεδο.
- Επίπεδο πληροφορίας.
- Επίπεδο επικοινωνίας.
- Επίπεδο αντικειμένου.

Παρακάτω γίνεται μια περιγραφή του κάθε επιπέδου σε σχέση με το SG-AM και προτείνεται ποιο από τα σχήματα πιστοποίησης μπορεί να εφαρμοστεί σε κάθε επίπεδο.

Επιχειρηματικό επίπεδο (Business Layer)

Αυτό το επίπεδο αντιπροσωπεύει την επιχειρηματική άποψη στην ανταλλαγή πληροφορίας σχετικά με τα Έξυπνα Δίκτυα. Το SG-AM μπορεί να χρησιμοποιηθεί για να αντιστοιχήσει κανονιστικές και οικονομικές δομές και πολιτικές, επιχειρηματικά μοντέλα και επιχειρηματικά χαρτοφυλάκια των εμπλεκόμενων μερών της αγοράς. Επίσης σε αυτό το επίπεδο μπορούν να συμπεριληφθούν και οι επιχειρηματικές δυνατότητες και οι επιχειρηματικές διαδικασίες. Με αυτό τον τρόπο υποστηρίζεται η λήψη αποφάσεων για νέα επιχειρηματικά μοντέλα και συγκεκριμένα επιχειρηματικά έργα όπως και κανόνες για την υιοθέτηση νέων μοντέλων αγορών.

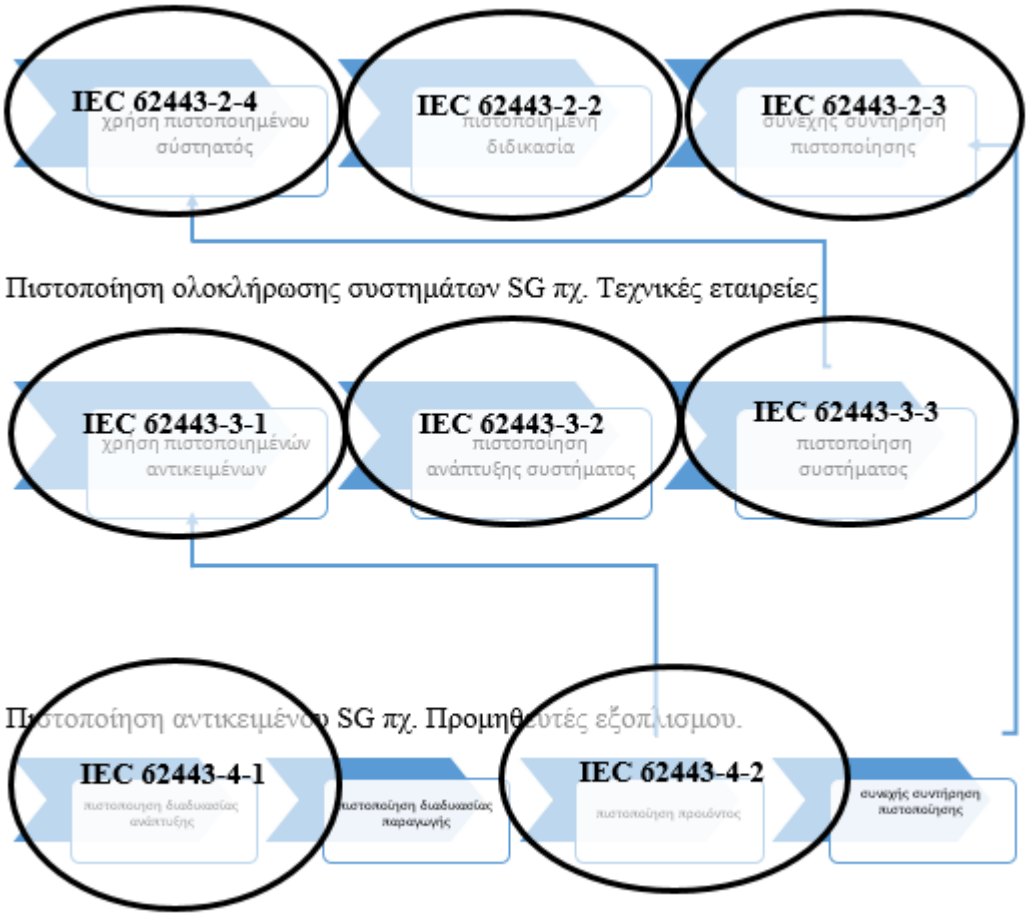


Σχήμα 6.7 : Επιχειρηματικό επίπεδο

Λειτουργικό επίπεδο (Functional Layer)

Το λειτουργικό επίπεδο περιγράφει λειτουργίες και υπηρεσίες μαζί με τις συσχετίσεις τους από αρχιτεκτονική οπτική. Οι λειτουργίες αναπαριστώνται ανεξάρτητες από παράγοντες και φυσικές εφαρμογές. Οι λειτουργίες πηγάζουν από τις λειτουργίες της περίπτωσης χρήσης. Το IEC62443 παρέχει απαιτήσεις και οδηγό για λειτουργίες ασφάλειας σε βιομηχανικά συστήματα ελέγχου. Δυστυχώς δεν παρέχουν όλα τα μέρη του προτύπου επίσημα σχήματα πιστοποίησης. Επιπλέον το πρότυπο επικεντρώνεται στις απαιτήσεις ασφάλειας και στον σχεδιασμό αλλά δεν παρέχει λεπτομερείς

περιγραφή των αντικειμένων και των πρωτοκόλλων επικοινωνίας. Στο παρακάτω σχήμα αντιστοιχίζεται σε διάφορα επίπεδα της αλυσίδας εμπιστοσύνης.



Σχήμα 6.8: Λειτουργικό επίπεδο

Επίπεδο πληροφορίας (Information Layer)

Αυτό το επίπεδο περιγράφει την πληροφορία που χρησιμοποιείται και ανταλλάσσεται μεταξύ των διαδικασιών των υπηρεσιών και των αντικειμένων. Περιλαμβάνει αντικείμενα πληροφορίας και μοντέλα δεδομένων. Στο επίπεδο πληροφορίας δεν υπάρχει διαθέσιμη πιστοποίηση ασφάλειας. Τέτοια πιστοποίηση θα έπρεπε να επικεντρώνει στην διασφάλιση της ανταλλαγής της πληροφορίας σε τεχνικό επίπεδο.

Αυτό μπορεί περιλαμβάνει παραμετροποίηση, μοντέλα δεδομένων και κρυπτογράφηση βάσης δεδομένων αλλά θα μπορούσε να συνεπάγεται και παραγωγή, εγκαθίδρυση και διαμοιρασμό κλειδιών και καθημερινή διαχείριση των ευαίσθητων δεδομένων.

Επίπεδο επικοινωνίας (Communication layer).

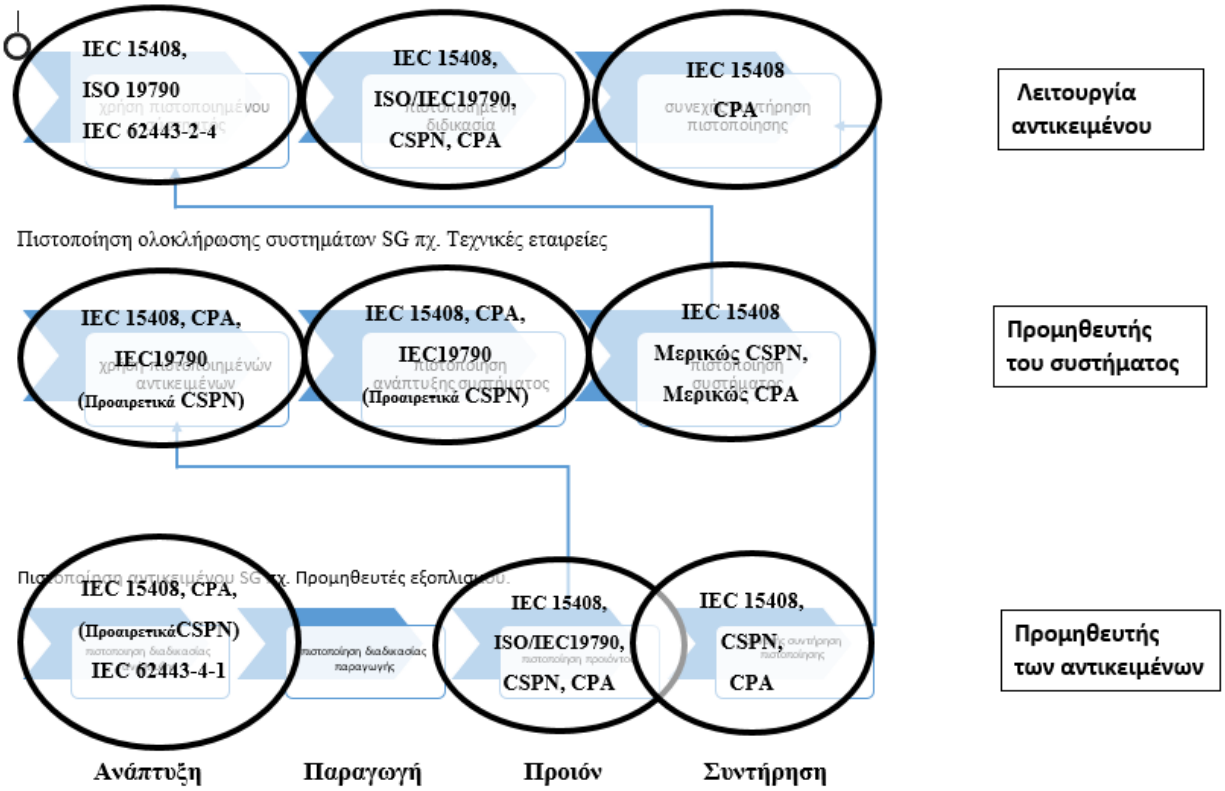
Υπάρχουν πρότυπα για ασφαλείς επικοινωνίες όπως το IEC62351 και DLMS/IEC 62056. Αυτά τα πρότυπα συστήνουν την εφαρμογή μέτρων ασφάλειας επικοινωνίας όπως η κρυπτογράφηση και η αυθεντικοποίηση. Όμως δεν υπάρχουν σχήματα πιστοποίησης για να δοκιμάσουν επίσημα την ασφάλεια επικοινωνίας συσκευών.

Επίπεδο αντικειμένου (component layer).

Αυτό το επίπεδο επικεντρώνεται στην ασφάλεια των αντικειμένων που χρησιμοποιούνται σ' ένα Έξυπνο Δίκτυο. Αφορά στην ασφάλεια των μεμονωμένων μερών στον εξοπλισμό στο λογισμικό και στις λειτουργίες που οι συσκευές υποστηρίζουν.

Έως τώρα δεν υπάρχει σχήμα πιστοποίησης που να καλύπτει όλες τις πτυχές των Έξυπνων Δικτύων. Επίσης δεν υπάρχει συνδυασμός σχημάτων που να μπορεί να καλύψει τα πάντα σ' ένα SG αφού τα επίπεδα πληροφορίας και επικοινωνίας δεν διαθέτουν πιστοποιητικά που να επικεντρώνουν επισήμως σε αυτές τις περιπτώσεις.

Αυτό δεν αποτελεί σημαντικό ζήτημα γιατί πρακτικά οι εφαρμογές των Έξυπνων Δικτύων δεν καλύπτουν όλες τις πτυχές του SG μοντέλου.



Σχήμα 6.9: Επίπεδο αντικειμένου.

6.8 Κενά και προκλήσεις

1. Δεν έχει καθιερωθεί μοντέλο για αλυσίδα εμπιστοσύνης στα Έξυπνα Δίκτυα στην ΕΕ.
2. Δεν υπάρχουν κοινά μοντέλα αναφοράς όπως το SG- AM για το σύνολο των Έξυπνων Δικτύων στην ΕΕ.
3. ΔΕ υπάρχει κοινή βάση για τις απαιτήσεις ασφάλειας που θα μπορούν να αναγνωρίζονται από όλα τα μέλη της ΕΕ.
4. Σε Ευρωπαϊκό επίπεδο ισοδύναμα επίπεδα ασφάλειας και κινδύνων παρέχονται από το M/490 SG-IS πλαίσιο, αλλά δεν είναι επίσημα αναγνωρισμένο ως ένα Ευρωπαϊκό ευρύ πρότυπο για ασφάλεια Έξυπνων Δικτύων.
5. Υπάρχουν σχήματα πιστοποίησης για αντικείμενα και λειτουργίες αλλά δεν υπάρχει πιστοποίηση για συστήματα.

6. Δεν υπάρχει ένα μοναδικό σχήμα που να αποτελεί Ευρωπαϊκή οδηγία για εφαρμογή και υποστήριξη των εθνικών νομοθεσιών για την ασφάλεια στα Έξυπνα Δίκτυα.

6.9 Συστάσεις - προτάσεις

Παρακάτω υπάρχει μια συνοπτική καταγραφή των προτάσεων που βασίζονται στην τρέχουσα κατάσταση στην ΕΕ, την επιθυμητή κατάσταση και στα κενά και τις προκλήσεις που υπάρχουν.

1. Η Ευρωπαϊκή Επιτροπή θα πρέπει να οργανώσει επιτροπή συντονισμού για δραστηριότητες πιστοποίησης Έξυπνων Δικτύων.
2. Η συντονιστική επιτροπή θα πρέπει να εκδώσει οδηγία και μοντέλο αναφοράς για εφαρμογή αλυσίδας εμπιστοσύνης.
3. Χρήση των διαθέσιμων προτύπων και σχημάτων και βελτίωση επιπέδου συνεργασίας και εναρμόνισης μεταξύ των μελών της ΕΕ. Η συντονιστική επιτροπή θα μπορούσε να συμβουλεύει τα μέλη της ΕΕ στο πώς να αντιστοιχήσουν τα πρότυπα τους στο μοντέλο SG-AM.
4. Η συντονιστική επιτροπή θα πρέπει να προάγει την διεθνή αναγνώριση των σχημάτων πιστοποίησης και την ευθυγράμμιση των μελών της ΕΕ με αυτά.
5. Η συντονιστική επιτροπή θα πρέπει να διασφαλίσει κατάλληλα επίπεδα ασφάλειας για τις περιπτώσεις χρήσης των Έξυπνων Δικτύων.
6. Θα πρέπει να διευκολύνεται η υπάρχει ευελιξία στη αναβάθμιση των προφίλ για να μπορούν να κινούνται στους ρυθμούς των εξελίξεων στον τομέα της ασφάλειας.
7. Τα μέλη της ΕΕ θα πρέπει να χρησιμοποιούν τα δικά τους εξειδικευμένα προφίλ που αντανακλούν στις τοπικές απαιτήσεις και ιδιαιτερότητες των Έξυπνων Δικτύων που όμως θα ευθυγραμμίζονται με τα διεθνή πρότυπα πιστοποιήσεων.
8. Η Ευρωπαϊκή Επιτροπή θα πρέπει να περιλαμβάνει τεχνικές επιτροπές που σε συνεργασία με τις Ευρωπαϊκές αρχές ενέργειας θα δημιουργούν τα Ευρωπαϊκά προφίλ.
9. Θα πρέπει να παρέχεται επίσημη πιστοποίηση από 3^{ο} μέρος.

10. Να προωθηθεί η συμμόρφωση και ο εναρμονισμός των πρακτικών πιστοποίησης στα Έξυπνα Δίκτυα σαν οικονομικό πλεονέκτημα.

6.10 Σύνοψη

Το σχήμα 6.10 παρουσιάζει το πλαίσιο στο οποίο λειτουργεί η πιστοποίηση ασφάλειας Έξυπνων Δικτύων βασιζόμενη σε περιπτώσεις χρήσης. Το πιστοποιητικό πρέπει να καθιστά σαφές το ποιο αντικείμενο πιστοποιείται και ποία άλλα πιστοποιητικά χρησιμοποιούνται για την δημιουργία της αλυσίδας εμπιστοσύνης. Το σχήμα αναφέρεται σε μια περίπτωση ενός ιδιοκτήτη αγαθού που θέλει να παρέχει μια συσκευή Έξυπνου Δικτύου σύμφωνα με τις εναρμονισμένες πρακτικές πιστοποίησης ασφάλειας που παρουσιάστηκαν παραπάνω.

