ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΑΣΦΑΛΕΙΑ ΚΑΙ ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΟ ΕΞΥΠΝΟ ΔΙΚΤΥΟ

Διπλωματική Εργασία

Γιαννόπουλος Δημήτριος

Επιβλέπων: Μπαργιώτας Δημήτριος, Αναπληρωτής Καθηγητής

Βόλος 2020

ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΑΣΦΑΛΕΙΑ ΚΑΙ ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΟ ΕΞΥΠΝΟ ΔΙΚΤΥΟ

Διπλωματική Εργασία

Γιαννόπουλος Δημήτριος

Επιβλέπων: Μπαργιώτας Δημήτριος, Αναπληρωτής Καθηγητής

Βόλος 2020

UNIVERSITY OF THESSALY

SCHOOL OF ENGINEERING

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

SECURITY AND PRIVACY IN SMART GRID

Diploma Thesis

Giannopoulos Dimitrios

Supervisor: Dimitrios Bargiotas, Associate Professor

Volos 2020

ΕΥΧΑΡΙΣΤΙΕΣ

Αρχικά θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή, κύριο Δημήτριο Μπαργιώτα, για την εμπιστοσύνη και την πολύτιμη βοήθεια που μου παρείχε καθ' όλη τη διάρκεια εκπόνησης της διπλωματικής μου εργασίας. Στη συνέχεια, θα ήθελα να ευχαριστήσω την οικογένειά μου για όλα τα εφόδια και τη διαρκή στήριξη που μου παρείχαν σε όλη τη διάρκεια των σπουδών μου.

ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ ΠΕΡΙ ΑΚΑΔΗΜΑΪΚΗΣ ΔΕΟΝΤΟΛΟΓΙΑΣ ΚΑΙ ΠΝΕΥΜΑΤΙΚΩΝ ΔΙΚΑΙΩΜΑΤΩΝ

«Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, δηλώνω ρητά ότι η παρούσα διπλωματική εργασία, καθώς και τα ηλεκτρονικά αρχεία και πηγαίοι κώδικες που αναπτύχθηκαν ή τροποποιήθηκαν στα πλαίσια αυτής της εργασίας, αποτελεί αποκλειστικά προϊόν προσωπικής μου εργασίας, δεν προσβάλλει κάθε μορφής δικαιώματα διανοητικής ιδιοκτησίας, προσωπικότητας και προσωπικών δεδομένων τρίτων, δεν περιέχει έργα/εισφορές τρίτων για τα οποία απαιτείται άδεια των δημιουργών/δικαιούχων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής, οι πηγές δε που χρησιμοποιήθηκαν περιορίζονται στις βιβλιογραφικές αναφορές και μόνον και πληρούν τους κανόνες της επιστημονικής παράθεσης. Τα σημεία όπου έχω χρησιμοποιήσει ιδέες, κείμενο, αρχεία ή/και πηγές άλλων συγγραφέων, αναφέρονται ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή. Αναλαμβάνω πλήρως, ατομικά και προσωπικά, όλες τις νομικές και διοικητικές συνέπειες που δύναται να προκύψουν στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής».

Ο Δηλών

Γιαννόπουλος Δημήτριος

Φεβρουάριος 2020

ΠΕΡΙΛΗΨΗ

Ο όρος “έξυπνο δίκτυο” έχει επινοηθεί και χρησιμοποιείται εδώ και αρκετά χρόνια για να περιγράψει τις τρέχουσες προσπάθειες για τον εκσυγχρονισμό του υπάρχοντος δικτύου ηλεκτρικής ενέργειας. Οι προσπάθειες αυτές αποσκοπούν στην αυτοϊαση, την ενεργειακή απόδοση, την αξιοπιστία και την ασφάλεια με τη χρήση αμφίδρομων ψηφιακών επικοινωνιών και τεχνολογίας ελέγχου μαζί με πληθώρα άλλων πολύτιμων χαρακτηριστικών. Η αμφίδρομη επικοινωνία και ροή ενέργειας επιτρέπουν τόσο στις επιχειρήσεις ηλεκτρισμού όσο και στους πελάτες να παρακολουθούν, να προβλέπουν και να διαχειρίζονται την κατανάλωση της ενέργειας. Το έξυπνο δίκτυο προάγει επίσης την ενεργειακή και περιβαλλοντική βιωσιμότητα μέσω της ενσωμάτωσης απέραντων κατανεμημένων ενεργειακών πόρων. Η υλοποίηση ενός τέτοιου ¨πράσινου¨ συστήματος έχει τεράστια οικονομικά και κοινωνικά οφέλη. Οι αισθητήρες νέας γενιάς, οι έξυπνοι μετρητές και οι ηλεκτρονικές συσκευές αποτελούν αναπόσπαστα στοιχεία του έξυπνου δικτύου. Ωστόσο, η επερχόμενη ανάπτυξη των έξυπνων συσκευών σε διαφορετικά επίπεδα και η ενσωμάτωση τους στα δίκτυα επικοινωνίας ενδέχεται να προκαλέσει απειλές στον κυβερνοχώρο. Η αδυναμία αντιμετώπισης αυτών των προβλημάτων θα δημιουργήσει δυσκολίες στον εκσυγχρονισμό του υπάρχοντος συστήματος ηλεκτρικής ενέργειας. Ένα ακόμα βασικό μέλημα είναι η προστασία της ιδιωτικότητας που σχετίζεται με τη συλλογή και τη χρήση δεδομένων ενεργειακής κατανάλωσης. Σκοπός της παρούσας διπλωματικής είναι η κατηγοριοποίηση και η σύνοψη ευπαθειών, απειλών, επιθέσεων αλλά και θεμάτων που αφορούν την ιδιωτικότητα στο έξυπνο δίκτυο. Επιπλέον, παρατίθενται όλα τα πρότυπα που περιγράφουν θέματα κυβερνοασφάλειας και παρέχονται πληροφορίες για το περιεχόμενο τους. Ακόμα, περιγράφονται γνωστά αντίμετρα τα οποία μπορούν να χρησιμοποιηθούν για το μετριασμό ή την εξάλειψη των επιθέσεων που μπορούν να εκμεταλλευτούν τις ευπάθειες στο έξυπνο δίκτυο.

Λέξεις Κλειδιά: έξυπνο δίκτυο, κυβερνοασφάλεια, ιδιωτικότητα, έξυπνοι μετρητές, επιθέσεις, απειλές

ABSTRACT

The term ¨Smart Grid¨ has been coined and used for several years to describe the efforts of the current power grid modernization. This effort plans to self-healing, energy efficiency, reliability, and security using two-way digital communications and control technology, along with a host of other attributes. Bi-directional communication and electricity flow enable both utilities and customers to monitor, predict, and manage energy usage. It also advances energy and environmental sustainability through the integration of vast distributed energy resources. Deploying such a green electric system has enormous economic and social benefits. The new generation sensors, smart meters and electronic devices are integral components of smart grid. However, the upcoming deployment of smart devices at different layers and their integration with communication networks may introduce cyber threats. Failure to address these problems will hinder the modernization of the existing power system. A crucial concern is the privacy related to the collection and use of energy consumption data. The aim of this thesis is to categorize and summarize vulnerabilities, threats along with privacy issues in smart grid. Furthermore, all smart grid standards that describe cybersecurity issues are listed and information regarding their contents are provided. In addition, known countermeasures which can be used to mitigate or eliminate attacks which exploit vulnerabilities in smart grid are described.

Key Words: smart grid, cybersecurity, privacy, smart meters, attacks, threats

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΛΙΣΤΑ ΣΥΝΤΟΜΟΓΡΑΦΙΩΝ

ΣΗΕ	Σύστημα Ηλεκτρικής Ενέργειας
3DES	Triple Data Encryption Standard
AC	Alternating Current
AES	Advanced Encryption Standard
AGC	Automatic Generation Control
AMI	Advanced Metering Infrastructure
AVR	Automatic Voltage Regulator
BAN	Building Area Network
CA	Certification Authority
CBCMAC	Cipher Block Chaining Message Authentication Code
CCA	Chosen Ciphertext Attack
CIS	Customer Information System
COSEM	Companion Specification for Energy Metering
CPS	Cyber-Physical Systems
CSR	Customer Service Representative
CSRF	Cross-Site Request Forgery
CSS	Chirp spread spectrum
DC	Direct Current
DCS	Distributed Control System
DDoS	Distributed Denial of Service
DER	Distributed Energy Resource
DLMS	Device Language Message Specification
DMS	Distribution Management Systems
DNP3	Distributed Network Protocol 3
DoS	Denial of Service
DRMS	Demand Response Management System
DSL	Digital Subscriber Line

EAP	Extensible Authentication Protocol
EMS	Energy Management System
EPON	Ethernet Passive Optical Networks
EPRI	Electric Power Research Institute
ESP	Energy Service Provider
EUMD	Energy Usage Metering Device
EVSE	Electric Vehicle Service Element
FACTS	Flexible Alternating Current Transmission Systems
FAN	Field Area Networks
FDA	Forensic Data Analytics
FHSS	Frequency-hopping Spread Spectrum
GIS	Geographic Information Systems
GPS	Global Positioning System
HDA	Human–factor-aware Differential Aggregation
HAN	Home Area Network
HES	Head End System
HVDC	High Voltage Direct Current
IACS	Industrial Automation and Control System
IAN	Industrial Area Network
IBE	Identity-Based Encryption
ICCP	Inter-control Center Communications Protocol
ICS	Industrial Control System
ICT	Information and communications technology
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISA	International Society of Automation
ISO	Independent System Operator

ISO	International Organization for Standardization
IVR	Interactive Voice Response
LAN	Local Area Network
LMR	Land Mobile Radio
LMS	Load Management Systems
LTE	Long Term Evolution
MAC	Media Access Control
MDMS	Meter Data Management System
MITM	Man In the Middle
NAN	Neighborhood Area Network
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OMS	Outage Management System
PEV	Plug-in Electric Vehicle
PHEV	Plug-in Hybrid Electric Vehicle
PIA	Privacy Impact Assessment
PII	Personally identifiable information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKMv2	Privacy and Key Management version 2
PLC	Power Line Communication
PLC	Programmable Logic Controller
PMU	Phasor Measurement Unit
POS	Point of Sale
RF	Radio Frequency
RSA	Rivest–Shamir–Adleman
RSSI	Received Signal Strength Information
RTO	Regional Transmission Organization

RTP	Real-time Transport Protocol
RTU	Remote Terminal Unit
SCADA	Distribution Supervisory Control and Data Acquisition
SDLC	Systems Development Life Cycle
SG	Smart Grid
SGIP	Smart Grid Interoperability Panel
SIEM	Security Information and Event Management
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
URL	Uniform Resource Locator
USB	Universal Serial Bus
V2G	Vehicle to Grid
VPN	Virtual Private Network
WAMS	Wide Area Measurement System
WAN	Wide Area Network
WASA	Wide Area Situation Awareness
WiFi	Wireless Fidelity
WiMax	Worldwide Interoperability Microwave Access
WMS	Work Management System

ΚΕΦΑΛΑΙΟ 1

ΕΙΣΑΓΩΓΗ

Η διανομή ηλεκτρικής ενέργειας καθίσταται δυνατή από το δίκτυο διανομής ηλεκτρικής ενέργειας, ένα σύστημα μέσων μετάδοσης που επιτρέπει τη μεταφορά ηλεκτρισμού με διαφορετικές τάσεις από το σημείο παραγωγής στο σπίτι μας. Το σύστημα αυτό προέκυψε από τις ανάγκες του συνεχώς αυξανόμενου πληθυσμού για ηλεκτρική ενέργεια και την εκβιομηχάνιση. Στις αρχές της δεκαετίας του 1870 αλλά και του 1880, τα συστήματα Συνεχούς Ρεύματος (DC) ήταν δημοφιλή. Λόγω της λειτουργίας τους με σταθερή τάση από το σημείο παραγωγής στην κατανάλωση, ενσωματώθηκαν στα εργοστάσια και σε ορισμένα σημεία αστικών κέντρων που είχαν ευνοϊκές οικονομικές συνθήκες, αφήνοντας έτσι μεγάλα κομμάτια πληθυσμού χωρίς πρόσβαση στον ηλεκτρισμό. Ωστόσο, το Εναλλασσόμενο Ρεύμα (AC), ήταν η πρώτη κύρια εξέλιξη για την αλλαγή των τότε δεδομένων. Πρωτοπαρουσιάστηκε από Γάλλους τη δεκαετία του 1860, και αποτέλεσε το 1886 στο Γκρέιτ Μπάρινγκτον στη Μασαχουσέτη, το πρώτο ολοκληρωμένο AC σύστημα ηλεκτρικής ενέργειας. Το AC είχε το πλεονέκτημα της δυνατότητας της αύξησης και της μείωσης στο μέσο μετάδοσης, που επέτρεπε τον χειρισμό της τάσης και είχε ως αποτέλεσμα την ανάπτυξη ενός δικτύου που ο καθένας μπορούσε να έχει πρόσβαση. Το Westinghouse ήταν η πρώτη εταιρεία που μονοπώλησε την τροφοδοσία AC στις ΗΠΑ, κατέχοντας τα δικαιώματα των ευρεσιτεχνιών του Nikola Tesla που αφορούσαν τα πολυφασικά εναλλασσόμενα ρεύματα. Η παραγωγή από διάφορες πηγές έγινε δυνατή και σε τοποθεσίες μακρινές του τελικού καταναλωτή. Για παράδειγμα, μια ανεμογεννήτρια θα μπορούσε να παράγει ενέργεια από την τη περιστροφή ενός στροβίλου και στη συνέχεια με την αύξηση της τάσης θα διένυε μια μεγάλη απόσταση προκειμένου να φτάσει στον τελικό χρήστη, όπου με την πτώση της τάσης θα έπεφτε στην πιο κατάλληλη τιμή των 120V για μια λάμπα οικιακής χρήσης. Πολλαπλές γεννήτριες συνδέονται σε μια μεγάλη περιοχή μειώνοντας το κόστος παραγωγής και βελτιώνοντας τις οικονομίες κλίμακας. Η εξέλιξη όμως του δικτύου ηλεκτρικής ενέργειας σταματά ουσιαστικά σε αυτό το σημείο με την τελευταία σημαντική βελτίωση να γίνεται να γίνεται στις αρχές του 20^{ου} αιώνα. Η γρήγορη εκβιομηχάνιση που ακολούθησε τα επόμενα χρόνια αποτέλεσε σημαντικό παράγοντα ώστε το ηλεκτρικό δίκτυο να αποτελέσει κρίσιμο κομμάτι των υποδομών μιας χώρας. Παρά τη συνεχή ανάπτυξη και βελτιστοποίηση του, συνεχίζει να παραμένει σήμερα σε μεγάλο βαθμό όπως ήταν τότε: μια τεχνολογία που αναπτύχθηκε τον 19^{ο} αιώνα. Αυτό δημιουργεί ένα πρόβλημα στην σημερινή εποχή. Δεδομένου της εξάρτησης από το δίκτυο, είναι σημαντικό να γίνουν αλλαγές στο πλαίσιο της υποδομής του τρέχοντος δικτύου με σκοπό τη βελτίωση της αποτελεσματικότητάς του και της μείωσης όχι μόνο των ανούσιων δαπανών αλλά του αποτυπώματος του άνθρακα.

Το τρέχον δίκτυο ηλεκτρικής ενέργειας αντιμετωπίζει πολλές προκλήσεις που περιγράφονται συνοπτικά σε τρεις κατηγορίες. Πρώτον, υπάρχουν προβλήματα υποδομής λόγω του γεγονότος ότι το σύστημα είναι ξεπερασμένο και ακατάλληλο να αντιμετωπίσει την αυξανόμενη ζήτηση. Αυτό έχει ως αποτέλεσμα να προκύπτουν συχνά συμφορήσεις στο δίκτυο, λόγω του ότι δεν έχει τη δυνατότητα να αντιδρά σε τέτοια θέματα εγκαίρως. Τελικά, τέτοιες ανισορροπίες μπορούν να οδηγήσουν σε διακοπές ρεύματος που είναι εξαιρετικά δαπανηρές για εταιρείες παροχής ηλεκτρικού ρεύματος, κυρίως επειδή εξαπλώνονται εύκολα λόγω της έλλειψης επικοινωνίας μεταξύ του δικτύου και των κέντρων ελέγχου. Ένα δεύτερο μειονέκτημα είναι η ανάγκη για περισσότερες πληροφορίες και διαφάνεια για τους πελάτες έτσι ώστε να λαμβάνει τις βέλτιστες αποφάσεις σχετικά με την αγορά προκειμένου να μειωθεί η κατανάλωση τις ώρες αιχμής. Τέλος, ένα τρίτο πρόβλημα είναι η έλλειψη ευελιξίας του σημερινού δικτύου, το οποίο δεν μπορεί να στηρίξει την ανάπτυξη ανανεώσιμων πηγών ενέργειας ή άλλων μορφών τεχνολογιών που θα το καθιστούσαν πιο βιώσιμο. Ειδικότερα, το γεγονός ότι οι ανανεώσιμες πηγές ενέργειας όπως η αιολική και η ηλιακή ενέργεια είναι διακοπτόμενες δημιουργεί ένα σημαντικό πρόβλημα για ένα δίκτυο το οποίο δεν διαδίδει γρήγορα τις πληροφορίες στα κέντρα ελέγχου. Όλα αυτά τα προβλήματα αντιμετωπίζονται από το Έξυπνο Δίκτυο (Smart Grid) μέσω βελτιωμένης τεχνολογίας επικοινωνιών, με πολλαπλά οφέλη στην αγορά της ηλεκτρικής ενέργειας, τόσο για την πλευρά της παροχής όσο και για την πλευρά της ζήτησης. Αντί για την πλήρη αντικατάσταση του σημερινού δικτύου, η μετάβαση σε ένα έξυπνο δίκτυο είναι απλώς μια σημαντική ανανέωσή του με τεχνολογίες όπως μετρητές, αισθητήρες και μετρητές διανυσμάτων τάσης σύγχρονης επικοινωνίας. Όταν προστεθούν στην υπάρχουσα υποδομή αυτές οι τεχνολογίες θα παρέχουν τεράστιες ποσότητες δεδομένων σχετικά με την κατανάλωση, την τάση, την υγεία των υποδομών και πολλές άλλες πτυχές της παροχής ηλεκτρικού ρεύματος στα κέντρα ελέγχου. Με βελτιωμένες επικοινωνίες, το έξυπνο δίκτυο επιλύει πολλά από τα προβλήματα που αναφέρονται παραπάνω και προσφέρει οφέλη στους καταναλωτές και τους προμηθευτές.

ΚΕΦΑΛΑΙΟ 2

ΕΞΥΠΝΟ ΔΙΚΤΥΟ

2.1 Η έννοια και τα βασικά χαρακτηριστικά του Έξυπνου Δικτύου

Το έξυπνο δίκτυο (Smart Grid – SG), που αποκαλείται και έξυπνο ηλεκτρικό δίκτυο ή ευφυή δίκτυο, είναι μια βελτιστοποίηση του δικτύου ηλεκτρικής ενέργειας του 20ου αιώνα. Το παραδοσιακά ηλεκτρικά δίκτυα χρησιμοποιούνται γενικά για τη μεταφορά ενέργειας από κεντρικές γεννήτριες σε ένα μεγάλο αριθμό χρηστών ή καταναλωτών. Αντίθετα το SG χρησιμοποιεί αμφίδρομη ροή ηλεκτρικής ενέργειας και πληροφορίας για τη δημιουργία αυτοματοποιημένης και κατανεμημένης παροχής ενέργειας στο δίκτυο. Στον Πίνακα 1 καταγράφονται συνοπτικά οι διαφορές μεταξύ του υπάρχοντος δικτύου και του SG. Χρησιμοποιώντας σύγχρονες τεχνολογίες πληροφοριών, το SG είναι ικανό να παρέχει ενέργεια με αποτελεσματικότερους τρόπους και να ανταποκριθεί σε πολλές διαφορετικές καταστάσεις και συνθήκες οπουδήποτε κι αν προκύπτουν στο δίκτυο (παραγωγή, μετάδοση, διανομή, κατανάλωση) και να υιοθετήσουν τις κατάλληλες στρατηγικές. Για παράδειγμα, όταν προκύψει μια διακοπή λειτουργίας σε έναν μετασχηματιστή μέσης τάσης στο δίκτυο διανομής, το SG μπορεί αυτόματα να αλλάξει τη ροή ισχύος και να ανακτήσει την υπηρεσία παροχής ενέργειας. Ένα άλλο παράδειγμα διαμόρφωσης ζήτησης αφορά τη μείωση φορτίου αιχμής και του μέσου φορτίου που έχει ως αποτέλεσμα τον περιορισμό των απαιτήσεων του σταθμού παραγωγής και του κεφαλαιακού κόστους. Σε περιόδους αιχμής η εταιρεία ηλεκτρισμού μπορεί χρησιμοποιήσει τιμολόγηση σε πραγματικό χρόνο για να πείσει ορισμένους χρήστες να μειώσουν τις απαιτήσεις τους για ενέργεια, έτσι ώστε να μπορεί να εξομαλυνθεί το συνολικό φορτίο.

Πίνακας 1 - Οι διαφορές του υπάρχοντος δικτύου σε σύγκριση με το Smart Grid [1]

Χαρακτηριστικά	**Υπάρχον Δίκτυο**	**Smart Grid**
Εξοπλισμός	Ηλεκτρομηχανικός	Ψηφιακός
Ροή Πληροφοριών	Μονόδρομη	Αμφίδρομη
Παραγωγή	Κεντρική	Κατανεμημένη
Τοπολογία Δικτύου	Ακτινική	Διασυνδεδεμένη
Αισθητήρες	Λίγοι	Πολλοί
Παρακολούθηση	Χειροκίνητη	Αυτόματη
Αποκατάσταση	Χειροκίνητη	Αυτόματη
Ικανότητα Προστασίας	Πολύπλοκη	Απλή
Τύπος Ελέγχου	Περιορισμένος/Χειροκίνητος	Πλήρης/Απομακρυσμένος
Επίπεδα Μόλυνσης	Υψηλά	Χαμηλά

Αποτελεσματικότητα	Χαμηλή	Υψηλή
Επιλογές Πελατών	Ελάχιστες	Πλήθος Επιλογών

Πιο συγκεκριμένα, το SG μπορεί να θεωρηθεί ως ένα ηλεκτρικό σύστημα που χρησιμοποιεί τεχνολογίες πληροφοριών, ασφαλείς τεχνολογίες αμφίδρομης επικοινωνίας και υπολογιστική νοημοσύνη με έναν ολοκληρωμένο τρόπο στην παραγωγή, τη μετάδοση, τους υποσταθμούς, τη διανομή και την κατανάλωση για την επίτευξη ενός συστήματος που είναι καθαρό, ασφαλές, αξιόπιστο, ανθεκτικό, αποτελεσματικό και βιώσιμο. Αυτή η περιγραφή καλύπτει ολόκληρο το φάσμα του συστήματος ενέργειας από την παραγωγή έως και τελικά σημεία κατανάλωσης του ρεύματος. Το τελικό SG είναι ένα όραμα. Είναι μια ευρύτερη ενσωμάτωση συμπληρωματικών στοιχείων, υποσυστημάτων, λειτουργιών και υπηρεσιών κάτω από τον διάχυτο έλεγχο ευφυών συστημάτων διαχείρισης και ελέγχου.[2]

Από τεχνικής άποψης το SG διαιρείται σε τρία κύρια συστήματα: Σύστημα έξυπνης υποδομής, σύστημα έξυπνης διαχείρισης και σύστημα έξυπνης προστασίας.

1) **Σύστημα Έξυπνης υποδομής**: Το σύστημα έξυπνης υποδομής (Smart Infrastructure System) είναι η ενέργεια, η πληροφορία και η υποδομή της επικοινωνίας που αποτελεί τη βάση του SG. Υποστηρίζει αμφίδρομη ροή ενέργειας κα πληροφορίας. Η έννοια της αμφίδρομης επικοινωνίας για την πληροφορία είναι σαφής. Η ΄΄αμφίδρομη ροή ενέργειας΄΄ σημαίνει ότι η παροχή ενέργειας δεν είναι πλέον μονής κατεύθυνσης. Για παράδειγμα, στο παραδοσιακό δίκτυο, η ενέργεια παράγεται από το σταθμό παραγωγής, έπειτα προωθείται από το δίκτυο μετάδοσης, διανομής και τελικά φτάνει στους χρήστες. Στο SG η ηλεκτρική ενέργεια μπορεί να επιστραφεί πίσω στο δίκτυο από τους χρήστες. Για παράδειγμα, οι χρήστες μπορούν να παράγουν ενέργεια χρησιμοποιώντας ηλιακά πάνελ στα σπίτια τους και να την επιστρέφουν στο δίκτυο ή τα ηλεκτρικά οχήματα μπορούν να παρέχουν ενέργεια για να βοηθήσουν στην εξισορρόπηση του φορτίου, στέλνοντας ‘την πίσω στο δίκτυο όταν η ζήτηση είναι υψηλή. Αυτή η ανάποδη ροή είναι σημαντική. Για παράδειγμα μπορεί να φανεί πολύ χρήσιμη σε ένα μικροδίκτυο που έχει απομονωθεί λόγω διακοπής ρεύματος. Το μικροδίκτυο μπορεί να λειτουργήσει αν και σε μειωμένα πλέον επίπεδα, με τη βοήθεια της ανατροφοδότησης από τους χρήστες. Το σύστημα έξυπνης υποδομής μπορεί επίσης να χωριστεί σε τρία υποσυστήματα: Υποσύστημα έξυπνης ενέργειας, υποσύστημα έξυπνης πληροφορίας και υποσύστημα έξυπνης επικοινωνίας.
    - Το υποσύστημα έξυπνης ενέργειας είναι υπεύθυνο για την προηγμένη παραγωγή ηλεκτρικής ενέργειας, τη διανομή και την κατανάλωση.

- Το υποσύστημα έξυπνης πληροφορίας είναι υπεύθυνο για προηγμένες μετρήσεις, παρακολούθηση και διαχείριση στο πλαίσιο του SG.
- Το υποσύστημα έξυπνης επικοινωνίας είναι υπεύθυνο για τη συνδεσιμότητα επικοινωνίας και τις πληροφορίες μετάδοσης μεταξύ συστημάτων, συσκευών και εφαρμογών στο πλαίσιο του SG.

2) **Σύστημα Έξυπνης Διαχείρισης**: Το σύστημα έξυπνης διαχείρισης (Smart Management System) είναι το υποσύστημα του SG που παρέχει προηγμένες υπηρεσίες και λειτουργίες διαχείρισης και ελέγχου. Ο κύριος λόγος για τον οποίο μπορεί το SG να φέρει επανάσταση στο υπάρχον δίκτυο είναι η μεγάλη αύξηση της λειτουργικότητας που βασίζεται στην έξυπνη υποδομή του. Με την ανάπτυξη νέων εφαρμογών διαχείρισης και υπηρεσιών που μπορούν να αξιοποιήσουν την τεχνολογία και την ικανότητα αναβαθμίσεων που ενεργοποιούνται από αυτή την προηγμένη υποδομή, το δίκτυο θα συνεχίσει να γίνεται ΄΄εξυπνότερο΄΄. Το έξυπνο σύστημα διαχείρισης εκμεταλλεύεται την έξυπνη υποδομή για την ανάλυση προηγμένων στόχων διαχείρισης. Μέχρι στιγμής, οι περισσότεροι από αυτούς τους στόχους σχετίζονται με τη βελτίωση της ενεργειακής απόδοσης, την ισορροπία μεταξύ ζήτησης και προσφοράς, τον έλεγχο των εκπομπών, τη μείωση του κόστους λειτουργίας και τη μεγιστοποίηση χρησιμότητας.

3) **Έξυπνο Σύστημα Προστασίας**: Το σύστημα έξυπνης προστασίας (Smart Protection System) είναι το υποσύστημα του SG που παρέχει ανάλυση αξιοπιστίας, προστασία από διακοπές ρεύματος και υπηρεσίες που αφορούν την ασφάλεια και προστασία προσωπικών δεδομένων. Αξιοποιώντας την έξυπνη υποδομή, το SG δεν πρέπει μόνο να υλοποιήσει ένα εξυπνότερο σύστημα διαχείρισης, αλλά επίσης να παρέχει εξυπνότερο σύστημα προστασίας που θα μπορεί πιο αποτελεσματικά και αποδοτικά να υποστηρίξει μηχανισμούς προστασίας από διακοπές λειτουργίας, να διευθετήσει θέματα ασφαλείας στον κυβερνοχώρο και να διατηρήσει την ιδιωτικότητα.