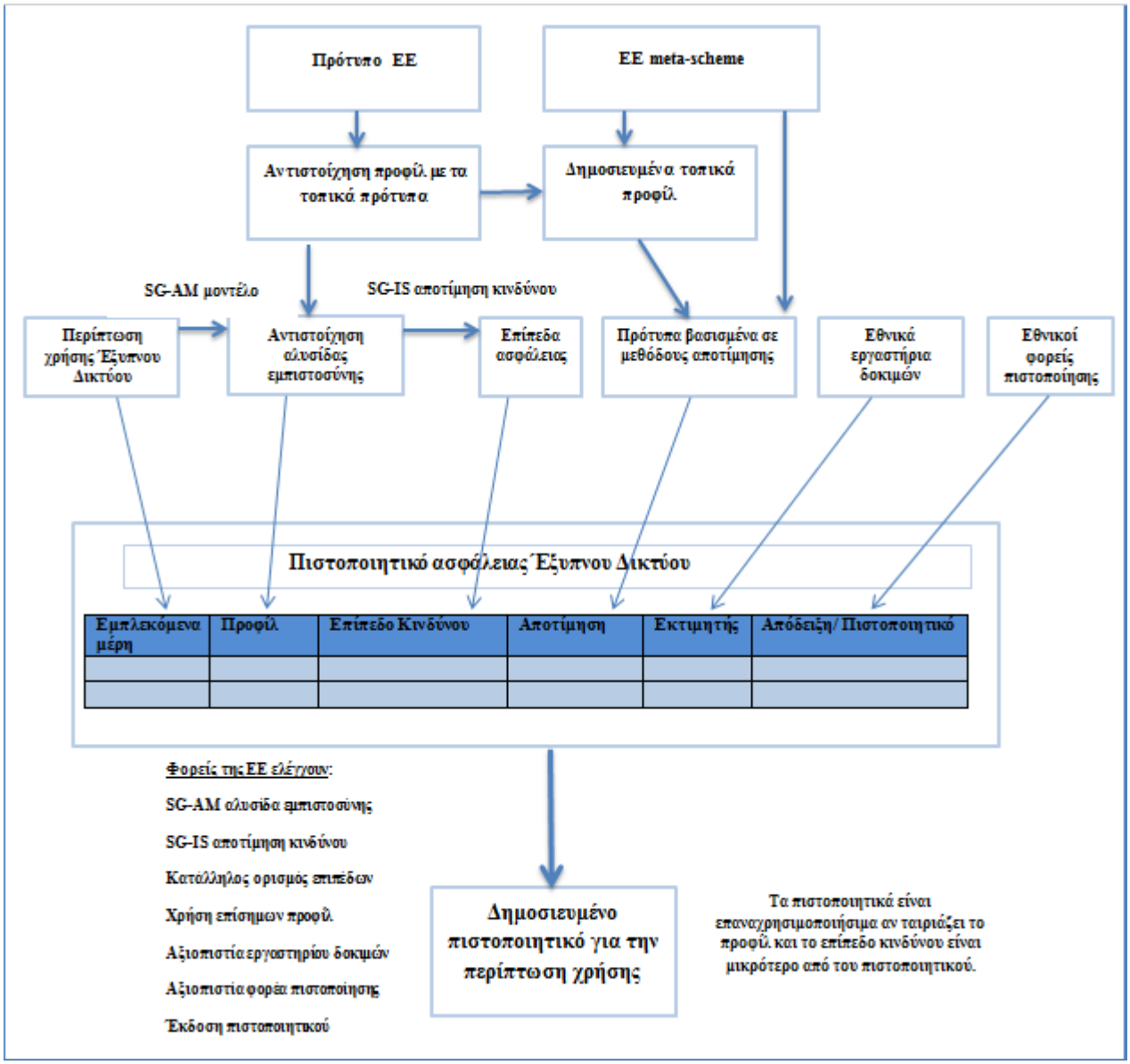
Κάθε συσκευή πρέπει να ευθυγραμμίζεται τουλάχιστον με τις περιπτώσεις χρήσης της χώρας που πρόκειται να προμηθευτεί με το προϊόν. Οι τοπικές ειδικές περιπτώσεις χρήσης μπορούν να περιγραφούν με το SG-AM μοντέλο το οποίο μπορεί να χρησιμοποιηθεί ως βάση για την δημιουργία μοντέλου αλυσίδας εμπιστοσύνης.

Αυτό το μοντέλο αλυσίδας εμπιστοσύνης μπορεί να χρησιμοποιηθεί για τον καθορισμό του προφίλ των τοπικών απαιτήσεων και του τοπικού σχήματος πιστοποίησης για τη δημιουργία αλυσίδας εμπιστοσύνης για την συγκεκριμένη περίπτωση χρήσης και θα υποδείξει τα επίπεδα ασφάλειας που πρέπει να παρέχει ο ιδιοκτήτης που θα ευθυγραμμίζονται με το SG-IS πλαίσιο εκτίμησης κινδύνου.

Το τοπικό σχήμα που θα προκύψει πρέπει να υποβληθεί στην επιτροπή συντονισμού της ΕΕ για διαχείριση από την τεχνική επιτροπή. Το τοπικό σχήμα κανονικά θα δημιουργηθεί από τοπική τεχνική επιτροπή που θα αποτελείται από τα ενδιαφερόμενα μέρη. Αυτή η επιτροπή θα πρέπει να αναπτύξει ένα SG-IS πλαίσιο εργασίας που θα ευθυγραμμίζεται με την τοπική περίπτωση χρήσης και μπορεί να λάβει συμβουλές από την Ευρωπαϊκή επιτροπή συντονισμού για σωστή εφαρμογή. Το τοπικό σχήμα που θα αναπτυχθεί θα μπορεί για παράδειγμα να αναδεικνύει την ανάγκη δημιουργίας πιστοποιητικού για ασφαλή ανάπτυξη και παραγωγή για το χτίσιμο αλυσίδας εμπιστοσύνης στο επίπεδο του αντικειμένου. Ανάλογα με το αν ο κατασκευαστής διαθέτει πιστοποιητικά για το ίδιο ή υψηλότερο επίπεδο απ' αυτό που προκύπτει από

την αποτίμηση κινδύνου τα διαθέσιμα πιστοποιητικά μπορούν να χρησιμοποιηθούν σαν αποδεικτικό αλυσίδας εμπιστοσύνης. Όταν όλα τα πιστοποιητικά αποκτηθούν μπορούν να σταλούν στην Ευρωπαϊκή επιτροπή για θεώρηση και δημοσίευση.

Μετά τη δημοσίευση πιθανό να είναι εύκολο χρησιμοποιηθεί και για άλλες περιπτώσεις χρήσης αν το επίπεδο ασφάλειας του πιστοποιητικού καλύπτει το απαιτούμενο επίπεδο ασφάλειας της περίπτωσης χρήσης.



Σχήμα 6.10: Διαδικασία πιστοποίησης Έξυπνων Δικτύων

ΚΕΦΑΛΑΙΟ ΕΒΔΟΜΟ

7. Ανάλυση επικινδυνότητας για Smart Grid[32]

Σε αυτό το κεφάλαιο θα χρησιμοποιήσουμε τη μέθοδο CORAS για ανάλυση επικινδυνότητας σχετικά με την διαχείριση ασφάλειας στα Έξυπνα Δίκτυα και με βάση το πρότυπο ISO27002 θα εντοπίσουμε τις απαιτήσεις ασφάλειας και του ελέγχους για να εξαλειφθούν οι κίνδυνοι που θα αναγνωριστούν. Το σενάριο στο οποίο θα επικεντρωθούμε αφορά στην ανάγνωση των στοιχείων που έχουν καταγράψει οι Smart Meters προκειμένου να γίνουν οι ανάλογες τιμολογήσεις. Ο Secondary Station Node (SSN) σε περιοδικά διαστήματα συλλέγει αυτή την πληροφορία από τους SMs που είναι συνδεδεμένοι σε αυτόν. Αποθηκεύει αυτή την πληροφορία σε εσωτερική βάση δεδομένων και σε περιοδικά διαστήματα προωθεί την πληροφορία στη βάση δεδομένων του Middle Ware (MW). Σε προκαθορισμένα χρονικά διαστήματα αυτή η πληροφορία αποστέλλεται από το MW στο Low / Medium Voltage Related Company System (LMVRCS) της εταιρείας κοινής ωφέλειας.

Η CORAS είναι μια μέθοδος για τη διεξαγωγή ανάλυσης επικινδυνότητας. Βασίζεται στη γλώσσα UML για τη μοντελοποίηση των χαρακτηριστικών εκτίμησης κινδύνων, και στη συνέχεια εξελίχθηκε σε μια συγκεκριμένη «γλώσσα κινδύνων» που χρησιμοποιείται ως κοινή γλώσσα μεταξύ εμπλεκόμενων από διαφορετικούς τομείς κρίσιμων υποδομών παρέχοντας κοινή κατανόηση των όρων και των σχέσεων που χρησιμοποιούνται στην εκτίμηση κινδύνων. Η μέθοδος CORAS περιλαμβάνει τη χρήση ειδικών πινάκων και διαγραμμάτων για κάθε στάδιο της διαδικασίας εκτίμησης κινδύνων οι οποίοι, όπως και με τις μεθόδους ανάλυσης, χρησιμοποιούνται διαδοχικά για την παροχή εισροών σε μετέπειτα δραστηριότητες. Η μέθοδος CORAS φαίνεται να είναι γενικά εφαρμόσιμη στους περισσότερους τύπους εκτίμησης κινδύνων και τύπων υποδομών. Ωστόσο, χρειάζεται κατάλληλη εκπαίδευση των χρηστών για να μην γίνει υπερεκτίμηση ή υποτίμηση του επιπέδου ενός κινδύνου **http://coras.sourceforge.net/**

Στη μέθοδο CORAS η ανάλυση επικινδυνότητας διεξάγεται σε οκτώ βήματα στα οποία γίνεται ανάλυση παρακάτω:

- Προετοιμασία για την ανάλυση.
- Παρουσίαση πελάτη όσο αφορά τον στόχο.

- Περαιτέρω επεξεργασία της περιγραφής του στόχου χρησιμοποιώντας διαγράμματα περιουσιακών στοιχείων.
- Έγκριση της περιγραφής του στόχου.
- Αναγνώριση του κινδύνου με την χρήση διαγραμμάτων απειλής.
- Εκτίμηση του κινδύνου με την χρήση διαγραμμάτων απειλής.
- Αξιολόγηση του κινδύνου χρησιμοποιώντας το διάγραμμα κινδύνου.
- Ο χειρισμός κινδύνου χρησιμοποιώντας το διάγραμμα μεταχείρισης.

7.1 Αναγνώριση περιουσιακών στοιχείων και κινδύνων

7.1.1 . Προετοιμασία για την ανάλυση (βήμα 1)

Το πρώτο βήμα είναι οι αρχικές προετοιμασίες για την ανάλυση κινδύνου. Ο κύριος στόχος είναι η κατανόηση του στόχου και του μεγέθους της ανάλυσης έτσι ώστε να μπορούν να γίνουν οι απαραίτητες προετοιμασίες για τις πραγματικές εργασίες ανάλυσης.

Με βάση το σενάριο στόχο, οι στόχοι των επιχειρήσεων και οι περιορισμοί έχουν εντοπιστεί.

Βασικοί στόχοι επιχειρήσεων:

BO1. Απόκτηση σωστών ενδείξεων του μετρητή από την SM, SSN, MW

BO2. Έκδοση σωστών λογαριασμών για τους πελάτες

BO3. Προστασία των ευαίσθητων δεδομένων των επιχειρήσεων (τα στοιχεία των πελατών, πληροφορίες συμβάσεων παροχής υπηρεσιών, τα στοιχεία χρέωσης)

BO4. Προστασία των δεδομένων της ένδειξης του μετρητή από τρίτους.

BO5. Η ανάγνωση μετρητών, το είδος της σύμβασης και οι πληροφορίες λογαριασμών να είναι διαθέσιμα στην διαδικτυακή πύλη για τον πελάτη

Απαιτήσεις συμμόρφωσης

(Πρόκειται για τη νομική συμμόρφωση και όχι απαιτήσεις ασφαλείας)

Σύμφωνα με τους *Κανόνες δημόσιων συμβάσεων έργων, προμηθειών και υπηρεσιών, οι οποίοι εφαρμόζονται έως το 2016* http://eur-lex.europa.eu/legal-content/EL/TXT/?uri=URISERV:l22009.

C1. Η εταιρεία κοινής ωφέλειας και ο πελάτης θα πρέπει να έχουν συμβόλαιο παροχής υπηρεσιών που να περιλαμβάνει λεπτομέρειες σχετικά με τις υπηρεσίες που πρέπει να παρέχονται, χρήση εμπιστευτικών και τα προσωπικά δεδομένα.

Σύμφωνα με τον νόμο *Επεξεργασίας δεδομένων προσωπικού χαρακτήρα* http://eur-lex.europa.eu/legal-content/EL/TXT/?uri=URISERV:l14012

C2. Οι πληροφορίες των πελατών προστατεύονται από μη εξουσιοδοτημένους .

C3. Οι πληροφορίες του πελάτη χρησιμοποιούνται μόνο για τους σκοπούς που συμφωνήθηκαν.

C4. Το απόρρητο του πελάτη προστατεύεται.

7.1.2. Παρουσίαση του στόχου στον πελάτη (βήμα 2)

Στην περίπτωσή των Smart grid η συνάντηση με τον πελάτη δεν είναι εφικτή. Παρόλα αυτά σύμφωνα με τη γνώση που υπάρχει για το σενάριο που αναφερόμαστε, ο στόχος και το πεδίο της ανάλυσης προσδιορίζονται ως εξής.

Στόχοι ανάλυσης

> Προσδιορισμός των κινδύνων του συστήματος Smart Grid σχετικά με την ανάγνωση των δεδομένων των SMs και καθορισμός ενός συνόλου απαιτήσεων ασφάλειας και ελέγχων με σκοπό την προστασία των περιουσιακών στοιχείων και την κάλυψη των επιχειρηματικών στόχων τηρώντας τους περιορισμούς απαιτήσεων.

Σκοπός ανάλυσης

- ✓ Η ανάλυση γίνεται από την πλευρά της εταιρείας κοινής ωφέλειας, ωστόσο, ορισμένα πολύτιμα περιουσιακά στοιχεία, όπως προσωπικά στοιχεία και η ιδιωτικότητα των καταναλωτών θα πρέπει να λαμβάνονται υπόψη λόγω των απαιτήσεων.
- ✓ Περιορισμός ανάλυσης για το σενάριο ανάγνωσης στοιχείων από τους SMs με σκοπό την τιμολόγηση των καταναλωτών.
- ✓ Δίνεται έμφαση μόνο στα στοιχεία της ένδειξης του μετρητή, στα δεδομένων πελατών, στην τιμολόγηση και τη διαθεσιμότητα εμπιστευτικότητα και ακεραιότητα τους.
- ✓ Οι εσωτερικές επιχειρηματικές διαδικασίες και τα συστήματα (εκτός εκείνων που αναφέρονται ρητά στο σενάριο χρέωσης που εμπλέκονται στην επιχείρηση χειρισμό ευαίσθητων δεδομένων και ένδειξη μετρητή) θεωρούμε ότι είναι ασφαλείς.
- ✓ Η ποιότητα της υπηρεσίας είναι εξασφαλισμένη από τις επιχειρήσεις κοινής ωφέλειας. Οι πηγές τροφοδοσίας ρεύματος είναι ασφαλείς και εφεδρικά συστήματα ισχύος είναι στη θέση τους. Μη προγραμματισμένες διακοπές στην παροχή ηλεκτρικής ενέργειας που προκαλείται από τρίτους μέσω απομακρυσμένου ελέγχου του δικτύου βρίσκεται εκτός του πεδίου εφαρμογής.
- ✓ Παράγοντες που εμπλέκονται στα σενάρια αυτά περιορίζονται στους τελικούς χρήστες (πελάτες), στις επιχειρήσεις κοινής ωφέλειας, στους έξυπνους μετρητές, SSN, MW, και LMVRCS. Άλλοι παράγοντες, όπως η κυβέρνηση, που μπορεί επίσης να ενδιαφέρονται για την ανάγνωση SM είναι εκτός εμβέλειας της παρούσας ανάλυσης.

7.1.3 Καθορισμός του στόχου με χρήση διαγραμμάτων (βήμα 3).

Εντοπισμός των μερών

Για την ανάλυση που θα γίνει έχει γίνει εντοπισμός 2 μερών, αυτό του πελάτη και αυτό της εταιρείας κοινής ωφέλειας.

Πελάτης: σπίτια, μικρά γραφεία, κτίρια που χρησιμοποιούν ηλεκτρική ενέργεια που παρέχεται από τις εταιρείες κοινής ωφέλειας. Η χρήση ηλεκτρικής ενέργειας του πελάτη καταγράφεται από τον μετρητή του Smart grid.

Εταιρεία κοινής ωφελείας: Οργανισμός που κατέχει πόρους και παρέχει ηλεκτρική ενέργεια σε πελάτες και λογαριασμούς με βάση τις αναγνώσεις έξυπνων μετρητών που λαμβάνονται από το Middle Ware (MW) σε περιοδική βάση ή σε ad-hoc αιτήματα.

Εντοπισμός περιουσιακών στοιχείων

Τα περιουσιακά στοιχεία αναγνωρίζονται με βάση την αξία που έχουν για τα εμπλεκόμενα μέρη. Στο παρακάτω πίνακα καταγράφονται τα περιουσιακά στοιχεία και οι ιδιοκτήτες τους .

	ΟΜΑΔΑ	**ΠΕΡΙΟΥΣΙΑΚΑ ΣΤΟΙΧΕΙΑ**	**ΤΥΠΟΣ**	**ΕΠΙΧΕΙΡΙΣΙΑΚΟΙ ΣΤΟΧΟΙ Ή ΠΕΡΙΟΡΙΣΜΟΙ**
A1	ΠΕΛΑΤΗΣ	Προσωπικές πληροφορίες	Άμεσα	C2
A2		Συμβόλαιο παροχής υπηρεσιών	Άμεσα	C1
A3		Ιδιωτικότητα	Έμμεσα	C4
A4	ΕΤΑΙΡΕΙΑ ΚΟΙΝΗΣ ΩΦΕΛΕΙΑΣ	Ευαίσθητες πληροφορίες εταιρείας πληροφορίες πελάτη ,τύπους συμβολαίων & τιμολόγησης	Άμεσα	BO2,BO3,BO5,C2,C3
A5		Στοιχεία μετρητών	Άμεσα	BO1,C4
A6		Φήμη της εταιρείας	Έμμεσα	BO2,BO3,BO4,C2,C3,C4
A7		Συμμόρφωση με το συμβόλαιο	Έμμεσα	C1

Πίνακας7. 1: Περιουσιακά στοιχεία

Περιγραφή περιουσιακών στοιχείων

A1. Προσωπικά στοιχεία – δεδομένα του πελάτη.

A2. Σύμβαση παροχής υπηρεσιών μεταξύ του πελάτη και της εταιρείας κοινής ωφέλειας. Αποτελεί περιουσιακό στοιχείο για τον πελάτη ο οποίος τηρεί και αντίγραφο αυτής που μπορεί να χρησιμοποιήσει σε περίπτωση που η εταιρεία αθετήσει τους όρους της.

A3. Η ιδιωτικότητα του πελάτη. Η ιδιωτικότητα μπορεί να παραβιαστεί έμμεσα από μη εξουσιοδοτημένη πρόσβαση στον μετρητή της παροχής , καθώς από εκεί μπορούν

να εξαχθούν στοιχεία που αφορούν συνήθειες του καταναλωτή και άλλα προσωπικά στοιχεία.

A4. Ευαίσθητα δεδομένα επιχειρήσεων που μπορεί να περιλαμβάνουν πληροφορίες πελατών και στοιχεία συμβολαίων, αποτελούν περιουσιακό στοιχείο καθότι η διαρροή τους μπορεί να είναι επωφελής για κάποιον ανταγωνιστή ή τρίτο μέρος.

A5. Στοιχεία μετρητών που είναι τα στοιχεία που συγκεντρώνονται από τους Έξυπνους Μετρητές των καταναλωτών είτε σε περιοδική είτε σε τυχαία συχνότητα. Αυτά περιλαμβάνουν όλα τα δεδομένα κατανάλωσης που αποθηκεύονται ή στέλνονται από τον Έξυπνο Μετρητή, SSN,MW και φτάνουν στα LMVRCS. Ο φυσικός εξοπλισμός των SM,SSN,MW θεωρείται ασφαλές και γι' αυτό δεν αναφέρεται σαν περιουσιακό στοιχείο της εταιρείας. Η όποια αναφορά σε αυτά αφορά τα δεδομένα που τηρούν ή διακινούν.

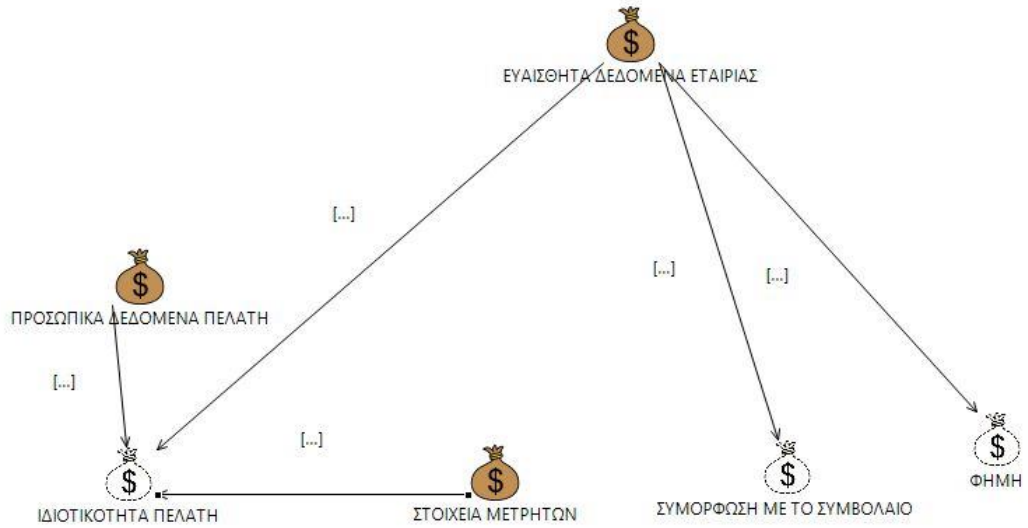
A6. Η φήμη της εταιρείας κοινής ωφέλειας και η ποιότητα που οι πελάτες κρίνουν ότι διαθέτει, έχει καθοριστική σημασία για την εταιρεία.

A7. Η εναρμόνιση της εταιρείας με τη σύμβαση παροχής υπηρεσιών που έχει συνάψει με τον καταναλωτή.

Συσχετίσεις περιουσιακών στοιχείων

- Η όποια βλάβη προκληθεί στα ευαίσθητα δεδομένα μιας επιχείρησης , έχει επιπτώσεις:
    - στο συμβόλαιο παροχής υπηρεσιών και επομένως στα συμβόλαια των καταναλωτών.
    - προσωπικά δεδομένα πελατών της που περιέχονται στις συμβάσεις.
    - στην ιδιωτικότητα των πελατών της επιχείρησης στην περίπτωση που διαρρεύσουν προσωπικά δεδομένα και στοιχεία κατανάλωσης.
    - στην εναρμόνιση της εταιρείας με τα συμβόλαια των πελατών στην περίπτωση που αυτά χαθούν ή αλλοιωθούν.
    - Στην φήμη της εταιρείας στην περίπτωση που διαρρεύσουν προσωπικά δεδομένα πελατών ή ευαίσθητα δεδομένα της εταιρείας σε ανταγωνιστές της.

- Η βλάβη στα δεδομένα των μετρητών μπορεί να βλάψει την ιδιωτικότητα των καταναλωτών έμμεσα όπως αναφέρεται και παραπάνω.



Σχήμα 7.1: Διάγραμμα περιουσιακών στοιχείων

Βασικά ανεπιθύμητα συμβάντα

Αιτία	**Πώς; Τι μπορεί να συμβεί; Τι μπορεί να βλάψει;**	**Τι το καθιστά πιθανό;**
Εισβολέας (πελάτης)	Αλλαγή των στοιχείων του μετρητή για να κερδίσει δωρεάν ηλεκτρική ενέργεια	Οι έξυπνοι μετρητές επιτρέπουν read –write διαδικασίες στη βάση δεδομένων από το interface τους ή από εξωτερικές θύρες. Δεν γίνεται συχνά αυτό - έλεγχος εφεδρείας δεδομένων των μετρητών. Δεν γίνεται συχνά αυτό - έλεγχος εφεδρείας δεδομένων των SSN ή των MW. Η διαδικτυακή πύλη επιτρέπει read – write διαδικασίες στους πελάτες.
Ακούσια ατυχήματα από τους πελάτες	Προκαλούν απώλεια δεδομένων λόγω βλάβη στην συσκευή του μετρητή ή αποσύνδεση του μετρητή από το δίκτυο.	Ο έξυπνος μετρητής τοποθετείται σε ορατό και εύκολα προσβάσιμο σημείο. Έλλειψη μηχανισμού ανάκτησης δεδομένων από τους μετρητές.
Φυσικές –	Η συσκευή του μετρητή έχει καταστραφεί και	Ο μετρητής τοποθετείται σε μη

Ανθρώπινες καταστροφές	όλα τα δεδομένα του έχουν χαθεί.	ασφαλές μέρος. Έλλειψη μηχανισμού ανάκτησης δεδομένων. Έλλειψη σαφών οδηγιών για το που πρέπει να τοποθετούνται οι μετρητές.
Εισβολέας	Κλοπή της συσκευής του μετρητή για πώληση στην αγορά.	Έλλειψη ασφάλειας στο χώρο του καταναλωτή. Ανύπαρκτος νομικός έλεγχος εμπορικών συναλλαγών από μη εξουσιοδοτημένα πρόσωπα.
Εισβολέας	Αποκτά πρόσβαση στον υπολογιστή του χρήστη και διαβάζει προσωπικά δεδομένα από την διαδικτυακή πύλη.	Έλλειψη ασφάλειας στο χώρο του καταναλωτή. Έλλειψη ασφαλούς αυθεντικοποίησης στην διαδικτυακή πύλη.
Εισβολέας	Αποκτά πρόσβαση στο λογισμικό του μετρητή και κλέβει ή παραποιεί δεδομένα από την βάση του.	Έλλειψη ασφαλούς αυθεντικοποίησης για πρόσβαση στη βάση δεδομένων του μετρητή.
Εισβολέας	Προκαλεί φυσική βλάβη στον SSN, διακόπτει την επικοινωνία μεταξύ των μετρητών και του MW προκαλώντας απώλεια δεδομένων.	Έλλειψη ασφάλειας στις εγκαταστάσεις. Τοποθέτηση του SSN σε ανοιχτό ορατό εύκολα προσβάσιμο μέρος. Έλλειψη αντιγράφων ασφάλειας. Έλλειψη μηχανισμού ειδοποίησης των MW ή LMVRCS όταν ο SSN τίθεται εκτός δικτύου.
Εισβολέας	Αποκτά πρόσβαση στη βάση δεδομένων του SSN και κλέβει ή παραποιεί δεδομένα.	Έλλειψη ασφαλούς αυθεντικοποίησης για πρόσβαση στη βάση δεδομένων του SSN. Έλλειψη μηχανισμού ειδοποίησης για μη εξουσιοδοτημένη πρόσβαση στην βάση δεδομένων. Έλλειψη έλεγχου εφεδρείας δεδομένων εσωτερικά ή από τον MW.
Εισβολέας	Αποκτά πρόσβαση στο λογισμικό του SSN και αποστέλλει μη εξουσιοδοτημένα αιτήματα ανάγνωσης των στοιχείων των μετρητών και κλέβει δεδομένα.	Έλλειψη αυθεντικοποίησης και επικύρωσης εντολών του SSN από τους έξυπνους μετρητές.
Εισβολέας	Διαδίδει κακόβουλο λογισμικό μέσω των SM, SSN,MW ή LMVRCS.	Έλλειψη τοίχους προστασίας στην εισερχόμενη και εξερχόμενη επικοινωνία. Έλλειψη λογισμικού anti virus. Έλλειψη μηχανισμού ελέγχου αλλοίωσης του λογισμικού.
Εισβολέας	Αποκτά πρόσβαση στο λογισμικό του MW και στέλνει ψεύτικες εντολές στους SSN ή SM για μη προγραμματισμένη ανάγνωση των δεδομένων των μετρητών και έτσι κλέβει δεδομένα.	Έλλειψη ασφαλούς αυθεντικοποίησης ή ελέγχου πρόσβασης για αποστολή MW εντολών. Έλλειψη επικύρωσης εντολών του MW από τους SSN και SM. Έλλειψη μηχανισμού ειδοποίησης για μη εξουσιοδοτημένες ή μη προγραμματισμένες εντολές του MW.
Εισβολέας	Αποκτά πρόσβαση στη βάση δεδομένων του MW και κλέβει ή παραποιεί δεδομένα.	Έλλειψη ασφαλούς αυθεντικοποίησης στη βάση

		δεδομένων του MW. Έλλειψη ελέγχου εφεδρείας δεδομένων εσωτερικά ή από τα LMVRCs.
Εισβολέας	Φυσική βλάβη στον εξοπλισμό των MW για να προκαλέσει απώλεια δεομένων και διακοπή της επικοινωνίας μεταξύ των MW,SSN,γLMVRCS,SMs.	Έλλειψη ασφάλειας στις εγκαταστάσεις. Τοποθέτηση του MW σε ανοιχτό ορατό εύκολα προσβάσιμο μέρος. Έλλειψη αντιγράφων ασφαλείας. Έλλειψη μηχανισμού ειδοποίησης του LMVRCS όταν τίθεται εκτός δικτύου.
Κακόβουλος εργαζόμενος	Αποκτά πρόσβαση στην βάση δεδομένων της εταιρείας και κλέβει ευαίσθητα δεδομένα για να τα πουλήσει στους ανταγωνιστές.	Έλλειψη ελεγχόμενης πρόσβασης και αυθεντικοποίησης. Έλλειψη πολιτικής ασφάλειας και εκπαίδευσης. Έλλειψη εσωτερικού ελέγχου.
Εργαζόμενος	Χειροκίνητα αλλάζει ή διαγράφει στοιχεία των μετρητών ή ευαίσθητα στοιχεία της εταιρείας , εκ παραδρομής.	Έλλειψη εκπαίδευσης. Έλλειψη αντιγράφων ασφαλείας. Έλλειψη εσωτερικού ελέγχου.
Πρόεδρος εταιρείας / Διοίκηση εταιρείας	Χρησιμοποιεί τα στοιχεία των μετρητών για επιθετική τιμολόγηση (με βάση στατιστικά στοιχεία για την κατανάλωση, προσαρμόζει τα τιμολόγια του προς όφελος της εταιρείας).	Έλλειψη εξωτερικών ελέγχων. Έλλειψη συμφωνίας με τους καταναλωτές για την χρήση των ευαίσθητων δεδομένων. Έλλειψη προστασίας των δικαιωμάτων των καταναλωτών.
Εισβολέας	Με Denial of Service επίθεση στο LMVRCS που προκαλεί μη διαθεσιμότητα στα ευαίσθητα δεδομένα της εταιρείας και στα στοιχεία των μετρητών.	Έλλειψη ανίχνευσης εισβολών. Έλλειψη πλάνου ανάκαμψης όταν το σύστημα τίθεται εκτός λειτουργίας.
Εισβολέας	Ζημίες στο φυσικό εξοπλισμό του LMVRCS που προκαλεί αλλοίωση ή απώλεια των ευαίσθητων δεδομένων της εταιρείας.	Έλλειψη προσωπικού φυσικής ασφάλειας. Έλλειψη αντιγράφων ασφαλείας των δεδομένων.
Εισβολέας	Αποκτά πρόσβαση στα ευαίσθητα δεδομένα της εταιρείας και στα στοιχεία των μετρητών μέσω της διαδικτυακής πύλης, και τα πουλάει στους ανταγωνιστές.	Έλλειψη ασφαλούς αυθεντικοποίησης στην διαδικτυακή πύλη και ελεγχόμενης πρόσβασης στη βάση δεδομένων.