Η αρχική έννοια του SG ξεκίνησε με την ιδέα της προηγμένης υποδομής μέτρησης (Advanced Metering Infrastructure - AMI) με σκοπό τη βελτίωση της διαχείρισης της ζήτησης και της ενεργειακής απόδοσης, και την κατασκευή ενός αξιόπιστου δικτύου, με δυνατότητες αυτοΐασης και προστασίας απέναντι σε κακόβουλες επιθέσεις και φυσικές καταστροφές. Ωστόσο, οι νέες απαιτήσεις οδήγησαν τις βιομηχανίες ηλεκτρικής ενέργειας, ερευνητικούς οργανισμούς και τις κυβερνήσεις να ξανασκεφτούν και να επεκτείνουν το αρχικά αντιληπτό πλαίσιο του SG. Το Εθνικό Ινστιτούτο Ενέργειας και Τεχνολογίας (NIST) ανέλαβε να συντονίσει την έρευνα και την ανάπτυξη ενός πλαισίου με σκοπό την επίτευξη της διαλειτουργικότητας συστημάτων και συσκευών του SG. Αν και

ακριβής ορισμός δεν έχει προταθεί ακόμα, σύμφωνα με την αναφορά του NIST, τα αναμενόμενα οφέλη και απαιτήσεις του SG είναι τα εξής:

1) Βελτίωση της αξιοπιστίας και της ποιότητας της ενέργειας.
2) Βελτιστοποίηση της αξιοποίησης των εγκαταστάσεων και αποτροπή δημιουργίας εφεδρικών σταθμών παραγωγής.
3) Αύξηση των δυνατοτήτων και της αποτελεσματικότητας των υφιστάμενων δικτύων.
4) Βελτίωση της ανθεκτικότητας στις διαταραχές.
5) Ενεργοποίηση προβλεπόμενης συντήρησης και αυτοϊασης απέναντι στις διαταραχές του συστήματος.
6) Διευκόλυνση της ευρύτερης ανάπτυξης των ανανεώσιμων πηγών ενέργειας.
7) Εξοικονόμηση κατανεμημένων ενεργειακών πόρων.
8) Αυτοματοποίηση συντήρησης και λειτουργίας.
9) Μείωση των εκπομπών αερίων του θερμοκηπίου με τη χρήση ηλεκτρικών οχημάτων και εναλλακτικών πηγών ενέργειας.
10) Δημιουργία ευκαιριών για την βελτίωση της ασφάλειας του δικτύου.
11) Ενεργοποίηση της μετάβασης σε plug-in ηλεκτρικά οχήματα και νέες επιλογές αποθήκευσης ενέργειας.
12) Αύξηση των επιλογών των καταναλωτών.
13) Ενεργοποίηση νέων προϊόντων, υπηρεσιών και αγορών.[3]

Το Ινστιτούτο Ερευνών Ηλεκτρικής Ενέργειας, το αμερικάνικο Εθνικό Τεχνολογικό Εργαστήριο και η Ευρωπαϊκή Τεχνολογική Πλατφόρμα Έξυπνων Δικτύων έχουν ορίσει ως κύρια χαρακτηριστικά του SG:

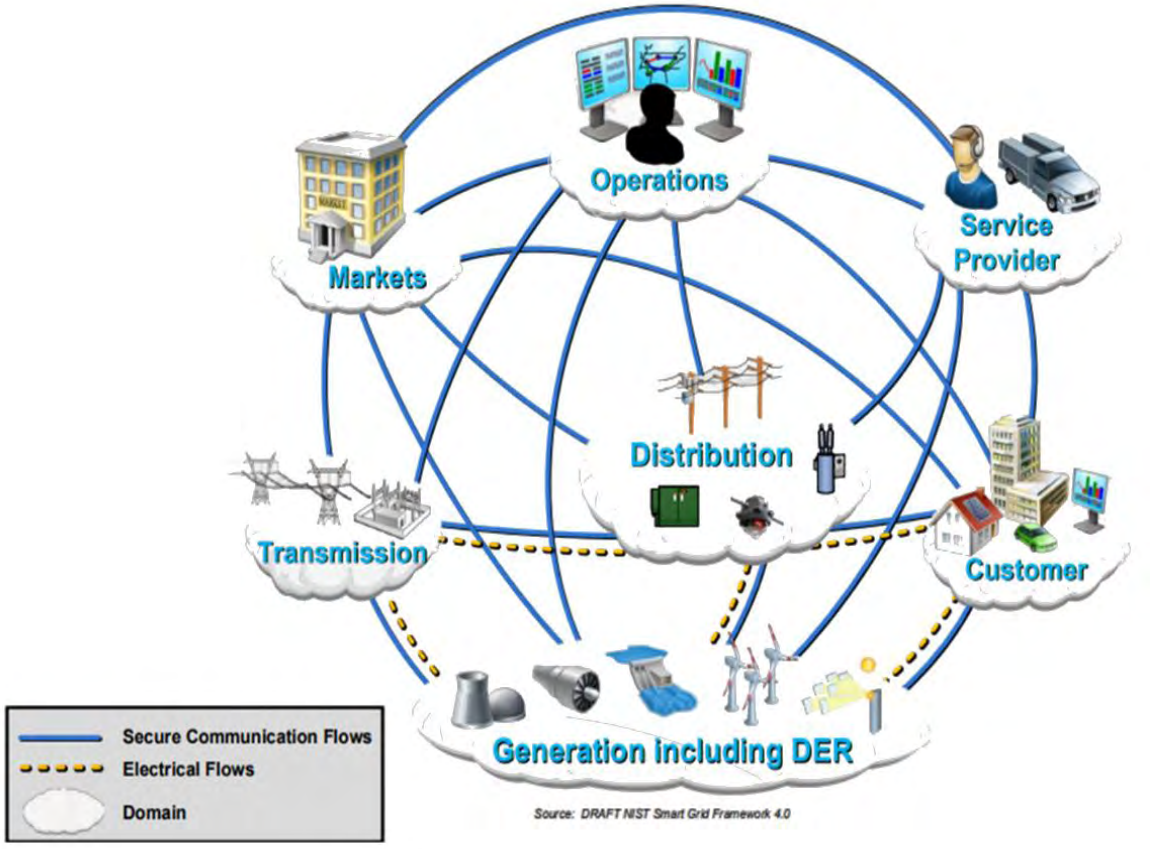
1) **Ασφαλές και Αξιόπιστο**: Το SG θα παραμείνει η κύρια πηγή ενέργειας για τους χρήστες, ακόμα κι αν συμβεί μια διακοπή ρεύματος σε μια μεγάλη περιοχή λόγω διαταραχών στο δίκτυο, ένα σφάλμα, φυσικές καταστροφές και ακραίες καιρικές συνθήκες ή ανθρώπινη παρέμβαση.
2) **Αποδοτικό και Οικονομικό**: Το SG μπορεί να βελτιώσει τα οικονομικά οφέλη μέσω καινοτόμων τεχνολογιών, ενεργειακής απόδοσης, διαχείρισης και ανταγωνισμού στην αγορά. Το SG επίσης, παρέχει υποστήριξη στην αγορά και τις συναλλαγές ενέργειας για να πετύχει την ορθολογική κατανομή των πηγών, να μειώσει τις απώλειες ενέργειας και τελικά και τελικά να βελτιώσει την αποδοτικότητα.
3) **Καθαρό και Οικολογικό**: Το δίκτυο μπορεί να τροφοδοτηθεί με ανανεώσιμες πηγές προκείμενου να μειωθούν πιθανές επιπτώσεις στο περιβάλλον.
4) **Βελτιστοποίηση**: Το SG μπορεί να βελτιώσει την αξιοπιστία και την ασφάλεια τροφοδοσίας για να περάσει τη ζήτηση ηλεκτρικής ενέργειας στην ψηφιακή εποχή. Επιπλέον, το SG μπορεί να βελτιστοποιήσει τη χρήση εργαλείων και να μειώσει τα επενδυτικά και λειτουργιά κόστη καθώς και τα κόστη συντήρησης.

Μπορεί επίσης να παρέχει ποιότητα ενέργειας που να ανταποκρίνεται στα πρότυπα των βιομηχανιών, τις ανάγκες των καταναλωτών και γενικότερα σε οποιοδήποτε επίπεδο ποιότητας απαιτείται για το εύρος των αναγκών.

5) **Διαδραστικό**: Με τη διαδραστικότητα και την απόκριση στην αγορά και τους καταναλωτές σε πραγματικό χρόνο, αυξάνονται οι υπηρεσίες που μπορεί να προσφέρει το δίκτυο.
6) **Αυτοΐαση:** Το SG έχει δυνατότητες αξιολόγησης και ανάλυσης ασφαλείας online και σε πραγματικό χρόνο, ισχυρό σύστημα ελέγχου για έγκαιρη προειδοποίηση και προστασία ελέγχου αυτόματης διάγνωσης σφαλμάτων, αυτόματης απομόνωσης σφαλμάτων και ικανότητα αυτόματης αποκατάστασης του συστήματος. Έχει επίσης τη δυνατότητα αυτόματης αποκατάστασης και προσαρμοστικότητας για τη διόρθωση προβλημάτων πριν γίνουν έκτακτης ανάγκης. Λειτουργεί με βάση την πρόβλεψη καταστάσεων παρά με την αντίδραση προκειμένου να εμποδίσει μια άσχημη κατάσταση παρά να την επιλύσει μετά. Είναι ανθεκτικό στις επιθέσεις και τις φυσικές καταστροφές με δυνατότητες ταχείας αποκατάστασης.
7) **Ευέλικτο και Συμβατό:** Το SG μπορεί να υποστηρίξει τη σωστή και λογική ενσωμάτωση των ανανεώσιμων πηγών ενέργειας και είναι κατάλληλο για την ενσωμάτωση κατανεμημένης παραγωγής και μικροδικτύων. Ακόμα μπορεί να βελτιώσει τη λειτουργία διαχείρισης στην πλευρά της ζήτησης για την επίτευξη αποτελεσματικής αλληλεπίδρασης με τους χρήστες. Ικανοποιεί όλες τις επιλογές παραγωγής και αποθήκευσης. Διαθέτει μεγάλο αριθμό διαφορετικών κατανεμημένων γεννητριών και αποθηκευτικών συσκευών για να συμπληρώσει τους μεγάλους σταθμούς παραγωγής.
8) **Ενοποιημένο:** Στο SG χρησιμοποιείται ενιαία πλατφόρμα και μοντέλα. Μπορεί να πετύχει υψηλό βαθμό ενσωμάτωσης και ανταλλαγής πληροφοριών του ηλεκτρικού δικτύου, καθώς και εξειδικευμένη διαχείριση καταφέρνοντας έτσι να ενσωματώνει τις υποδομές, τις διαδικασίες, τις συσκευές, τις πληροφορίες και τη δομή της αγοράς ώστε η ενέργεια να μπορεί να παραχθεί, διανεμηθεί και καταναλωθεί αποτελεσματικότερα και οικονομικά αποδοτικότερα. Με αυτό τον τρόπο επιτυγχάνεται ένα πιο ανθεκτικό, ασφαλές και αξιόπιστο ενεργειακό σύστημα.[4]

2.2 Η δομή του Έξυπνου Δικτύου

Το εννοιολογικό μοντέλο του SG υποστηρίζει τη σχεδίαση, τις απαιτήσεις, την ανάπτυξη, την τεκμηρίωση και την οργάνωση της ποικίλης και διευρυμένης συλλογής διασυνδεδεμένων δικτύων και του εξοπλισμού που θα συνθέσουν το δίκτυο. Γι’ αυτό το λόγο το NIST χώρισε το SG σε εφτά τομείς όπως φαίνεται στην Εικόνα 1, και περιγράφονται παρακάτω.



Εικόνα 1 - Εννοιολογικό μοντέλο Smart Grid [5]

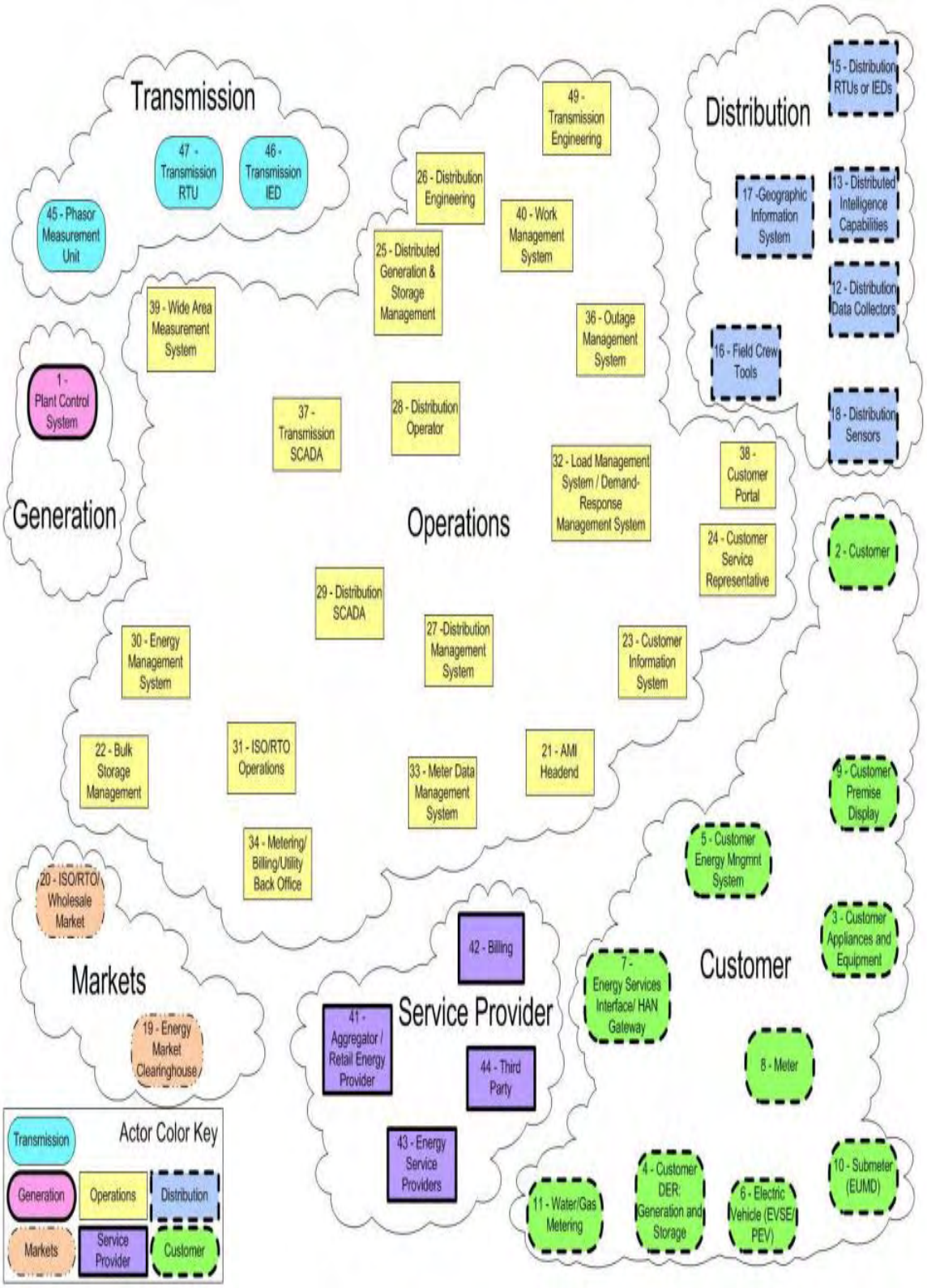
Κάθε τομέας και οι υποκατηγορίες του, συμπεριλαμβάνει τους εννοιολογικούς ρόλους κα υπηρεσίες του SG που περιγράφονται συνοπτικά στον Πίνακα 2. Περιλαμβάνουν τύπους υπηρεσιών, αλληλεπιδράσεις, και ενδιαφερόμενους φορείς που λαμβάνουν αποφασίσεις και ανταλλάσσουν πληροφορίες απαραίτητες για την επίτευξη καθοριστικών στόχων όπως: διαχείριση πελατών, συγκέντρωση κατανεμημένης παραγωγής κα διαχείριση σφαλμάτων. Οι υπηρεσίες εκτελούνται από έναν ή περισσότερους ρόλους εντός του τομέα. Για παράδειγμα, οι αντίστοιχες υπηρεσίες μπορεί να περιλαμβάνουν οικιακό αυτοματισμό, κατανεμημένους ενεργειακούς πόρους (Distributed Energy Resource – DER) και απόκριση στη ζήτηση πελατών, έλεγχο φορτίου και επίγνωση της κατάστασης ευρείας περιοχής σχεδόν σε πραγματικό χρόνο (Wide Area Situation Awareness – WASA).

Γενικά οι ρόλοι στον ίδιο τομέα έχουν παρόμοιους στόχους. Ωστόσο οι επικοινωνίες εντός του ίδιου τομέα μπορεί να έχουν διαφορετικά χαρακτηριστικά και μπορεί να πληρούν διαφορετικές απαιτήσεις για την επίτευξη της διαλειτουργικότητας.[5]

Πίνακας 2 - Τομείς και Ρόλοι/Υπηρεσίες στο εννοιολογικό μοντέλο του NIST [5]

	Τομέας	**Ρόλοι/Υπηρεσίες στον Τομέα**
1	Πελάτης	Τελικός χρήστης της ενέργειας. Μπορεί επίσης να παράγει, να αποθηκεύσει και να διαχειριστεί τη χρήση της ενέργειας. Παραδοσιακά, διακρίνεται σε τρεις κατηγορίες, κάθε μία με τον δικός της τομέα: οικιακός, εμπορικός και βιομηχανικός.
2	Αγορά	Οι φορείς εκμετάλλευσης και οι συμμετέχοντες στην αγορά ηλεκτρικής ενέργειας.
3	Πάροχοι Υπηρεσιών	Οι οργανισμοί που παρέχουν υπηρεσίες στους πελάτες και τις εταιρείες ηλεκτρισμού.
4	Χειρισμός	Οι διαχειριστές της διακίνησης ηλεκτρικής ενέργειας.
5	Παραγωγή	Οι γεννήτριες ηλεκτρικής ενέργειας. Μπορεί επίσης να αποθηκεύει ενέργεια για διανομή αργότερα. Αυτός ο τομέας περιλαμβάνει παραδοσιακούς πόρους ενέργειας αλλά και κατανεμημένους πόρους (DER). Σε λογικά επίπεδα, η παραγωγή συμπεριλαμβάνει παραγωγή από άνθρακα, πυρηνική ενέργεια και μεγάλης κλίμακας υδροηλεκτρική παραγωγή. Οι κατανεμημένοι πόροι (DER) σχετίζονται με παραγωγή και την αποθήκευση που παρέχονται από τον τομέα πελατών και διανομής, αλλά και με τους ενεργειακούς πόρους που παρέχονται από τον τομέα παρόχων υπηρεσιών.
6	Μεταφορά	Τα μέσα μεταφοράς ρευμάτων σε υψηλές τάσεις για μακρινές αποστάσεις. Μπορεί επίσης να παράγει και να αποθηκεύει ενέργεια.
7	Διανομή	Τα μέσα διανομής ηλεκτρισμού από και προς τους χρήστες. Μπορεί επίσης να παράγει και να αποθηκεύει ενέργεια.

Κάθε τομέας του SG είναι μια γενική ομαδοποίηση οργανισμών, κτιρίων, ατόμων, συστημάτων, συσκευών, ή άλλων οντοτήτων και βασίζεται (ή συμμετέχει) σε εφαρμογές παρόμοιου τύπου. Οι διάφορες οντότητες είναι απαραίτητες για τη μεταφορά, την αποθήκευση, τη διόρθωση και την επεξεργασία των πληροφοριών που χρειάζονται στο πλαίσιο του SG. Για την επίτευξη της λειτουργικότητας του SG, οι οντότητες σε ένα συγκεκριμένο τομέα συχνά αλληλοεπιδρούν με οντότητες σε άλλους τομείς. Το διάγραμμα στην Εικόνα 2 συνθέτει μια γενική οπτική των οντοτήτων μέσα σε κάθε τομέα του SG. Αυτό το γενικό διάγραμμα παρέχεται ως μοντέλο αναφοράς. Οι οντότητες είναι συσκευές, συστήματα ή προγράμματα που παίρνουν αποφάσεις και ανταλλάσσουν πληροφορίες, απαραίτητες για την εκτέλεση εφαρμογών μέσα στο SG. Στον Πίνακα 3 ακολουθεί η περιγραφή των οντοτήτων σε κάθε τομέα.[6]



Εικόνα 2 - Σύνθεση γενικής οπτικής των οντοτήτων στους Τομείς του Smart Grid [6]

Πίνακας 3 - Συνοπτική περιγραφή των οντοτήτων στους τομείς του Smart Grid [6]

Αριθμός Οντότητας	**Τομέας**	**Οντότητα**	**Περιγραφή**
1	Παραγωγή	Σύστημα Ελέγχου Μονάδας – Κατανεμημένο Σύστημα Ελέγχου (DCS)	Ένα τοπικό σύστημα ελέγχου σε σταθμούς μαζικής παραγωγής. Μερικές φορές αποκαλείται Κατανεμημένο Σύστημα Ελέγχου (DCS).
2	Πελάτης	Πελάτης	Μία οντότητα που πληρώνει για ηλεκτρικές συσκευές ή υπηρεσίες. Ένας πελάτης μιας εταιρείας ηλεκτρισμού, συμπεριλαμβανομένου των πελατών που παρέχουν περισσότερη ενέργεια από ότι καταναλώνουν.
3	Πελάτης	Συσκευές και Εξοπλισμός Πελατών	Μια συσκευή ή ένα όργανο σχεδιασμένο για συγκεκριμένες λειτουργίες και ειδικότερα ηλεκτρικές συσκευές οικιακής χρήσης. Μια ηλεκτρική συσκευή ή μηχάνημα που μπορεί να έχει τη δυνατότητα να παρακολουθείται, να ελέγχεται και/ή να προβάλλεται σε οθόνη.
4	Πελάτης	Κατανεμημένοι Πόροι Ενέργειας του Πελάτη(DER): Παραγωγή και Αποθήκευση	Πόροι ενέργειας όπως ο ήλιος ή ο άνεμος, που χρησιμοποιούνται για την παραγωγή και τη αποθήκευση ενέργειας (στην τοποθεσία του πελάτη) καθώς και για να διασυνδεθούν μέσω του διαχειριστή με σκοπό την εκτέλεση ενεργειακών δραστηριοτήτων.

5	Πελάτης	Σύστημα Διαχείρισης Ενέργειας Πελάτη(EMS)	Μια υπηρεσία εφαρμογής ή συσκευή που επικοινωνεί με άλλες συσκευές στο σπίτι. Η υπηρεσία εφαρμογής ή η συσκευή μπορεί να έχει διεπαφές με τον μετρητή για να διαβάζει δεδομένα χρήσης, ή με τον τομέα χειρισμού για να παίρνει τιμές ή άλλες πληροφορίες για αυτοματοποιημένες αποφάσεις για τον αποτελεσματικότερο έλεγχο της κατανάλωσης ενέργειας. Το EMS μπορεί να είναι μια υπηρεσία συνδρομής σε εταιρεία ηλεκτρισμού, ένας τρίτος πάροχος, μια πολιτική που καθορίζεται από τον πελάτη, μια συσκευή που ανήκει στον πελάτη ή ένας χειροκίνητος έλεγχος από την εταιρεία ή τον πελάτη.
6	Πελάτης	Plug-in Ηλεκτρικό Όχημα(PEV) - Υποδομή Υπηρεσίας Ηλεκτρικού Οχήματος(EVSE)	Το PEV είναι ένα όχημα που χρησιμοποιεί ηλεκτρικό κινητήρα και λειτουργεί με επαναφορτιζόμενη μπαταρία. Μπορεί να επαναφορτιστεί χρησιμοποιώντας μια εξωτερική πηγή τροφοδοσίας. Όταν η εξωτερική πηγή είναι το ηλεκτρικό δίκτυο, το EV συνδέεται μέσω EVSE που παρέχει ενέργεια και επικοινωνία.
7	Πελάτης	Πύλη Οικιακού Δικτύου(HAN Gateway)	Μία διεπαφή μεταξύ του τομέα πελατών, διανομής, χειρισμού και παρόχων υπηρεσιών και των συσκευών μέσα στον τομέα πελατών.
8	Πελάτης	Μετρητής	POS συσκευή που χρησιμοποιείται για τη μεταφορά αποτελεσμάτων μετρήσεων κατανάλωσης ενέργειας και υλικών από έναν τομέα/σύστημα σε έναν άλλο.

9	Πελάτης	Εμφάνιση Δεδομένων Πελατών	Μια συσκευή που εμφανίζει δεδομένα κατανάλωσης και κόστους στην τοποθεσία του πελάτη.
10	Πελάτης	Υπομετρητής – Συσκευή Μέτρησης Κατανάλωσης Ενέργειας(EUMD)	Ένας μετρητής που συνδέεται μετά τον κύριο μετρητή χρέωσης. Μπορεί να είναι ή να μην είναι μετρητής χρέωσης και συνήθως χρησιμοποιείται για σκοπούς παρακολούθησης πληροφοριών.
11	Πελάτης	Μετρητής Νερού/Φυσικού Αερίου	POS συσκευή που χρησιμοποιείται για τη μεταφορά αποτελεσμάτων μετρήσεων κατανάλωσης ενέργειας και υλικών (νερό και φυσικό αέριο) από ένα τομέα/σύστημα σε ένα άλλο.
12	Διανομή	Συλλέκτης Δεδομένων Διανομής	Ένας συλλέκτης δεδομένων που συγκεντρώνει δεδομένα από διαφορετικές πηγές και τα τροποποιεί.
13	Διανομή	Δυνατότητες Κατανεμημένης Ευφυΐας	Προηγμένη αυτοματοποιημένη/ευφυής εφαρμογή που λειτουργεί αυτόνομα από τον κεντρικό έλεγχο για την αύξηση της αξιοπιστίας και της ταχύτητας απόκρισης.
15	Διανομή	Απομακρυσμένη Τερματική Μονάδα(RTU) - Ευφυής Ηλεκτρονική Συσκευή(IED)	Λαμβάνουν δεδομένα από αισθητήρες και ενεργειακό εξοπλισμό, και μπορούν να δώσουν εντολές ελέγχου, όπως η ενεργοποίηση διακοπτών αν εντοπίσουν ανωμαλίες τάσης, ρεύματος ή συχνότητας. Οι RTUs και/ή οι IEDs μπορούν να αυξήσουν/χαμηλώσουν τα επίπεδα τάσης για να την διατηρήσουν στο επιθυμητό εύρος.
16	Διανομή	Εργαλεία Πεδίου	Ένα σύνολο εργαλείων μηχανικής και συντήρησης, που περιλαμβάνει φορητές υπολογιστικές συσκευές επικοινωνίας.

17	Διανομή	Γεωγραφικό Σύστημα Πληροφοριών (GIS)	Ένα σύστημα χωροταξικής διαχείρισης εργαλείων που παρέχει στις εταιρείες ηλεκτρισμού χρήσιμες πληροφορίες και συνδεσιμότητα δικτύου για προηγμένες εφαρμογές.
18	Διανομή	Αισθητήρας Διανομής	Μία συσκευή που μετρά φυσική ποσότητα και που μπορεί να διαβαστεί από έναν παρατηρητή ή ένα όργανο.
19	Αγορά	Κέντρο Ανταλλαγής Πληροφοριών για την Ενεργειακή Αγορά	Σύστημα λειτουργίας της αγοράς ενέργειας ευρείας περιοχής που παρέχει υψηλού επιπέδου σήματα για εταιρείες διανομής.
20	Αγορά	Σύστημα Ανεξάρτητου Διαχειριστή(ISO)-Περιφερειακός Οργανισμός Μεταφοράς Χονδρικής Αγοράς(RTO)	Ένα ISO/RTO είναι ένα κέντρο ελέγχου που συμμετέχει στην αγορά αλλά δεν χειρίζεται την αγορά.
21	Χειρισμός	Κέντρο Ελέγχου Προηγμένης Υποδομής Μέτρησης(AMI)	Αυτό το σύστημα διαχειρίζεται τα πληροφορίες μεταξύ άλλων συστημάτων, όπως το σύστημα διαχείρισης δεδομένων μετρητών (MDMS), και του δικτύου AMI.
22	Χειρισμός	Διαχείριση Μαζικής Αποθήκευσης	Παρέχει διαχείριση για ενεργειακή αποθήκευση που συνδέεται με το σύστημα μαζικής παραγωγής.
23	Χειρισμός	Σύστημα Πληροφοριών Πελάτη(CIS)	Εφαρμογές λογισμικού που επιτρέπουν στις εταιρείες να διαχειρίζονται πτυχές των σχέσεων τους με τους πελάτες.
24	Χειρισμός	Εκπρόσωπος Εξυπηρέτησης Πελατών(CSR)	Εξυπηρέτηση πελατών που παρέχεται από ένα άτομο (για παράδειγμα εκπρόσωπος πωλήσεων και υπηρεσιών) ή αυτοματοποιημένα μέσα (για παράδειγμα διαδραστικό σύστημα φωνητικής απόκρισης - IVR).

25	Χειρισμός	Διαχείριση Κατανεμημένης Παραγωγής και Αποθήκευσης	Η κατανεμημένη παραγωγή είναι η διαδικασία παραγωγής ενέργειας από πολλές μικρές τοπικές πηγές. Η διαχείριση της αποθήκευσης επιτρέπει την αποτελεσματική ενσωμάτωση των κατανεμημένων πηγών παραγωγής στο δίκτυο.
26	Χειρισμός	Τεχνολογία Διανομής	Μια τεχνική λειτουργία σχεδιασμού ή διαχείρισης του σχεδιασμού ή της αναβάθμισης του συστήματος διανομής. Για παράδειγμα: • Η προσθήκη νέων πελατών. • Η κατασκευή για νέο φορτίο. • Οι ρυθμίσεις και/ή οι επενδύσεις για τη βελτίωση της αξιοπιστίας του συστήματος.
27	Χειρισμός	Συστήματα Διαχείρισης Διανομής(DMS)	Μια σειρά εφαρμογών λογισμικού που υποστηρίζουν τους χειρισμούς του συστήματος ηλεκτρικής ενέργειας. Παραδείγματα τέτοιων εφαρμογών περιλαμβάνουν επεξεργαστή τοπολογίας, ανάλυση διαταραχών, ανάλυση λειτουργίας μάθησης, διαχείρισης αλλαγής εντολών, ανάλυση βραχυκυκλώματος, διαχείριση Volt/VAR, και ανάλυση απωλειών. Αυτές οι εφαρμογές παρέχουν στο λειτουργικό προσωπικό και το τεχνικό προσωπικό πληροφορίες και εργαλεία για την επίτευξη των στόχων τους.
28	Χειρισμός	Χειριστής Διανομής	Ένα άτομο που διαχειρίζεται το σύστημα διανομής.

29	Χειρισμός	Συστήματα Βιομηχανικού Αυτομάτου Ελέγχου και Τηλεμετρίας (SCADA) Διανομής	Ένα εποπτικό αυτοματοποιημένο σύστημα που συλλέγει και επεξεργάζεται δεδομένα και εφαρμόζει λειτουργικό έλεγχο για συστήματα διανομής .
30	Χειρισμός	Σύστημα Διαχείρισης Ενέργειας (EMS)	Ένα σύστημα που χρησιμοποιείται από τους διαχειριστές του ηλεκτρικού δικτύου για την παρακολούθηση, τον έλεγχο και τη βελτιστοποίηση της απόδοσης των συστημάτων παραγωγής και/ή μεταφοράς.
31	Χειρισμός	Λειτουργίες ISO/RTO	Κέντρο ελέγχου του συστήματος ηλεκτρικής ενέργειας ευρείας περιοχής, παρέχει γενική διαχείριση φορτίου και ανάλυση ασφαλείας για το δίκτυο μεταφοράς συνήθως με τη χρήση EMS με εφαρμογές παραγωγής και ανάλυσης δικτύου.
32	Χειρισμός	Συστήματα Διαχείρισης Φορτίου(LMS) - Σύστημα Διαχείρισης Απόκρισης της Ζήτησης(DRMS)	Ένα LMS δίνει εντολές διαχείρισης φορτίου σε συσκευές ή εξοπλισμό πελατών, προκειμένου να μειωθεί το φορτίο στις περιόδους αιχμής ή έκτακτης ανάγκης. Το DRMS δίνει κοστολόγηση ή άλλα σήματα σε συσκευές και εξοπλισμό πελατών για να μειώσουν ή να αυξήσουν τα φορτία τους ως απόκριση στα σήματα.
33	Χειρισμός	Σύστημα Διαχείρισης Δεδομένων Μετρητών (MDMS)	Σύστημα που αποθηκεύει δεδομένα μετρητών (όπως κατανάλωση ενέργειας, παραγωγή ενέργειας, μετρήσεις και αποτελέσματα δοκιμών του μετρητή) και καθιστά τα δεδομένα διαθέσιμα σε εξουσιοδοτημένα συστήματα. Αυτό το σύστημα είναι ένα τμήμα του συστήματος επικοινωνίας του πελάτη.