Πίνακας 7.2: Βασικά ανεπιθύμητα περιστατικά

7.1.4 Αποδοχή της περιγραφής του στόχου (βήμα 4)

Κατηγοριοποίηση των περιουσιακών στοιχείων

Η ανάλυση γίνεται από την άποψη της εταιρείας και επομένως τα περιουσιακά στοιχεία κατηγοριοποιούνται με βάση τις πιθανές επιπτώσεις ή βλάβες που μπορεί να προκληθούν στα έσοδα της εταιρείας.

- Τα ευαίσθητα δεδομένα της επιχείρησης και τα στοιχεία των μετρητών είναι τα βασικότερα μέσα για την εισροή εσόδων στην επιχείρηση.

- Τα προσωπικά δεδομένα , τα συμβόλαια και η ιδιωτικότητα των πελατών δημιουργούν το περιοριστικό πλαίσιο μέσα στο οποίο ή εταιρεία ενεργεί για να πετύχει το κέρδος.
- Η φήμη της εταιρείας είναι σημαντική στην διασφάλιση της επιχειρησιακής συνέχειας. Ωστόσο μπορεί να διατηρηθεί προστατεύοντας τα υπόλοιπα περιουσιακά στοιχεία και γι' αυτό κατατάσσεται στην χαμηλότερη βαθμίδα.

Περιουσιακό στοιχείο	**Περιγραφή**	**Διαβάθμιση**
A1	Προσωπικά Δεδομένα	2
A2	Συμβόλαιο Παροχής Υπηρεσιών	2
A3	Ιδιωτικότητα	2
A4	Ευαίσθητες πληροφορίες εταιρείας	1
A5	Στοιχεία μετρητών	1
A6	Φήμη της εταιρείας	3
A7	Συμμόρφωση με το συμβόλαιο	2

Πίνακας 7.3: Περιουσιακά στοιχεία με τις διαβαθμίσεις τους

Κλίμακα πιθανότητας συμβάντος

Για να ορίσουμε τις διαβαθμίσεις πιθανότητας συμβάντος βασιζόμαστε σε legacy σύστημα που χρησιμοποιούν πολλαπλές κατανεμημένες βάσεις δεδομένων και ανταλλάσουν κρίσιμα δεδομένα σε 2-way επικοινωνία μεταξύ των μερών[33].

Πιθανότητα	**Περιγραφή**
Σίγουρα	Το περιστατικό είναι πολύ πιθανόν να συμβεί σε αυτό το σύστημα ίσως και πολλές φορές και έχει συμβεί πολλές φορές σε παρόμοια συστήματα.
Πολύ πιθανό	Το περιστατικό είναι πιθανό να συμβεί σε αυτό το σύστημα και έχει συμβεί τουλάχιστον μία φορά στα περισσότερα παρόμοια συστήματα.
Πιθανό	Το περιστατικό έχει συμβεί σε κάποια παρόμοια συστήματα.
Απίθανο	Δεδομένων των πρακτικών και των διαδικασιών του συστήματος είναι απίθανο να συμβεί το περιστατικό.
Σπάνια	Τελείως απίθανο να συμβεί στη διάρκεια ζωής αυτού του συστήματος.

Πίνακας 7.4: Κλίμακα Πιθανότητας Συμβάντος

Διαβάθμιση συνεπειών συμβάντος για τις ευαίσθητες πληροφορίες της εταιρίας.

Τα ευαίσθητα δεδομένα της εταιρείας είναι το περιουσιακό στοιχείο με την μεγαλύτερη αξία καθότι περιλαμβάνει δεδομένα απαραίτητα για την ύπαρξη και λειτουργία της εταιρείας. Συνεπώς η αλλοίωση ή κλοπή αυτών των δεδομένων μπορεί να αποβεί εντελώς καταστροφική για την συνέχεια λειτουργίας της επιχείρησης.

Συνέπειες	**Περιγραφή**
Καταστροφικές	Όλα τα ευαίσθητα δεδομένα της εταιρείας αλλοιώνονται και δεν μπορούν να αποκατασταθούν, κάτι που μπορεί να θέσει την εταιρεία εκτός λειτουργίας .
Σοβαρές	Κλοπή των ευαίσθητων δεδομένων της εταιρίας από μη εξουσιοδοτημένο τρίτο μέρος και διάθεση στους ανταγωνιστές που τα χρησιμοποιούν για να προσελκύσουν τους πελάτες.
	Κλοπή των ευαίσθητων δεδομένων της εταιρείας και πώληση τους που επιφέρει νομικές συνέπειες και βλάπτει την εταιρεία. Τα ευαίσθητα δεδομένα της εταιρείας είναι μη διαθέσιμα για παρατεταμένο χρονικό διάστημα.
Μέτριες	Ένας λογικός όγκος των ευαίσθητων δεδομένων της εταιρείας έχει κλαπεί, χαθεί ή αλλοιωθεί.
Μικρές	Μερικά ευαίσθητα δεδομένα της εταιρείας έχουν κλαπεί, χαθεί ή αλλοιωθεί.
Ασήμαντες	Κανένα ευαίσθητο δεδομένο της εταιρείας δεν έχει κλαπεί, χαθεί ή αλλοιωθεί.

Πίνακας7. 5: Κλίμακα συνεπειών συμβάντων για τα ευαίσθητα δεδομένα

Διαβάθμιση συνεπειών άντλησης στοιχείων από τους μετρητές

Η μη διαθεσιμότητα ή αλλοίωση των δεδομένων των μετρητών επιφέρει αδυναμία σωστής χρέωσης των καταναλωτών και συνεπώς απώλειες στα έσοδα της εταιρείας. Επίσης η κλοπή τους μπορεί να βλάψει την ιδιωτικότητα των πελατών και έτσι να θιγεί σοβαρά η φήμη της εταιρείας.

Συνέπειες	Περιγραφή
Καταστροφικές	Η πλειοψηφία των δεδομένων των μετρητών έχει χαθεί ή καταστραφεί και δεν μπορεί να ανακτηθεί. Η πλειοψηφία των δεδομένων των μετρητών έχει κλαπεί και κινδυνεύει η ιδιωτικότητα των καταναλωτών.
Σοβαρές	Η πλειοψηφία των δεδομένων των μετρητών έχει χαθεί ή καταστραφεί και για να ανακτηθεί απαιτείται μεγάλο κόστος. Η πλειοψηφία των δεδομένων είναι μη διαθέσιμη για επεξεργασία από την εταιρεία για παρατεταμένο χρονικό διάστημα. Πολλά από τα δεδομένα των μετρητών έχουν κλαπεί και κινδυνεύει η ιδιωτικότητα πολλών καταναλωτών. Κακή χρήση των δεδομένων των μετρητών που επηρεάζει την ιδιωτικότητα των καταναλωτών.
Μέτριες	Ένας μέτριος όγκος δεδομένων των μετρητών έχει χαθεί ή καταστραφεί και για να ανακτηθεί απαιτείται μέτριο κόστος. Κινδυνεύει η ιδιωτικότητα μερικών καταναλωτών.
Μικρές	Μερικά δεδομένα των μετρητών έχουν χαθεί ή καταστραφεί και για να ανακτηθούν απαιτείται ελάχιστο κόστος.
Ασήμαντες	Κανένα δεδομένο των μετρητών δεν έχει χαθεί ή καταστραφεί .

Πίνακας 7.6 : Κλίμακα συνεπειών συμβάντων για τους Έξυπνους Μετρητές

Διαβάθμιση συνεπειών συμβάντος στα προσωπικά δεδομένα

Για τα προσωπικά δεδομένα των πελατών της εταιρείας απαιτείται εμπιστευτικότητα. Η διαρροή τους μπορεί να θίξει την ιδιωτικότητα των πελατών και τότε οι συνέπειες είναι σοβαρές.

Συνέπειες	Περιγραφή
Καταστροφικές	Όλα τα προσωπικά δεδομένα έχουν χαθεί και χρησιμοποιούνται με παράνομο τρόπο που μπορεί να βλάψει την ιδιωτικότητα.
Σοβαρές	Η πλειοψηφία των προσωπικών δεδομένων έχει χαθεί και μπορεί να χρησιμοποιηθεί με παράνομο τρόπο που όμως δεν μπορεί να βλάψει την ιδιωτικότητα.
Μέτριες	Μερικά προσωπικά δεδομένα έχουν χαθεί και αλλά δεν μπορούν να

	χρησιμοποιηθούν με παράνομο τρόπο ούτε να βλάψουν την ιδιωτικότητα.
Μικρές	Ελάχιστα προσωπικά δεδομένα έχουν χαθεί.
Ασήμαντες	Κανένα προσωπικό δεδομένο δεν έχει χαθεί.

Πίνακας 7.7 : Κλίμακα συνεπειών συμβάντων για τα Προσωπικά Δεδομένα

Διαβάθμιση συνεπειών συμβάντος στα συμβόλαια παροχής υπηρεσιών

Η απώλεια του συμβολαίου μπορεί να έχει συνέπειες για τον πελάτη σε περίπτωση νομικής χρήσης. Από πλευράς εταιρείας δεν υπάρχουν αξιοσημείωτες συνέπειες καθότι η εταιρεία τηρεί τα δικά της αντίγραφα συμβολαίων.

Συνέπειες	**Περιγραφή**
Σοβαρές	Το συμβόλαιο έχει χαθεί και δεν μπορεί να ανακτηθεί.
Ασήμαντες	Μερικά συμβόλαια έχουν χαθεί ή κανένα συμβόλαιο δεν έχει χαθεί.

Πίνακας 7.8 : Κλίμακα συνεπειών συμβάντων για τα Συμβόλαια Παροχής Υπηρεσιών

Πίνακες επικινδυνότητας περιουσιακών στοιχείων

Συνδυάζοντας το βαθμό πιθανότητας συμβάντος και το βαθμό των συνεπειών προκύπτουν πίνακες επικινδυνότητας για κάθε περιουσιακό στοιχείο.

	Για μετριασμό
	Για παρακολούθηση
	Για αποδοχή

ΕΥΑΙΣΘΗΤΑ ΔΕΔΟΜΕΝΑ ΕΤΑΙΡΕΙΑΣ					
ΣΥΝΕΠΕΙΕΣ ΠΙΘΑΝΟΤΗΤΑ	ΑΣΗΜΑΝΤΕΣ	ΜΙΚΡΕΣ	ΜΕΤΡΙΕΣ	ΣΟΒΑΡΕΣ	ΚΑΤΑΣΤΡΟΦΙΚΕΣ
ΣΠΑΝΙΑ					
ΑΠΙΘΑΝΟ					
ΠΙΘΑΝΟΝ					

ΠΟΛΥ ΠΙΘΑΝΟ					
ΣΙΓΟΥΡΟ					

Πίνακας 7.9 : Πίνακας κινδύνων για τα ευαίσθητα δεδομένα της εταιρείας

ΣΤΟΙΧΕΙΑ ΜΕΤΡΗΤΩΝ					
ΣΥΝΕΠΕΙΕΣ ΠΙΘΑΝΟΤΗΤΑ	ΑΣΗΜΑΝΤΕΣ	ΜΙΚΡΕΣ	ΜΕΤΡΙΕΣ	ΣΟΒΑΡΕΣ	ΚΑΤΑΣΤΡΟΦΙΚΕΣ
ΣΠΑΝΙΑ					
ΑΠΙΘΑΝΟ					
ΠΙΘΑΝΟΝ					
ΠΟΛΥ ΠΙΘΑΝΟ					
ΣΙΓΟΥΡΟ					

Πίνακας 7.10 : Πίνακας κινδύνων για τα στοιχεία των μετρητών

ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΈΝΑ					
ΣΥΝΕΠΕΙΕΣ ΠΙΘΑΝΟΤΗΤΑ	ΑΣΗΜΑΝΤΕΣ	ΜΙΚΡΕΣ	ΜΕΤΡΙΕΣ	ΣΟΒΑΡΕΣ	ΚΑΤΑΣΤΡΟΦΙΚΕΣ
ΣΠΑΝΙΑ					
ΑΠΙΘΑΝΟ					
ΠΙΘΑΝΟ					
ΠΟΛΥ ΠΙΘΑΝΟ					
ΣΙΓΟΥΡΟ					

Πίνακας 7.11 : Πίνακας κινδύνων για τα προσωπικά δεδομένα

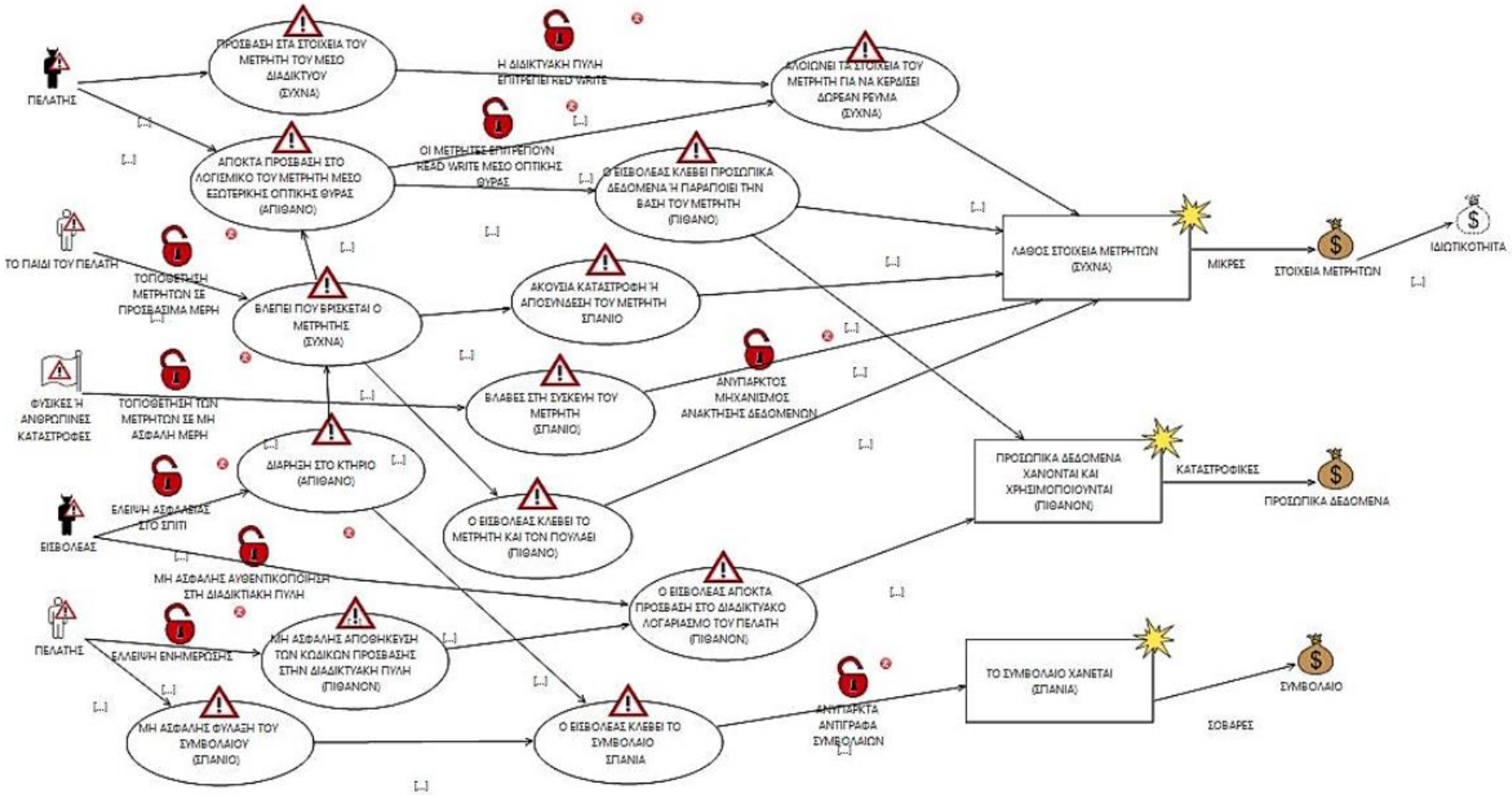
ΣΥΜΒΟΛΑΙΟ ΠΑΡΟΧΗΣ ΥΠΗΡΕΣΙΩΝ		
ΣΥΝΕΠΕΙΕΣ ΠΙΘΑΝΟΤΗΤΑ	ΑΣΗΜΑΝΤΕΣ	ΣΟΒΑΡΕΣ
ΣΠΑΝΙΑ		
ΑΠΙΘΑΝΟ		
ΠΙΘΑΝΟ		
ΠΟΛΥ ΠΙΘΑΝΟ		
ΣΙΓΟΥΡΟ		