34	Χειρισμός	Γραφείο Υποστήριξης Μετρήσεων-Κοστολόγησης	Γραφείο υποστήριξης μετρήσεων και κοστολόγησης όλων των συστημάτων που χρησιμοποιεί μια εταιρεία ηλεκτρικής ενέργειας.
36	Χειρισμός	Σύστημα Διαχείρισης Διακοπής Λειτουργείας (OMS)	Το OMS είναι ένα υπολογιστικό σύστημα που χρησιμοποιείται από τους διαχειριστές διανομής για να βοηθήσει στην ανίχνευση και την αποκατάσταση διακοπών λειτουργείας. Οι κύριες λειτουργίες ενός OMS περιλαμβάνουν: • Καταχώρηση όλων πελατών που έχουν διακοπές. • Πρόβλεψη της τοποθεσίας της ασφάλειας ή του διακόπτη που άνοιξε κατά το σφάλμα. • Να βάλει σε σειρά προτεραιότητας τις προσπάθειες αποκατάστασης και να διαχειριστεί τους πόρους βάσει κριτηρίων όπως η τοποθεσία των εγκαταστάσεων έκτακτης ανάγκης, το μέγεθος και η διάρκεια των διακοπών. • Παροχή πληροφοριών σχετικά με την έκταση των διακοπών και τον αριθμό των πελατών που επηρεάζονται. • Εκτίμηση του χρόνου αποκατάστασης. • Διαχείριση και υπολογισμός του προσωπικού που βοηθά στην αποκατάσταση.

37	Χειρισμός	SCADA Μεταφοράς	Ένα εποπτικό αυτοματοποιημένο σύστημα που συλλέγει και επεξεργάζεται δεδομένα (για παράδειγμα την κατάσταση της συσκευής μεταφοράς) και εφαρμόζει λειτουργικό έλεγχο για συστήματα μεταφοράς .
38	Χειρισμός	Πύλη Πελατών	Η online διεπαφή μέσω της οποίας ένας πελάτης μπορεί να αλληλοεπιδράσει με έναν πάροχο υπηρεσιών ενέργειας. Συνήθως τέτοιες υπηρεσίες περιλαμβάνουν: την προβολή από τον πελάτη των ενεργειακών και χρεωστικών πληροφοριών online, εγγραφή σε προπληρωμένες ηλεκτρικές υπηρεσίες, την ενεργοποίηση της παρακολούθησης και του ελέγχου του πελάτη από τρίτη οντότητα (Third Party Service) .
39	Χειρισμός	Σύστημα Μέτρησης Ευρείας Περιοχής(WAMS)	Σύστημα επικοινωνίας που παρακολουθεί όλες τις μετρήσεις φάσης και τον εξοπλισμό του υποσταθμού σε μα μεγάλη γεωγραφική βάση που μπορεί να χρησιμοποιήσει τη μοντελοποίηση και άλλες τεχνικές για την παροχή πληροφοριών συστήματος στους διαχειριστές του ηλεκτρικού συστήματος.
40	Χειρισμός	Σύστημα Διαχείρισης Εργασίας(WMS)	Ένα σύστημα που παρέχει πληροφορίες ερευνητικών σχεδίων και χρονοδιαγράμματα για την κατασκευή και τη συντήρηση της υποδομής του συστήματος ενέργειας.
41	Πάροχοι Υπηρεσιών	Νέοι Πάροχοι Λιανικής Αγοράς Ενέργειας	Οποιοσδήποτε έμπορος, μεσάζοντας, δημόσιος οργανισμός, πόλη, χώρα ή περιφέρεια που συνδυάζει τα φορτία πολλαπλών πελατών για τη διευκόλυνση της πώλησης και της αγοράς ηλεκτρικής ενέργειας, της μεταφοράς και άλλων υπηρεσιών για λογαριασμό αυτών των πελατών.

42	Πάροχοι Υπηρεσιών	Τιμολόγηση	Μια οντότητα που εκτελεί τη λειτουργία δημιουργίας τιμολόγησης για να λάβει πληρωμή από τον πελάτη.
43	Πάροχοι Υπηρεσιών	Πάροχος Υπηρεσιών Ενέργειας(ESP)	Παρέχει ηλεκτρική ενέργεια, φυσικό αέριο και επιλογές καθαρής ενέργειας, καθώς και προϊόντα και υπηρεσίες ενεργειακής απόδοσης.
44	Πάροχοι Υπηρεσιών	Τρίτη Οντότητα	Ένας τρίτος πάροχος που παρέχει υπηρεσίες στην αγορά ενέργειας ανεξάρτητα από τις εταιρείες ηλεκτρισμού.
45	Μεταφορά	Μονάδα Μέτρησης Φάσορα(PMU)	Μία συσκευή που μετράει τις ηλεκτρικές παραμέτρους ενός δικτύου, συγχρονισμένο με την συντονισμένη παγκόσμια ώρα(UTC), όπως η γωνία φάσης, το πλάτος και η συχνότητα για τον προσδιορισμό της κατάστασης τους συστήματος,
46	Μεταφορά	Ευφυής Ηλεκτρονική Συσκευή Μετάδοσης(IED)	Μια συσκευή που λαμβάνει δεδομένα από αισθητήρες που βρίσκονται στο δίκτυο και τον εξοπλισμό ηλεκτρικής ενέργειας και μπορεί να δώσει εντολές ελέγχου, όπως η ενεργοποίηση διακοπτών, αν αισθανθούν ανωμαλίες της τάσης, ρεύματος ή συχνότητας, η αύξηση/μείωση των επιπέδων τάσης για να τη διατηρήσουν στα επιθυμητά επίπεδα. Μια συσκευή που στέλνει δεδομένα σε έναν συλλέκτη δεδομένων για πιθανή αναδιαμόρφωση.
47	Μεταφορά	Απομακρυσμένη Τερματική Μονάδα(RTU) Μεταφοράς	Μια απομακρυσμένη τερματική μονάδα που περνάει τα δεδομένα κατάστασης και μέτρησης από τον υποσταθμό μετάδοσης ή τον εξοπλισμό τροφοδοσίας σε συστήματα SCADA και τις εντολές μετάδοσης που αποστέλλονται από το σύστημα SCADA στο πεδίο εξοπλισμού.

48	Χειρισμός	Διαχείριση Ασφαλείας, Δικτύου, Συστήματος	Μία οντότητα που παρακολουθεί και ρυθμίζει τις συσκευές ασφαλείας, δικτύου και συστήματος.
49	Χειρισμός	Τεχνολογία Μετάδοσης	Μια τεχνική λειτουργία σχεδιασμού ή διαχείρισης του σχεδιασμού ή της αναβάθμισης του συστήματος μεταφοράς (για παράδειγμα εξοπλισμός σχεδιασμένος για περισσότερα από 350,000 Volts μεταξύ των αγωγών).

2.3 Τεχνολογίες Επικοινωνιών του Έξυπνου Δικτύου

Ένα σύστημα επικοινωνίας αποτελεί ένα από τα βασικά συστατικά της υποδομής του SG. Με την ενσωμάτωση προηγμένων τεχνολογιών κα εφαρμογών για την επίτευξη μας εξυπνότερης υποδομής του δικτύου, μια τεράστια ποσότητα δεδομένων θα παράγεται για περαιτέρω ανάλυση, έλεγχο και τιμολόγηση σε πραγματικό χρόνο. Συνεπώς, είναι πολύ σημαντικό για τις επιχειρήσεις ηλεκτρισμού να καθορίσουν τις απαιτήσεις επικοινωνίας και να βρουν την καλύτερη υποδομή επικοινωνιών για τη διαχείριση αυτών των δεδομένων και την παροχή αξιόπιστων, ασφαλών, οικονομικά αποδοτικών υπηρεσιών σε όλο το σύστημα. Οι επιχειρήσεις θα προσπαθήσουν να προσελκύσουν την προσοχή των πελατών για τη συμμετοχή τους στο σύστημα του SG προκειμένου να βελτιωθούν οι υπηρεσίες και η αποτελεσματικότητα του δικτύου. Επιπλέον , οι διακοπές λειτουργίας λόγω καταστροφών στη δομή του υπάρχοντος δικτύου καθιστούν σημαντική τη βελτίωση της επικοινωνίας ανάμεσα στο ηλεκτρικό δίκτυο και τα συστήματα επικοινωνίας.

Διαφορετικές τεχνολογίες επικοινωνιών υποστηρίζονται από δύο κύρια μέσα επικοινωνίας, δηλαδή τα ενσύρματα και τα ασύρματα, και μπορούν να χρησιμοποιηθούν για τη μεταφορά δεδομένων ανάμεσα στους έξυπνους μετρητές και τις εταιρείες ηλεκτρισμού. Σε ορισμένες περιπτώσεις, οι ασύρματες επικοινωνίες έχουν κάποια πλεονεκτήματα σε σχέση με τις ενσύρματες τεχνολογίες, όπως η μικρού κόστους υποδομή και η ευκολία σύνδεσης σε απρόσιτες περιοχές. Ωστόσο, λόγω της φύσης της μετάδοσης, το σήμα μπορεί να εξασθενίσει. Από την άλλη πλευρά, οι ενσύρματες δεν έχουν προβλήματα παρεμβολής και οι λειτουργίες τους δεν εξαρτώνται από μπαταρίες όπως συχνά στις ασύρματες.

Βασικά, χρειάζονται δύο τύποι υποδομής πληροφοριών για τη ροή πληροφοριών σε ένα έξυπνο δίκτυο. Η πρώτη ροή είναι από τον αισθητήρα και τις ηλεκτρικές συσκευές στους έξυπνους μετρητές, και η δεύτερη ανάμεσα στους έξυπνους μετρητές και στα κέντρα δεδομένων του δικτύου. Η πρώτη ροή δεδομένων μπορεί να επιτευχθεί μέσω επικοινωνιών ηλεκτρικής γραμμής (PLC) ή ασύρματων επικοινωνιών όπως ZigBee, 6LowPAN, Z-wave, και άλλες. Για τη δεύτερη ροή πληροφοριών, κυψελωτές τεχνολογίες ή το internet μπορούν να χρησιμοποιηθούν. Παρόλα αυτά, υπάρχουν βασικοί περιοριστικοί παράγοντες που πρέπει να ληφθούν υπόψη στη διαδικασία έξυπνης μέτρησης, όπως ο χρόνος εγκατάστασης, οι λειτουργικές δαπάνες, η διαθεσιμότητα της τεχνολογίας και το υπαίθριο/αστικό ή το εσωτερικό/εξωτερικό περιβάλλον. Η επιλογή τεχνολογίας που ταιριάζει σε ένα περιβάλλον μπορεί να μην είναι κατάλληλη για κάποιο άλλο. Στη συνέχεια περιγράφονται συνοπτικά κάποιες τεχνολογίες επικοινωνιών στο SG.

- **ZigBee**

Το ZigBee είναι μα τεχνολογία ασύρματων επικοινωνιών που κυμαίνεται σε χαμηλά επίπεδα κατανάλωσης ενέργειας, ρυθμού δεδομένων, πολυπλοκότητας και κόστους ανάπτυξης. Είναι μια ιδανική τεχνολογία για έξυπνο φωτισμό, παρακολούθηση της ενέργειας, οικιακό αυτοματισμό και αυτόματους μετρητές. Το ZigBee και το ZigBee Smart Energy Profile (SEP) έχουν χαρακτηριστεί ως τα πιο κατάλληλα πρότυπα επικοινωνίας για τον τομέα του οικιακού δικτύου του SG σύμφωνα με το NIST. Η επικοινωνία μεταξύ έξυπνων μετρητών, καθώς και έξυπνων οικιακών συσκευών είναι πολύ σημαντική. Πολλοί κατασκευαστές AMI προτιμούν τους έξυπνους μετρητές, οι οποίοι μπορούν να ενσωματώσουν το πρωτόκολλο ZigBee. Όταν το ZigBee ενσωματωθεί στους μετρητές, μπορεί να επικοινωνεί με άλλες συσκευές που είναι ενσωματωμένο και να τις ελέγχει. Το ZigBee SEP παρέχει τη δυνατότητα αποστολής ενημερωτικών μηνυμάτων στους ιδιοκτήτες των σπιτιών έτσι ώστε να ενημερώνονται για την κατανάλωση σε πραγματικό χρόνο.

- **Wireless Mesh**

Το ασύρματο δίκτυο πλέγματος είναι ένα ευέλικτο δίκτυο που αποτελείται από ένα σύνολο κόμβων, όπου νέοι κόμβοι μπορούν να ενταχθούν σε αυτό το σύνολο και κάθε κόμβος μπορεί να λειτουργήσει ως ανεξάρτητος δρομολογητής. Το χαρακτηριστικό της αυτοϊασης του δικτύου ενεργοποιεί τα σήματα επικοινωνίας για να βρουν μία άλλη διαδρομή μέσω ενεργών κόμβων, αν κάποιος κόμβος χρειαστεί να εγκαταλείψει το δίκτυο. Στη Βόρεια Αμερική τα συστήματα ραδιοσυχνοτήτων (RF) είναι πολύ δημοφιλή. Στο σύστημα έξυπνου μετρητή της εταιρείας PG&E, κάθε συσκευή είναι εξοπλισμένη με μονάδα ραδιοεπικοινωνίας και καθεμία από αυτές δρομολογεί τα δεδομένα μετρήσεων μέσω κοντινών μετρητών. Κάθε μετρητής ενεργεί ως επαναλήπτης σήματος έως ότου τα δεδομένα που συλλέχθηκαν φτάσουν στο σημείο πρόσβασης του ηλεκτρικού δικτύου. Στη συνέχεια τα δεδομένα που συλλέγονται φτάνουν στην εταιρεία ηλεκτρισμού μέσω του δικτύου επικοινωνίας.

- **Cellular Network Communication**

Τα υφιστάμενα κυψελωτά δίκτυα μπορούν να αποτελέσουν μία καλή επιλογή για την επικοινωνία μεταξύ έξυπνων μετρητών και εταιρειών ηλεκτρισμού και μεταξύ απομακρυσμένων κόμβων. Η υπάρχουσα υποδομή επικοινωνιών αποτρέπει τις εταιρείες από το να σπαταλούν λειτουργικά κόστη και επιπρόσθετο χρόνο για την κατασκευή μιας ειδικής υποδομής επικοινωνιών. Τα κυψελωτά δίκτυα επίσης ενεργοποιούν την ανάπτυξη έξυπνης μέτρησης σε ένα ευρύ περιβάλλον. Το 2G, 2.5G, 3G, WiMAX και LTE είναι οι τεχνολογίες επικοινωνιών που είναι διαθέσιμες στις εταιρείες για τη ανάπτυξη έξυπνων μετρήσεων. Όταν χρησιμοποιείται ένα διάστημα μεταφοράς δεδομένων 15 λεπτών μεταξύ μετρητή και εταιρείας, μια τεράστια ποσότητα δεδομένων θα παράγεται και ένας υψηλός ρυθμός σύνδεσης θα χρειαστεί για τη μεταφορά δεδομένων στην εταιρεία.

- **Powerline Communication**

Οι επικοινωνίες ηλεκτρικής γραμμής (PLC) είναι μια τεχνική που χρησιμοποιεί τις ήδη υπάρχουσες γραμμές ρεύματος για τη μετάδοση σημάτων δεδομένων υψηλής ταχύτητας (2–3 Mb/s) από μία συσκευή σε μία άλλη. Οι PLC αποτελούν μια σημαντική επιλογή για επικοινωνία με το μετρητή ηλεκτρικής ενέργειας λόγω της απευθείας σύνδεσης με τον μετρητή και των επιτυχημένων υλοποιήσεων AMI σε αστικές περιοχές όπου άλλες τεχνολογίες αδυνατούν να καλύψουν τις ανάγκες των εταιρειών. Τα συστήματα PLC που βασίζονται σε δίκτυα διανομής χαμηλής τάσης αποτελούν ένα από τα κύρια ερευνητικά θέματα για τις εφαρμογές του SG στην Κίνα. Σε ένα τυπικό PLC δίκτυο, οι έξυπνο μετρητές συνδέονται με τον συλλέκτη δεδομένων μέσω γραμμών ρεύματος και τα δεδομένα μεταφέρονται στο κέντρο δεδομένων μέσω τεχνολογιών κυψελωτών δικτύων. Για παράδειγμα, οποιαδήποτε ηλεκτρική συσκευή, όπως μετρητής ηλεκτρικής γραμμής που λειτουργεί ως πομποδέκτης, μπορεί να συνδεθεί στη γραμμή ρεύματος και να χρησιμοποιηθεί για την μετάδοση δεδομένων μέτρησης σε μια κεντρική τοποθεσία.

- **Digital Subscriber Lines**

Οι ψηφιακές συνδρομητικές γραμμές (DSLs) είναι μια τεχνολογία μεταφοράς ψηφιακών δεδομένων υψηλής ταχύτητας που χρησιμοποιεί καλώδια του τηλεφωνικού δικτύου. Είναι σύνηθες οι συχνότητες μέσω τηλεφωνικής γραμμής με ADSL να ξεπερνούν το 1 MHz. Η ήδη υπάρχουσα υποδομή των γραμμών DSL μειώνει το κόστος εγκατάστασης, γι’ αυτό και πολλές εταιρείες επιλέγουν την τεχνολογία DSL για τα ερευνητικά τους σχέδια πάνω στο SG. Ωστόσο, η απόδοση της σύνδεσης DSL εξαρτάται από το πόσο μακριά βρίσκεται ο συνδρομητής από το κέντρο τηλεφωνικής εξυπηρέτησης, γεγονός που δυσκολεύει τον προσδιορισμό της απόδοσης της τεχνολογίας DSL.

Συμπερασματικά, οι ενσύρματες τεχνολογίες όπως DSL, PLC, οπτική ίνα, έχουν μεγάλο κόστος για δίκτυα ευρείας ζώνης αλλά έχουν τη δυνατότητα να αυξήσουν τη

χωρητικότητα, την αξιοπιστία και την ασφάλεια των επικοινωνιών. Από την άλλη, οι ασύρματες τεχνολογίες, μπορούν να μειώσουν τα κόστη εγκατάστασης, αλλά παρέχουν περιορισμένο εύρος ζώνης και περιορισμένες επιλογές ασφαλείας.[7]

2.4 Το Έξυπνο Δίκτυο ως κυβερνο-φυσικό σύστημα

Οι δυνατότητες επικοινωνίας και πληροφορικής θα ενσωματωθούν σύντομα σε όλα τα είδη των αντικειμένων και των δομών στο φυσικό περιβάλλον. Εφαρμογές με τεράστιο κοινωνικό αντίκτυπο και οικονομικό όφελος θα δημιουργηθούν αξιοποιώντας αυτές τις δυνατότητες τόσο σε χώρο όσο και σε χρόνο. Τέτοια συστήματα, που ενώνουν τον κυβερνόκοσμο και τις επικοινωνίες με το φυσικό κόσμο ορίζονται ως κυβερνο-φυσικά συστήματα. Τα κυβερνο-φυσικά συστήματα (Cyber-physical systems - CPS) είναι φυσικά και μηχανικά συστήματα των οποίων οι λειτουργίες παρακολουθούνται, συντονίζονται, ελέγχονται και ενσωματώνονται από ένα κέντρο πληροφορικής και επικοινωνίας. Το διαδίκτυο άλλαξε τον τρόπο με τον οποίο οι άνθρωποι επικοινωνούν και αλληλοεπιδρούν μεταξύ τους, έφερε επανάσταση στο πως και στο που οι πληροφορίες είναι προσβάσιμες, και άλλαξε ακόμα και τον τρόπο με τον οποίο οι άνθρωπο αγοράζουν και πωλούν προϊόντα. Όμοίως τα CPS θα αλλάξουν τον τρόπο με τον οποίο οι άνθρωποι ελέγχουν και αλληλοεπιδρούν με το φυσικό κόσμο γύρω τους.

Παραδείγματα CPS περιλαμβάνουν το έξυπνο δίκτυο, ιατρικές συσκευές και συστήματα, αυτόνομα συστήματα αυτοκινήτων, ευφυή συστήματα μεταφοράς και αυτοκινητοδρόμων, αμυντικά συστήματα, ρομποτικά συστήματα και συστήματα βιομηχανικού ελέγχου. Τα CPS αλληλοεπιδρούν με το φυσικό κόσμο και πρέπει να λειτουργούν αξιόπιστα, με ασφάλεια, αποδοτικά και σε πραγματικό χρόνο. Μπορούν επίσης να θεωρηθούν ως συνδυασμός ενσωματωμένων συστημάτων (embedded systems), συστημάτων πραγματικού χρόνου και κατανεμημένων συστημάτων αισθητήρων και ελέγχου.[8]

Το SG ενσωματώνει τα φυσικά συστήματα (υποδομή ενεργειακού δικτύου) και κυβερνο-συστήματα (αισθητήρες, τεχνολογίες πληροφορικής και επικοινωνιών και άλλες προηγμένες τεχνολογίες), και παρουσιάζει τυπικά χαρακτηριστικά των CPS όπως:

- Ενσωμάτωση πραγματικών και εικονικών κόσμων σε ένα περιβάλλον όπου οι καταστάσεις από τα φυσικά συστήματα τροφοδοτούν τα κέντρα ελέγχου των CPS ως όρισμα και προσαρμόζουν τα μοντέλα προσομοίωσης ώστε να επιδρούν στο πως αποδίδουν μελλοντικά τα φυσικά συστήματα.
- Δυναμικές συνδέσεις και αλληλοεπιδράσεις μεταξύ συνιστωσών φυσικών συστημάτων και κυβερνο-συστημάτων μέσω δικτύων επικοινωνίας (για

παράδειγμα ad hoc δίκτυα) όπου οι έγκυρες αποκρίσεις είναι σημαντικές στη δυναμική τους σύμπραξη.

- Παράλληλος υπολογισμός σε πραγματικό χρόνο και επεξεργασία κατανεμημένων πληροφοριών, μεγάλων δεδομένων και ροών δεδομένων απαιτούνται προκειμένου να συμβάλλουν στην έγκαιρη λήψη αποφάσεων για τις λειτουργίες του SG στη μεταφορά και τη διανομή και τον προγραμματισμό των επιπέδων μέσω του CPS.
- Αυτο-προσαρμογή, αυτο-οργάνωση και αυτο-μάθηση, με τις οποίες το CPS μπορεί να ανταποκριθεί σε σφάλματα, επιθέσεις και έκτακτες ανάγκες προκειμένου να καταστεί δυνατή η ασφάλεια και η ανθεκτικότητα των SG και η ασφαλής παροχή ενέργειας.

Μια ερώτηση που δεν μπορεί να απαντηθεί ευθέως παραμένει το αν οι διαθέσιμες τεχνολογίες CPS είναι εύκολα εφαρμόσιμες. Το κύριο ζήτημα είναι το κατά πόσο μπορούν ενοποιηθούν τα φυσικά συστήματα και τα κυβερνο-συστήματα. Συχνά οι τεχνολογίες στον κυβερνοχώρο όπως δίκτυα επικοινωνίας και συσκευές αισθητήρων, ενσωματώνονται στα ενεργειακά συστήματα χωρίς να έχει γίνει η κατάλληλη προσαρμογή τους για να ταιριάζουν με τα χαρακτηριστικά τους: πολλή βαθμονόμηση και εξαρτήματα επιδιόρθωσης απαιτούνται συνήθως για μπορέσουν να λειτουργήσουν μαζί προκειμένου να ανταποκριθούν στις απαιτήσεις ασφαλείας του SG. Για παράδειγμα τα πρωτόκολλα τηλεπικοινωνίας για ασύρματα δίκτυα επικοινωνίας χρησιμοποιούνται για ανάκτηση μετρήσεων από έξυπνους μετρητές που έχουν εγκατεστημένες κάρτες SIM και λειτουργούν μέσω δικτύων δημόσιας επικοινωνίας. Αυτό καθιστά την ανίχνευση δεδομένων επιρρεπή στη συμφόρηση, εμποδίζοντας τη λήψη αποφάσεων που βασίζεται στα δεδομένα της έξυπνης μέτρησης (για παράδειγμα ανάγνωση κατανάλωσης από εκατομμύρια μετρητές την ίδια στιγμή) όταν υπάρχουν απαιτήσεις για τους χρόνους επικοινωνίας κατά τη διάρκεια των ωρών αιχμής. Ένα άλλο παράδειγμα είναι ο κατανεμημένος έλεγχος μέσω δικτύων επικοινωνίας που πέφτει θύμα της χρονικής καθυστέρησης, των χαμένων ή εσφαλμένων πακέτων, της διακοπής της απόδοσης ελέγχου, και σε ένα χειρότερο σενάριο προκαλεί την κατάρρευση του δικτύου.

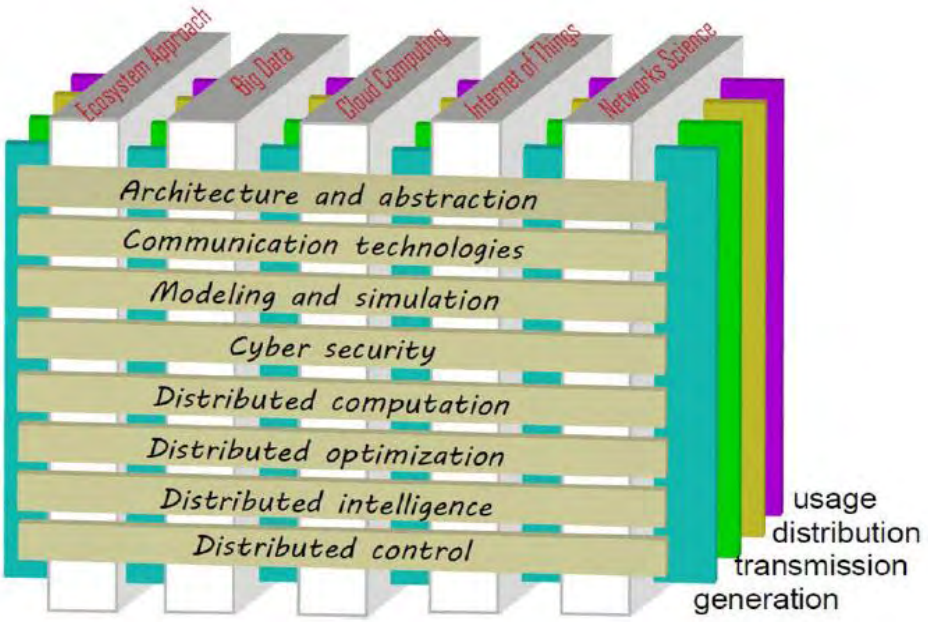
Μία ομαλή ενσωμάτωση αυτών των δύο (κυβερνο-συστημάτων και φυσικών συστημάτων) θα επιφέρει τεράστια οφέλη στο SG, όπως ακριβώς επέφερε η μηχατρονική στη βιομηχανία κατασκευής αυτοκινήτων, όπου ένας συνδυασμός μηχανικών, ηλεκτρικών, τηλεπικοινωνιών και μηχανικής υπολογιστών προσφέρει πολύ απλουστευμένο μηχανικό σχεδιασμό, γρήγορη εγκατάσταση μηχανών, δοκιμές ταχείας ανάπτυξης, βελτιστοποιημένη απόδοση, παραγωγικότητα, αξιοπιστία και οικονομική προσιτότητα. Στην Εικόνα 3 απεικονίζεται το πλαίσιο του SG από την οπτική των κυβερνο-φυσικών συστημάτων.

Υπάρχουν συγκεκριμένα χαρακτηριστικά των ενεργειακών συστημάτων που άλλα φυσικά συστήματα δε διαθέτουν, και έτσι δημιουργούν νέες προκλήσεις για τα CPS. Τα συστήματα ενεργειακών δικτύων απαιτούν χρονικά κρίσιμες, υψηλά συνδεδεμένες συνιστώσες να λειτουργούν μαζί σε πραγματικό χρόνο για την επίτευξη της σταθερότητα του συστήματος, της σωστής ρύθμισης της τάσης και της συχνότητας και της γρηγορότερης απόκρισης όταν υπάρχουν νέες ενεργειακές απαιτήσεις. Όλα αυτά γίνονται θέμα σε διάφορες εξωτερικές αβεβαιότητες και διαταραχές. Ειδικότερα για τα SG όταν οι απαιτήσεις από ανανεώσιμες πηγές, που εξαρτώνται από τις αβέβαιες καιρικές συνθήκες, είναι συγκεκριμένες. Σε αυτή την ομάδα δραστηριοτήτων, η εξισορρόπηση σε πραγματικό χρόνο, ο συντονισμός και η συνεργασία μεταξύ συμμετεχόντων πρέπει να ελέγχεται ιδανικά και κατανεμημένα προκειμένου να ακολουθήσει επιτυχώς μια ρουτίνα σχεδιασμού απόδοσης εκ των προτέρων. Στα SG, η συνδεσιμότητα και η δυναμική εξάρτηση της διατήρησης της σταθερότητας και της λειτουργικότητας του δικτύου είναι πιο κρίσιμη από οποιοδήποτε άλλο μηχανικό δίκτυο, όπως τα δίκτυα διανομής και logistic, ακόμα και τα δίκτυα επικοινωνίας, όπου μία απότομη πτώση της κάλυψης κινητού τηλεφώνου μπορεί να εμφανιστεί ανά πάσα στιγμή όταν υπάρχει συμφόρηση στο δίκτυο. Τέτοια περιστατικά δε μπορούν να επιτραπούν στα SG καθώς ένα κρίσιμος χρονικά έλεγχος πρέπει να εκτελείται και να διατηρείται η σταθερότητα προκειμένου να είναι δυνατή η αδιάλειπτη παροχή ενέργειας ανεξάρτητα από αβεβαιότητες και διαταραχές. Αυτές οι αυστηρές μηχανικές απατήσεις επιζητούν τη συντηρητική προσέγγιση στο σχεδιασμό και τη διαχείριση, επιτρέποντας σημαντικό πλεονασμό που μπορεί να μην είναι απαραίτητος. Τα CPS μπορούν να συμβάλλουν στη μείωση του πλεονασμού διατηρώντας παράλληλα τη σταθερότητα και τη λειτουργικότητα του SG.[22]

Προκειμένου να βελτιωθεί ο συσχετισμός κυβερνο-συστημάτων και φυσικών συστημάτων στο SG, απαιτούνται έξι βασικές λειτουργίες:

1) Υψηλή αξιοπιστία έτσι ώστε το σύστημα να μπορεί να επισκευαστεί με απλό και έγκαιρο τρόπο όταν συμβεί ένα σφάλμα, διατηρώντας την προσβασιμότητα ακόμη κι αν αυτό προκύψει, ενώ την ίδια στιγμή δεν προκαλεί καμία βλάβη όταν κάποιο μέρος παρουσιάζει δυσλειτουργίες.
2) Υψηλή αξιοπιστία σε ανοιχτά, εξελισσόμενα και αβέβαια περιβάλλοντα, έτσι ώστε το σύστημα να μπορεί να συνεχίσει τη λειτουργία του ακόμα και παρουσία βλαβών χωρίς θεμελιώδης αλλαγές στις αρχικές του ρυθμίσεις.
3) Υψηλή προβλεψιμότητα που εγγυάται συγκεκριμένα αποτελέσματα εντός του χρονικού διαστήματος που απαιτείται για να λειτουργεί με ακρίβεια.
4) Υψηλή βιωσιμότητα με ενσωματωμένη αυτοΐαση και μηχανισμούς διόρθωσης και προσαρμογής σε μεταβαλλόμενα περιβάλλοντα.
5) Υψηλή ασφάλεια ώστε το σύστημα να διαθέτει επαρκής τρόπους για να προστατευθεί από μη εξουσιοδοτημένη πρόσβαση και επιθέσεις.
6) Υψηλή διαλειτουργικότητα που ενεργοποιεί το σύστημα ώστε να παρέχει ή να δέχεται υπηρεσίες που συμβάλλουν στην αποτελεσματικότητα της

επικοινωνίας και της διαλειτουργικότητας μεταξύ των στοιχείων του συστήματος.[10]



Εικόνα 3 - Το Smart Grid από την οπτική των κυβερνο-φυσικών συστημάτων [9]

2.5 Προκλήσεις στο Έξυπνο Δίκτυο

Πολλές από τις κύριες λειτουργίες του SG έχουν ήδη οριστεί. Το SG πρέπει να διαθέτει την ικανότητα αυτοΐασης, παροχής ενέργειας υψηλής ποιότητας, να προσφέρει πλήθος επιλογών στην παραγωγή και την αποθήκευση, να είναι πιο αποδοτικό και να δίνει κίνητρα στους καταναλωτές ώστε να είναι πιο ενεργοί στη διαδικασία απόκρισης στη ζήτηση. Για να μπορέσει να πραγματοποιήσει αυτές τα λειτουργίες, διεξάγονται προηγμένες έρευνες από πανεπιστήμια και κρατικούς οργανισμούς. Για κάθε λειτουργία, το SG αντιμετωπίζει μια σειρά προκλήσεων. Στον τομέα της ποιότητας της ενέργειας, η έρευνα επικεντρώνεται κυρίως στους έξυπνους μετρητές για την ανίχνευση, τον εντοπισμό και την αξιολόγηση διαφορετικών τύπων παραμόρφωσης, ενώ η ανάπτυξη προηγμένων τεχνολογιών ενέργειας βοηθά στην καταστολή αυτών των παραμορφώσεων. Άλλες προκλήσεις όπως η ενσωμάτωση ανανεώσιμων πηγών ενέργειας στο ηλεκτρικό δίκτυο, η παραγωγή βασισμένη στην πρόβλεψη των αναγκών, η ανάπτυξη μονάδων αποστολής και συστημάτων αποθήκευσης ενέργειας χρειάζονται περαιτέρω διερεύνηση. Στη συνέχεια περιγράφονται οι πιο πιθανές προκλήσεις που θα χρειαστεί να ξεπεράσει το έξυπνο δίκτυο προκειμένου να υλοποιηθεί.

1) Ενέργειες Αυτοΐασης

Ένα SG έχει την ικανότητα αυτοΐασης: αυτό σημαίνει ότι θα πρέπει είναι σε θέση να αναλάβει δράση προκειμένου να συνεχίσει την παροχή ενέργειας μετά από ένα ενδεχόμενο συμβάν. Για να γίνει αυτό, πρέπει ένας μικροελεγκτής να συνδέεται με όλα τα στοιχεία του δικτύου, και μέσω αξιόπιστου συστήματος επικοινωνίας με ένα κέντρο ελέγχου. Οι προκλήσεις που πρέπει να αντιμετωπιστούν σε αυτό το επίπεδο:

- **Ασφάλεια**: Όταν ένα ηλεκτρικό δίκτυο ψηφιοποιείται, εκτίθεται σε όλους τους κινδύνους και επιθέσεις του διαδικτύου όπως spams, διαδικτυακά ¨σκουλήκια¨ (worms) και ιούς. Επίσης το ηλεκτρικό δίκτυο που μπορεί να αντιπροσωπεύει οποιοδήποτε έθνος, πρέπει να είναι προστατευμένο απέναντι σε επιθέσεις, όπου με την ψηφιοποίησή του ενδεχομένως να γίνει πιο προσβάσιμο και ευάλωτο απέναντι σε επιθέσεις από χάκερς.
- **Αξιοπιστία**: Η λειτουργία του δικτύου εξαρτάται από το δίκτυο επικοινωνίας που είναι ευάλωτο απέναντι σε φυσικές καταστροφές όπως καταιγίδες , αστραπές, πυρκαγιές. Αυτό το γεγονός μπορεί να μειώσει σημαντικά την αξιοπιστία του δικτύου και να προκαλέσει διακοπές λειτουργίας που έχουν πολύ μεγάλη επίδραση στο δίκτυο.

2) Ενσωμάτωση Ανανεώσιμων Πηγών Ενέργειας στο Δίκτυο

Αποτελεί ένα πολύ ενεργό πεδίο στον ερευνητικό τομέα. Με την ενσωμάτωση ανανεώσιμων πηγών ενέργειας όπως τα αιολικά και ηλιακά συστήματα παραγωγής στο δίκτυο μπορούν να προκύψουν προκλήσεις όπως:

- **Πρόγνωση ανέμου**: Για την πρόβλεψη της απαιτούμενης παραγωγής σε μια χρονική περίοδο, πρέπει να υπάρχει ακριβής πρόβλεψη της ταχύτητας και της κατεύθυνσης του ανέμου και στη συνέχεια να υπολογιστεί η παραγομένη ενέργεια. Επειδή ο άνεμος είναι διακοπτόμενος, δεν είναι εύκολο να γίνει πρόβλεψη και ειδικά μακροπρόθεσμα.
- **Διαχείριση παραγωγής από άνεμο**: Η λειτουργία ενός αιολικού συστήματος μπορεί να θεωρηθεί εξαρτημένη από τον καιρό και αυτό μπορεί να επηρεάσει τη διαχείριση της παραγωγής.
- **Βελτιστοποίηση ροής ισχύος**: Η αιολική παραγωγή υφίσταται σε περιοχές όπου υπάρχουν οι κατάλληλες συνθήκες, και αυτές οι περιοχές μπορεί να βρίσκονται σε διαφορετική τοποθεσία από όπου είναι το φορτίο. Η κύρια συνέπεια είναι η υψηλή συμφόρηση των γραμμών μεταφοράς. Μιας και η κατασκευή νέων γραμμών δεν είναι οικονομικά εφικτή, οι τρόποι μεταφοράς ενέργειας σε διαφορετικά σημεία με μεγάλες αποστάσεις αποτελεί σοβαρή πρόκληση.
- **Σταθερότητα συστήματος ηλεκτρικής ενέργειας**: Ο μετασχηματιστής του συστήματος αιολικής ενέργειας, διαχωρίζει την ανεμογεννήτρια από το υπόλοιπο

δίκτυο. Αυτό μπορεί να έχει μία δυσμενή επίδραση στη σταθερότητα του συστήματος λόγω της μειωμένης αδράνειας, ειδικά όταν πρόκειται για υψηλή αιολική “διείσδυση”.[11]

3) Συστήματα Αποθήκευσης Ενέργειας

Όταν πλέον τα συστήματα παραγωγής ενέργειας βασίζονται σε ανανεώσιμες πηγές ενέργειας, είναι σημαντική η ενσωμάτωση περισσότερων συστημάτων αποθήκευσης ενέργειας καθώς το επίπεδο συστημάτων που βασίζεται στην παραγωγή από ανανεώσιμες πηγές αυξάνεται στο δίκτυο ηλεκτρικής ενέργειας προκειμένου να διογκωθεί η μεταβλητότητα και η διαθεσιμότητα του ανέμου. Οι προκλήσεις που αφορούν τα συστήματα αποθήκευσης ενέργειας είναι:

- **Κόστη**: Τα συστήματα αποθήκευσης ενέργειας είναι δαπανηρά και απαιτείται περαιτέρω έρευνα για τη μείωση του κόστους τέτοιων συστημάτων.
- **Πολυπλοκότητα**: Η προσθήκη συστημάτων αποθήκευσης συνδέεται συχνά με την πολύπλοκη ανάλυση συστημάτων ηλεκτρικής ενέργειας. Κάθε σύστημα αποθήκευσης πρέπει να είναι κατάλληλα σχεδιασμένο για το σημείο του δικτύου που συνδέεται. Αυτό αυξάνει ακόμα περσότερο το κόστος των συσκευών που απαιτούνται.
- **Περιορισμένη ευελιξία:** Η προσθήκη νέων συστημάτων αποθήκευσης απαιτεί συχνά αρκετές μελέτες και υλικά που είναι δαπανηρά. Κάθε σύστημα αποθήκευσης είναι σχεδιασμένο για κάποια συγκεκριμένη διαμόρφωση του δικτύου και επομένως είναι δύσκολο να προσαρμοστεί στις αλλαγές του δικτύου, γεγονός που το καθιστά μη ευέλικτο. Με τη διαμόρφωση του μελλοντικού δικτύου, είναι απαραίτητο να βρεθούν τρόποι ώστε η τεχνολογία αυτών των συστημάτων να γίνει πιο ευέλικτη και προσαρμόσιμη στα διάφορα συστήματα.[12]

4) Κίνητρο Καταναλωτών

Μια κύρια λειτουργία του SG είναι να παρακινήσει τους καταναλωτές να συμμετέχουν ενεργά στη διαχείριση της ενέργειας του δικτύου. Η λειτουργία αυτή αντιμετωπίζει επίσης τρεις προκλήσεις:

- **Ιδιωτικότητα**: Οι καταναλωτές είναι απαραίτητο να επικοινωνούν με τις εταιρείες ηλεκτρισμού προκειμένου να συμμετέχουν στη διαχείριση της κατανάλωσής τους. Αυτό συνεπάγεται την ανταλλαγή δεδομένων μεταξύ των δύο αυτών οντοτήτων. Με αυτό τον τρόπο, οι εταιρείες μπορεί να έχουν πρόσβαση σε προσωπικές πληροφορίες των πελατών, μιας και οι έξυπνοι μετρητές θα συλλέγουν συνέχεια δεδομένα και θα τα στέλνουν σε αυτές.

- **Ασφάλεια**: Η συλλογή δεδομένων γίνεται πλέον με ασύρματες συσκευές. Έτσι, τα δεδομένα μπορούν να υποκλαπούν και να αλλοιωθούν από κακόβουλα άτομα. Αυτό μπορεί να βλάψει τόσο τον καταναλωτή όσο κα τις εταιρείες. Ωστόσο, αυτό το ζήτημα έχει μεγαλύτερη επίδραση στις εταιρείες καθώς ο καταναλωτής μπορεί πλέον να παράγει και να πουλάει ενέργεια στο δίκτυο. Σε αυτή την περίπτωση, ως συνέπεια της αλλοίωσης δεδομένων, οι εταιρείες μπορούν να οδηγηθούν σε τεράστια έξοδα.
- **Εκπαίδευση καταναλωτών**: Ο καταναλωτής εξακολουθεί να χρειάζεται να μάθει γιατί θα έπρεπε να παίζει ενεργό ρόλο στη διαχείριση της κατανάλωσης του.[13]

5) Αξιοπιστία

Το SG αναμένεται να διανέμει αξιόπιστη ενέργεια στους καταναλωτές. Η αξιοπιστία του δικτύου αξιολογείται από τη συχνότητα και τη διάρκεια των διακοπών λειτουργίας. Το SG χρειάζεται να μειώσει και του δύο αυτούς αριθμούς για να βελτιώσει την αξιοπιστία του συστήματος. Οι πιθανές προκλήσεις που αντιμετωπίζει η βελτίωση της αξιοπιστίας είναι:

- **Αυτοματισμός του δικτύου**: Το δίκτυο πρέπει από μόνο του να μπορεί να ανιχνεύσει ένα σφάλμα, να το διορθώσει και να συνεχίσει την κανονική κατάσταση λειτουργίας του. Προφανώς, καταστέλλοντας την ανθρώπινη αλληλεπίδραση, ο χρόνος αποκατάστασης μειώνεται αρκετά. Αλλά για να το πετύχει αυτό, πρέπει να καταβληθεί σημαντική προσπάθεια στην οικοδόμηση ενός ισχυρού συστήματος δρομολόγησης δεδομένων. Ισχυρή και αξιόπιστη προστασία, έλεγχος και επικοινωνία του δικτύου πρέπει να τεθούν σε εφαρμογή.
- **Αναδιαμόρφωση του δικτύου**: Ένα άλλο χαρακτηριστικό του SG είναι η ικανότητα του να σπάει σε μικρότερα δίκτυα που είναι αυτόνομα όταν συμβεί μία απρόσμενη κατάσταση. Έτσι, ο καταναλωτής στο τέλος (ή την αρχή) της ηλεκτρικής γραμμής θα αντιμετωπίσει λιγότερες διακοπές. Αυτό καθιστά για το SG ένα αρκετά πολύπλοκο θέμα. Πολλά άλλα θέματα όπως η σταθερότητα του δικτύου και η ισορροπία παραγωγής-ζήτησης σε αυτά τα μικρότερα δίκτυα πρέπει να διευθετηθούν προκειμένου να τεθεί σε εφαρμογή το SG.[14]

6) Ποιότητα Ενέργειας

Το SG είναι απαραίτητο να παρέχει ενέργεια υψηλής ποιότητας στους καταναλωτές μέσω των ακόλουθων χαρακτηριστικών:

- **Προσδιορισμός διαταραχών**: Το SG πρέπει να εντοπίζει τη σωστή αιτία παραμόρφωσης του δικτύου για να προσδιορίζει αν η διαταραχή είναι από την

πλευρά της παραγωγής ή του φορτίου. Αυτό το θέμα βρίσκεται ακόμα σε πρώιμα στάδια έρευνας.

- **Καταστολή των Αρμονικών**: Προκειμένου να παρέχει υψηλή ποσότητα ενέργειας το SG, πρέπει να αναπτυχθούν τεχνικές μείωσης των αρμονικών παραμορφώσεων όπως η καταστολή των αρμονικών και άλλων γεγονότων που επηρεάζουν την τη ποιότητα της ενέργειας όπως οι πτώσεις ή διογκώσεις τάσης, οι κρουστικές υπερτάσεις, ή μεταβολές τάσης όπως οι υπερβολικά υψηλές ή χαμηλές τάσεις, οι διακυμάνσεις τάσης, η απόκλιση συχνότητας και η ανισορροπία τάσης.[11]

ΚΕΦΑΛΑΙΟ 3

ΑΣΦΑΛΕΙΑ ΚΑΙ ΙΔΙΩΤΙΚΟΤΗΤΑ ΣΤΟ ΕΞΥΠΝΟ ΔΚΤΥΟ

3.1 Ευπάθειες στο Έξυπνο Δίκτυο

Ένας από τους στόχους του SG είναι η βελτίωση της αξιοπιστίας και της ασφάλειας του δικτύου ηλεκτρικής ενέργειας. Ωστόσο με την ευρεία ενσωμάτωση τεχνολογιών πληροφορίας και δικτύου, το ηλεκτρικό δίκτυο θα γίνει εκτεθειμένο απέναντι σε ευπάθειες που αφορούν τα υπολογιστικά συστήματα και έναν αυξανόμενο αριθμό επιτιθέμενων με διάφορα κίνητρα. Οι έξυπνες συσκευές που χρησιμοποιούνται στο SG βασίζονται κυρίως σε κοινό υλικό και λογισμικό που τις καθιστά ευάλωτες στις ευπάθειες της ασφαλείας των άλλων διασυνδεδεμένων συσκευών. Για παράδειγμα, ¨σκουλήκια¨ μεταξύ έξυπνων μετρητών, αυτοματοποιημένα προγράμματα (bots) μετρητών, επιθέσεις άρνησης εξυπηρέτησης (Denial of Service - DoS), καταγραφείς στοιχείων χρήσης, ιοί τύπου rootkit και άλλοι ιοί στους έξυπνους μετρητές καθώς και κακόβουλα λογισμικά αναμένεται να εμφανιστούν στο μέλλον.

Εκτός από αυτές τα ευπάθειες, η εκτεταμένη χρήση νέων έξυπνων συσκευών θα αυξήσει τον αριθμό των σημείων εισόδου που μπορούν να εκμεταλλευτούν οι επιτιθέμενοι. Η ομοιότητα πολλών συσκευών σημαίνει ότι μια ευπάθεια που βρίσκεται σε μία συσκευή μπορεί να εκμεταλλευτεί πολλές, επιτρέποντας στους επιτιθέμενους (εξ αποστάσεως) να ξεκινούν επιθέσεις ευρείας κλίμακας. Πριν την εμφάνιση των έξυπνων μετρητών, κάποιος μπορούσε να επιτεθεί σε έναν μόνο μετρητή χρησιμοποιώντας μηχανικές συσκευές απλής τεχνολογίας. Οι παλιές επιθέσεις περιλαμβάνουν επιθέσεις που γυρίζουν το μετρητή και τον κάνουν να τρέξει προς τα πίσω, μαγνήτες υψηλής έντασης που χαμήλωναν την ένδειξη των δεικτών του μετρητή και απλή φυσική καταστροφή των έξυπνων μετρητών. Οι συνέπειες αυτών των επιθέσεων αφορούσαν μόνο ένα σπίτι. Επιπλέον, οι επιθέσεις αυτές ήταν εύκολο ανιχνεύσιμες από έναν υπάλληλο που διαβάζει το μετρητή.

Οι έξυπνοι μετρητές είναι κοινές συσκευές χαμηλού κόστους που είναι εγκατεστημένες σε φυσικά μη ασφαλείς τοποθεσίες. Οι επιτιθέμενοι (σε αυτή την περίπτωση οι ιδιοκτήτες του σπιτιού) μπορούν να εκθέσουν έναν μετρητή και να προσαρμόσουν προσεκτικά τις αλλαγές για να χειραγωγήσουν το ενεργειακό κόστος χωρίς να ανιχνευθούν. Τα συστήματα AMI, έχουν εισαγάγει νέες απειλές στη μέτρηση ενέργειας επιτρέποντας σε αυτές τις επιθέσεις να πραγματοποιηθούν εξ αποστάσεως, σε ευρύτερη κλίμακα και με μικρότερη πιθανότητα ανίχνευσης. Αυτό οφείλεται στο γεγονός ότι το AMI αφαιρεί την ανάγκη για τακτική ανάγνωση των μετρητών από υπαλλήλους. Μόλις αυτές

οι επιθέσεις γίνουν εφικτές, κάθε νέα σημαντική ευπάθεια θα αποτελέσει ένα σημαντικό ελάττωμα για τη βιομηχανία, του οποίου το κόστος δεν θα καθορίζεται μόνο από την απάτη καταναλωτών αλλά κα το κόστος επιδιόρθωσης εκατοντάδων εκατομμυρίων μετρητών.

Η δυνατότητα επηρεασμού πολλών στοιχείων του δικτύου ταυτόχρονα και εξ αποστάσεως αποτελεί ένα κρίσιμο σημείο για την αξιοπιστία του. Η αξιοπιστία των συστημάτων ηλεκτρικής ενέργειας μαζικής παραγωγής σήμερα βασίζεται στην παραδοχή τοπικών σφαλμάτων και επιθέσεων. Με τη νέα υποδομή, αυτή η παραδοχή απορρίπτεται πλέον και νέα μοντέλα κινδύνου της αξιοπιστίας πρέπει να αναπτυχθούν για την ενσωμάτωση της δυνατότητας ταυτόχρονης απώλειας πολλαπλών στοιχείων και σφαλμάτων των συσκευών.

Ένα άλλο σημαντικό ζήτημα που αφορά την ασφάλεια στο SG είναι ότι οι μελλοντικοί επιτιθέμενοι θα έχουν περισσότερα κίνητρα για να θέσουν σε κίνδυνο τις έξυπνες συσκευές. Συσκευές με νέες λειτουργίες όπως ο ηλεκτρονόμος απόστασης στην αυτοματοποίηση της διανομής, ή οι έξυπνοι μετρητές με επιλογές απομακρυσμένης αποσύνδεσης είναι ένας ελκυστικός στόχος για οργανισμούς ή ομάδες που έχουν ως σκοπό να διαταράξουν την κανονική λειτουργία του δικτύου και να προκαλέσουν διακοπές ρεύματος. Οι συνέπειες των επιθέσεων αυτών θα είναι διαφορετικές από αυτές των παραδοσιακών επιθέσεων: οι επιθέσεις στο SG μπορεί να έχουν καταστροφικές επιπτώσεις σε άλλες υποδομές στο φυσικό κόσμο. Για την ανάδειξη του πως θα μπορούσαν να χρησιμοποιηθούν οι επιθέσεις στον κυβερνοχώρο για την εκμετάλλευση ευπαθειών και την πρόκληση ζημιών των φυσικών συστημάτων, το Τμήμα Εθνικής Ασφάλειας των Ηνωμένων Πολιτειών απέδειξε την ικανότητα για πρόκληση βλάβης σε μια ηλεκτρογεννήτρια από μια επίθεση στο κυβερνοχώρο, με τη δημιουργία ενός προσεκτικά επιλεγμένου κακόβουλου σήματος ελέγχου.[15]

Επιπροσθέτως στα τεχνικά ζητήματα ασφάλειας, υπάρχουν πολλά οργανωτικά ζητήματα που συμπεριλαμβάνουν τον ανθρώπινο παράγοντα και τα ρυθμιστικά προβλήματα, τα οποία μπορούν να επηρεάσουν την ασφάλεια των εγκαταστάσεων του SG:

1) **Έλλειψη πληροφοριών**: Οι καταναλωτές δεν είναι επαρκώς ενημερωμένοι σχετικά με τα οφέλη, τα κόστη και τους κινδύνους που σχετίζονται με τα συστήματα του SG. Αυτό μπορεί να περιορίσει το βαθμό στον οποίο οι καταναλωτές θα είναι πρόθυμοι να πληρώσουν για ασφαλή και αξιόπιστα συστήματα, γεγονός που μπορεί να προκαλέσει την διστακτικότητα των ρυθμιστικών φορέων για αύξηση των φόρων που σχετίζονται με την ασφάλεια στον κυβερνοχώρο. Ως εκ τούτου, οι

εταιρείες ηλεκτρισμού μπορεί να μην επενδύσουν στον τομέα της ασφάλειας, αυξάνοντας έτσι τον κίνδυνο επιθέσεων.

2) **Έλλειψη εστίασης**: Οι εταιρείες ηλεκτρισμού επικεντρώνονται περισσότερο στην κανονιστική ρύθμιση παρά στην ολοκληρωμένη ασφάλεια. Συγκεκριμένα οι εταιρείες επικεντρώνονται στην επίτευξη ελάχιστων κανονιστικών απαιτήσεων, οι οποίες είναι ελλιπείς.

3) **Έλλειψη χαρακτηριστικών ασφαλείας**: Η ασφάλεια δεν είναι πάντα ενσωματωμένη στις συσκευές του SG. Πολλοί έξυπνοι μετρητές δεν υποστηρίζουν τα απαραίτητα χαρακτηριστικά ασφαλείας όπως η καταγραφή γεγονότων και παράξενων ενεργειών, που χρειάζονται για την ανίχνευση και την ανάλυση επιθέσεων. Επιπλέον τα HAN του SG δε διαθέτουν επαρκή ασφάλεια στη δομή τους.

4) **Ανταλλαγή πληροφοριών**: Η βιομηχανία ηλεκτρισμού στερείται αποτελεσματικού μηχανισμού για την αποκάλυψη πληροφοριών σχετικά με τις ευπάθειες της ασφάλειας στον κυβερνοχώρο του SG, περιστατικών, απειλών, διδαγμάτων και βέλτιστων πρακτικών σε αυτό τον τομέα. Χωρίς ποιοτικές μεθόδους για την ανταλλαγή πληροφοριών, οι εταιρείες δεν έχουν τις απαραίτητες πληροφορίες για να προστατεύσουν επαρκώς τα δομικά τους στοιχεία.

5) **Μέτρο επιτυχίας**: Η ηλεκτρική βιομηχανία δεν έχει μεθόδους μέτρησης της ασφάλειας στον κυβερνοχώρο, κάνοντας έτσι δύσκολη την εκτίμηση του μεγέθους των επενδύσεων που χρειάζονται για την ασφάλεια στον κυβερνοχώρο, προκειμένου να βελτιώσει την ασφάλεια των συστημάτων του SG. Αν κα αυτές οι μέθοδοι είναι δύσκολο να αναπτυχθούν, θα μπορούσαν να βοηθήσουν να καθοριστεί ένας συνδυασμός λύσεων ασφαλείας που θα επιφέρει το πιο ασφαλές σύστημα.

6) **Ρυθμιστικά ζητήματα**: Η νομική αρμοδιότητα μεταξύ κρατικών και ομοσπονδιακών ρυθμιστικών αρχών ιστορικά καθορίζεται από το αν η τεχνολογία βρίσκεται στα συστήματα μετάδοσης ή διανομής. Η τεχνολογία του SG περιπλέκει τα πράγματα επειδή οι έξυπνες συσκευές στη διανομή, στο σύνολό τους, μπορούν να έχουν αντίκτυπο στην αξιοπιστία της μετάδοσης που είναι ευθύνη της ομοσπονδιακής ρυθμιστικής επιτροπής ενέργειας.[16]

Το SG εισάγει ενισχυμένες και βελτιωμένες δυνατότητες στο παραδοσιακό δίκτυο ηλεκτρικής ενέργειας με αποτέλεσμα να μετατρέπεται σε πιο πολύπλοκο και ευάλωτο σε διάφορους τύπους επιθέσεων. Αυτές οι ευπάθειες θα μπορούσαν να επιτρέψουν στους επιτιθέμενους να έχουν πρόσβαση στο δίκτυο, να ¨σπάσουν¨ την εμπιστευτικότητα και την ακεραιότητα των δεδομένων, και να κάνουν μία υπηρεσία μη διαθέσιμη. Οι πιο σημαντικές ευπάθειες στα SG είναι:

1) **Ασφάλεια καταναλωτών**: Οι έξυπνοι μετρητές συλλέγουν αυτόνομα μεγάλες ποσότητες δεδομένων και τις μεταφέρουν στις εταιρείες ηλεκτρισμού, τους καταναλωτές και τους παρόχους υπηρεσιών. Αυτά τα δεδομένα περιλαμβάνουν προσωπικές πληροφορίες που θα μπορούσαν να χρησιμοποιηθούν για την εξαγωγή πληροφοριών σχετικά με τις δραστηριότητες των καταναλωτών, τις συσκευές που χρησιμοποιούν και τις ώρες τις οποίες τα σπίτια είναι άδεια.

2) **Μεγαλύτερος αριθμός έξυπνων συσκευών**: Ένα SG έχει πολλές έξυπνες συσκευές που εμπλέκονται τόσο στη διαχείριση της παροχής ενέργειας όσο και στη ζήτηση του δικτύου. Αυτές οι συσκευές μπορούν να λειτουργήσουν ως σημεία εισόδου στο δίκτυο. Επιπλέον το μέγεθος του δικτύου (εκατό με χίλιες φορές μεγαλύτερο από αυτό του ίντερνετ) καθιστά εξαιρετικά δύσκολη την παρακολούθηση και τη διαχείρισή του.

3) **Φυσική ασφάλεια**: Σε αντίθεση με το παραδοσιακό σύστημα ενέργειας, το SG περιλαμβάνει πολλά δομικά στοιχεία και τα περισσότερα από αυτά βρίσκονται εκτός των εγκαταστάσεων των εταιρειών ηλεκτρισμού. Αυτό το γεγονός αυξάνει τον αριθμό των φυσικών τοποθεσιών που είναι μη ασφαλείς και τις καθιστά ευάλωτες σε φυσική πρόσβαση.

4) **Η διάρκεια ζωής των συστημάτων ηλεκτρικής ενέργειας**: Δεδομένου ότι τα συστήματα ηλεκτρικής ενέργειας συνυπάρχουν με τη σχετικά μικρής διάρκειας ζωή των συστημάτων τεχνολογίας πληροφοριών, είναι αναπόφευκτο οι απαρχαιωμένοι εξοπλισμοί να θέτονται ακόμα σε χρήση. Τέτοιου είδους εξοπλισμοί μπορούν να λειτουργήσουν ως τρωτά σημεία ασφαλείας και ενδεχομένως να είναι μη συμβατοί με τις σύγχρονες συσκευές.

5) **Απεριόριστη εμπιστοσύνη μεταξύ παραδοσιακών ηλεκτρικών συσκευών**: Η επικοινωνία μεταξύ συσκευών στο σύστημα ελέγχου είναι ευάλωτη στην πλαστογράφηση (spoofing) δεδομένων όπου η κατάσταση μίας συσκευής επηρεάζει τις ενέργειες κάποιας άλλης. Για παράδειγμα, μία συσκευή που στέλνει

μία ψευδή κατάσταση κάνει άλλες συσκευές να συμπεριφέρονται με ανεπιθύμητο τρόπο.

6) **Διαφορετικό υπόβαθρο μεταξύ συνόλων εργαζομένων**: Η ανεπαρκής και ανοργάνωτη επικοινωνία μεταξύ συνόλων εργαζομένων μπορεί να επιφέρει πολλές λανθασμένες αποφάσεις που θα οδηγήσουν σε ευπάθεια.

7) **Χρήση πρωτοκόλλου ίντερνετ (IP) και εμπορικού υλικού και λογισμικού**: Η χρήση των προτύπων IP στα SG προσφέρει ένα μεγάλο πλεονέκτημα με το να παρέχει συμβατότητα μεταξύ διαφόρων δομικών στοιχείων. Ωστόσο οι συσκευές που χρησιμοποιούν IP, είναι αρκετά ευάλωτες σε επιθέσεις που στηρίζονται σε IP, όπως IP spoofing, DoS και άλλες.