Πίνακας 7.12: Πίνακας κινδύνων συμβολαίου παροχής υπηρεσιών

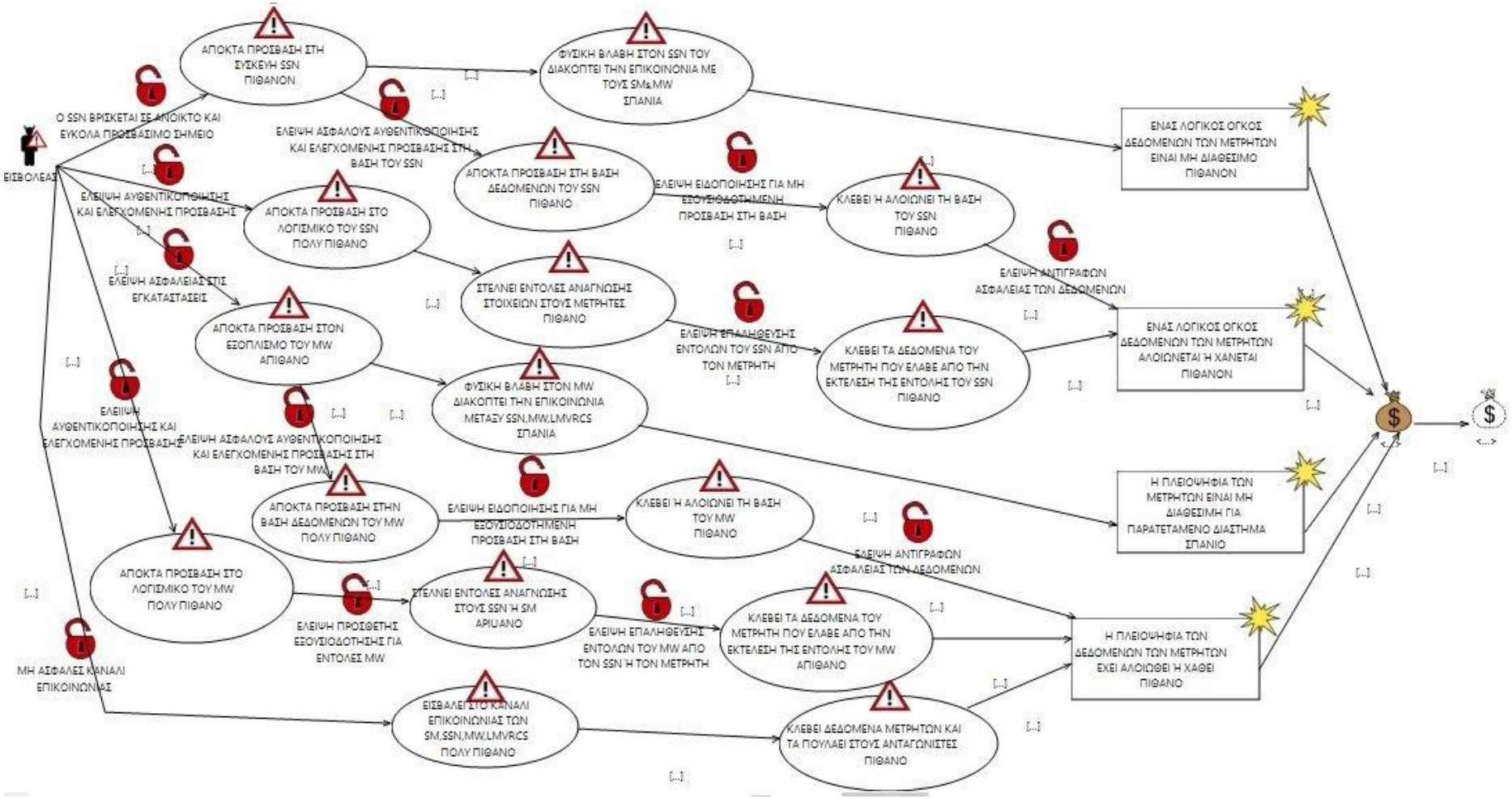
7.1.5 Αναγνώριση κινδύνων με χρήση διαγραμμάτων απειλών (βήμα 5)

Έχοντας αναγνωρίσει τα περιουσιακά στοιχεία και τα βασικά ανεπιθύμητα περιστατικά προχωράμε στην αναγνώριση των κινδύνων. Με τα διαγράμματα απειλών φαίνεται η πηγή της απειλής και οι πιθανές συνέπειες που θέτουν σε κίνδυνο ένα ή περισσότερα περιουσιακά στοιχεία. Στη συνέχεια εντοπίζονται οι ευπάθειες που επιτρέπουν να συμβούν τα ανεπιθύμητα περιστατικά και οδηγούν στον κίνδυνο. Το διάγραμμα απειλών θα το χωρίσουμε σε 3 μέρη:

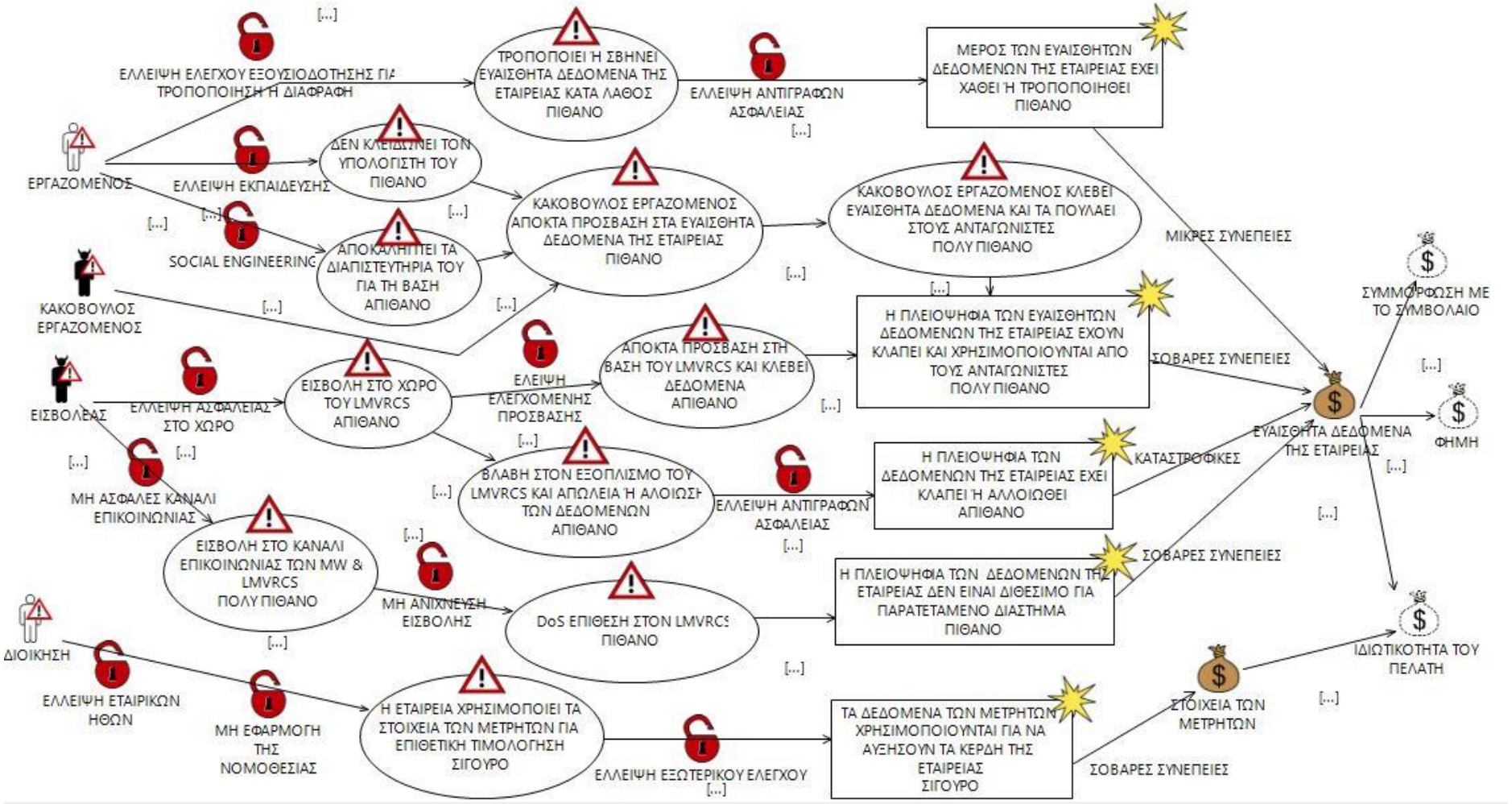
- Σε αυτό με τις ευπάθειες από πλευράς του καταναλωτή.
- Σε αυτό με τις ευπάθειες στους SSN και MW.
- Σε αυτό με τις ευπάθειες στον LMVRCS.



Σχήμα 7.2: Διάγραμμα απειλών από πλευράς καταναλωτή.



Σχήμα 7.3: Διάγραμμα απειλών από πλευράς SSN,MW.



Σχήμα 7.4 :Διάγραμμα απειλών από πλευράς του LMVRCS.

7.1.6 Υπολογισμός πιθανότητας κινδύνου (βήμα 6)

Πηγή απειλής	**Σενάριο**	**Πιθανότητα απειλής**	**Ανεπιθύμητα συμβάντα**	**Κίνδυνος**	**Πιθανότητα κινδύνου**	**Συνέπειες**	**Περιουσιακό στοιχείο**
Πελάτης	Αλλάζει τα δεδομένα του μετρητή για να κερδίσει δωρεάν ενέργεια.	Πολύ πιθανό	Κάποια στοιχεία των μετρητών είναι λανθασμένα , χαμένα ή κλεμμένα.	MR1	Πολύ πιθανό	Μικρές	Στοιχεία μετρητών
Πελάτης (όχι σκόπιμα)	Χαλάει ή απενεργοποιεί τη συσκευή του μετρητή.	Σπάνια					
Φυσική ή ανθρώπινη καταστροφή	Καταστρέφει τη συσκευή του μετρητή.	Σπάνια					
Εισβολέας	Κλέβει τη συσκευή του μετρητή και την πουλάει.						
	Κλέβει δεδομένα του μετρητή για να αντλήσει προσωπικές πληροφορίες	Πιθανό					

	Φυσική βλάβη στον εξοπλισμό του SSN.	Σπάνια	Μέρος των δεδομένων των μετρητών είναι μη διαθέσιμα.	MR2	Απίθανο	Μέτριες συνέπειες.	
	Αποκτά πρόσβαση στη βάση του SSN και κλέβει ή αλλοιώνει δεδομένα.	Πιθανό	Μέρος των δεδομένων των μετρητών έχει χαθεί ή αλλοιωθεί.	MR3	Πιθανό	Μέτριες	
	Στέλνει εντολές ανάγνωσης στοιχείων του μετρητή και κλέβει δεδομένα.	Πιθανό					
	Φυσική βλάβη στον εξοπλισμό του MW.	Σπάνια	Η πλειοψηφία των δεδομένων των μετρητών είναι μη διαθέσιμη.	MR4	Πιθανόν	Σοβαρές	

	Αποκτά πρόσβαση στη βάση του MW και κλέβει ή αλλοιώνει δεδομένα.	Πολύ πιθανό	Η πλειοψηφία των δεδομένων των μετρητών έχει χαθεί ή αλλοιωθεί.	MR5	Πολύ πιθανό	Καταστροφικές	
	Στέλνει εντολές ανάγνωσης στον SSN και κλέβει δεδομένα.	Πολύ πιθανό					
	Εισβάλει στο κανάλι επικοινωνίας και κλέβει δεδομένα.	Σίγουρο					
	Αποκτά πρόσβαση στον LMVRCS και κλέβει ευαίσθητα δεδομένα της εταιρείας.	Πολύ πιθανό	Η πλειοψηφία των δεδομένων της εταιρείας έχουν κλαπεί και χρησιμοποιούνται από τους ανταγωνιστές	BR1	Πολύ πιθανό	Σοβαρές	Ευαίσθητα δεδομένα εταιρείας

Κακόβουλος εργαζόμενος.	Αποκτά πρόσβαση στα ευαίσθητα δεδομένα της εταιρείας και τα κλέβει για να τα πουλήσει.	Πιθανό					
Εισβολέας	Φυσική βλάβη τον εξοπλισμό του LMVRCS που προκαλεί αλλοίωση και απώλεια δεδομένων.	Απίθανο	Η πλειοψηφία των ευαίσθητων δεδομένων της εταιρείας χάνεται ή αλλοιώνεται.	BR2	Απίθανο	Καταστροφικές	
	DoS επίθεση στον LMVRCS.	Πιθανό	Η πλειοψηφία των ευαίσθητων δεδομένων δεν είναι διαθέσιμα.	BR3	Απίθανο	Σοβαρές	
	Κλέβει προσωπικά δεδομένα μέσω των μετρητών.	Πιθανό	Προσωπικά δεδομένα έχουν κλαπεί για παράνομη χρήση.	PR1	Πιθανό	Καταστροφικές	Ιδιωτικότητα
	Κλέβει προσωπικά δεδομένα από την διαδικτυακή πύλη.	Πιθανό					

	Κλέβει το συμβόλαιο παροχής υπηρεσιών.	Σπάνια	Το συμβόλαιο έχει χαθεί και δεν μπορεί να ανακτηθεί.	SR1	Σπάνια	Σοβαρές	Συμβόλαιο
Εργαζόμενος (όχι σκόπιμα)	Τροποποιεί ή διαγράφει ευαίσθητα δεδομένα της εταιρείας.	Πιθανό	Μέρος των δεδομένων της εταιρείας τροποποιείται ή χάνεται.	BR4	Πιθανό	Μικρές	Ευαίσθητα δεδομένα της εταιρείας
Πρόεδρος / Διοίκηση εταιρείας	Χρήση των στοιχείων των μετρητών για επιθετική τιμολόγηση.	Σίγουρο	Τα δεδομένα των μετρητών χρησιμοποιούνται για αύξηση των εσόδων της εταιρείας.	MR6	Σίγουρο	Σοβαρές	

Πίνακας7. 13: Πίνακας υπολογισμού κινδύνου

7.1.7 Αποτίμηση κινδύνου (βήμα 7)

Σε αυτό το βήμα αναγνωρίζουμε τους κινδύνους που χρειάζονται αντιμετώπιση, βασιζόμενοι στην υπολογισμό κινδύνων από το προηγούμενο βήμα.

ΠΙΝΑΚΑΣ ΑΠΟΤΙΜΗΣΗΣ ΚΙΝΔΥΝΩΝ – ΕΥΑΙΣΘΗΤΑ ΔΕΔΟΜΕΝΑ ΕΤΑΙΡΕΙΑΣ					
ΣΥΝΕΠΕΙΕΣ ΠΙΘΑΝΟΤΗΤΑ	ΑΣΗΜΑΝΤΕΣ	ΜΙΚΡΕΣ	ΜΕΤΡΙΕΣ	ΣΟΒΑΡΕΣ	ΚΑΤΑΣΤΡΟΦΙΚΕΣ
ΣΠΑΝΙΑ					
ΑΠΙΘΑΝΟ					**BR2**
ΠΙΘΑΝΟΝ		**BR4**		**BR3**	
ΠΟΛΥ ΠΙΘΑΝΟ				**BR1**	
ΣΙΓΟΥΡΟ					

Πίνακας7. 14: ΠΙΝΑΚΑΣ ΑΠΟΤΙΜΗΣΗΣ ΚΙΝΔΥΝΩΝ

ΠΙΝΑΚΑΣ ΑΠΟΤΙΜΗΣΗΣ ΚΙΝΔΥΝΩΝ – ΔΕΔΟΜΕΝΑ ΜΕΤΡΗΤΩΝ					
ΣΥΝΕΠΕΙΕΣ/ ΠΙΘΑΝΟΤΗΤΑ	ΑΣΗΜΑΝΤΕΣ	ΜΙΚΡΕΣ	ΜΕΤΡΙΕΣ	ΣΟΒΑΡΕΣ	ΚΑΤΑΣΤΡΟΦΙΚΕΣ
ΣΠΑΝΙΑ					
ΑΠΙΘΑΝΟ			**MR2**		
ΠΙΘΑΝΟΝ			**MR3**	**MR4**	
ΠΟΛΥ ΠΙΘΑΝΟ		**MR1**			**MR5**
ΣΙΓΟΥΡΟ					**MR6**

Πίνακας 7.15: ΠΙΝΑΚΑΣ ΑΠΟΤΙΜΗΣΗΣ ΚΙΝΔΥΝΩΝ

ΠΙΝΑΚΑΣ ΑΠΟΤΙΜΗΣΗΣ ΚΙΝΔΥΝΩΝ – ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ					
ΣΥΝΕΠΕΙΕΣ/ ΠΙΘΑΝΟΤΗΤΑ	ΑΣΗΜΑΝΤΕΣ	ΜΙΚΡΕΣ	ΜΕΤΡΙΕΣ	ΣΟΒΑΡΕΣ	ΚΑΤΑΣΤΡΟΦΙΚΕΣ
ΣΠΑΝΙΑ					
ΑΠΙΘΑΝΟ					
ΠΙΘΑΝΟΝ					**PR1**
ΠΟΛΥ ΠΙΘΑΝΟ					
ΣΙΓΟΥΡΟ					

Πίνακας7. 16: ΠΙΝΑΚΑΣ ΑΠΟΤΙΜΗΣΗΣ ΚΙΝΔΥΝΩΝ

ΠΙΝΑΚΑΣ ΑΠΟΤΙΜΗΣΗΣ ΚΙΝΔΥΝΩΝ – ΣΥΜΒΟΛΑΙΟ		
ΣΥΝΕΠΕΙΕΣ ΠΙΘΑΝΟΤΗΤΑ	ΑΣΗΜΑΝΤΕΣ	ΣΟΒΑΡΕΣ
ΣΠΑΝΙΑ		**SR1**
ΑΠΙΘΑΝΟ		
ΠΙΘΑΝΟΝ		
ΠΟΛΥ ΠΙΘΑΝΟ		
ΣΙΓΟΥΡΟ		

Πίνακας 7.17: ΠΙΝΑΚΑΣ ΑΠΟΤΙΜΗΣΗΣ ΚΙΝΔΥΝΩΝ

Στον παρακάτω πίνακα αναγράφονται οι κίνδυνοι που πρέπει να μετριαστούν.

Κίνδυνος	**Προέλευση απειλής**	**Αποτίμηση**
BR1	Εργαζόμενος (κακόβουλος) , Εισβολέας	Μετριασμός
BR2	Εισβολέας	Μετριασμός
BR3	Εισβολέας	Μετριασμός
BR4	Εργαζόμενος (όχι σκόπιμα)	Έλεγχος
MR1	Πελάτης (όχι σκόπιμα), Εισβολέας, Φυσικές ή ανθρώπινες καταστροφές	Έλεγχος
MR2	Εισβολέας	Έλεγχος
MR3	Εισβολέας	Έλεγχος
MR4	Εισβολέας	Μετριασμός
MR5	Εισβολέας	Μετριασμός
MR6	Πρόεδρος εταιρείας	Μετριασμός
PR1	Εισβολέας	Μετριασμός

Πίνακας7. 18: ΚΙΝΔΥΝΟΙ ΠΟΥ ΠΡΕΠΕΙ ΝΑ ΑΝΤΙΜΕΤΩΠΙΣΤΟΥΝ

7.1.8 Αντιμετώπιση κινδύνου (βήμα 8)

Σε αυτό το βήμα περιγράφονται μέτρα για την αντιμετώπιση των κινδύνων που πρέπει να μετριαστούν ή να αντιμετωπιστούν. Στον πίνακα 18 φαίνονται όλα τα μέτρα για τις εντοπισμένες ευπάθειες καθώς και ο στόχος των μέτρων και η πηγή της απειλής. Εδώ παρέχονται μέτρα και για τους κινδύνους που πρέπει να μετριαστούν και για τους

κινδύνους που πρέπει να είναι ελεγχόμενοι. Η διαφορά μεταξύ τους είναι ότι για τους κινδύνους που πρέπει να είναι ελεγχόμενοι εφαρμόζουμε κάποια από τα μέτρα ενώ για αυτούς που πρέπει να μετριαστούν εφαρμόζουμε όλα τα εφικτά μέτρα.

Στον πίνακα οι κίνδυνοι με χρώμα κίτρινο είναι αυτοί που πρέπει να είναι ελεγχόμενοι και με κόκκινο αυτοί που πρέπει να μετριαστούν.

Κίνδυνος	**Μέτρα αντιμετώπισης**	**Στόχος μέτρων**	**Πηγή απειλής**
MR1	Αυθεντικοποίηση για πρόσβαση στους έξυπνους μετρητές μέσω οπτικής θύρας.	Οπτική θύρα έξυπνων μετρητών	Πελάτης (σκόπιμα) Εισβολέας
	Τοποθέτηση των SMs σε ψηλό σημείο μακριά από εύφλεκτα αντικείμενα. Οι SMs να τηρούν αντίγραφα ασφάλειας δεδομένων.	SM's τοποθεσία. SM's λογισμικό.	Φυσική / ανθρώπινη καταστροφή Ο πελάτης (όχι σκόπιμα) Εισβολέας
MR2	Τοποθέτηση των SSN σε ασφαλές μέρος.	Τοποθεσία εξοπλισμού SSNs.	Εισβολέας
MR3	Αυθεντικοποίηση και ελεγχόμενη πρόσβαση στα δεδομένα. Ειδοποίηση για μη εξουσιοδοτημένη πρόσβαση στη βάση του SSN. Τακτική λήψη αντιγράφων ασφαλείας των δεδομένων.	Βάση δεδομένων των SSN's	Εισβολέας

	Αυθεντικοποίηση για πρόσβαση στο λογισμικό των SSN's. Επαλήθευση και έλεγχος εγκυρότητας των εντολών για ανάγνωση δεδομένων των μετρητών.	Λογισμικό των SSN's	Εισβολέας
MR4	Τοποθέτηση του MW σε ασφαλές μέρος.	Εξοπλισμός MW	Εισβολέας
MR5	Αυθεντικοποίηση και ελεγχόμενη πρόσβαση στα δεδομένα. Ειδοποίηση για μη εξουσιοδοτημένη πρόσβαση στη βάση του MW. Τακτική λήψη αντιγράφων ασφαλείας.	Βάση δεδομένων του MW	Εισβολέας
	Αυθεντικοποίηση για πρόσβαση στο λογισμικό του MW. Επαλήθευση και έλεγχος εγκυρότητας των εντολών για ανάγνωση δεδομένων των μετρητών.	Λογισμικό του MW	Εισβολέας
	Χρήση ασφαλούς καναλιού επικοινωνίας.	Κανάλι επικοινωνίας	Εισβολέας
MR6	Υιοθέτηση και επιβολή επιχειρηματικών ηθών. Συμμόρφωση με την ισχύουσα νομοθεσία για την προστασία των προσωπικών δεδομένων των πελατών. Διενέργεια τακτικών εξωτερικών ελέγχων.	Διοίκηση της εταιρείας	Διοίκηση της εταιρείας (όχι σκόπιμα)

BR1	Πολιτικές για την αντιμετώπιση του social engineering. Τακτικοί εσωτερικοί έλεγχοι.	Πολιτικές ασφάλειας της εταιρείας. Βάση δεδομένων του LMVRCS	Εργαζόμενος (κακόβουλος)
	Ελεγχόμενη πρόσβαση στη βάση δεδομένων του LMVRCS.		Εισβολέας
BR2	Φυσική φύλαξη του χώρου και τοποθέτηση κάμερας στον χώρο που φιλοξενεί τον εξοπλισμό του LMVRCS. Τακτική λήψη αντιγράφων ασφαλείας.	Τοποθεσία LMVRCS	Εισβολέας
BR3	Χρήση ασφαλούς καναλιού επικοινωνίας. Χρήση firewall και συστήματος ανίχνευσης εισβολής.	Κανάλι επικοινωνίας.	Εισβολέας
BR4	Μόνο εξουσιοδοτημένοι χρήστες μπορούν να τροποποιούν ή να διαγράφουν δεδομένα. Εκπαίδευση υπαλλήλων σε θέματα ασφάλειας. Τακτική λήψη αντιγράφων ασφάλειας.	Λογισμικό LMVRCS Εργαζόμενοι στην εταιρεία κοινής ωφέλειας.	Εργαζόμενος (όχι σκόπιμα)
PR1	Αυθεντικοποίηση στην πρόσβαση στους SM μέσω οπτικής θύρας.	Οπτική θύρα SM.	Εισβολέας
	Αυθεντικοποίηση χρήστη για είσοδο στη διαδικτυακή πύλη.	Διαδικτυακή πύλη	Εισβολέας

Πίνακας7. 19: ΚΙΝΔΥΝΟΙ ΚΑΙ ΑΝΤΙΜΕΤΩΠΙΣΗ ΤΟΥΣ

7.2 Απαιτήσεις ασφάλειας

Βασιζόμενοι στην αποτίμηση των κινδύνων και στην αντιμετώπιση τους , προσδιορίζουμε τις απαιτήσεις ασφάλειας.

SREQ1: διασφάλιση ακεραιότητας και διαθεσιμότητας των δεδομένων των SMs και των ευαίσθητων δεδομένων της εταιρείας.

SREQ2: διασφάλιση της εμπιστευτικότητας των προσωπικών δεδομένων και των ευαίσθητων δεδομένων της εταιρείας.

SREQ3: διασφάλιση ασφαλούς επικοινωνίας μεταξύ των SM, SSN, MW, LMVRCS.

SREQ4: διασφάλιση ότι δεν θα εξαχθούν σημαντικά δεδομένα από τα μηνύματα που ανταλλάσσονται μεταξύ των SM, SSN, MW, LMVRCS από τρίτο μέρος.

SREQ5: διασφάλιση ότι δεν θα υπάρχει μη εξουσιοδοτημένη πρόσβαση στα ευαίσθητα δεδομένα της εταιρείας και στα δεδομένα των SMs.

SREQ6: διασφάλιση ότι τα εξουσιοδοτημένα μέρη μπορούν να μεταβάλουν μόνο στοιχεία για τα οποία έχουν εξουσιοδότηση.

SREQ7: διασφάλιση φυσικού εξοπλισμού των SM, SSN, MW, LMVRCS.

SREQ8: διασφάλιση προστασίας λογισμικού των SM, SSN, MW, LMVRCS από αλλοιώσεις.

SREQ9: διασφάλιση ότι η άντληση των στοιχείων των μετρητών προορίζεται μόνο για την προβλεπόμενη από το συμβόλαιο με τον καταναλωτή χρήση.

Στον πίνακα 20 φαίνονται οι συσχετίσεις μεταξύ των απαιτήσεων ασφαλείας και των κινδύνων.

Περιουσιακά Στοιχεία	SREQ / Risks	SREQ1	SREQ2	SREQ3	SREQ4	SREQ5	SREQ6	SREQ7	SREQ8	SREQ9
Στοιχεία Μετρητών	MR1	x				x	x	x		
	MR2	x						x		
	MR3	x				x			x	
	MR4	x						x		
	MR5	x		X	x	x			x	
	MR6									x
Ευαίσθητα Δεδομένα Εταιρείας	BR1		x			x	x			
	BR2	x						x		
	BR3	x		X						
	BR4	x					x			
Προσωπικά Δεδομένα	FR1		x			x		x		

Πίνακας7. 20: ΣΥΣΧΕΤΙΣΕΙΣ ΑΠΑΙΤΗΣΕΩΝ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΚΙΝΔΥΝΩΝ

7.3 Μέτρα ασφάλειας

Τα μέτρα ασφάλειας διαχωρίζονται ανάλογα με το που εφαρμόζονται. Στον πίνακα 21 φαίνονται οι σχέσεις μεταξύ των μέτρων ασφάλειας και των απαιτήσεων ασφάλειας.

- Μέτρα στο διαχειριστικό τμήμα της εταιρείας.

CR1: η εταιρεία πρέπει να έχει καθορίσει πολιτική ασφάλειας αναφορικά με το τρόπο που χρησιμοποιούν οι εργαζόμενοι τα στοιχεία των SMs και τα ευαίσθητα δεδομένα.

CR2: η εταιρεία πρέπει να διαθέτει υπεύθυνο διαχείρισης ζητημάτων ασφάλειας για να εξασφαλίσει ότι οι εργαζόμενοι, οι εξωτερικοί συνεργάτες και τα τρίτα μέρη συμμορφώνονται με την πολιτική ασφάλειας της εταιρείας.

CR3: η εταιρεία πρέπει να διενεργεί ελέγχους σχετικά με την χρήση των ευαίσθητων δεδομένων της εταιρείας και των δεδομένων των μετρητών.

CR4: όλοι οι εργαζόμενοι πρέπει να εκπαιδεύονται σε ζητήματα ασφάλειας για να αναβαθμίζουν τις σχετικές γνώσεις τους.

- Μέτρα στη ασφάλεια του εξοπλισμού των SM,SSN,MW,LMVRCS

CR5: οι έξυπνοι μετρητές πρέπει να τοποθετούνται σε ψηλό κοντινό μέρος στην περιοχή του καταναλωτή μακριά από εύφλεκτα αντικείμενα. Αυτές οι οδηγίες πρέπει να περιλαμβάνονται στον οδηγό εγκατάστασης.

CR6: ο SSN πρέπει να τοποθετείται σε μέρος δυσπρόσιτο μακριά από πολυκοσμία και θα πρέπει να παρακολουθείται με κάμερα.

CR7: ο MW πρέπει να τοποθετείται σε μέρος δυσπρόσιτο μακριά από πολυκοσμία, θα πρέπει να παρακολουθείται με κάμερα και να διατίθεται σύστημα συναγερμού σε περίπτωση εισβολής στην περιοχή.

CR8: οι SM, SSN, MW πρέπει να προστατεύονται από φυσικά φαινόμενα και από μη εξουσιοδοτημένη πρόσβαση.

CR9: το LMVRCS πρέπει να βρίσκεται σε ασφαλές μέρος εντός των κτιριακών εγκαταστάσεων με προσωπικό ασφάλειας, κάμερα και σύστημα συναγερμού.

- Μέτρα στην βάση δεδομένων

CR10: η ομάδα διαχείρισης ασφάλειας πρέπει να παρέχει κωδικούς αυθεντικοποίησης χρηστών και συστημάτων που προσπελαύνουν τις βάσεις δεδομένων των SM, SSN, MW οι οποίοι θα αλλάζουν σε τακτική βάση.

CR11: δεν πρέπει να επιτρέπεται μεταβολή ή αντιγραφή των στοιχείων της βάσης των μετρητών εκτός από τους SSN, MW.

CR12: δεν πρέπει να επιτρέπεται μεταβολή ή αντιγραφή των στοιχείων της βάσης των SSNs εκτός από το MW.

CR13: δεν πρέπει να επιτρέπεται μεταβολή ή αντιγραφή των στοιχείων της βάσης των MWs εκτός από το LMVRCS.

CR14: θα πρέπει να εφαρμόζεται Role Based Access Control για πρόσβαση στα δεδομένα των SM, SSN, MW, LMVRCS.

CR15: οι SM, SSN, MW πρέπει να διαθέτουν σύστημα ελέγχου εφεδρείας των δεδομένων τους και επιπλέον ο SSN να ελέγχει τα δεδομένα που λαμβάνει από τον SM και ο MW αυτά που λαμβάνει από τον SSN.

CR16: ο SM πρέπει να ενημερώνει τον SSN εάν αλλοιωθούν δεδομένα και ο SSN το προωθεί στο MW και ο MW στο LMVRCS.