8) **Περισσότεροι συμμέτοχοι**: Με την αύξηση των συμμετεχόντων μπορεί να προκληθεί η αύξηση ενός επικίνδυνου είδους επιθέσεων: εσωτερικές επιθέσεις.[17]

3.2 Απειλές στο Έξυπνο Δίκτυο

3.2.1 Στόχοι και απαιτήσεις

Υπάρχουν πολλοί οργανισμοί που έχουν κάνει εκτεταμένη έρευνα πάνω στην ανάπτυξη των στόχων και των απαιτήσεων της κυβερνοασφάλειας συμπεριλαμβανομένου του Ινστιτούτου Έρευνας Ηλεκτρικής Ενέργειας (EPRI), του Εθνικού Ινστιτούτου Ενέργειας και Τεχνολογίας (NIST), της Επιτροπής Διαλειτουργικότητας του Έξυπνου Δικτύου (SGIP) και του Ινστιτούτου Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών (IEEE). Σύμφωνα με το NIST, οι τρείς γενικοί στόχοι της κυβερνοασφάλειας είναι οι εξής: διαθεσιμότητα, ακεραιότητα και εμπιστευτικότητα. Εκτός από τους στόχους της κυβερνοασφάλειας το NIST διευθετεί επίσης κάποιες συγκεκριμένες απαιτήσεις όπως ταυτοποίηση, αυθεντικοποίηση, εξουσιοδότηση, εμπιστοσύνη, έλεγχος πρόσβασης και προστασία της ιδιωτικότητας. Τα πλαίσια και οι κατευθυντήριες γραμμές ορίζονται από φορείς που χρειάζεται να εξελίσσονται συνεχώς προκειμένου να εξασφαλίζουν την ασφαλή, αξιόπιστη και με δυνατότητες ανάπτυξης λειτουργία του SG. Στη συνέχεια περιγράφονται συνοπτικά οι στόχοι της προστασίας της υποδομής του κυβερνοχώρου του SG.

- **Εμπιστευτικότητα**: Η αποτροπή μη εξουσιοδοτημένης πρόσβασης κάποιου άλλου προσώπου σε πληροφορίες υψίστης ασφαλείας, όπως η χρήση ενέργειας,

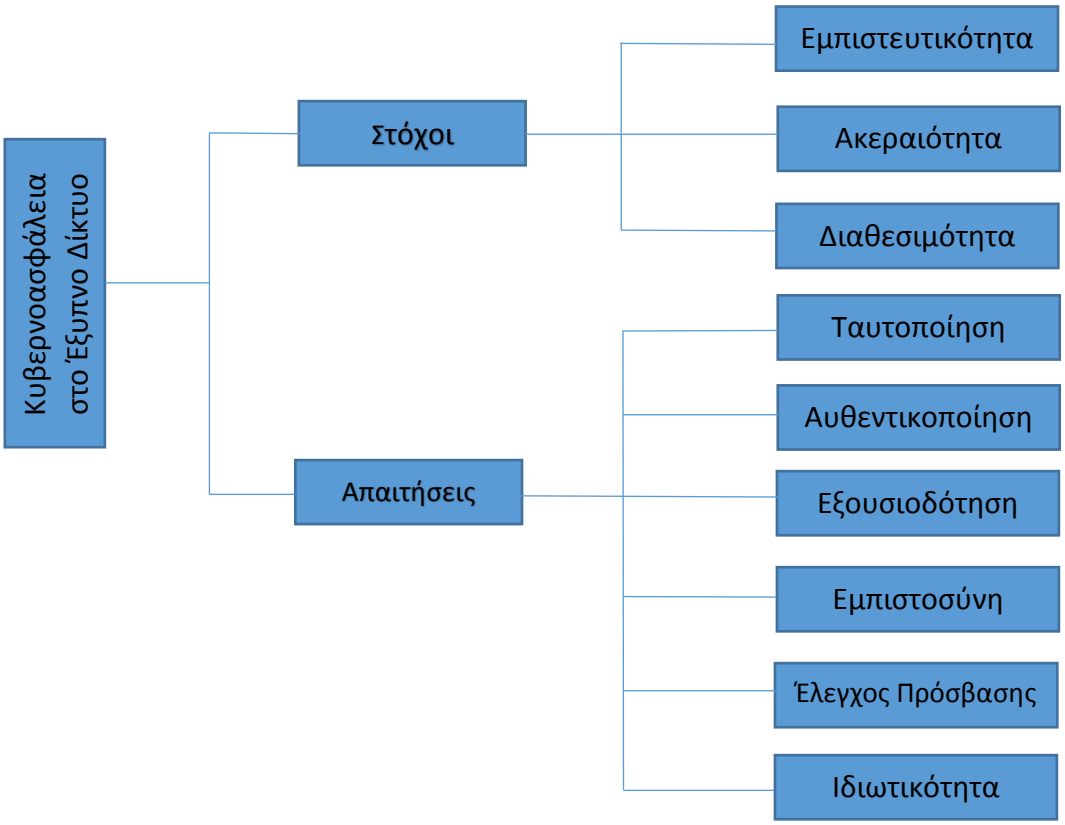
πληροφορίες για τις τιμές και εντολές ελέγχου, που παραβιάζει την ιδιωτικότητα των πελατών και αποκαλύπτει απόρρητες πληροφορίες των εταιρειών ηλεκτρισμού καλείται εμπιστευτικότητα. Ωστόσο, η εμπιστευτικότητα του λογισμικού δεν θα έπρεπε να θεωρείται και τόσο σημαντική, αλλά θα πρέπει να δοθεί έμφαση στη μυστικότητα των κλειδιών.

- **Ακεραιότητα**: Η αποτροπή τροποποίησης κρίσιμων πληροφοριών αισθητήριων συσκευών, ηλεκτρονικού εξοπλισμού (για παράδειγμα έξυπνοι μετρητές), λογισμικού και εντολών ελέγχου που θα μπορούσε να διαταράξει τη λήψη αποφάσεων και να διαβάλει την ανταλλαγή δεδομένων του SG καλείται ακεραιότητα. Η απορρόφηση εσφαλμένων δεδομένων, αντίθετα στην εκτίμηση της κατάστασης μπορεί να θέσει σε κίνδυνο την ακεραιότητα του SG και να προκαλέσει κακοδιαχείριση της ενέργειας. Σε αντίθεση με την εμπιστευτικότητα, η ακεραιότητα του λογισμικού παραμένει κρίσιμης σημασίας επειδή μέσω κακόβουλου λογισμικού μπορεί να ελέγχει κάποιος άλλος μια συσκευή ή έναν ηλεκτρονικό εξοπλισμό .

- **Διαθεσιμότητα**: Η αποτροπή ενός άλλου προσώπου από το να μην παρέχει πρόσβαση ή έλεγχο του συστήματος σε εξουσιοδοτημένο προσωπικό καλείται διαθεσιμότητα. Οι επιθέσεις άρνησης της εξυπηρέτησης (DoS) και κατανεμημένες επιθέσεις άρνησης εξυπηρέτησης (DDoS) μπορούν να καθυστερήσουν, να εμποδίσουν ή να αλλοιώσουν μια πληροφορία που προκαλεί μη διαθεσιμότητα της ενέργειας ή αποτρέπει την ανταλλαγή πληροφοριών στο SG. Σε αυτή την περίπτωση, η διαθεσιμότητα της εντολής ελέγχου και των πληροφοριών για τις τιμές είναι κρίσιμη, καθώς μπορεί να προκαλέσει απώλεια εσόδων.[18]

Από την οπτική της αξιοπιστίας του συστήματος, η διαθεσιμότητα και η ακεραιότητα είναι οι σημαντικότεροι στόχοι της ασφάλειας στο SG. Η εμπιστευτικότητα είναι η λιγότερο σημαντική για την αξιοπιστία του συστήματος. Ωστόσο, καθίσταται όλο και πιο σημαντική, ιδιαίτερα σε συστήματα που περιλαμβάνουν αλληλοεπιδράσεις με πελάτες όπως η απόκριση στη ζήτηση και τα δίκτυα AMI.

Στο Σχήμα 1 φαίνονται οι στόχοι της κυβερνοασφάλειας στο SG και συγκεκριμένες απαιτήσεις ασφαλείας. Οι συγκεκριμένες απαιτήσεις ασφαλείας είναι σημαντικές για την προστασία της υποδομής του κυβερνοχώρου προκειμένου να μειωθεί η ευθύνη και να αυξηθεί η επάρκεια της αγοράς της ηλεκτρικής ενέργειας.



Σχήμα 1 - Στόχοι κυβερνοασφάλειας και συγκεκριμένες απαιτήσεις ασφαλείας [19]

3.2.2 Καθορισμός απειλών και επιθέσεων

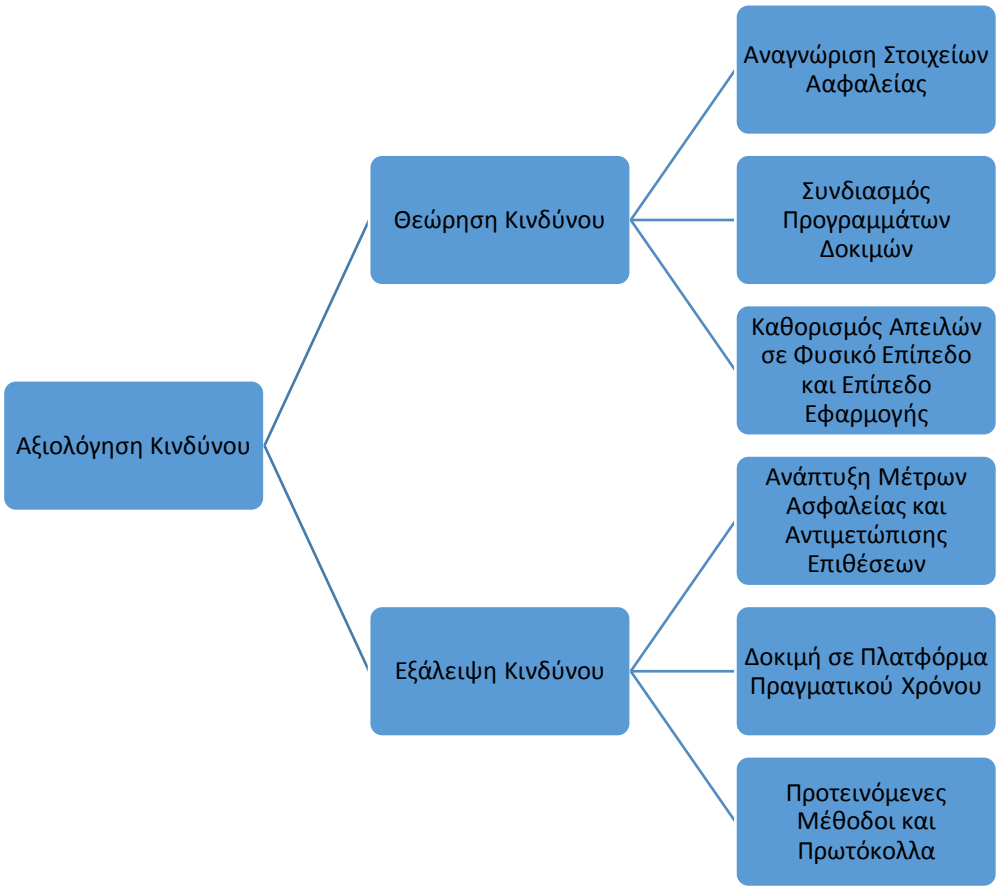
Η κατανόηση των ενδεχόμενων απειλών στο SG αποτελεί μια ανάγκη υψίστης σημασίας. Η μεθοδολογία αξιολόγησης του κινδύνου παρέχει μία βάση για την εκμετάλλευση των πιθανών σημείων εισόδου που είναι ευάλωτα σε κακόβουλες επιθέσεις.

Α. Θεώρηση και Εξάλειψη Κινδύνου

Κίνδυνος είναι το ενδεχόμενο να προκύψει ένα ανεπιθύμητο αποτέλεσμα από εσωτερικούς ή εξωτερικούς παράγοντες, που καθορίζεται από την πιθανότητα εμφάνισης ενός γεγονότος και τις σχετικές συνέπειες του. Ο απλός κίνδυνος μπορεί να οριστεί ως η ένωση της πιθανότητας μίας επίθεσης, των πιθανών ενεργειών που μπορεί να ακολουθήσουν από τον επιτιθέμενο και των επακόλουθων συνεπειών της.

Κίνδυνος = Πιθανότητα Επίθεσης x Πιθανές Ενέργειες x Επακόλουθες Συνέπειες

Το πρώτο βήμα στη θεώρηση του κινδύνου είναι η αναγνώριση των στοιχείων ασφαλείας στον κυβερνοχώρο όπως συσκευές, παράμετροι δικτύου, λογισμικά και πρωτόκολλα επικοινωνίας. Έπειτα, θα πρέπει να συνδυαστούν πολλαπλά προγράμματα δοκιμών για να ελέγξουν οποιαδήποτε ευπάθεια στο υφιστάμενο σύστημα ηλεκτρικής ενέργειας. Αφού αναγνωριστούν οι ευπάθειες στον κυβερνοχώρο, μία πλήρη ανάλυση θα προσδιορίσει την επίδραση της επίθεσης στο επίπεδο εφαρμογής και στο φυσικό επίπεδο της δομής του SG. Η ανάλυση αυτή μπορεί να γίνει με την προσομοίωση ενός μοντέλου σε πραγματικό χρόνο και με την εσκεμμένη δημιουργία μιας ψευδο-επίθεσης στον κυβερνοχώρο για την ανάλυση των επιπτώσεων. Διάφορες έρευνες έχουν γίνει στο πλαίσιο αυτού του τομέα για να βοηθήσουν στην ανάλυση αυτών των πιθανών απειλών και των επιπτώσεων. Εφόσον γίνει η ανάλυση και αναγνωριστούν οι πιθανές απειλές και οι επιπτώσεις τους στο περιβάλλον του συστήματος, το επόμενο βήμα είναι η εύρεση τρόπων αντιμετώπισης αυτών των ενδεχόμενων επιθέσεων. Επιθυμητά μέτρα ασφαλείας και αντιμετώπισης επιθέσεων πρέπει να αναπτυχθούν και να ελεγχθούν σε περιβάλλον πραγματικού χρόνου. Τα αποτελέσματα από τις δοκιμές πρέπει να εξεταστούν κατάλληλα ώστε να μειωθεί η δυνατότητα περαιτέρω ευπαθειών και να προταθούν σωστές μέθοδοι και πρωτόκολλα για το μετριασμό αυτών των επιθέσεων. Επίσης, καθοδήγηση από σύμβουλους ασφαλείας και προμηθευτές καθώς και η υπάρχουσα γνώση πάνω στα μέτρα ασφαλείας, πρέπει να χρησιμοποιηθούν για τη δημιουργία μιας ανθεκτικής υποδομής στον κυβερνοχώρο. Μία σύνοψη της αξιολόγησης του κινδύνου φαίνεται στο Σχήμα 2.[20]



Σχήμα 2 - Διαδικασία Αξιολόγησης Κινδύνου [19]

Β. Πιθανά Σημεία Επιθέσεων και Επακόλουθες Ενέργειες

Η υποδομή του κυβερνοχώρου στο SG πρέπει να μοντελοποιηθεί με τέτοιο τρόπο ώστε να είναι αδιαπέραστη σε οποιαδήποτε εισβολή στον κυβερνοχώρο. Αυτό μπορεί να επιτευχθεί μόνο αν τα πιθανά σημεία εισόδου που επιτρέπουν στον επιτιθέμενο να εισβάλει στο σύστημα έχουν αξιολογηθεί κατάλληλα. Τα συστήματα παλαιάς τεχνολογίας που δεν διαθέτουν ενσωματωμένες μονάδες ασφαλείας σε πολλές συσκευές και εφαρμογές καθιστούν το σύστημα ευάλωτο. Επιπλέον, για ένα σύστημα με τόσο μεγάλο αριθμό ηλεκτρικών και ηλεκτρονικών συνδέσεων με απέραντα κανάλια επικοινωνίας, είναι πολύ δύσκολο να γίνει ολόκληρο το SG ανθεκτικό απέναντι στις κυβερνοεπιθέσεις. Ωστόσο, η ανάλυση των διαφόρων σημείων επίθεσης θα μπορούσε να βοηθήσει στη σχεδίαση και την ανάπτυξη αρχιτεκτονικών συστημάτων και πρωτοκόλλων που μπορούν να καταστήσουν ανθεκτικό το SG απέναντι στις επιθέσεις. Τα διάφορα σημεία επίθεσης στην αλυσίδα της βιομηχανίας της ηλεκτρικής ενέργειας παρατίθενται παρακάτω:

1) **Σύστημα Παραγωγής**:

- Οι αριθμητικοί ηλεκτρονόμοι στις μονάδες παραγωγής υιοθετούν το πρωτόκολλο IEC 61850 που βασίζεται στο Ethernet για την ανταλλαγή πληροφοριών. Ένας επιτιθέμενος μπορεί να ξεκινήσει μια επίθεση DoS και να προκαλέσει τη λειτουργία του ηλεκτρονόμου κάτω από συνθήκες σφάλματος ή μπορεί ακόμα να τροποποιήσει τις ρυθμίσεις του ηλεκτρονόμου προκαλώντας έτσι την ακούσια διακοπή του. Για παράδειγμα, αν ένας επιτιθέμενος καθυστερεί με επιτυχία τη μετάδοση μηνυμάτων για την προστασία από σφάλμα στους σταθμούς παραγωγής, τότε μπορεί να προκαλέσει σοβαρή ζημία στον ηλεκτρικό εξοπλισμό.
- Διάφοροι τοπικοί βρόχοι ελέγχου συμπεριλαμβανομένου του ελέγχου ταχύτητας, της βαλβίδας ελέγχου και των αυτόματων σταθεροποιητών τάσης (AVR) συνδέονται με το κέντρο ελέγχου του σταθμού μέσω Ethernet. Αν ένας επιτιθέμενος καταφέρει να εντοπίσει κενά ασφαλείας, τότε μπορεί να αποκτήσει πρόσβαση στο τοπικό δίκτυο (LAN) και να τοποθετήσει κακόβουλο λογισμικό (τύπου Trojan) ή να βρει μία παράνομη είσοδο, και με αυτό τον τρόπο να θέσει σε κίνδυνο τις ψηφιακές μονάδες ελέγχου διαταράσσοντας το λογικό έλεγχο. Αυτό θα μπορούσε να είναι το υψηλότερο επίπεδο απειλής για την ασφάλεια.
- Οι μονάδες παραγωγής παρακολουθούνται και ελέγχονται από τα συστήματα SCADA. Τα συστήματα SCADA παλαιάς τεχνολογίας ακόμα χρησιμοποιούν μη κρυπτογραφημένους κωδικούς πρόσβασης, γλώσσα ηλεκτρολογικών γραφικών (Ladder) και παρουσιάζουν έλλειψη αυθεντικοποίησης. Ένας επιτιθέμενος μπορεί εύκολα να εισβάλει σε ένα σύστημα SCADA και να αλλάξει τη συχνότητα μετρήσεων που παρέχεται στη μονάδα αυτομάτου ελέγχου παραγωγής (AGC). Μία τέτοια επίθεση μπορεί να επηρεάσει άμεσα τη σταθερότητα του συστήματος.

- Οι απομακρυσμένες τερματικές μονάδες (RTU) και οι προγραμματιζόμενοι λογικοί ελεγκτές (PLC) γενικά χρησιμοποιούν το πρωτόκολλο επικοινωνίας MODBUS ή το DNP3. Το πρωτόκολλο MODBUS δεν παρέχει ασφάλεια ενάντια σε μη εξουσιοδοτημένη είσοδο. Έτσι ένας επιτιθέμενος με συνδεσιμότητα IP μπορεί να διαβάλει τις RTUs και τους PLCs οδηγώντας σε μία ανεπιθύμητη λειτουργία του συστήματος. Παρομοίως, το DNP3 επίσης δεν χρησιμοποιεί κρυπτογράφηση, αυθεντικοποίηση και εξουσιοδότηση. Έτσι, ένας επιτιθέμενος με πρόσβαση στο δίκτυο, μπορεί εύκολα να αλλοιώσει τα μηνύματα. Ακόμα, επιθέσεις όπως υπερχείλιση της μνήμης buffer μπορούν εύκολα να πραγματοποιηθούν σε ένα δίκτυο SCADA που χρησιμοποιεί DNP3. Είναι επίσης πιθανή η δημιουργία επίθεσης Man In The Middle Attack (MiTM) ανάμεσα στο SCADA και τις συσκευές (RTU και PLC) για την απόκτηση πληροφοριών σχετικά με την τοπολογία του δικτύου και τη λειτουργικότητα της συσκευής.[21]

2) Σύστημα Μεταφοράς:

- Το SCADA είναι η ¨καρδιά¨ του συστήματος μεταφοράς στα κέντρα ελέγχου και κατανομής φορτίου. Τώρα εφαρμόζεται σε μεγαλύτερα δίκτυα (WANs) λόγω της εξέλιξης της τεχνολογίας πληροφοριών. Αν και τα κέντρα κατανομής φορτίου διαθέτουν ανεξάρτητο έλεγχο, συνδέονται επίσης σε άλλα κέντρα μέσω κοινής επικοινωνιακής υποδομής. Σήμερα, πολλές εταιρείες μεταφοράς έχουν ενσωματώσει το διαδίκτυο στο δίκτυο επικοινωνίας για μεγαλύτερη αποδοτικότητα και αξιοπιστία. Αυτό όμως θέτει σε μεγάλο κίνδυνο ολόκληρο το σύστημα, γιατί αν κάποιος επιτιθέμενος καταφέρει να διεισδύσει σε κάποιο από τα δίκτυα του SCADA μπορεί να προκαλέσει σοβαρά προβλήματα στη λειτουργία ολόκληρου του δικτύου.
- Οι RTUs και οι PLCs παρουσιάζουν επίσης τις ίδιες ευπάθειες στο σύστημα μεταφοράς με αυτές που αναφέρθηκαν στο σύστημα παραγωγής. Ένας επιτιθέμενος μπορεί να δημιουργήσει ειδικά μία διεύθυνση URL και να τη στείλει σε οποιονδήποτε στο κέντρο ελέγχου. Όταν η URL ανοιχθεί από κάποιο μηχάνημα που είναι συνδεδεμένο στο δίκτυο, απόσπασμα κακόβουλου JavaScript κώδικα εκτελείται στο πρόγραμμα περιήγησης ιστού. Έπειτα αυτό ανιχνεύει αυτόματα τα PLCs που είναι συνδεδεμένα στο δίκτυο και εισβάλλει στο σύστημα. Τέτοιες επιθέσεις κατηγοριοποιούνται ως επιθέσεις πλαστογράφησης αίτησης δεδομένων μεταξύ ιστοτόπων (CSRF).
- Μελέτες για την εκτίμηση της κατάστασης, τη βέλτιστη ροή ισχύος, την οικονομική κατανομή φορτίου και την ένταξη μονάδων παραγωγής, έχουν γίνει με αλγορίθμους ενσωματωμένους σε λογισμικό που είναι σχεδιασμένο για να εκτελεί υπολογισμούς χρησιμοποιώντας χιλιάδες μετρήσεις. Αν ένας επιτιθέμενος καταφέρει να διεισδύσει στο δίκτυο και να εισάγει εσφαλμένα δεδομένα τότε το σύστημα θα στραφεί αμέσως σε ασταθείς συνθήκες λειτουργίας καθώς επίσης θα προκαλέσει οικονομικές επιπτώσεις στο SG.

- Οι γραμμές συνεχούς ρεύματος υψηλής τάσης (HVDC) γίνονται υψίστης σημασίας για τη μαζική μεταφορά ενέργειας. Η κυβερνοασφάλεια της υποδομής στις συνδέσεις HVDC είναι υποβαθμισμένη καθώς δεν διαθέτει τα χαρακτηριστικά της εξουσιοδότησης και του ελέγχου πρόσβασης στα δίκτυα SCADA. Ένας επιτιθέμενος μπορεί να στείλει σήματα ελέγχου για να αλλάξει τη γωνία μεταγωγής ή ακόμα και να μπλοκάρει τη ροή ισχύος προκαλώντας σοβαρή απώλεια σε μια στοχευμένη περιοχή.
- Οι σύγχρονες συσκευές εναλλασσόμενου ρεύματος FACTS χρησιμοποιούν επικοινωνία υψηλής ταχύτητας για ανταλλαγή πληροφοριών μεταξύ τους κατά τη διάρκεια λειτουργίας, αυξάνοντας έτσι τις ευπάθειες στο σύστημα. Ένας επιτιθέμενος μπορεί να στείλει εσφαλμένα λειτουργικά δεδομένα στις συσκευές FACTS με αποτέλεσμα να προκαλέσει μη απαραίτητη αντιστάθμιση VAR οδηγώντας έτσι σε αστάθεια.
- Για την ενσωμάτωση προβλέψεων για ανανεώσιμες πηγές ενέργειας σε λειτουργίες συστήματος σε πραγματικό χρόνο απαιτείται προηγμένη τεχνολογία πληροφοριών. Ο χειρισμός των δεδομένων αιολικής και ηλιακής ενέργειας που αποστέλλονται στο κέντρο ελέγχου μπορεί να κάνει το ηλεκτρικό σύστημα να βγει εκτός ελέγχου, επηρεάζοντας τις λειτουργίες του όπως ο προγραμματισμός παραγωγής, η εξισορρόπηση σε πραγματικό χρόνο, και η κατανομή φορτίου. Οι χάκερς θα μπορούσαν να το πάνε ακόμα ένα βήμα παραπάνω επαναρυθμίζοντας ολόκληρο το ενεργειακό κέρδος και προγραμματίζοντας την αντιστροφή της κατεύθυνσης μίας ανεμογεννήτριας. Με αυτό τον τρόπο δεν θα βλάψουν μόνο τη λειτουργίας τους συστήματος, αλλά θα προκαλέσουν ζημιά και στα αιολικά πάρκα.[22]

3) Σύστημα Διανομής:

- Ένας συμβατικός μετρητής μπορεί να τροποποιηθεί αντιστρέφοντας τις ενδείξεις του ή να παραποιηθεί για να ελέγχει την ηλεκτρική ροή. Οι συσκευές IED όπως έξυπνοι μετρητές μπορούν να ελεγχθούν για την ανάπτυξη διαφόρων λειτουργιών από μία απομακρυσμένη περιοχή. Αυτό επιτρέπει σε έναν επιτιθέμενο να συνδέσει ή αποσυνδέσει συσκευές εξ αποστάσεως ή να αλλοιώσει τα δεδομένα που αποστέλλονται στον διαχειριστή του συστήματος ή να αποκτήσει πρόσβαση σε εμπιστευτικά δεδομένα καταναλωτών. Επίσης, αν ένας επιτιθέμενος καταφέρει να στείλει πακέτα ψευδών δεδομένων για να εισάγει αρνητική τιμολόγηση στο σύστημα, θα έχει ως αποτέλεσμα την έλλειψη ενέργειας για συγκεκριμένη περιοχή που θα προκαλέσει απώλεια εσόδων στην εταιρεία ηλεκτρισμού. Δεδομένου του ότι υπάρχουν εκατομμύρια συμβατικοί/έξυπνοι μετρητές στο σύστημα, είναι δύσκολο να εξασφαλιστεί η προστασία κάθε κόμβου, αυξάνοντας έτσι τις ευπάθειες του συστήματος σε μεγάλο βαθμό. Έρευνες έχουν δείξει ότι ένας επιτιθέμενος θα μπορούσε να απενεργοποιήσει εξ αποστάσεως εκατομμύρια έξυπνους μετρητές ταυτόχρονα. Οι έξυπνοι μετρητές αποτυγχάνουν επίσης να

υπακούν σε πρότυπα Open Web Application Security Project (OWASP), όπως έγχυση (Injection), αυθεντικοποήση (Authentication), Μη Ασφαλές Άμεσο Αντικείμενο Αναφοράς (Insecure Direct Object References), Cross-Site Scripting (XSS), Λανθασμένες Ρυθμίσεις Ασφαλείας (Security Misconfiguration), Έκθεση Ευαίσθητων Πληροφοριών (Sensitive Data Exposure) και Έλλειψη Ελέγχου Πρόσβασης σε Επίπεδο Συνάρτησης (Missing Function Level Access Control).

- Η δικτύωση και η επικοινωνία στη υποδομή AMI βασίζεται σε τεχνολογίες όπως WLAN, ZigBee, RF mesh, WiMax, WiFi και PLC. Τα δίκτυα WLAN ακολουθούν τα πρότυπα IEEE 802.11, τα οποία δε διαθέτουν από προεπιλογή μηχανισμούς εξουσιοδότησης. Αυτό το πρωτόκολλο είναι επίσης ευάλωτο σε επιθέσεις όπως ανάλυση της κίνησης (traffic analysis), υποκλοπή (eavesdropping), υφαρπαγή συνόδου (Session hijacking attack). Οι ZigBee βασίζονται στα πρότυπα IEEE 802.15.4 που είναι ευάλωτα σε επιθέσεις εμπλοκής (jamming). Το συμβατικό ZigBee υποφέρει από καθυστερήσεις λόγω πολυεπίπεδων (multi-tier) τοπολογιών Cluster-tree του δικτύου. Τα μέσα κινητής επικοινωνίας είναι γενικά απροστάτευτα και μπορούν εύκολα να αποκαλύψουν δεδομένα κατανάλωσης ενέργειας και να αποδειχθούν ευάλωτα στην προστασία της ιδιωτικότητας. Οι τεχνολογίες του συστήματος ασύρματων δικτύων ευριζωνικότητας (WiMAX) ακολουθούν το πρότυπο IEEE 802.16 το οποίο είναι ευάλωτο απέναντι σε επιθέσεις κρυπτογράφησης (scrambling) και αναμετάδοσης (replay). Οι επικοινωνίες PLC μπορεί να είναι ευάλωτες σε απειλές από εχθρικούς χρήστες στο δίκτυο που χρησιμοποιούν έλεγχο πρόσβασης για την παραπλάνηση υπηρεσιών. Σήμερα, τα παθητικά οπτικά δίκτυα Ethernet (EPON) είναι δημοφιλή στην αυτοματοποίηση συστημάτων διανομής ενέργειας στο SG, αν και παραμένουν ευάλωτα σε επιθέσεις όπως άρνηση της εξυπηρέτησης (DoS), υποκλοπή (eavesdropping) και πλαστογράφηση (spoofing).
- Ένας επιτιθέμενος μπορεί να παραβιάσει ένα εικονικό ιδιωτικό δίκτυο (VPN) των εταιρειών διανομής. Οι επιπτώσεις ενός ιού τύπου σκουλήκι (slammer worm) που έφτασε μέσω σύνδεσης VPN στο SCADA έχουν καταγραφεί σε διάφορες έρευνες. Το σκουλήκι κατάφερε να μολύνει το κέντρο ελέγχου του LAN και μπλόκαρε την κίνηση του SCADA. Τέτοιες επιθέσεις είναι ιδιαίτερα επικίνδυνες καθώς μπορούν να ελεγχθούν και να παρακολουθηθούν εξ αποστάσεως.
- Λόγω έλλειψης αυθεντικοποίσης και κρυπτογράφησης στο σύστημα Head End (HES), ένας επιτιθέμενος μπορεί εύκολα να παραβιάσει το Σύστημα Διαχείρισης Δεδομένων Μετρητών (MDMS) και να στείλει εξουσιοδοτημένα σήματα στους έξυπνους μετρητές. Επίσης, ένας επιτιθέμενος μπορεί να παραποιήσει τις συνδέσεις των μετρητών των καταναλωτών και να στείλει ψευδή σήματα κατανάλωσης ενέργειας στο κέντρο ελέγχου. Το λογισμικό που είναι εγκατεστημένο στο HES δεν μπορεί να εντοπίσει αυτή την ενέργεια, έτσι εκτελεί τον απαιτούμενο έλεγχο και στέλνει την εντολή για την απενεργοποίηση του μετρητή. Τέτοιες επιθέσεις είναι πολύ δύσκολο να ανιχνευθούν καθώς ο επιτιθέμενος παριστάνει έναν έξυπνο μετρητή. Έρευνες έχουν δείξει ότι ο επιτιθέμενος μπορεί να επιτεθεί και στο Σύστημα Διαχείρισης Ενέργειας (EMS) χρησιμοποιώντας ψευδή δεδομένα μετρητών. Το λογισμικό του HES μπορεί να

παραποιηθεί αλλάζοντας τους αλγορίθμους λόγω έλλειψης σωστού ελέγχου πρόσβασης.

- Οι καταναλωτές που έχουν σύστημα μέτρησης εγκατεστημένο στο χώρο τους, μπορούν επίσης να παραποιήσουν τα δεδομένα κατανάλωσης που στέλνονται στο κέντρο ελέγχου των εταιρειών χακάροντας το δίκτυο επικοινωνίας του AMI. Ο επιτιθέμενος μπορεί να μειώσει το λογαριασμό ρεύματος ή να πιστώσει λογαριασμό άλλου καταναλωτή αν αυτός δεν πουλάει ενέργεια στο δίκτυο. Αυτό δεν επηρεάζει άμεσα τη λειτουργία του συστήματος αλλά αυξάνει τις απώλειες των εταιρειών διανομής.[19],[23]

4) Υποδομή Τηλεμετρίας:

Τα συστήματα τηλεμετρίας συχνά παραμελούνται κατά τη διάρκεια του σχεδιασμού ασφαλείας και της διεργασίας ελέγχου και αξιολόγησης. Συνδέονται με συστήματα ελέγχου και την αρχιτεκτονική SCADA διαφόρων στοιχείων του SG όπως συστήματα παραγωγής, μεταφοράς, διανομής και μικροδίκτυα. Το σύστημα τηλεμετρίας στα συστήματα ηλεκτρικής ενέργειας χρησιμοποιεί πρωτόκολλα επικοινωνίας όπως Modbus, IEC 870-5-10x, DNP3, Profibus/Profinet. Ανεξάρτητα από τον τύπο πρωτοκόλλου που χρησιμοποιείται, τα πρωτόκολλα ICS (Industrial Control System) λειτουργούν σε μοντέλα Master – Slave με ελάχιστα ή και καθόλου χαρακτηριστικά ασφαλείας κι έτσι είναι ευάλωτα σε κακόβουλες επιθέσεις του δικτύου. Αν ένας επιτιθέμενος αποκτήσει πρόσβαση στο εσωτερικό της συσκευής Master, τότε η συσκευή Slave μπορεί στη συνέχεια να αναγκαστεί να λειτουργεί ψευδώς ή ακόμη και να διαγράψει κρίσιμα δεδομένα. Αυτά που αναφέρθηκαν, επισημαίνουν τις επιθέσεις που μπορούν να γίνουν στο σύστημα χωρίς τη φυσική παρουσία ενός επιτιθέμενου. Ωστόσο υπάρχουν ορισμένοι τρόποι με τους οποίους μπορεί κάποιος να διεισδύσει στο σύστημα με φυσικό τρόπο.

- Ένας δυσαρεστημένος υπάλληλος που διαθέτει το προνόμιο της πρόσβασης στα στοιχεία του συστήματος θα μπορούσε να αλλάξει τους αλγορίθμους του λογισμικού ή ακόμα και να αλλάξει τις ρυθμίσεις των συσκευών προκαλώντας μία μη φυσιολογική λειτουργία. Επιπλέον, μπορούν να κλαπούν εταιρικά δεδομένα από τη βάση δεδομένων για κάποιον αντίπαλο πάροχο υπηρεσιών. Ο επιτιθέμενος μπορεί να χρησιμοποιήσει λογισμικό καταγραφής δεδομένων για να αποκτήσει πρόσβαση σε ονόματα και κωδικούς χρηστών του συστήματος. Τέτοιες ενέργειες δεν είναι απλά μόνο δύσκολο να ανιχνευθούν αλλά και να αντιμετωπιστούν.
- Ακούσια διείσδυση μέσω μολυσμένων συσκευών: Κακόβουλα μέσα ή συσκευές μπορούν ακούσια να διεισδύσουν εντός της ασφαλούς ζώνης από το προσωπικό. Για παράδειγμα, οι μνήμες USB έχουν γίνει ένα

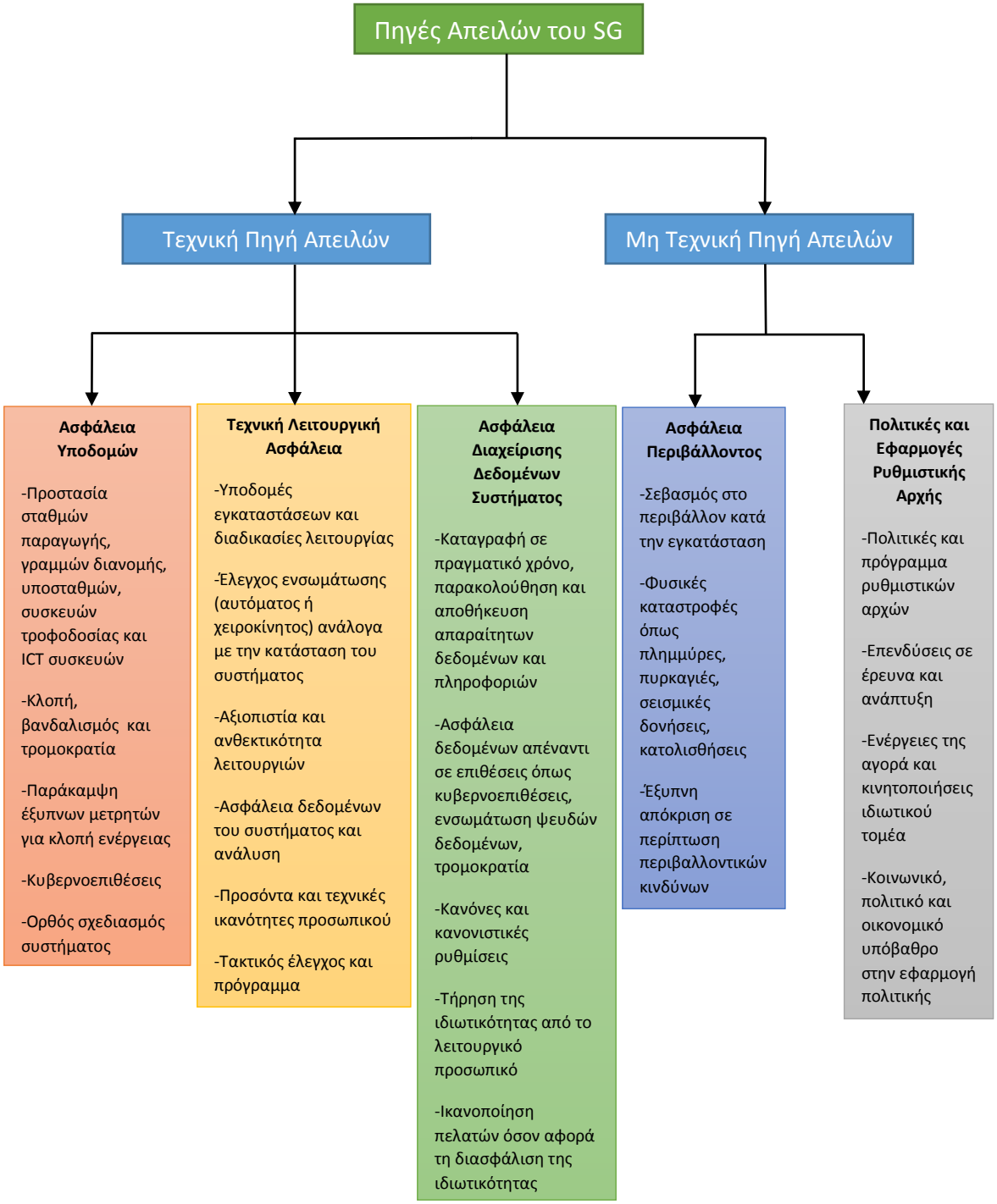
δημοφιλές εργαλείο για την παράκαμψη των μέσων άμυνας της ασφαλούς ζώνης: μερικά μη αξιόπιστα USB μπορεί να χρησιμοποιηθούν από τους υπαλλήλους και να συνδεθούν σε ασφαλείς συσκευές εντός της ασφαλούς ζώνης, επιτρέποντας έτσι σε κακόβουλα λογισμικά που βρίσκονται στις μνήμες USB να μολύνουν άμεσα τις συσκευές. Παρομοίως, οι συσκευές που χρησιμοποιούνται τόσο εντός όσο και εκτός της ασφαλούς ζώνης μπορούν να μολυνθούν από κακόβουλο λογισμικό όταν βρίσκονται εκτός και διεισδύσουν το κακόβουλο λογισμικό όταν χρησιμοποιηθούν εντός. Συνηθισμένο παράδειγμα αποτελούν οι εταιρικοί φορητοί υπολογιστές που μπορούν να χρησιμοποιηθούν προσωπικά από υπαλλήλους εκτός εργασίας.

- Εκτεθειμένη εφοδιαστική αλυσίδα: Ένας επιτιθέμενος μπορεί να προεγκαταστήσει κακόβουλους κώδικες ή ψηφιακές ¨κερκόπορτες¨ (backdoors) σε μία συσκευή πριν από την αποστολή σε μία τοποθεσία προορισμού, που αποκαλείται επίθεση εφοδιαστικής αλυσίδας (supply chain attack). Κατά συννέπεια, η ανάγκη παροχής ασφάλειας στη διαδικασία ανάπτυξης και παραγωγής λογισμικού, υλικολογισμικού (firmware) και εξοπλισμού είναι κρίσιμη για την προστασία της εφοδιαστικής αλυσίδας (που αφορά προμηθευτές τεχνολογικών μέσων και προγραμματιστές) στον κυβερνοχώρο.[24]

3.2.3 Κατηγοριοποίηση βάσει των πηγών των απειλών

Έχοντας εντοπίσει διάφορες απειλές και προκλήσεις που αντιμετωπίζει το σύστημα του SG, οι απειλές πρέπει να είναι σαφώς καθορισμένες και πρέπει να ακολουθείται μια ολοκληρωμένη προσέγγιση όσον αφορά τις λειτουργικές διατάξεις ασφαλείας. Έτσι, προκύπτει η ανάγκη περαιτέρω μελέτης των πηγών των απειλών. Παρόλο που οι απειλές μπορούν να θεωρηθούν από πολλές οπτικές, μία προσέγγιση αποτελεί ο διαχωρισμός σε τεχνικές και μη τεχνικές.

Οι προσδιορισμένες απειλές ομαδοποιούνται με βάση διάφορες κατηγοριοποιημένες πηγές που φαίνονται στο Σχήμα 3. Το σχήμα δίνει μία πλήρη σύνοψη κάθε κατηγορίας απειλών, όπου η αναγνώριση τους θεωρείται πολύ σημαντική για την ανάπτυξη ενός καλά ασφαλισμένου και ανθεκτικού συστήματος. Αυτή η κατηγοριοποίηση μπορεί να τροποποιηθεί περαιτέρω, καθώς το σχήμα δε δίνει μία αποκλειστική κατηγοριοποίηση, αλλά ένα μοντέλο ανοικτό για κατάλληλη τροποποίηση και αναδιαβάθμιση σε πιθανώς μικρότερα τμήματα για την σωστή συγκρότηση μέτρων πρόληψης και αποκατάστασης.



Σχήμα 3 - Κατηγοριοποίηση των πηγών των απειλών στο Smart Grid [25]

Τεχνικές Πηγές Απειλών

Αυτή η κατηγοριοποίηση που παρουσιάζεται, βασίζεται σε αναγνωρισμένες απειλές που μπορούν να εντοπιστούν στις τεχνικές πτυχές του SG. Διακρίνονται τρεις βασικές πτυχές των τεχνικών πηγών αυτών των απειλών οι οποίες είναι η ασφάλεια των

υποδομών, η τεχνική λειτουργική ασφάλεια και η ασφάλεια διαχείρισης δεδομένων του συστήματος.

- *Ασφάλεια Υποδομών*: Η υποδομή του SG είναι ένα περίπλοκο σύστημα που είναι γεωγραφικά, λογικά και οικονομικά κατανεμημένο: διασυνδεδεμένοι χρήστες, μονάδες παραγωγής, επιχειρήσεις, μεταφορές, διανομές, υποσταθμοί, μετασχηματιστές καθώς και προηγμένη υποδομή μέτρησης (AMI), συσκευές τεχνολογίας πληροφορικής και επικοινωνιών (ICT) όπως ασύρματο δίκτυο, οπτική ίνα, ηλεκτρικές γραμμές (PLC), καλώδιο Ethernet. Όλα αυτά καθιστούν το SG ένα σύστημα υψηλής ευφυΐας για το οποίο η ασφάλεια της υποδομής γίνεται κρίσιμης σημασίας.
- *Τεχνική Λειτουργική Ασφάλεια:* Η πολυπλοκότητα του δικτύου απαιτεί ασφαλή λειτουργικά συστήματα. Αυτό οφείλεται στο γεγονός ότι οι αποτυχίες ενδεχομένως θα έχουν σοβαρό αντίκτυπο, δεδομένου του ότι οι κρίσιμες υποδομές εξαρτώνται από τις ασφαλείς και αξιόπιστες λειτουργίες και παροχές ενέργειας και ελέγχου. Ορισμένες από αυτές τις λειτουργίες του συστήματος υπόκεινται στον έλεγχο του υπολογιστή, αλλά ορισμένα τμήματα των λειτουργιών απαιτούν την προσοχή των χειριστών στα κέντρα ελέγχου και ειδικότερα σε ορισμένες περιπτώσεις έκτακτης ανάγκης. Η τεχνική λειτουργική ασφάλεια καλύπτει τις εγκαταστάσεις υποδομής και τις διαδικασίες λειτουργίας, τον έλεγχο ενσωμάτωσης (αυτόματο ή χειροκίνητο) ανάλογα με την κατάσταση του συστήματος, την αξιοπιστία και την ανθεκτικότητα των λειτουργιών, το επίπεδο πληροφοριών του συστήματος, την ασφάλεια και την ανάλυση δεδομένων του συστήματος, τα προσόντα και τις τεχνικές ικανότητες του προσωπικού και το πρόγραμμα ελέγχου και συντήρησης.
- *Ασφάλεια Διαχείρισης Δεδομένων του Συστήματος:* Αυτή η πτυχή καλύπτει την καταγραφή, την παρακολούθηση και την αποθήκευση απαραίτητων δεδομένων και πληροφοριών σε πραγματικό χρόνο, την ασφάλεια δεδομένων απέναντι σε επιθέσεις, κανόνες και κανονιστικές ρυθμίσεις, την τήρηση της ιδιωτικότητας από το λειτουργικό προσωπικό και την ικανοποίηση των πελατών όσον αφορά τη διασφάλιση της ιδιωτικότητάς τους.

Μη Τεχνικές Πηγές Απειλών

Οι μη τεχνικές πηγές απειλών του SG εξετάζουν τους παράγοντες που θα μπορούσαν να εμποδίσουν τη λειτουργική ανάπτυξη. Τέτοιοι παράγοντες περιλαμβάνουν φυσικούς ή ανθρωπογενείς περιβαλλοντικούς κινδύνους όπως σεισμούς, πλημμύρες, πυρκαγιές, όπως επίσης και πολιτικές, εφαρμογές και σχεδιασμό ρυθμιστικών αρχών ή ακόμα και ενέργειες της αγοράς και κινητοποιήσεις του ιδιωτικού τομέα. Αν και λαμβάνοντας υπόψη την αιτία που επιδρούν ορισμένοι από αυτούς τους παράγοντες, κατατάσσονται σε μη τεχνικές πηγές απειλών, ωστόσο ίσως χρειάζεται τεχνική προσέγγιση για την αντιμετώπιση τους.

- *Ασφάλεια περιβάλλοντος*: Η παροχή περιβαλλοντικής ασφάλειας είναι πολύ σημαντική για την υλοποίηση του SG, καθώς βοηθά στον έλεγχο και την αποφυγή πιθανών καταστροφικών επιπτώσεων στις υποδομές λόγω οποιουδήποτε φυσικού ή τεχνητού περιβαλλοντικού κινδύνου, όπως πλημμύρες, σεισμοί, κατολισθήσεις, πυρκαγιές, πτώσεις δέντρων, με την έξυπνη απόκριση. Η έξυπνη απόκριση που βασίζεται σε περιβαλλοντικές μελέτες επιτυγχάνεται κυρίως με την αποστολή κατάλληλης προειδοποίησης βάσει ληφθέντων δεδομένων και με την τροφοδοσία εναλλακτικού παρόχου για μία κρίσιμη υποδομή σε περιπτώσεις έκτακτης ανάγκης. Παρόλο που αυτή η πτυχή της ασφάλειας του SG χαρακτηρίζεται εδώ ως μη τεχνική, κάποιο τμήμα της έχει τόσο τεχνικές όσο και μη τεχνικές επιπτώσεις.
- *Πολιτικές και Εφαρμογές Ρυθμιστικής Αρχής*: Καθώς οι ευκαιρίες στις τεχνολογίες και τις υπηρεσίες του SG διευρύνονται, αντιμετωπίζονται συνεχώς και περισσότερες προκλήσεις για την απαίτηση νέων τεχνολογιών, πολιτικών, αυξανόμενης ζήτησης και επιχειρηματικών μοντέλων που εμπλέκονται στη διαμόρφωση του SG. Συνεπώς, η εμπλοκή των κυβερνήσεων στην παροχή των απαιτούμενων ρυθμιστικών πολιτικών για την ενίσχυση της ομαλής λειτουργίας της αγοράς και τις κινητοποιήσεις του ιδιωτικού τομέα είναι σημαντική για την επίτευξη καθορισμένων στόχων για την ανάπτυξη του SG. Οι τεχνικές, κοινωνικές, πολιτικές, περιβαλλοντικές, νομοθετικές και οικονομικές επιπτώσεις θα μπορούσαν να αποδειχτούν καθοριστικός παράγοντας ενάντια στην επίτευξη της επιθυμητής ανάπτυξης, εκτός από την απαραίτητη δέσμευση των κυβερνήσεων για την σωστή εφαρμογή των πολιτικών τους.[25]

3.3 Θέματα κυβερνοασφάλειας στο Smart Grid

3.3.1 Θέματα συσκευών

Συσκευές όπως PLCs, RTUs, και IEDs στα συστήματα διανομής ηλεκτρικής ενέργειας επιτρέπουν στους διαχειριστές εκτελούν λειτουργίες συντήρησης ή κατανομής εξ αποστάσεως. Αυτή η δυνατότητα επιτρέπει επίσης σε κακόβουλους χρήστες να χειριστούν τη συσκευή και να διακόψουν τις κανονικές λειτουργίες του δικτύου, όπως το κλείσιμο ενεργών συσκευών για τη διακοπή παροχών ενέργειας ή την αλλοίωση ευαίσθητων δεδομένων για την παραπλάνηση των διαχειριστών. Όσο για τις συσκευές μετρητών, ένας συμβατικός μετρητής μπορεί να τροποποιηθεί αντιστρέφοντας τον εσωτερικό δείκτη μέτρησης (meter inversion) ή να χειραγωγηθεί για να ελέγχει τον υπολογισμό του ρεύματος. Για τις διεπαφές του πελάτη και τα PHEVs σε πολλές έρευνες δεν παρουσιάζονται πιθανά ζητήματα ασφαλείας αλλά εστιάζουν περισσότερο σε ζητήματα κακόβουλων επιθέσεων και κρυπτογράφησης. Στον Πίνακα 4 περιγράφονται τα πιθανά προβλήματα των εφαρμογών του έξυπνου μετρητή, των διεπαφών του πελάτη και των PHEVs.[13],[26]

Πίνακας 4 - Πιθανά προβλήματα συσκευών [27]

Θέμα	Θέματα Κυβερνοασφάλειας		
	Λέξεις Κλειδιά	**Πιθανά Προβλήματα**	**Πιθανές Λύσεις**
Συσκευές	Έξυπνος Μετρητής	• Η τιμολόγηση των πελατών ποικίλει αναλόγως κι επομένως οι παραβιάσεις των δεδομένων μέτρησης μπορούν να οδηγήσουν σε διαφορετικούς λογαριασμούς. • Οι μετρητές μπορούν να υποστούν φυσικές επιθέσεις όπως αλλαγή μπαταρίας, αφαίρεση και τροποποίηση. • Λειτουργίες όπως απομακρυσμένη σύνδεση και αποσύνδεση μετρητών και αναφορά διακοπής μπορεί να χρησιμοποιηθούν από μη αξιόπιστα άτομα.	• Διασφάλιση της ακεραιότητας των δεδομένων των μετρητών. • Ασφάλεια συντήρησης των μετρητών. • Ανίχνευση μη εξουσιοδοτημένων αλλαγών στους μετρητές. • Εξουσιοδότηση όλων των προσβάσεων από και προς τα δίκτυα της υποδομής AMI.
	Διεπαφές Πελάτη	• Οι οικιακές συσκευές μπορούν να αλληλοεπιδρούν με τους παρόχους υπηρεσιών ή άλλες συσκευές AMI. Όταν χειραγωγηθούν από κακόβουλους εισβολείς μπορούν να αποτελέσουν μη ασφαλείς παράγοντες σε κατοικημένες περιοχές. • Οι πληροφορίες σχετικά με την ενέργεια μπορούν να αποκαλυφθούν στις IEDs ή στο διαδίκτυο. Τα μη αξιόπιστα δεδομένα μπορούν να παραπλανήσουν τις αποφάσεις των χρηστών.	• Έλεγχος πρόσβασης στις διεπαφές όλων των πελατών. • Επικύρωση των ληφθέντων πληροφοριών. • Βελτίωση της ασφάλειας των αναβαθμίσεων υλικού και λογισμικού.

Συσκευές	PHEV	• Το PHEV μπορεί να χρεωθεί σε διαφορετικές τοποθεσίες. Λανθασμένη χρέωση ή μη αξιόπιστη παροχή υπηρεσίας μπορεί να διαταράξει τις λειτουργίες της αγοράς.	• Δημιουργία προτύπων ηλεκτρικών οχημάτων.

3.3.2 Θέματα Δικτύων

Τα πιθανά προβλήματα δικτύωσης στο SG επικεντρώνονται κυρίως σε θέματα του διαδικτύου, των ασύρματων δικτύων και των δικτύων αισθητήρων. Όπως ακριβώς στο διαδίκτυο, πολλαπλές τεχνολογίες δικτύωσης μπορούν να χρησιμοποιηθούν για το SG συμπεριλαμβανομένων των οπτικών ινών, του συστήματος κινητών επικοινωνιών (LMR - Land Mobile Radio), του 3G/4G (WiMax - Worldwide Interoperability Microwave Access), των σειριακών επικοινωνιών RS-232/RS-485, της τεχνολογίας ασύρματης δικτύωσης WiFi και άλλων. Το ποια πρέπει να χρησιμοποιηθεί εξαρτάται από τις απαιτήσεις του περιβάλλοντος δικτύου και αποτελεί ένα ανοικτό ζήτημα στην ανάπτυξη νέων προτύπων επικοινωνίας του SG.[28]

Για ενσύρματα δίκτυα, τα παθητικά οπτικά δίκτυα Ethernet (EPON) θα μπορούσαν να αποτελέσουν μια πολλά υποσχόμενη λύση για τα δίκτυα ευρυζωνικής πρόσβασης του SG λόγω των ακόλουθων χαρακτηριστικών: 1) οπισθόφορη συμβατότητα, 2) χαμηλό κόστος χρήσης και συντήρησης ινών, και 3) ελάχιστη επιβάρυνση πληροφοριών πρωτοκόλλων δικτύου (protocol overhead). Το EPON έχει επίσης χαρακτηριστεί ως η επόμενη γενιά Gigabit-Ethernet από το πρότυπο IEEE 802.3ah. Ωστόσο το EPON μπορεί να γίνει εύκολα ευάλωτο απέναντι σε επιθέσεις άρνησης εξυπηρέτησης, πλαστογράφησης και υποκλοπής.[29]

Για ασύρματα δίκτυα, τα ραδιοκύματα θα μπορούσαν να αποτελέσουν πιθανές ευπάθειες απέναντι σε επιτιθέμενους. Πιο συγκεκριμένα, ένα τέτοιο απροστάτευτο φυσικό μέσο μπορεί να αποκαλύψει δεδομένα κατανάλωσης ενέργειας κι έτσι να προκαλέσει εισβολή σε προσωπικά δεδομένα. Το NIST ισχυρίζεται πως το πρότυπο ασφάλειας ασύρματων τοπικών δικτύων IEEE 802.11i μπορεί να βοηθήσει στην ασφάλεια της ανάπτυξης ασύρματων δικτύων στο SG. Άλλες έρευνες υποστηρίζουν πως τα ασύρματα δίκτυα του SG μπορούν γίνουν πιο ασφαλή με τη χρήση υπαρχόντων προτύπων όπως το IEEE 802.16e (Mobile WiMax), και της τεχνολογία αιχμής 3GPP LTE. Πιθανές τεχνολογίες που χρησιμοποιούνται για την ασφάλεια στα ασύρματα δίκτυα είναι τα πρωτόκολλα EAP (Extensible Authentication Protocol), 4-way handshake, AES-CCMP (AES-Counter Mode CBC-MAC Protocol), CBCMAC (Cipher Block Chaining Message Authentication Code), PKMv2 (Privacy and Key Management version 2), οι αλγόριθμοι 128

group encryption key, 3DES (Triple Data Encryption Standard), RSA acknowledgement message και άλλες. Ωστόσο δεν έχει αναλυθεί περαιτέρω η δυνατότητα εφαρμογής τους στο SG.[6],[28]

Για τα δίκτυα αισθητήρων, μέχρι σήμερα, οι ερευνητές έχουν φτάσει στην κοινή συναίνεση ότι τα ασύρματα δίκτυα πλέγματος πρέπει να χρησιμοποιηθούν στην υποδομή AMI. Κύριο λόγο για αυτό, αποτελεί το γεγονός ότι τα δίκτυα πλέγματος μπορούν να ξεπεράσουν ¨κακούς¨ κόμβους χρησιμοποιώντας εφεδρικά μονοπάτια επικοινωνίας. Παρόλα αυτά, η βιομηχανία της τεχνολογίας πληροφοριών έχει καταγράψει μία σειρά επιθέσεων απέναντι σε τεχνολογίες ασύρματων δικτύων πλέγματος όπως έγχυση πακέτων μεταξύ επιπέδων (cross-layer traffic injection), πλαστοπροσωπία κόμβου (node impersonation), έγχυση διαδρομών (route injection), τροποποίηση μηνυμάτων και άλλες. Τα περισσότερα υπάρχοντα πρωτόκολλα δρομολόγησης δεν έχουν συγκεκριμένες στρατηγικές για να εξασφαλίζουν τα μονοπάτια και τα δεδομένα λόγω των εγγενών χαρακτηριστικών κατανομής που διαθέτουν. Χωρίς την ασφάλεια της δρομολόγησης, η κίνηση στο δίκτυο AMI δεν είναι αξιόπιστη. Στον Πίνακα 5 συγκεντρώνονται τα πιθανά προβλήματα του διαδικτύου, του ασύρματου δικτύου και του δικτύου αισθητήρων στο SG.[6],[30]

Πίνακας 5 - Πιθανά προβλήματα δικτύων [27]

Θέμα	**Θέματα Κυβερνοασφάλειας**		
	Λέξεις Κλειδιά	**Πιθανά Προβλήματα**	**Πιθανές Λύσεις**
Δίκτυα	Διαδίκτυο	• Ορισμένες εφαρμογές που ενδεχομένως να είναι ενσωματωμένες στο διαδίκτυο. Εγγενή προβλήματα όπως κακόβουλο λογισμικό και επιθέσεις DoS είναι απειλές για το SG.	• Υιοθέτηση πρωτοκόλλου TCP/IP στα δίκτυα του SG. • Πρωτόκολλα IPsec VPN, SSH και SL/TLS. • Εφαρμογές ανίχνευσης εισβολής και τείχη προστασίας.

Δίκτυα	Ασύρματο Δίκτυο	• Στα ασύρματα δίκτυα, το επίπεδο 2/3 είναι ευάλωτο σε επιθέσεις τροποποίησης και έγχυσης πακέτων. Χωρίς την ασφάλεια της δρομολόγησης, η κίνηση σε αυτά τα επίπεδα δεν είναι αξιόπιστη.	• Προστασία πρωτοκόλλων δρομολόγησης στα επίπεδα του δικτύου 2 και 3. • Δυνατότητες ασφάλειας των προτύπων 802.11i, 802.16e και της τεχνολογίας 3GPP LTE.
	Δίκτυο Αισθητήρων	• Τα δεδομένα των αισθητήρων είναι κρίσιμης σημασίας για το SG. Η υποκλοπή, παραποίηση, διαστρέβλωση, ή πλαστογράφηση αυτών των δεδομένων μπορεί να βλάψει το SG.	• Κρυπτογράφηση AES (Advanced Encryption Standard).