CR17: ο SSN πρέπει να ενημερώνει το MW εάν αλλοιωθούν δεδομένα και το MW το προωθεί στο LMVRCS.

CR18: το MW πρέπει να ενημερώνει το LMVRCS εάν αλλοιωθούν δεδομένα.

CR19: το MW πρέπει να κρατάει backup των στοιχείων των μετρητών που λαμβάνει από τον SSN, για την περίπτωση που αλλοιωθούν δεδομένα στον SM ή στον SSN.

CR20: το LMVRCS πρέπει να κρατάει backup των στοιχείων των μετρητών που λαμβάνει από τον MW για την περίπτωση που αλλοιωθούν δεδομένα MW.

CR21: το LMVRCS πρέπει να κρατάει backup των ευαίσθητων δεδομένων της εταιρείας. Η λήψη backup θα είναι αυτοματοποιημένη και δεν θα μπορεί κανένας χρήστης ή σύστημα να μεταβάλει δεδομένα του backup.

CR22: το LMVRCS δεν πρέπει να επιτρέπει τροποποίηση ή διαγραφή μεγαλύτερη του 10% του όγκου της βάσης δεδομένων χωρίς ειδική έγκριση από manager.

- Μέτρα στο λογισμικό των SM, SSN, MW, LMVRCS

CR23: το λογισμικό των SN, SSN, MW πρέπει να απαιτεί κωδικό πρόσβασης από τους εξουσιοδοτημένους χρήστες και συστήματα. Τους κωδικούς πρόσβασης τους διαχειρίζεται το LMVRCS και πρέπει να αλλάζονται σε τακτική περιοδική βάση.

CR24: η πρόσβαση στους έξυπνους μετρητές θα πρέπει να γίνεται με κωδικό που θα δίνεται από την εταιρεία στους τεχνικούς και θα πρέπει να αλλάζει τακτικά. Η αλλαγή του κωδικού πρόσβασης στους μετρητές θα περνάει από το LMNVRCS στο MW και θα γίνεται remotely από το MW.

CR25: οι μετρητές θα επαληθεύουν τις εντολές για ανάγνωση των δεδομένων από τους SSN με ψηφιακές υπογραφές.

CR26: ο SSN δεν πρέπει να μπορεί να στέλνει από μόνος του εντολές ανάγνωσης προς τον μετρητή αλλά μόνο μέσω του MW.

CR27: το MW δεν πρέπει να μπορεί να στέλνει από μόνος του εντολές ανάγνωσης προς τον μετρητή αλλά μόνο μέσω του LMVRCS.

CR28: όταν ο SSN λαβαίνει εντολή από το MW θα πρέπει να ελέγχει ότι έχει ξεκινήσει από το LMVCRS.

CR29: ο LMVRCS δεν πρέπει να μπορεί να στέλνει τυχαίας συχνότητας αιτήματα ανάγνωσης από τους μετρητές παρά μόνο με έγκριση αρμόδιου υπευθύνου από την εταιρεία.

CR30: ο LMVRCS πρέπει να μπορεί να στέλνει αιτήματα ανάγνωσης απευθείας ακόμα κι αν οι SSN, MW είναι εκτός λειτουργίας ή χωρίς σύνδεση.

- Μέτρα στην επικοινωνία μεταξύ των SM,SSN,MW,IMVRCS

CR31: όλες οι επικοινωνίες των SM, SSN, MW, LMVRCS θα χρησιμοποιούν TLS (Transport Layer Security) πρωτόκολλο.

CR32: όλα τα μηνύματα που ανταλλάσσονται μεταξύ των SM, SSN, MW, LMVRCS πρέπει να είναι κρυπτογραφημένα.

SREQ / Control ID	SREQ1	SREQ2	SREQ3	SREQ4	SREQ5	SREQ6	SREQ7	SREQ8	SREQ9	Risk ID
CR1		X							X	MR6,BR1
CR2		X							X	MR6
CR3		X							X	MR6,BR1
CR4	X	X				X				BR1,BR4
CR5	X						X			MR1
CR6	X						X			MR2
CR7	X						X			MR4
CR8	X						X			MR2,MR4
CR10	X				X					MR3,MR5,BR1
CR11		X			X					MR1,PR1
CR12	X				X					MR3
CR13	X				X					MR5
CR14					X	X				MR1,MR3,MR5,BR1
CR15	X									MR1,MR3,MR5
CR16	X									MR1
CR17	X									MR3
CR18	X									MR5
CR19	X									MR1
CR20	X									MR5
CR21	X							X		BR2,BR4
CR23								X		MR3,MR5
CR24					X					MR1,PR1
CR25								X		MR3
CR26								X		MR3
CR27								X		MR5
CR28								X		MR5
CR29			X					X		MR5
CR31			X	X						BR3,MR5
CR32				X						MR5
CR33					X					PR1
CR34						X				MR1,PR1
CR35						X				MR1,PR1
CR9							X			BR2
CR22	X					X				BR4
CR30	X									MR2,MR4

Πίνακας7. 21: Σχέση των μέτρων αντιμετώπισης των απαιτήσεων και του περιορισμού των κινδύνων

- Μέτρα στην διαδικτυακή πύλη.

CR33: η είσοδος των χρηστών θα γίνεται με διαπιστευτήρια που θα παρέχει η εταιρεία μετά την υπογραφή του συμβολαίου.

CR34: οι χρήστες δεν θα πρέπει να έχουν δικαίωμα να μεταβάλλουν το περιεχόμενο του συμβολαίου, τις ενδείξεις του μετρητή ή στοιχεία λογαριασμών μέσω του portal.

CR35: οι πελάτες θα μπορούν μόνο να αλλάζουν το προφίλ του μέσω του portal μετά από σχετική επιβεβαίωση από το service contact center της εταιρείας και προτού γίνει η οριστική αλλαγή στη βάση του LMVCRS.

Παρακάτω φαίνεται πως τα μέτρα αντιμετώπισης μειώνουν τους κινδύνους για κάθε περιουσιακό στοιχείο. Στους κινδύνους που είναι ελεγχόμενοι δεν θα εφαρμοστούν όλα τα μέτρα ασφάλειας αλλά μόνο για τα πιο επικίνδυνα σενάρια.

BR1: Η πλειοψηφία των ευαίσθητων δεδομένων της εταιρείας έχει κλαπεί και έχει διαρρεύσει στον ανταγωνισμό. Εφαρμόσιμα μέτρα : CR1, CR2, CR3, CR4, CR10, CR14.

Στόχος είναι να γίνουν όλοι οι κίνδυνοι ελεγχόμενοι και να μεταπέσουν σε αποδεκτά επίπεδα. Στους κινδύνους που πρέπει να μετριαστούν εφαρμόζονται όλα τα μέτρα ασφάλειας που μπορούν να εφαρμοστούν από την εταιρεία.

Τα μέτρα εφαρμόζονται για να μετριαστεί ο κίνδυνος και να μετατρέψουμε την πιθανότητα συμβάντος από πιθανή σε απίθανη και την κατηγορία των συνεπειών από σοβαρές σε ασήμαντες. Πρέπει να εξασφαλιστεί ότι η εταιρεία διαθέτει ισχυρή πολιτική ασφάλειας σε ότι αφορά τους εργαζόμενους και ότι όλοι οι εργαζόμενοι εκπαιδεύονται σχετικά. Η μείωση του βαθμού των συνεπειών επιτυγχάνεται διασφαλίζοντας αφενός ότι η λειτουργία αντιγραφής από τη βάση δεδομένων δεν είναι εφικτή από χρήστες ή μη εξουσιοδοτημένα συστήματα και αφετέρου με το ότι η εταιρεία θα διενεργεί τακτικούς εσωτερικούς ελέγχους.

BR2: Η πλειοψηφία των ευαίσθητων δεδομένων της εταιρείας χάνεται ή αλλοιώνεται. Εφαρμόσιμα μέτρα : CR9, CR21.

Στόχος είναι να μετριαστεί η πιθανότητα από απίθανη σε σπάνια και οι συνέπειες από καταστροφικές σε ασήμαντες.

Αυτό εξασφαλίζεται με την φύλαξη του εξοπλισμού του MW, την παρακολούθηση του με κάμερες ασφάλειας και την εγκατάσταση συστήματος συναγερμού, καθώς και με την τακτική λήψη αντιγράφων ασφαλείας στα δεδομένα του MW.

BR3: Η πλειοψηφία των ευαίσθητων δεδομένων της εταιρείας είναι μη διαθέσιμο για παρατεταμένο χρονικό διάστημα. Εφαρμόσιμα μέτρα : CR29.

Τα μέτρα εφαρμόζονται για να μειωθεί η πιθανότητα από πιθανή σε σπάνια και οι συνέπειες από σοβαρές σε ασήμαντες.

BR4: Μέρος των ευαίσθητων δεδομένων της εταιρείας τροποποιείται ή χάνεται. Εφαρμόσιμα μέτρα : CR22, CR25, CR21.

Τα μέτρα CR22, CR25 εφαρμόζονται για να μειωθεί η πιθανότητα από πολύ πιθανή σε απίθανη και οι συνέπειες από σοβαρές σε ασήμαντες. Το LMVRCS δεν θα πρέπει να επιτρέπει την μεταβολή ή διαγραφή μεγαλύτερου μέρους από το 10% των δεδομένων , ανά χρήστη και ανά εντολή και με κατάλληλη εκπαίδευση του προσωπικού η πιθανότητα λάθους στη βάση δεδομένων από του χρήστες, μειώνεται πάρα πολύ.

ΠΙΝΑΚΑΣ ΑΠΟΤΙΜΗΣΗΣ ΚΙΝΔΥΝΩΝ – ΕΥΑΙΣΘΗΤΑ ΔΕΔΟΜΕΝΑ ΕΤΑΙΡΕΙΑΣ ΜΕΤΑ ΤΟΥΣ ΕΛΕΓΧΟΥΣ					
ΣΥΝΕΠΕΙΕΣ	ΑΣΗΜΑΝΤΕΣ	ΜΙΚΡΕΣ	ΜΕΤΡΙΕΣ	ΣΟΒΑΡΕΣ	ΚΑΤΑΣΤΡΟΦΙΚΕΣ
ΠΙΘΑΝΟΤΗΤΑ					
ΣΠΑΝΙΑ	BR3	BR2			
ΑΠΙΘΑΝΟ		BR1			BR2
ΠΙΘΑΝΟΝ	BR4	BR4		BR3	
ΠΟΛΥ ΠΙΘΑΝΟ				BR1	
ΣΙΓΟΥΡΟ					

Πίνακας7. 22: ΠΙΝΑΚΑΣ ΑΠΟΤΙΜΗΣΗΣ ΚΙΝΔΥΝΩΝ – ΕΥΑΙΣΘΗΤΑ ΔΕΔΟΜΕΝΑ ΕΤΑΙΡΕΙΑΣ

MR1: Μερικά δεδομένα των μετρητών είναι παραποιημένα ή έχουν χαθεί ή κλαπεί. Εφαρμόσιμα μέτρα CR5, CR11, CR14,CR16, CR19, CR24, CR34,CR35.

Εφαρμόζουμε τα μέτρα CR5, CR11, , CR24 και CR34 για να μειώσουμε την πιθανότητα από πιθανή σε απίθανη και τον CR19 για να μειώσουμε τις συνέπειες από

μικρές σε ασήμαντες. Αυτό επιτυγχάνεται διασφαλίζοντας ότι οι SM τοποθετούνται σε ασφαλές μέρος, ότι δεν επιτρέπονται οι ενέργειες write – copy στην βάση δεδομένων των SM, ότι μη εξουσιοδοτημένα άτομα δεν έχουν πρόσβαση στη βάση μέσω οπτικής θύρας και ότι οι καταναλωτές δεν μπορούν να αλλάξουν τα στοιχεία του μετρητή μέσω της διαδικτυακής πύλης.

MR2: Μεγάλο μέρος των δεδομένων των μετρητών είναι μη διαθέσιμα. Εφαρμόσιμα μέτρα CR6, CR8, CR30.

Με την εφαρμογή των CR6, CR39 μειώνουμε την πιθανότητα από απίθανη σε σπάνια και τις συνέπειες από μέτριες σε ασήμαντες. Αυτό επιτυγχάνεται τοποθετώντας τους εξοπλισμούς σε προστατευόμενες τοποθεσίες που σε κάποιες περιπτώσεις παρακολουθούνται με κάμερα και εξασφαλίζοντας ότι το LMVRCS μπορεί να αντλήσει δεδομένα απευθείας από τους SM ακόμα κι αν ο SSN είναι εκτός λειτουργίας ή εκτός σύνδεσης.

MR3: Μεγάλο μέρος των δεδομένων των μετρητών είναι παραποιημένα ή έχουν χαθεί ή κλαπεί. Εφαρμόσιμα μέτρα CR10, CR12, CR14, CR15,CR17,CR19,CR23,CR25,CR26.

Εφαρμόζοντας τα μέτρα CR14, CR19, CR23,CR26 μειώνουμε την πιθανότητα από πολύ πιθανή σε σπάνια εξασφαλίζοντας ότι δεν είναι εφικτή η μη εξουσιοδοτημένη πρόσβαση στη βάση και στο λογισμικό των SSNs και ότι ο SSN δεν μπορεί από μόνος του να υποβάλει αιτήματα ανάγνωσης στους SMs. Μειώνονται οι συνέπειες από μέτριες σε ασήμαντες εξασφαλίζοντας ότι τηρούνται τακτικά αντίγραφα ασφαλείας στα δεδομένα των SSNs.

MR4: Η πλειοψηφία των δεδομένων των μετρητών είναι μη διαθέσιμα. Εφαρμόσιμα μέτρα CR7, CR8, CR30.

Εφαρμόζοντας όλους τα μέτρα μειώνουμε την πιθανότητα από πολύ πιθανή σε σπάνια εξασφαλίζοντας ότι ο εξοπλισμός του MW είναι σε ασφαλές και παρακολουθούμενο μέρος που διαθέτει συναγερμό. Οι συνέπειες μειώνονται από σοβαρές σε πολύ μικρές διασφαλίζοντας ότι το LMVRCS μπορεί να αντλήσει απευθείας δεδομένα από τους SM όταν το MW είναι εκτός λειτουργίας ή σύνδεσης.

MR5: Η πλειοψηφία των δεδομένων των μετρητών είναι παραποιημένα ή έχουν χαθεί ή κλαπεί. Εφαρμόσιμα μέτρα CR10, CR13, CR14, CR15,CR18,CR20,CR23,CR27,CR28, CR29,CR31,CR32.

Εφαρμόζουμε όλους τα μέτρα για να μειωθεί η πιθανότητα από πιθανή σε απίθανη απαιτώντας αυθεντικοποίηση για πρόσβαση στη βάση του MW απαγορεύοντας τις ενέργειες write – copy στη βάση του MWκαι καθιερώνοντας πολιτική ελεγχόμενης πρόσβασης. Οι συνέπειες από καταστροφικές γίνονται ασήμαντες εξασφαλίζοντας τήρηση εφεδρικών δεδομένων από το MW και ειδοποίηση από ο LMVRCS όταν συμβεί αλλοίωση των δεδομένων, τηρώντας τακτικά αντίγραφα ασφάλειας στο MW και διασφαλίζοντας ότι το MW δεν μπορεί να στείλει μη εξουσιοδοτημένα αιτήματα ανάγνωσης δεδομένων στους SMs. Επιπλέον όλες οι επικοινωνίες μεταξύ των SM, SSN,MW, LMVRCS πρέπει να είναι μέσω ασφαλούς καναλιού και κρυπτογραφημένες.

MR6: Τα δεδομένα των μετρητών χρησιμοποιούνται για αύξηση των κερδών της εταιρείας. Εφαρμόσιμα μέτρα CR1, CR2, CR3.

Εφαρμόζοντας όλους τα μέτρα περιορίζουμε την πιθανότητα από βέβαιη σε απίθανη και τις συνέπειες από καταστροφικές σε μικρές εξασφαλίζοντας ότι η εταιρεία διαθέτει ισχυρή πολιτική ασφάλειας αναφορικά με την χρήση των δεδομένων από τους εργαζόμενους, ότι οι εργαζόμενοι εκπαιδεύονται σε θέματα ασφάλειας και ότι διενεργούνται τακτικοί εξωτερικοί έλεγχοι.