3.3.3 Θέματα κατανομής και διαχείρισης

Το SG μπορεί να θεωρηθεί ως ένας συνδυασμός μικροδικτύων. Κάθε μικροδίκτυο λειτουργεί αυτόνομα στο τοπικό σύστημα SCADA και αλληλοεπιδρά με άλλα όπως το φαινόμενο της νησιδοποίησης. Εν τω μεταξύ, όλα τα μικροδίκτυα θα ελέγχονται από ένα κεντρικό σύστημα master SCADA στο οποίο κάθε τοπικό SCADA λειτουργεί ως ελεγκτής slave παρέχοντας πληροφορίες που σχετίζονται με την ενέργεια στον κεντρικό ελεγκτή. Αυτό το πλαίσιο εξασφαλίζει την αξιοπιστία του SG και έτσι έχει εγκριθεί από το πρότυπο IEEE-1547. Παραδοσιακά, αυτά συστήματα SCADA είναι απομονωμένα και ελέγχονται από εξουσιοδοτημένο προσωπικό. Τα περισσότερα από αυτά δε διαθέτουν δυνατότητες ελέγχου και παρακολούθησης σε πραγματικό χρόνο. Μέχρι προσφάτως, οι μονάδες μέτρησης φάσορα (PMU) με χρονοσήμανση GPS προσέφεραν μία λύση σε αυτό το πρόβλημα. Για την αντιμετώπιση του προβλήματος του συγχρονισμού του ρολογιού στο κατανεμημένο πλαίσιο, χρησιμοποιήθηκαν στο σύστημα SCADA το Πρωτόκολλο Δικτυακού Χρόνου (Network Time Protocol – NTP) και το πρότυπο IEEE 1588. Αυτό είχε ως αποτέλεσμα την αύξηση της διαλειτουργικότητας των συστημάτων SCADA, ωστόσο, τα έκανε πιο προσιτά σε δημόσιους χρήστες, γεγονός που αυξάνει αναπόφευκτα την πιθανότητα να τεθεί σε κίνδυνο το σύστημα ως ακολούθως:

1) **Μη διαθεσιμότητα του διακομιστή (server)**: Αν η IP του διακομιστή του SCADA και το μονοπάτι του δικτύου είναι γνωστά στον επιτιθέμενο, ο διακομιστής μπορεί εύκολα να ¨πέσει¨ ή να τερματιστεί από το συνηθισμένο σφάλμα DoS ή απλά

διαγράφοντας τα αρχεία του συστήματος. Το DoS μπορεί να πραγματοποιηθεί αν στο TCP/IP συμβεί υπερφόρτωση. Η διαγραφή των αρχείων μπορεί να γίνει χακάροντας του κωδικούς των χρηστών ή την απόκτηση πρόσβασης στο φυσικό σύστημα. Οι επιθέσεις αυτές μπορούν επίσης να προκαλέσουν σοβαρό κίνδυνο σε μελλοντικές υπηρεσίες.

2) **Απόκτηση ελέγχου στο σύστημα**: Αυτό επιτυγχάνεται με την τοποθέτηση κακόβουλου λογισμικού Trojan ή από κακόβουλο λογισμικό (backdoor) στα αρχεία του συστήματος. Αυτό αποτελεί το υψηλότερο επίπεδο απειλής της ασφάλειας, με την οποία ένα ψευδές σήμα κινδύνου και παραποιημένοι έλεγχοι μπορούν να δημιουργούνται και να στέλνονται στις RTUs προκαλώντας μεγάλης κλίμακας καταρρεύσεις.
3) **Κλοπή εταιρικών δεδομένων**: Αυτά τα προβλήματα προκύπτουν εάν το επίπεδο ασφαλείας των επιχειρήσεων είναι χαμηλό και η αρχιτεκτονική του λογισμικού που χρησιμοποιείται δεν είναι ιδιαίτερα καλή. Τα εταιρικά δεδομένα μπορούν να κλαπούν από τη βάση δεδομένων λόγω εσωτερικής αντιπαλότητας των ανταγωνιστών παρόχων υπηρεσιών.
4) **Παραποίηση πληροφοριών χρέωσης**: Οι εισβολείς ενδεχομένως να έχουν πρόσβαση στους λογαριασμούς και σε άλλες οικονομικές πληροφορίες από το σύστημα για να αποκτήσουν τις λεπτομέρειες, που μπορούν να χρησιμοποιηθούν αργότερα και να προκαλέσουν σημαντικά προβλήματα στους καταναλωτές. Πρέπει να υπάρχει ένα ισχυρό τείχος προστασίας για να προστατεύει τους διακομιστές από απώλειες τέτοιων πληροφοριών.
5) **Πρόγραμμα καταγραφής (keylogger):** Οι επιτιθέμενοι τείνουν να χρησιμοποιούν πρόγραμμα καταγραφής για το πληκτρολόγιο του συστήματος για την απόκτηση πρόσβασης στους κωδικούς και τα ονόματα χρηστών του συστήματος
6) **Απόκτηση ανταγωνιστικού πλεονεκτήματος**: Οι επιτιθέμενοι από έναν πάροχο υπηρεσιών τείνουν να έχουν πρόσβαση σε δεδομένα άλλων για να γνωρίζουν τις στρατηγικές τους και έτσι να προσανατολίζουν τον σχεδιασμό τους με τέτοιο τρόπο ώστε τελικά να ωφελούνται στο ανταγωνιστικό περιβάλλον.
7) **Κατάχρηση των διακομιστών του SCADA**: Με αυτό τον τρόπο γίνονται επιθέσεις σε άλλους διακομιστές του συστήματος και οι επιτιθέμενοι αποκτούν πληροφορίες πρόσβασης σε πολύτιμες πληροφορίες των εταιρειών ηλεκτρικής ενέργειας.
8) **Παραποίηση μαθηματικών σημείων δεδομένων**: Με αυτό τον τρόπο οι επιτιθέμενοι αποπροσανατολίζουν τους χειριστές των εταιρειών ηλεκτρισμού, οι οποίοι συχνά τείνουν να ανιχνεύουν ψευδή σήματα κινδύνου και να τερματίζουν ή να αναδιαμορφώνουν το σύστημα προκαλώντας ανεπιθύμητες καθυστερήσεις.
9) **Αλλαγή αρχείων καταγραφής χρήστη απομακρυσμένα και απομακρυσμένο DBMS**: Αυτό μπορεί να επηρεάσει αθώους χρήστες καθώς και τις εταιρείες ηλεκτρισμού.[27],[31],[32]

Στον Πίνακα 6 περιγράφονται τα προβλήματα κυβερνοασφάλειας στα διαφορετικά πεδία του τομέα της κατανομής και της διαχείρισης.

Πίνακας 6 - Θέματα κυβερνοασφάλειας κατανομής & διαχείρισης [27]

Θέμα	Θέματα Κυβερνοασφάλειας		
	Λέξεις Κλειδιά	**Πιθανά Προβλήματα**	**Πιθανές Λύσεις**
Κατανομή & Διαχείριση	SCADA/ EMS/ DMS	• Οι εντολές ελέγχου διανομής και τα αρχεία καταγραφής είναι κρίσιμα για τα συστήματα SCADA. Η υποκλοπή, αλλοίωση ή πλαστογράφηση αυτών των δεδομένων μπορούν να βλάψουν το δίκτυο. • Ο συγχρονισμός δεδομένων με χρονοσήμανση σε ευρείες περιοχές είναι σημαντικός: χωρίς αυτόν δεν μπορεί να επιτευχθεί η ασφάλεια και η αξιοπιστία του συστήματος SCADA. • Κάθε απόφαση του SCADA προέρχεται από την ανάλυση των αρχικών δεδομένων που βασίζονται σε ένα λογικό μοντέλο. Τα ακατάλληλα μοντέλα ενδέχεται να παραπλανήσουν τις ενέργειες του διαχειριστή. Επιπλέον, τα διαφορετικά μοντέλα SCADA που χρησιμοποιούνται μπορούν να διαταράξουν τη σταθερότητα του δικτύου. • Η διαχείριση φορτίου του EMS παρέχει ενεργό και παθητικό έλεγχο από τον πάροχο υπηρεσιών και τον πελάτη. Προβλήματα στον έλεγχο του φορτίου μπορούν να προκαλέσουν αδικαιολόγητες διακοπές.	• Διασφάλιση ότι όλες οι εντολές και τα αρχεία καταγραφής είναι ακριβής και ασφαλή. • Χρήση κοινής αναφοράς χρόνου (χρονοσήμανση GPS) για συγχρονισμό. • Οι πελάτες μπορούν να υπογράψουν μία σύμβαση με τις εταιρείες που να επιτρέπει την υποστήριξη του φορτίου με τους πόρους DER που αυτοί διαθέτουν. • Χρήση πολυεπίπεδης ανίχνευσης εισβολών.

Κατανομή & Διαχείριση	SCADA/ EMS/ DMS	• Η διαχείριση των DER σταθμών περιλαμβάνει προβλέψεις φορτίου. Ψευδής προβλέψεις μπορούν να παραπλανήσουν τις ενέργειες του διαχειριστή.	
	Διαχείριση Περιουσιακών Στοιχείων	• Όταν κάτι πρέπει να αντικατασταθεί, μπορούν να προκύψουν απρόσμενες διακοπές και να προκληθεί ζημία στον εξοπλισμό. • Μπορούν να προκύψουν προβλήματα συμβατότητας με την ενσωμάτωση παλιών συσκευών στο δίκτυο, τα οποία μπορούν να προκαλέσουν βλάβη ή δυσλειτουργία στο σύστημα.	• Μεγιστοποίηση του κύκλου ζωής περιουσιακών στοιχείων μέσω συνεργασίας μεταξύ σχετικών διαχειριστών. • Δημιουργία αντιγράφων ασφαλείας δεδομένων της αγοράς. • Ενεργοποίηση οπισθόφορης συμβατότητας.
	Διαχείριση Κλειδιού Κρυπτογράφησης	• Η κρυπτογράφηση δεδομένων και οι ψηφιακές υπογραφές απαιτούνται στους αισθητήρες για την ασφάλεια των επικοινωνιών. Το μεγαλύτερο μέρος της υπάρχουσας κρυπτογραφικής τεχνικής στερείται της αποτελεσματικότητας κάτω από περιορισμένο χώρο και υπολογισμό. • Η πρόσβαση και η επικοινωνία μπορούν να εμφανιστούν σε διαφορετικούς τομείς. Η διαχείριση των δικών τους κλειδιών πιστοποίησης σε	• Υποδομή Δημόσιου Κλειδιού (PKI - Public Key Infrastructure). • Κρυπτογράφηση ταυτότητας (IBE - Identity-Based Encryption). • Ιεραρχικές, αποκεντρωμένες και εξουσιοδοτημένες τεχνικές και ο συνδυασμός τους. • Σχεδιασμός παράκαμψης για επείγοντα περιστατικά.

	Διαχείριση Κλειδιού Κρυπτογράφησης	διαφορετικές περιοχές είναι δύσκολη, ειδικά σε εθνικό επίπεδο. • Η συσκευή ή το σύστημα μπορεί να είναι κλειδωμένο όταν συμβεί ένα έκτακτο περιστατικό.	
Κατανομή & Διαχείριση	Λειτουργία Σε Πραγματικό Χρόνο	• Ορισμένες εφαρμογές πρέπει να πληρούν προϋποθέσεις περιορισμένου χρόνου. Η αύξηση της διαλειουργικότητας μπορεί να προκαλέσει απεριόριστες και ανεξέλεγκτες καθυστερήσεις του συστήματος ηλεκτρικής ενέργειας.	• Πρόβλεψη και ελαχιστοποίηση των επιπτώσεων του συγχρονισμού της προστασίας της ασφάλειας.

3.3.4 Θέματα ανίχνευσης ανωμαλιών

Οι αξιόπιστες λειτουργίες του SG απαιτούν ακριβή και έγκαιρη ανίχνευση ανώμαλων και απρόσμενων γεγονότων. Οι τρόποι ανίχνευσης σφαλμάτων και βλαβών στο ηλεκτρικό δίκτυο πρέπει να αναθεωρηθούν και να μελετηθούν σε ένα μοντέλο που περιλαμβάνει που περιλαμβάνει συστηματικό κακόβουλο χειρισμό.[6]

Για την ικανοποίηση των κριτηρίων για αυτοματοποιημένη ανάλυση σφαλμάτων στο SG πραγματοποιήθηκαν αρκετές μελέτες, πολλές από τις οποίες συνεχίζονται ακόμα. Αυτές περιλαμβάνουν: 1) σχέδιο για ανίχνευση, κατηγοριοποίηση και μετριασμό μίας σειράς γεγονότων στα δεδομένα ενδοεπικοινωνίας σε τοπικό επίπεδο αλλά και σε ολόκληρο το σύστημα, 2) εφαρμογή ενός βέλτιστου αλγορίθμου εντόπισης σφαλμάτων που χρησιμοποιούν δεδομένα από συσκευές IDEs υποσταθμών, καθώς και δεδομένα από το SCADA PI και δεδομένα προσομοίωσης από προγράμματα ανάλυσης βραχυκυκλωμάτων, 3) ανάπτυξη μίας μεθοδολογίας διαχείρισης περιουσιακών στοιχείων που βασίζεται στον κίνδυνο για τον προγραμματισμό της συντήρησης που λαμβάνει υπόψη δεδομένα που συλλέγονται από τις IEDs των υποσταθμών, 4) πρόταση ενός έξυπνου επεξεργαστή με σήμα κινδύνου για την εκμετάλλευση της ενισχυμένης προστασίας δεδομένων με ερμηνεία της σχέσης αιτίας και αποτελέσματος μεταξύ των

σημάτων, 5) προστατευτικό σύστημα αναμετάδοσης βασισμένο σε νευρωνικό δίκτυο που επιτρέπει ταυτόχρονες βελτιώσεις στην αξιοπιστία και την ασφάλεια της προστασίας των γραμμών μεταφοράς.[33]

Στον Πίνακα 7 περιγράφονται τα προβλήματα κυβερνοασφάλειας στα διαφορετικά πεδία του τομέα της ανίχνευσης ανωμαλιών.

Πίνακας 7 - Θέματα κυβερνοασφάλειας στην ανίχνευση ανωμαλιών [27]

Θέμα	**Θέματα Κυβερνοασφάλειας**		
	Λέξεις Κλειδιά	**Πιθανά Προβλήματα**	**Πιθανές Λύσεις**
Ανίχνευση Ανωμαλιών	Χρονικές Πληροφορίες	• Οι μη ασφαλείς χρονικές πληροφορίες μπορούν να χρησιμοποιηθούν για επιθέσεις αναμετάδοσης (replay attacks) και ελέγχου πρόσβασης, που έχουν σημαντική επίδραση στα πρωτόκολλα ασφαλείας. • Η χρονοσήμανση στα αρχεία καταγραφής συμβάντων μπορεί να αλλοιωθεί από κακόβουλα άτομα.	• Χρήση PMU για την εξασφάλιση της ακρίβειας των πληροφοριών. • Χρήση τεχνολογιών εγκληματολογικής ανάλυσης δεδομένων (FDA) για την εξασφάλιση της ακρίβειας των χρονικών αρχείων καταγραφής.
	Δεδομένα & Υπηρεσίες	• Οι συσκευές RTUs μπορούν να υποστούν βλάβη με διάφορους τρόπους. Επομένως η ακρίβεια των δεδομένων που μεταβιβάζονται και η ποιότητα των υπηρεσιών δεν μπορούν να είναι εγγυημένες.	• Χρήση μοντέλων και αλγορίθμων ανίχνευσης απάτης που χρησιμοποιούνται για την παρακολούθηση των συναλλαγών πιστωτικών καρτών.

3.3.5 Άλλα θέματα

Σχεδόν όλα τα πρωτόκολλα επικοινωνίας δεδομένων τηρούν ένα πρωτόκολλο ανταλλαγής μηνυμάτων που είναι καλά τεκμηριωμένο και διαθέσιμο στο δημόσιο τομέα. Το πρωτόκολλο DNP χρησιμοποιείται ευρέως από τις επιχειρήσεις ηλεκτρισμού στην Βόρεια Αμερική. Οι προδιαγραφές αυτού του πρωτοκόλλου μπορούν να επιτευχθούν με ονομαστική χρέωση του χρήστη. Η χρήση αυτών των τεκμηριωμένων πρωτοκόλλων μπορεί να επιτρέψει σε κάποιον εισβολέα να χρησιμοποιήσει τη μέθοδο της αντίστροφης μηχανικής (reverse engineering) του πρωτοκόλλου τηλεμετρίας και να εκμεταλλευθεί το πρωτόκολλο χρησιμοποιώντας επιθέσεις τύπου ¨Man-in-the-middle¨. Οι επιπτώσεις μπορούν να περιλαμβάνουν την αποστολή παραπλανητικών δεδομένων στη συσκευή ή στο κέντρο ελέγχου του διαχειριστή με αποτέλεσμα 1) οικονομική απώλεια αν η επίθεση οδηγεί σε υπερβολική παραγωγή, 2) φυσικό κίνδυνο εάν μία γραμμή είναι ενεργοποιημένη ενώ ο επιτηρητής γραμμών βρίσκεται στο χώρο συντήρησης των γραμμών και 3) βλάβη του εξοπλισμού σε περίπτωση που σταλθούν εντολές ελέγχου που οδηγούν σε συνθήκες υπερφόρτωσης. Στον Πίνακα 8 περιγράφονται κάποια άλλα προβλήματα κυβερνοασφάλειας στο SG.[26]

Πίνακας 8 - Άλλα θέματα κυβερνοασφάλειας [27]

Θέμα	**Θέματα Κυβερνοασφάλειας**		
	Λέξεις Κλειδιά	**Πιθανά Προβλήματα**	**Πιθανές Λύσεις**
Άλλα	Απόκριση Της Ζήτησης	• Η αλλοίωση πληροφοριών τιμολόγησης σε πραγματικό χρόνο (RTP) μπορεί να προκαλέσει οικονομικά και νομικά προβλήματα. • Τα κακόβουλα προγράμματα ενδέχεται να μολύνουν το δίκτυο, υποδεικνύοντας ψευδείς ενδείξεις ζήτησης και παροχής. Αυτό προκαλεί σημαντικές ζημιές στο σύστημα διανομής της ενέργειας.	• Έμπιστη υπολογιστική (trusted computing).

	Πρωτόκολλα & Πρότυπα	• Τα υπάρχοντα πρωτόκολλα μπορεί να έχουν κάποια εγγενή ελαττώματα ασφαλείας .	• Ανάπτυξη ασφαλέστερων προτύπων για τον αυτοματισμό και την επικοινωνία.

3.4 Ιδιωτικότητα και Προσωπικά Δεδομένα

3.4.1 Τι είναι η ιδιωτικότητα;

Δεν υπάρχει ένας καθολικός, διεθνώς αποδεκτός ορισμός της ¨ιδιωτικότητας¨ καθώς μπορεί να σημαίνει πολλά διαφορετικά πράγματα σε διαφορετικά άτομα. Αρχικά ο πρώτος ορισμός που δόθηκε από τους Samuel D. Warren και Louis D. Brandeis καθόριζε την ιδιωτικότητα ως ¨το δικαίωμα να είσαι μόνος¨. Η ιδιωτικότητα δεν είναι σαφώς οριοθετημένη έννοια και δεν είναι απλώς οι προδιαγραφές που παρέχονται από τους νόμους και τους κανονισμούς. Επιπλέον, η ιδιωτικότητα δεν πρέπει να συγχέεται, όπως συμβαίνει συχνά, με το απόρρητο και οι προσωπικές πληροφορίες με τις απόρρητες πληροφορίες. Οι απόρρητες πληροφορίες είναι πληροφορίες για τις οποίες η πρόσβαση θα πρέπει να προσδιορίζεται μόνο σε όσους έχουν επιχειρησιακή ανάγκη να τις γνωρίζουν και θα μπορούσε να έχει ως αποτέλεσμα την έκθεση σε κίνδυνο του συστήματος, των δεδομένων, των εφαρμογών ή άλλων επιχειρησιακών λειτουργιών αν αυτές κοινοποιηθούν σε άλλους.

Επιπροσθέτως, η προστασία της ιδιωτικότητας μπορεί συχνά να συγχέεται με την ασφάλεια, που αν και μπορεί να υπάρχει αλληλοεπικάλυψη μεταξύ αυτών των δύο, είναι επίσης ξεχωριστές έννοιες. Μπορεί να υπάρχει ασφάλεια χωρίς να υπάρχει ιδιωτικότητα, αλλά δεν μπορεί να υπάρχει ιδιωτικότητα χωρίς ασφάλεια: είναι ένα κομμάτι της ιδιωτικότητας. Η ασφάλεια περιλαμβάνει τη διασφάλιση της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας των δεδομένων. Ωστόσο, η προστασία της ιδιωτικότητας υπερβαίνει τη σωστή αυθεντικοποίηση και παρόμοιες προστασίες της ασφάλειας. Διευθετεί επίσης ανάγκες όπως η διασφάλιση των δεδομένων που πρέπει να χρησιμοποιούνται μόνο για το σκοπό για τον οποίο συλλέχθηκαν και να διατίθενται σωστά εφόσον δεν είναι πλέον αναγκαία για την επίτευξη αυτού του στόχου.

Είναι σημαντική η κατανόηση του ότι η θεώρηση της ιδιωτικότητας σε σχέση με το SG περιλαμβάνει την εξέταση των δικαιωμάτων, των αξιών και των ενδιαφερόντων των ατόμων: περιλαμβάνει τα σχετικά χαρακτηριστικά, τις περιγραφικές πληροφορίες και τους

προσδιορισμούς, τις δραστηριότητες και τις απόψεις των ατόμων. Το ιδιωτικό απόρρητο επηρεάζεται από τις πρακτικές των πελατών που παρέχουν και των οντοτήτων που συλλέγουν ή διαχειρίζονται αυτά τα δεδομένα.[6],[34]

Ως ευρύτερη ερμηνεία, η ιδιωτικότητα αφορά την ακεραιότητα του ατόμου κι επομένως καλύπτει όλες τις πτυχές των κοινωνικών αναγκών του. Για παράδειγμα, η ιδιωτικότητα μπορεί να διακριθεί στις τέσσερις κατηγορίες ως ακολούθως:

1) **Ιδιωτικότητα προσωπικών πληροφοριών**: Αυτή αποτελεί την πιο συνηθισμένη κατηγορία. Προσωπικές πληροφορίες είναι οποιεσδήποτε πληροφορίες σχετικά με ένα άτομο που μπορεί να αναγνωριστεί, άμεσα ή έμμεσα, από αυτές τις πληροφορίες και συγκεκριμένα μπορεί να αναφέρονται σε ένα προσωπικό αριθμό αναγνώρισης (PIN) ή ένα η περισσότερα ιδιαίτερα χαρακτηριστικά της σωματικής, ψυχικής, πολιτιστικής, οικονομικής, γεωγραφικής ή κοινωνικής του ταυτότητας. Η ιδιωτικότητα προσωπικών πληροφοριών περιλαμβάνει το δικαίωμα να ελέγχεται που, πότε, πως, σε ποιον, και σε ποιο βαθμό ένα άτομο μοιράζεται τις δικές του προσωπικές πληροφορίες, καθώς και το δικαίωμα πρόσβασης σε προσωπικές πληροφορίες που παρέχεται σε άλλους, η διόρθωσή του αλλά και η διασφάλιση της προστασίας του.
2) **Ιδιωτικότητα του ατόμου**: Αυτό είναι το δικαίωμα του ελέγχου της σωματικής ακεραιότητας. Καλύπτει πράγματα όπως φυσικές απαιτήσεις, προβλήματα υγείας και απαιτούμενες ιατρικές συσκευές.
3) **Ιδιωτικότητα προσωπικής συμπεριφοράς**: Αυτό είναι το δικαίωμα των ατόμων να διατηρούν οποιαδήποτε γνώση των δραστηριοτήτων τους και των επιλογών τους χωρίς να τις μοιράζονται με άλλους.
4) **Ιδιωτικότητα προσωπικών επικοινωνιών**: Αυτό είναι το δικαίωμα επικοινωνίας χωρίς υπερβολική επιτήρηση, παρακολούθηση ή λογοκρισία από άλλα άτομα ή οργανισμούς.[35]

Τα νέα δεδομένα σχετικά με την κατανάλωση ενέργειας που συλλέγονται εκτός των έξυπνων μετρητών, όπως τα οικιακά συστήματα διαχείρισης ενέργειας, δημιουργούνται επίσης μέσω εφαρμογών των τεχνολογιών του SG. Καθώς αυτά τα δεδομένα γίνονται πιο συγκεκριμένα και διατίθενται σε επιπλέον άτομα, αυξάνεται και η πολυπλοκότητα που σχετίζεται με θέματα προστασίας της ιδιωτικότητας. Η αναγνώριση αυτών των θεμάτων στο SG, καθώς και οι δυνατότητες αλλά και οι προτάσεις για το μετριασμό τους ανατέθηκε στο Privacy Subgroup του Cyber Security Working Group. Επιπλέον, αυτό το group προσπάθησε να αποσαφηνίσει τις προσδοκίες, τις πρακτικές και τα δικαιώματα που αφορούν την προστασία της ιδιωτικότητας στο SG.[36]

3.4.2 Εκτίμηση αντικτύπου σχετικά με την προστασία προσωπικών δεδομένων

Η εκτίμηση αντικτύπου σχετικά με την προστασία προσωπικών δεδομένων (PIA) είναι μία ολοκληρωμένη διαδικασία για τον προσδιορισμό των κινδύνων ιδιωτικότητας, εμπιστευτικότητας και ασφάλειας που σχετίζονται με τη συλλογή, τη χρήση και την αποκάλυψη προσωπικών πληροφοριών. Καθορίζει επίσης τα μέτρα που μπορούν να χρησιμοποιηθούν για το μετριασμό και την εξάλειψη αναγνωρισμένων κινδύνων. Η δραστηριότητα αυτή της διαδικασίας στο SG παρέχει μία δομημένη, επαναλαμβανόμενη ανάλυση που στοχεύει στον προσδιορισμό του τρόπου με τον οποίο μπορεί να αποκαλυφθούν προσωπικές πληροφορίες για τα άτομα ή τις ομάδες ατόμων από τα δεδομένα που συλλέγονται. Το πεδίο εφαρμογής της μπορεί να διαφέρει από ολόκληρο το δίκτυο μέχρι ένα συγκεκριμένο τμήμα του δικτύου. Οι κίνδυνοι της ιδιωτικότητας μπορούν να αντιμετωπιστούν και να μετριαστούν με πολιτικές και πρακτικές που θεσπίζονται καθ' όλη τη διάρκεια της εφαρμογής, της εξέλιξης και της διαρκούς διαχείρισης του SG.

Το Privacy Subgroup διεξήγαγε τη διαδικασία PIA το 2009 για το τμήμα καταναλωτή-επιχείρηση ηλεκτρισμού του SG. Αυτό το group στη συνέχεια εξέτασε επιπρόσθετες επιπτώσεις και κινδύνους της ιδιωτικότητας σε ολόκληρη τη δομή του δικτύου. Τα ακόλουθα ερωτήματα που προέκυψαν από την εκτέλεση της διαδικασίας σε αυτό το τμήμα του δικτύου είναι:

1) Ποιες προσωπικές πληροφορίες μπορούν να δημιουργηθούν, να αποθηκευτούν, να μεταδοθούν ή να διατηρηθούν από εφαρμογές και οντότητες που αποτελούν μέρος του SG;
2) Πώς είναι αυτές οι προσωπικές πληροφορίες σε σύγκριση με προσωπικές πληροφορίες σε άλλους τύπους συστημάτων και δικτύων;
3) Πώς είναι η χρήση αυτών των πληροφοριών στο SG σε σύγκριση με τις χρήσεις των πληροφοριών σε άλλους τύπους συστημάτων και δικτύων;
4) Ποιοι είναι οι νέοι και μοναδικοί τύποι κινδύνων της ιδιωτικότητας που μπορούν να δημιουργηθούν από τις εφαρμογές και τις οντότητες του SG;
5) Ποια είναι η πιθανότητα ότι οι ισχύοντες νόμοι, κανονισμοί και πρότυπα μπορούν να εφαρμοστούν για τις προσωπικές πληροφορίες που συλλέγονται, δημιουργούνται και διέρχονται μέσω των εφαρμογών του SG;
6) Πως θα μπορούσαν να είναι τα πρότυπα που αφορούν θέματα ιδιωτικότητας για όλες τις οντότητες που χρησιμοποιούν το SG έτσι ώστε η τήρησή τους να συμβάλει στην προστασία της ιδιωτικότητας και την μείωση των σχετικών κινδύνων;[6]

3.4.3 Προσωπικές πληροφορίες στο Smart Grid

Σύμφωνα με τη διαδικασία PIA, τα δεδομένα ενέργειας και οι προσωπικές πληροφορίες μπορούν να αποκαλύψουν κάτι συγκεκριμένο με άμεσο ή έμμεσο τρόπο για τα άτομα, τις ομάδες ατόμων ή τις δραστηριότητες αυτών των ατόμων. Τα δεδομένα του SG όπως οι μετρήσεις κατανάλωσης ενέργειας σε συνδυασμό την αυξημένη συχνότητα αναφορών χρήσης, τα δεδομένα παραγωγής ενέργειας και η χρήση οικιακών συσκευών αλλά και συσκευών ικανών να καταγράφουν την κατανάλωση δημιουργούν νέες πηγές προσωπικών πληροφοριών.

Οι άμεσες πληροφορίες που συλλέγονται παραδοσιακά από τις εταιρείες ηλεκτρισμού μπορούν να χρησιμοποιηθούν για τον εντοπισμό ατόμων μέσω στοιχείων όπως ο αριθμός κατοικίας και/ή διεύθυνση, το όνομα του ιδιοκτήτη του σπιτιού ή αυτού που κατοικεί εκεί, την ημερομηνία γέννησης καθώς και κάποια ψηφία του αριθμού κοινωνικής ασφάλισης.

Υπάρχουν πιθανές ακούσιες συνέπειες της συλλογής, αποθήκευσης και διασύνδεσης των φαινομενικά ανώνυμων δεδομένων του SG. Ενώ οι τωρινές πρακτικές ανωνυμοποίησης (anonymization) της ιδιωτικότητας τείνουν να επικεντρώνονται στην αφαίρεση συγκεκριμένων στοιχείων των προσωπικών πληροφοριών, οι μελέτες που αναφέρονται σε αυτό τον τομέα δείχνουν ότι μπορεί να συμβεί εκ νέου ταυτοποίηση και σύνδεση με ένα άτομο. Αυτό το ζήτημα, του επαναπροσδιορισμού των δεδομένων γίνεται σημαντικότερο καθώς αυξάνεται η ποσότητα και ο βαθμός λεπτομέρειας των δεδομένων που συλλέγονται κατά τη διάρκεια των λειτουργιών με την ανάπτυξη περισσότερων εφαρμογών του SG. Έπειτα γίνεται σημαντικό, από την άποψη της ιδιωτικότητας, για τις εταιρείες ηλεκτρισμού και τις τρίτες οντότητες που συμμετέχουν στο SG, να καθορίσουν σε ποια στοιχεία δεδομένων θα αφαιρέσουν τη δυνατότητα σύνδεσης με συγκεκριμένες διευθύνσεις ή άτομα όταν εκτελούν τις δραστηριότητες ανωνυμοποίησης δεδομένων.