ΠΙΝΑΚΑΣ ΑΠΟΤΙΜΗΣΗΣ ΚΙΝΔΥΝΩΝ – ΔΕΔΟΜΕΝΑ ΕΞΥΠΝΩΝ ΜΕΤΡΗΤΩΝ ΜΕΤΑ ΤΟΥΣ ΕΛΕΓΧΟΥΣ					
ΣΥΝΕΠΕΙΕΣ	ΑΣΗΜΑΝΤΕΣ	ΜΙΚΡΕΣ	ΜΕΤΡΙΕΣ	ΣΟΒΑΡΕΣ	ΚΑΤΑΣΤΡΟΦΙΚΕΣ
ΠΙΘΑΝΟΤΗΤΑ					
ΣΠΑΝΙΑ	MR2	MR4,MR6			
ΑΠΙΘΑΝΟ	MR5 MR3,MR1		MR2		
ΠΙΘΑΝΟΝ			MR3	MR4	
ΠΟΛΎ ΠΙΘΑΝΟ		MR1			MR5
ΣΙΓΟΥΡΟ					MR6

Πίνακας7. 23: ΠΙΝΑΚΑΣ ΑΠΟΤΙΜΗΣΗΣ ΚΙΝΔΥΝΩΝ – ΔΕΔΟΜΕΝΑ ΕΞΥΠΝΩΝ ΜΕΤΡΗΤΩΝ

PR1: Κλοπή προσωπικών δεδομένων για παράνομη χρήση. Εφαρμόσιμα μέτρα CR11, CR14, CR24, CR33.

Εφαρμόζοντας όλους τα μέτρα μειώνουμε την πιθανότητα από πολύ πιθανή σε απίθανη και τις συνέπειες από καταστροφικές σε μικρές, εξασφαλίζοντας ότι οι SM δεν επιτρέπουν ενέργειες write – copy εκτός των SSN, MW, ότι εφαρμόζεται πολιτική ελεγχόμενης πρόσβασης και ότι η οπτική θύρα των SM και η διαδικτυακή πύλη απαιτούν αυθεντικοποίηση.

ΠΙΝΑΚΑΣ ΑΠΟΤΙΜΗΣΗΣ ΚΙΝΔΥΝΩΝ – ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ					
ΣΥΝΕΠΕΙΕΣ ΠΙΘΑΝΟΤΗΤΑ	ΑΣΗΜΑΝΤΕΣ	ΜΙΚΡΕΣ	ΜΕΤΡΙΕΣ	ΣΟΒΑΡΕΣ	ΚΑΤΑΣΤΡΟΦΙΚΕΣ
ΣΠΑΝΙΑ					
ΑΠΙΘΑΝΟ		PR1			
ΠΙΘΑΝΟΝ					PR1
ΠΟΛΥ ΠΙΘΑΝΟ					
ΣΙΓΟΥΡΟ					

Πίνακας7. 24: ΠΙΝΑΚΑΣ ΑΠΟΤΙΜΗΣΗΣ ΚΙΝΔΥΝΩΝ – ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ

7.4 Σύνοψη αποτελεσμάτων

Στον πίνακα 25 συνοψίζονται όλα τα περιουσιακά στοιχεία, οι κίνδυνοι , οι απειλές οι απαιτήσεις ασφάλειας και τα μέτρα ασφάλειας. Τα μέτρα που εμφανίζονται με πράσινο χρώμα είναι αυτά που εφαρμόζονται για να περιορίσουν τους κινδύνους. Για τους κινδύνους που χαρακτηρίστηκαν ως είναι ελεγχόμενοι δε εφαρμόζονται όλοι τα υλοποιήσιμα μέτρα αλλά κάποιοι προκειμένου να γίνουν οι κίνδυνοι αποδεκτοί. Τα μέτρα που έχουν διαγραφεί είναι αυτά που είναι εφαρμόσιμα αλλά δεν επιλέχθηκαν για εφαρμογή.

Περιουσιακά στοιχεία	**Κίνδυνος**	**Περιγραφή κινδύνου**	**Μέτρα Ασφάλειας**	**Απαιτήσεις Ασφάλειας**	**Απειλή**
Στοιχεία Μετρητών	MR1	Κάποια στοιχεία των μετρητών είναι λάθος, χαμένα ή κλεμμένα	**CR24** **CR11** ~~CR14~~ ~~CR15~~ ~~CR16~~	SREQ1 SREQ5	Ο καταναλωτής αλλοιώνει τα στοιχεία του μετρητή σκόπιμα προς όφελος του.
					Εισβολέας κλέβει ή καταστρέφει τα στοιχεία των μετρητών μέσο της οπτικής θύρας του έξυπνου μετρητή.
			CR34 ~~CR35~~	SREQ6	Ο πελάτης σκόπιμα αλλάζει τα στοιχεία του μετρητή

					και τον τύπο του συμβολαίου μέσο της διαδικτυακής πύλης για να κερδίσει δωρεάν ή φθηνότερη ενέργεια.
			CR5 ~~CR19~~	SREQ1 SREQ7	Βλάβη στον έξυπνο μετρητή από φυσική ή ανθρώπινη καταστροφή και αλλοίωση ή απώλεια των στοιχείων του.
					Ο πελάτης όχι σκόπιμα καταστρέφει τον εξοπλισμό του μετρητή ή τον αποσυνδέει από το δίκτυο.
	MR2	Ένας λογικός όγκος των δεδομένων του μετρητή είναι μη διαθέσιμος.	**CR6** ~~CR8~~ **CR30**	SREQ1 SREQ7	Εισβολέας προκαλεί βλάβη στον εξοπλισμό του SSN.
	MR3	Ένας λογικός όγκος των δεδομένων του μετρητή έχει χαθεί, αλλοιωθεί ή κλαπεί.	~~CR10~~ ~~CR12~~ **CR14** ~~CR15~~ ~~CR17~~ **CR19**	SREQ1 SREQ5	Ο Εισβολέας αποκτά πρόσβαση στη βάση δεδομένων του SSN και κλέβει ή παραποιεί δεδομένα.
			CR23 ~~CR25~~	SREQ8	Ο Εισβολέας αποκτά πρόσβαση στο λογισμικό του SSN και στέλνει μη εξουσιοδοτημένα μηνύματα ανάγνωσης στους μετρητές και κλέβει δεδομένα.
			CR26		
	MR4	Η πλειοψηφία των δεδομένων του μετρητή είναι μη διαθέσιμη	**CR7** **CR8** **CR30**	SREQ1 SREQ7	Εισβολέας προκαλεί βλάβη στον εξοπλισμό του MW.
	MR5	Η πλειοψηφία των δεδομένων του μετρητή έχει χαθεί, αλλοιωθεί ή	**CR10** **CR13** **CR14**	SREQ1 SREQ5	Ο Εισβολέας αποκτά πρόσβαση στη βάση δεδομένων του MW και

		κλαπεί.	**CR15** **CR18** **CR20**		κλέβει ή παραποιεί δεδομένα.
			CR23 **CR27** **CR28** **CR29**	SREQ8	Ο Εισβολέας αποκτά πρόσβαση στο λογισμικό του MW και στέλνει μη εξουσιοδοτημένα μηνύματα ανάγνωσης στον SSN και κλέβει δεδομένα.
			CR31 **CR32**	SREQ3 SREQ4	Ο Εισβολέας επιτίθεται στο κανάλι επικοινωνίας των SM,SSM,MW,LMVRCS και κλέβει δεδομένα.
	MR6	Τα στοιχεία των μετρητών χρησιμοποιούνται με λάθος τρόπο για να αυξήσουν τα έσοδα της Εταιρίας	**CR1** **CR2** **CR3**	SREQ9	Ο διαχειριστής ακούσια χρησιμοποιεί τα δεδομένα των μετρητών για επιθετική τιμολόγηση
Ευαίσθητα δεδομένα εταιρείας	BR1	Η πλειοψηφία των ευαίσθητων δεδομένων της εταιρείας έχει κλαπεί και χρησιμοποιείται από τους ανταγωνιστές.	**CR1** **CR2** **CR3** **CR4**	SREQ2	Εργαζόμενος κλέβει ευαίσθητα δεδομένα της εταιρείας.
			CR10 **CR14**	SREQ5 SREQ6	Εισβολέας αποκτά πρόσβαση στη βάση δεδομένων του LMVRCS και κλέβει δεδομένα.
	BR2	Η πλειοψηφία των ευαίσθητων δεδομένων της εταιρείας έχει χαθεί ή αλλοιωθεί.	**CR9** **CR21**	SREQ1 SREQ7	Εισβολέας καταστρέφει τον εξοπλισμό του LMVRCS
	BR3	Η πλειοψηφία των ευαίσθητων δεδομένων της εταιρείας είναι προσωρινά μη διαθέσιμα.	**CR31**		Ο Εισβολέας πετυχαίνει DoS επίθεση στον LMVRCS

	BR4	Μέρος των ευαίσθητων δεδομένων της εταιρείας έχει χαθεί ή αλλοιωθεί.	**CR22** **CR4** ~~CR21~~		Εργαζόμενος από λάθος τροποποιεί ή διαγράφει δεδομένα της εταιρείας
Προσωπικά δεδομένα	PR1	Προσωπικά δεδομένα έχουν κλαπεί και χρησιμοποιούνται για παράνομο σκοπό.	**CR24** **CR11** **CR14**	SREQ2	Εισβολέας κλέβει προσωπικά δεδομένα από τους έξυπνους μετρητές μέσο οπτικής θύρας.
			CR24 **CR33**	SREQ5	Εισβολέας κλέβει προσωπικά δεδομένα μέσο διαδικτυακής πύλης

Πίνακας 7.25: ΠΙΝΑΚΑΣ ΣΥΝΟΨΗΣ ΑΠΟΤΕΛΕΣΜΑΤΩΝ

Επίλογος

Τα πρότυπα που απαιτούνται για να διαμορφωθεί η βάση της Ασφάλειας Πληροφοριών του Smart Grid είναι διαθέσιμα σήμερα. Παρ 'όλα αυτά υπάρχει η ανάγκη για βελτίωση και για πρόσθετα πρότυπα όσο αφορά την ενσωμάτωση των ειδικών αναγκών των Smart Grid και την εφαρμογή τους σε οργανισμούς και σε μέρη του συστήματος για την εξασφάλιση της διαλειτουργικότητας και τη συνεχή τήρηση ορθών πρακτικών. Αυτά, θα πρέπει να αντιμετωπιστούν τόσο λειτουργικά όσο και από πλευράς εφαρμογής της ασφάλειας.

Ο κίνδυνος της σύνδεσης του εξοπλισμού των Smart Grid υποδομών ζωτικής σημασίας σε δημόσια δίκτυα θα πρέπει να εξετάζεται προσεκτικά σε όλες τις εφαρμογές, καθώς και το ενδεχόμενο αποστολής κρυπτογραφημένων και επικυρωμένων εντολών σε εξαρτήμα του Smart Grid.

Φυσικά, αυτό δεν μπορεί να γίνει κατευθείαν και απαιτεί συνεχή προσπάθεια. Η πραγματική πρόκληση θα είναι η διατήρηση αυτής της προσπάθειας και να υπάρχουν πρότυπα που να εξελίσσονται τόσο γρήγορα όσο χρειάζεται η Ασφάλεια Πληροφοριών του Smart Grid.

Βιβλιογραφία

[1] N. I. of Technology-Calicut. “An Advanced Metering Infrastructure for Future Electricity Networks,”.

[2] Smart Grids: from innovation to deployment. EUROPEAN COMMISSION, 2011.

[3] Giordano, Vincenzo και Bossart, Steven. Assessing Smart Grid Benefits and Impacts: EU and U.S. Initiatives. s.l. : Joint Research Centre of the European Commission, 2012.

[4] National Energy Technology Laboratory. Understanding the Benefits of the Smart Grid. 2010.

[5] Sollecito, L), Smart grid: The road ahead, Protection and Control Journal, 8th edition,2009

[6] National Renewable Energy Laboratory of USA, Using Distributed Energy Resources: A How-To Guide for Federal Facility Managers, Federal Energy Management Program, 2002

[7] Sioshansi, F.P., Smart grid, Integrating Renewable, Distributed and Efficient Energy, USA, Elsevier,2010

[8] U.S. Department of Commerce, “NIST Special Publication 1108 NIST Framework and Roadmap for Smart Grid Interoperability Standards , NIST Special Publication 1108 NIST Framework and Roadmap for Smart Grid Interoperability Standards ,Release1.0”,2010.

[9] C. Lima, “Enabling a Smarter Grid”, 2010.

[10] D. Y. Xi Yang, Satyajayant Misra, Guoliang Xue, “Smart Grid – The New and Improved Power Grid : A Survey”,2011.

[11] D. He, C. Chen, and J. Bu, “Secure Service Provision in Smart Grid Communications, 2012.

[12] B. Y. Mo, T. H. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli,“Cyber – Physical Security of a Smart Grid Infrastructure, 2012.

[13] IEEE Standards Coordinating Committee 21, IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications , and Loads,2011.

[14] ENISA, “Smart Grid Security-Annex I-General Concepts and Dependencies withICT”, 2012.

[15]Tony Flick, Justin Morehouse “Securing The Smart Grid, Next Generation Power Grid Security

[16] A. V. A. V. P. C. MP Anastasopoulos, “A secure network management protocol for SmartGrid BPL networks: Design, implementation and experimental results” Computer Communication, 2008

[17] NIST, “NISTIR 7628 Guidelines for Smart Grid Cyber Security: Vol.1, Smart Grid Cyber Security Strategy, Architecture and High-Level Requirements,” 2010

[18] Y. Yang, L. Tim, S. Sezer, K. McLaughlin, and H. F. Wang,"Impact of cyber-security issues on Smart Grid," in Proc. 2nd IEEE PES International Conference and Exhibition on InnovativeSmart Grid Technologies, Manchester , Dec 2011

[19] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," IEEE Commun. Surveys Tuts. 2012

[20] Z. Zhang, H. Liu, S. Niu, and J. Mo, "Information security requirements and challenges in smart grid," in Proc. 6th IEEE Joint International Information Technology and Artificial Intelligence Conference, Chongqing, Aug 2011

[21]M. Apurva and K. Himanshu, "Towards addressing common security issues in smart grid specifications," ,5th International Symposium on Resilient Control Systems, Aug 2012

[22] V. Roberto, Y. Ender, and R. Carroline, "Smart grid security a smart meter-centric perspective," in Proc. 20th Telecommunications Forum, Nov 2012.

[23] H. Khurana, M. Hadley, L. Ning, and D. A. Frincke, "Smart-grid security issues," IEEE Security & Privacy Mag,Jan-Feb 2010

[24] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," IEEE Security & Privacy Mag, May-June 2009

[25] F. Skopik and M. Zhendong, "Attack vectors to metering data in smart grids under security constraints," in Proc. IEEE 36th Annual Computer Software and Applications Conference Workshops, Izmir, July 2012

[26] X. Wang and P. Yi, “Security framework for wireless communications in smart distribution grid,” IEEE Trans. Smart, 2011.

[27] L. Eun-Kyu, G. Mario, and O. Y. Soon, "Physical layer security in wireless smart grid," Communications Magazine, IEEE, August 2012.

[28] A. Rahman and M-R. Hamed, "False data injection attacks with incomplete information against smart power grids," in Proc. IEEE Global Communications Conference, Dec 2012.

[29] Enisa: Smart grid security certification in Europe Challenges and recommendations December 2014

[30]https://www.enisa.europa.eu/activities/Resilience-and-CIIP/workshops-1/2012/smart-grid-certificationcomponents/workshop-minutes

[31] Recommendation 2: Foster the creation of a Public-Private Partnership (PPP) entity to coordinate smart grid cyber security initiatives - http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructureand-services/smart-grids-and-smart-metering/ENISA-smart-grid-security

[32] Security Engineering Report on Smart Grids, Hyeon Kyeong Hwang, Natnael Gonfa Berihun

[33] Lund, Solhaug, Stolen. *Model-Driven Risk Analysis: The Coras Approach.* Chaper 3 (2011). Springer