Στον Πίνακα 9 εντοπίζονται και περιγράφονται στοιχεία δεδομένων εντός του SG που θα μπορούσαν να επηρεάσουν την ιδιωτικότητα εάν δεν προστατεύονται κατάλληλα. Δεν αποτελεί μια ολοκληρωμένη λίστα των στοιχείων δεδομένων σχετικά με τους πελάτες που θα μπορούσαν να θέσουν σε κίνδυνο την ιδιωτικότητα. Υπάρχει πρόσθετος κίνδυνος εκτός του SG γύρω από την πρόσβαση ορισμένων στοιχείων δεδομένων.[6]

Πίνακας 9 - Πιθανώς διαθέσιμες πληροφορίες μέσω του SG [6]

Στοιχείο Δεδομένων	**Περιγραφή**
Όνομα	Πρόσωπο υπεύθυνο για το λογαριασμό
Διεύθυνση	Τοποθεσία όπου παρέχεται η υπηρεσία

Αριθμός Λογαριασμού	Μοναδικό αναγνωριστικό για το λογαριασμό
Ανάγνωση Μετρητή	Κατανάλωση ενέργειας σε kWh που καταγράφηκε μεταξύ διαστημάτων 15 με 60 λεπτών και σε διάστημα μίας ημέρας κατά τη διάρκεια του τρέχοντος κύκλου χρέωσης
Οικονομικές πληροφορίες	Οι τρέχουσες ή παλαιότερες μετρήσεις, χρεώσεις, το διαθέσιμο υπόλοιπο, συμπεριλαμβανομένου του ιστορικού καθυστερημένων πληρωμών/αδυναμία πληρωμής εφόσον υπάρχουν
Συνήθειες	Πότε το σπίτι είναι κατειλημμένο και άδειο, πότε αυτοί που κατοικούν στο σπίτι είναι ξύπνιοι και κοιμούνται, πόσο χρησιμοποιούνται διάφορες οικιακές συσκευές
Κατανεμημένες Πηγές	Η παρουσία εσωτερικών εγκαταστάσεων παραγωγής και/ή αποθήκευσης, η κατάσταση λειτουργίας, η παροχή από τις κατανεμημένες πηγές ή η κατανάλωση από το δίκτυο, μοτίβα χρήσης
Μοναδικά Αναγνωριστικά Μετρητών	Η διεύθυνση πρωτοκόλλου Internet (IP), η φυσική διεύθυνση (MAC address), ή άλλα αναγνωριστικά δικτύου για το μετρητή εφόσον διαθέτει

3.4.5 Θέματα ιδιωτικότητας στο Smart Grid

Υπάρχει ένα ευρύ φάσμα θεμάτων που αφορούν την προστασία της ιδιωτικότητας στο SG που πρέπει να αντιμετωπιστούν. Αυτά μπορεί να έχουν αντίκτυπο στην εφαρμογή των συστημάτων του SG ή στην αποτελεσματικότητά τους. Για παράδειγμα, η έλλειψη εμπιστοσύνης των καταναλωτών στην ασφάλεια και την προστασία της ιδιωτικότητας των δεδομένων ενεργειακής τους χρήσης μπορεί να οδηγήσει σε έλλειψη αποδοχής και συμμετοχής των καταναλωτών, αν όχι σε δικαστικές διαμάχες. Σε γενικές γραμμές, τα θέματα σχετικά με την ιδιωτικότητα στο SG εμπίπτουν σε μία από τις δύο ευρείες κατηγορίες:

Κατηγορία 1: Προσωπικές πληροφορίες που δεν ήταν διαθέσιμες στο παρελθόν

Κατηγορία 2: Μηχανισμοί που δεν υπήρχαν προηγουμένως για την απόκτηση (ή τη χειραγώγηση) προσωπικών πληροφοριών

Παραδείγματα της πρώτης κατηγορίας περιλαμβάνουν λεπτομερείς πληροφορίες σχετικά με τις συσκευές και τον εξοπλισμό που χρησιμοποιούνται σε δεδομένη τοποθεσία, συμπεριλαμβανομένης της χρήσης συγκεκριμένων ιατρικών και άλλων ηλεκτρονικών συσκευών που υποδεικνύουν προσωπικά στοιχεία και χρονοδιαγράμματα νόμιμων ή πιθανώς παράνομων ενεργειών σε αυτή την τοποθεσία, καθώς και λεπτομερή χρονικά δεδομένα σχετικά με την κατανάλωση ενέργειας σε τοποθεσίες μετρήσεως και επιμέρους οικιακές συσκευές.

Η δεύτερη κατηγορία περιλαμβάνει περιπτώσεις όπου διατίθενται προσωπικές πληροφορίες από άλλες πηγές και το SG μπορεί να παρουσιάσει μία νέα πηγή για τις ίδιες πληροφορίες. Για παράδειγμα, η φυσική τοποθεσία ενός ατόμου σήμερα μπορεί να ανιχνευθεί από τη χρήση πιστωτικής κάρτας ή κινητού τηλεφώνου. Τα σημεία φόρτισης ηλεκτρικών οχημάτων (PEV) αυξάνουν τη δυνατότητα εντοπισμού της φυσικής θέσης μέσω των νέων δεδομένων κατανάλωσης ενέργειας.

Μπορούν να αντληθούν λεπτομερώς δραστηριότητες εντός ενός σπιτιού ή ενός κτιρίου από τα χαρακτηριστικά του ηλεκτρικού εξοπλισμού και το χρονικό τους μοτίβο. Αυτά μπορούν να αποτελέσουν τη βάση για την εξαγωγή συμπερασμάτων σχετικά με τις δραστηριότητες των ατόμων που βρίσκονται στο σπίτι ή το κτίριο (για παράδειγμα αν οι εγκαταστάσεις είναι άδειες).

Παρόλο που υπάρχει ήδη τεχνολογία άμεσης επικοινωνίας με συσκευές και άλλα στοιχεία ενεργειακής κατανάλωσης, η εφαρμογή του SG μπορεί να δημιουργήσει επιπλέον κίνητρα για τη χρήση τους. Οι συσκευές που είναι εφοδιασμένες με τέτοιο εξοπλισμό μπορούν να μεταδίδουν πληροφορίες ενεργειακής κατανάλωσης τόσο στους ιδιοκτήτες όσο και στους διαχειριστές αλλά και τους εξωτερικούς φορείς. [6]

Ο Πίνακας 10 περιγράφει μερικούς από τους πιθανούς τομείς θεμάτων που αφορούν την ιδιωτικότητα και παρέχει κάποια ανάλυση της φύσης των θεμάτων σύμφωνα με τις κατηγορίες που αναφέρθηκαν παραπάνω.

Πίνακας 10 - Πιθανά θέματα ιδιωτικότητας στο SG [6]

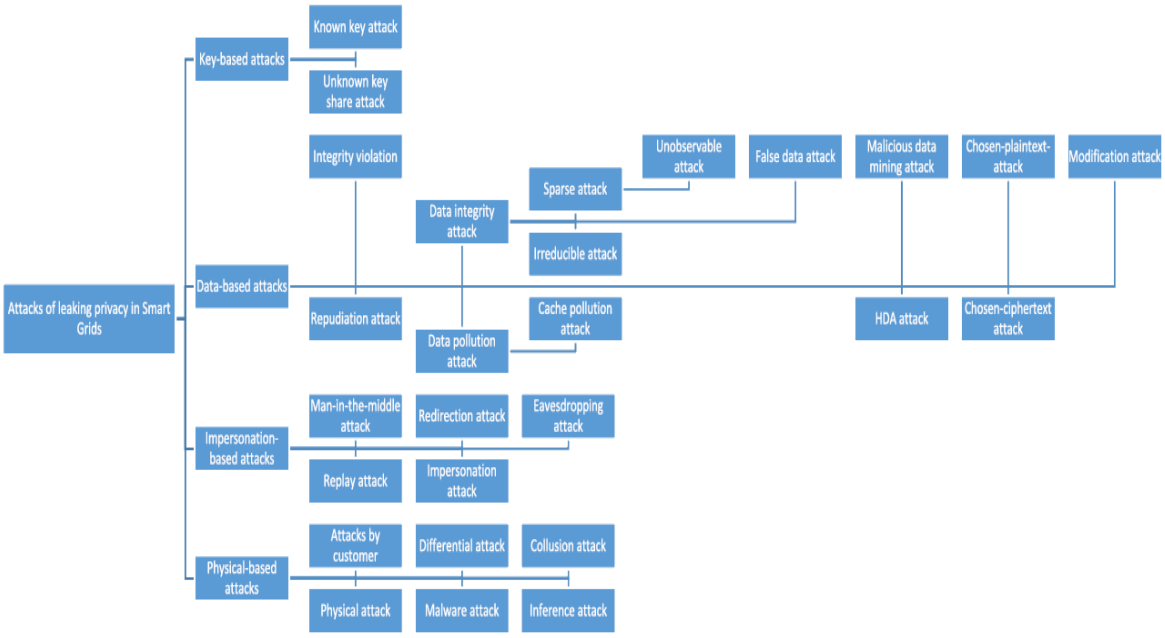
Θέματα Ιδιωτικότητας	**Περιγραφή**	**Κατηγοριοποίηση**
Αποκάλυψη προσωπικών δεδομένων	Μη εξουσιοδοτημένη αποκάλυψη ενεργειακής κατανάλωσης ή άλλων προσωπικών πληροφοριών.	Κατηγορία 2: Η παραδοσιακή μέθοδος ανάγνωσης κατανάλωσης των μετρητών (είτε χειροκίνητα είτε ηλεκτρονικά μέσω απομακρυσμένων συστημάτων ανάγνωσης μετρητών) μπορεί να επιτρέψει λιγότερες δυνατότητες για χειρισμό ή αποκάλυψη δεδομένων χωρίς τη συναίνεση του προσωπικού που τα διαχειρίζεται.

Προσδιορισμός μοτίβων προσωπικής συμπεριφοράς/ συσκευών που χρησιμοποιούνται	Οι έξυπνοι μετρητές σε συνδυασμό με τα δίκτυα αυτοματισμού οικιακής χρήσης ή άλλες τεχνολογίες μπορούν να ανιχνεύσουν τη χρήση συγκεκριμένων συσκευών. Η πρόσβαση σε δεδομένα χρήσης που μπορούν να αποκαλύψουν συγκεκριμένα χρονικά και τοπικά χαρακτηριστικά χρήσης ηλεκτρισμού σε συγκεκριμένες περιοχές του σπιτιού μπορούν επίσης να αποκαλύψουν τους τύπους δραστηριοτήτων και/ή τις συσκευές που χρησιμοποιούνται. Πιθανές χρήσεις για αυτές τις πληροφορίες περιλαμβάνουν: • Σκοπούς αξιοπιστίας και εγγύησης προϊόντων των κατασκευαστών των συσκευών • Στοχευμένο μάρκετινγκ	Κατηγορία 1: Ο τύπος των δεδομένων που διατίθενται από την εφαρμογή του SG μπορεί να διαθέτει περισσότερη λεπτομέρεια και διαθεσιμότητα σε ευρύτερη κλίμακα.
Εκτέλεση απομακρυσμένης επιτήρησης σε πραγματικό χρόνο	Η πρόσβαση σε δεδομένα ενεργειακής χρήσης τη στιγμή που συμβαίνουν μπορεί ενδεχομένως να αποκαλύψει πράγματα όπως αν υπάρχουν άνθρωποι στις εγκαταστάσεις, τι κάνουν, πότε ξυπνούν και πότε κοιμούνται, που και πόσοι βρίσκονται μέσα στο σπίτι/κτίριο.	Κατηγορία 2: Υπάρχουν Πολλές μέθοδοι επιτήρησης σε πραγματικό χρόνο. Η διαθεσιμότητα μηχανογραφημένων δεδομένων σε πραγματικό (ή σχεδόν) χρόνο θα δημιουργούσε έναν άλλο τρόπο με τον οποίο θα μπορούσε να διεξαχθεί μία τέτοια επιτήρηση.
Εμπορικές χρήσεις δεδομένων εκτός δικτύου	Η αποθήκευση δεδομένων για την κατανάλωση ενέργειας του πελάτη μπορεί να αποκαλύψει πληροφορίες για τον τρόπο ζωής του, που θα μπορούσαν να αξιοποιηθούν από πολλές οντότητες συμπεριλαμβανομένων των πωλητών ενός ευρέως φάσματος προϊόντων και υπηρεσιών. Οι πωλητές μπορούν αποκτήσουν λίστες χαρακτηριστικών για στοχευμένες καμπάνιες πωλήσεων και μάρκετινγκ που μπορεί να μην είναι αποδεκτό από κάποιους. Τα δεδομένα μπορούν επίσης να χρησιμοποιηθούν για ασφαλιστικούς σκοπούς.	Κατηγορία 2: Σύμφωνα με τα υφιστάμενα συστήματα μέτρησης και χρέωσης, τα δεδομένα των μετρητών δε διαθέτουν τόσο μεγάλο βαθμό λεπτομέρειας στις περισσότερες περιπτώσεις ώστε να αποκαλύψουν πράγματα σχετικά με τις δραστηριότητες. Ωστόσο, με τους έξυπνους μετρητές, ο χρόνος χρήσης, οι ρυθμοί ζήτησης και ο άμεσος έλεγχος του φορτίου μπορούν να δημιουργήσουν λεπτομερή δεδομένα τα οποία θα μπορούσαν να πωληθούν και να χρησιμοποιηθούν για αναλύσεις διαχείρισης της

		ενέργειας και peer comparison. Εφόσον αυτές οι πληροφορίες είναι ωφέλιμες για εξωτερικές οντότητες, η εκπαίδευση των καταναλωτών σχετικά με την προστασία αυτών των δεδομένων έχει σημαντικά θετικά αποτελέσματα.

3.4.6 Απειλές και επιθέσεις

Υπάρχουν πολλά είδη επιθέσεων διαρροής προσωπικών δεδομένων στο SG. Γενικά, η κατηγοριοποίηση των επιθέσεων στο SG πραγματοποιείται με τη χρήση διάφορων κριτηρίων όπως παθητικές ή ενεργητικές, εσωτερικές ή εξωτερικές και άλλων. Μία κατηγοριοποίηση των επιθέσεων διαρροής προσωπικών δεδομένων στο SG σε τέσσερις κατηγορίες παρουσιάζεται στην Εικόνα 4 και περιλαμβάνει: 1) επιθέσεις κλειδιού (key-based attacks), 2) επιθέσεις δεδομένων (data-based attacks), 3) επιθέσεις πλαστοπροσωπίας (impersonation-based attacks) και 4) φυσικές επιθέσεις (physical-based attacks).[37]



Εικόνα 4 - Κατηγοριοποίηση επιθέσεων διαρροής προσωπικών δεδομένων στο SG [37]

1) Επιθέσεις κλειδιού

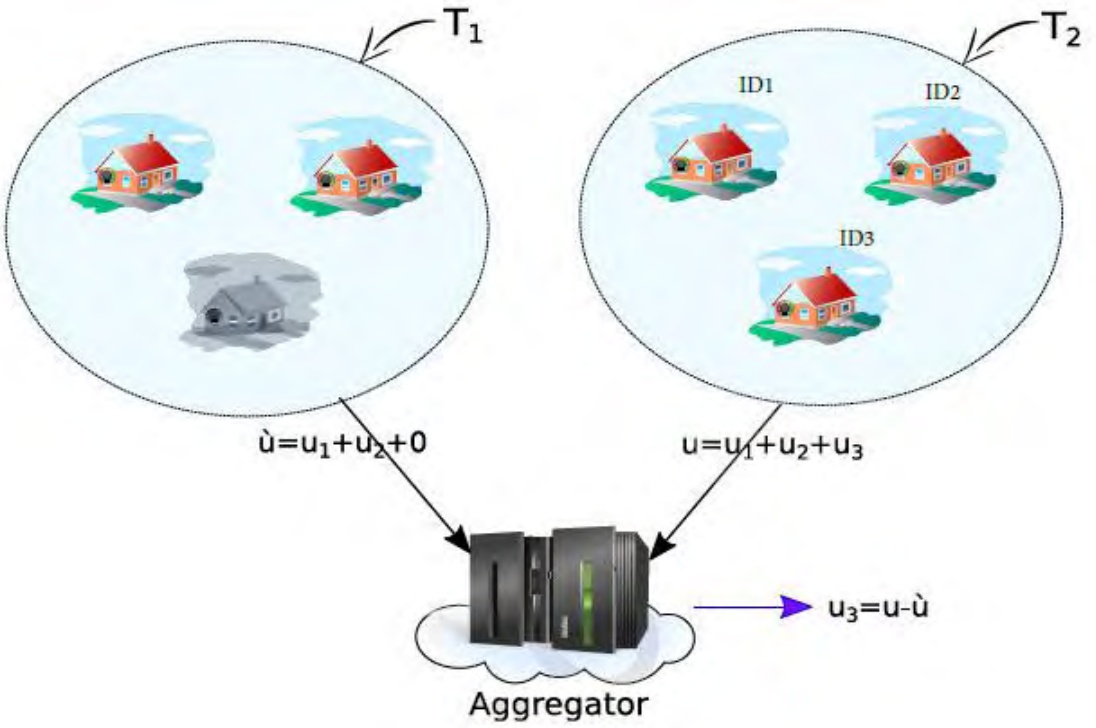
Γενικά, μετά τη φάση εγγραφής, κάθε τμήμα του SG έχει ένα μυστικό (ή συμμετρικό) κλειδί (secret key) ή ένα πιστοποιητικό (certificate) για την πραγματοποίηση της φάσης της αυθεντικοποίησης (authentication). Σε οποιαδήποτε στιγμή, ένας επιτιθέμενος (ο πελάτης ή οι διαχειριστές/προωπικό συντήρησης) μπορεί να εκτελέσει τόσο την επίθεση γνωστού κλειδιού (known-key attack) όσο και την επίθεση κοινής χρήσης άγνωστου κλειδιού (unknown key-share) σε μία αυθεντικοποιημένη συμφωνία κλειδιού ή σε μία αυθεντικοποιημένη συφμωνία κελιδιού με πληροφορίες κλειδιού. Πιο συγκεκριμένα, στην επίθεση γνωστού κλειδιού, το κλειδί θεωρείται γνωστό, και ο επιτιθέμενος καταφέρνει να διακρίνει εάν προσδιορίζει κάποια δομική ιδιότητα του κρυπτογραφικού αλγορίθμου (cipher). Κατά τη διάρκεια μίας επίθεσης κοινής χρήσης άγνωστου κλειδιού, ένας επιτιθέμενος χειρίζεται δύο οντότητες A και B, όπου η A καταλήγει να πιστεύει ότι μοιράζεται ένα κλειδί με τη B, και αν και αυτό συμβαίνει στην πραγματικότητα, η B πιστεύει όμως εσφαλμένα ότι μοιράζεται το κλειδί με μία οντότητα E ≠ A.[38],[39]

2) Επιθέσεις δεδομένων

Για την εξασφάλιση της ακεραιότητας των δεδομένων ηλεκτρικής ενέργειας στο SG, οι πελάτες μπορούν να βοηθήσουν με τη μετατόπιση της κατανάλωσης ενέργειας σε διαφορετικούς χρόνους, κάτι που δεν είναι πάντοτε δυνατό. Ωστόσο, ένας επιτιθέμενος μπορεί να ξεκινήσει διάφορες λειτουργίες τροποποίησης σχετικά με τα δεδομένα που περιέχουν πληροφορίες σχετικά με την κατανάλωση ηλεκτρικής ενέργειας. Σε αυτή την κατηγορία επιθέσεων υπάγονται εννιά είδη επιθέσεων: παραβίαση ακεραιότητας (integrity violation), επίθεση αποποίησης δεδομένων (repudiation attack), επίθεση εξόρυξης κακόβουλων δεδομένων (malicious data mining attack), επίθεση διαφορικής συνάθροισης σε ανθρώπινο παράγοντα (human-factor-aware dierential aggregation attack - HDA), επίθεση επιλεγμένου απλού κειμένου (Chosen plain text attack), επίθεση επιλεγμένου κρυπτογραφικού κειμένου (chosen ciphertext attack - CCA), επίθεση ακεραιότητας δεδομένων (data integrity attack), επίθεση θορυβωδών δεδομένων (data pollution attack) και επίθεση τροποποίησης (modification attack). [37],[40]

Αν ένας επιτιθέμενος καταφέρει την τροποποίηση μεταδιδόμενων δεδομένων, εκτελείται μία παραβίαση της ακεραιότητας. Η επίθεση αποποίησης δεδομένων αναφέρεται σε άρνηση συμμετοχής στο σύνολο ή σε μέρος του δικτύου επικοινωνίας στο SG. Αν ένας επιτιθέμενος καταφέρει να αλλοιώσει τον συναθροιστή (aggregator) και έτσι να λειτουργεί με παραβιασμένους μετρητές, εκτελείται μια επίθεση εξόρυξης κακόβουλων δεδομένων. Μία επίθεση HDA βασίζεται στην αποκωδικοποίηση της ανθρώπινης συμπεριφοράς, όπου ένας επιτιθέμενος μπορεί να αποκτήσει τις αναγνώσεις του μετρητή id3 συγκρίνοντας δύο συναθροιστικά αποτελέσματα όπως φαίνεται στην Εικόνα 5. Αν ένας επιτιθέμενος καταφέρει να διακρίνει ένα κρυπτογραφικό κείμενο όταν

δίνονται δύο αντίστοιχα απλά κείμενα, τότε εκτελείται επίθεση επιλεγμένου απλού κειμένου. Εάν ένας επιτιθέμενος γνωρίζει τα κρυπτογραφικά κείμενα που χρησιμοποιούνται στο SG και μπορεί να αποκτήσει τα επακόλουθα απλά κείμενα, εκτελείται η επίθεση επιλεγμένου κρυπτογραφικού κειμένου (CCA) η οποία μπορεί να οδηγήσει στην ανάκτηση του κρυμμένου μυστικού κλειδιού που χρησιμοποιείται για την αποκρυπτογράφηση. Μία επίθεση ακεραιότητας δεδομένων στο SG αποτελείται από ένα σύνολο παραβιασμένων μετρητών των οποίων οι ενδείξεις τροποποιούνται από έναν επιτιθέμενο. Κατά τη διάρκεια μίας επίθεσης θορυβωδών δεδομένων, ένας επιτιθέμενος μπορεί να αναγκάσει τις πύλες του δικτύου να αποθηκεύσουν στην cache μη συχνά χρησιμοποιούμενο περιεχόμενο για να επηρεάσει τη συνολική απόδοση του δικτύου και να αυξήσει τη μέση κίνηση σε ένα σύνδεσμο (link utilization).[41],[42],[43],[44],[45],[46]

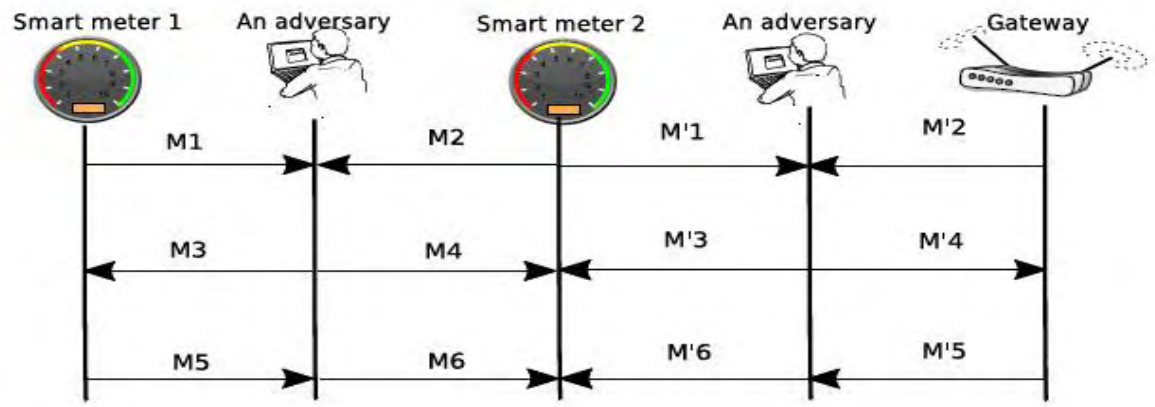


Εικόνα 5 - Επίθεση HDA στο SG [43]

3) Επιθέσεις πλαστοπροσωπίας

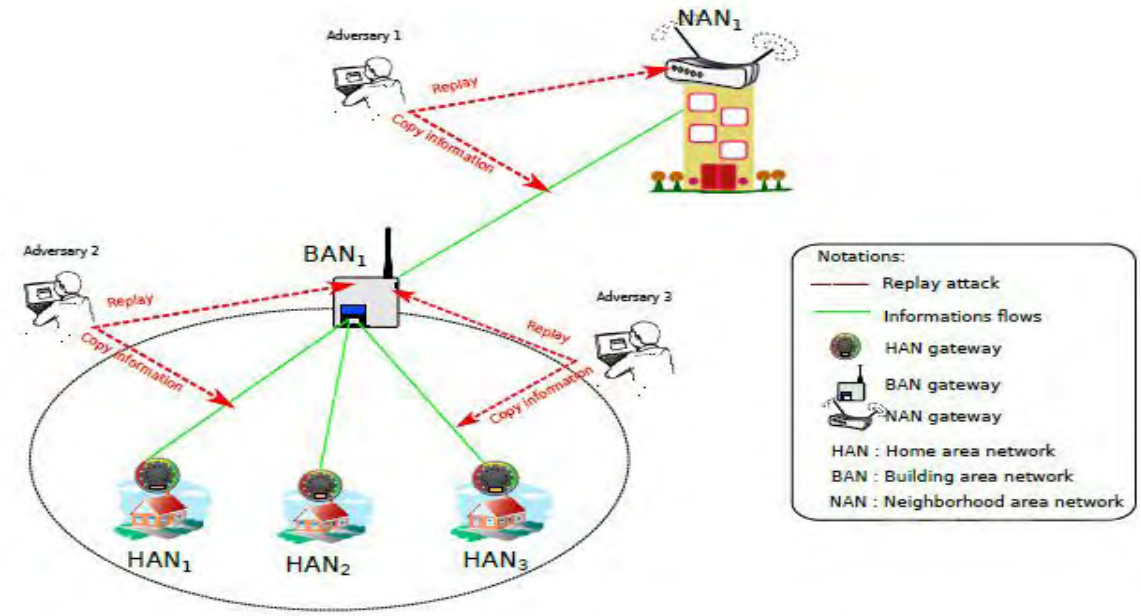
Ένας επιτιθέμενος μπορεί ανά πάσα στιγμή να καταγράψει δεδομένα του SG που μεταδίδονται από άλλους έξυπνους μετρητές και να διαβάσει το περιεχόμενο αυτών των δεδομένων για την ανάκτηση πληροφοριών που σχετίζονται με την ενεργειακή κατανάλωση στο έξυπνο σπίτι. Σε αυτή την κατηγορία υπάγονται πέντε είδη επιθέσεων: επίθεση ενδιάμεσου ατόμου (Man-in-the-middle attack - MITM), επίθεση αναμετάδοσης (replay attack), επίθεση ανακατεύθυνσης (redirection attack), επίθεση πλαστοπροσωπίας (impersonation attack) και επίθεση υποκλοπής (eavesdropping attack).[37]

Η επίθεση MITM είναι μία από τις πιο δημοφιλής επιθέσεις στη νέα γενιά δικτύων όπως το SG. Όπως φαίνεται στην Εικόνα 6 είναι η υποκλοπή των δεδομένων που διαβιβάζονται μεταξύ δύο έξυπνων μετρητών ή ενός έξυπνου μετρητή και μίας πύλης δικτύου για την τροποποίηση αυτών των δεδομένων χωρίς να το γνωρίζουν τα θύματα. Συγκεκριμένα, οι έξυπνοι μετρητές και η πύλη προσπαθούν να διαμορφώσουν ασφαλή επικοινωνία στέλνοντας το ένα στο άλλο το δημόσιο κλειδί (public key) τους (μηνύματα M1, M2, M'1, M'2). Ένας επιτιθέμενος υποκλέπτει τα μηνύματα M1,M2,M'1, και M'2 κι ως επιστροφή στέλνει το δημόσιο κλειδί του στα θύματα (μηνύματα M3, M4, M'3, M'4). Έπειτα, ο πρώτος έξυπνος μετρητής και η πύλη κρυπτογραφούν τα μηνύματά τους χρησιμοποιώντας το δημόσιο κλειδί του επιτιθέμενου και το στέλνουν στο δεύτερο έξυπνο μετρητή (μηνύματα M5 and M'5). Ο επιτιθέμενος υποκλέπτει τα μηνύματα M5 και M'5, και τα αποκρυπτογραφεί χρησιμοποιώντας το δικό του ιδιωτικό κλειδί (private key). Στη συνέχεια ο επιτιθέμενος κρυπτογραφεί το απλό κείμενο χρησιμοποιώντας το δημόσιο κλειδί του πρώτου έξυπνου μετρητή, και το στέλνει στο δεύτερο έξυπνο μετρητή (μηνύματα M6 και M'6).[47]



Εικόνα 6 - Επίθεση MITM [37]

Η επίθεση αναμετάδοσης είναι μία επίθεση τύπου MITM όπου ένας επιτιθέμενος υποκλέπτει πακέτα δεδομένων και τα αναμεταδίδει στο διακομιστή που προορίζονταν, όπως φαίνεται στην Εικόνα 7. Στα δίκτυα V2G (Vehicle to Grid), ένας επιτιθέμενος μπορεί να ανακατευθύνει τα μηνύματα του οχήματος σε ένα άλλο δίκτυο εκτός του αρχικού. Μία επίθεση ανακατεύθυνσης ενσωματώνεται σε μία επίθεση εξαπάτησης (phishing attack). Κατά τη διάρκεια αυθεντικοποίησης μεταξύ έξυπνων μετρητών και πυλών, ένας επιτιθέμενος μπορεί να ξεκινήσει μια επίθεση πλαστοπροσωπίας όταν μπορεί να πλαστογραφήσει την ταυτότητα έγκυρων οντοτήτων του SG. Η επίθεση υποκλοπής μπορεί να προκύψει όταν ένας επιτιθέμενος μπορεί να έχει πρόσβαση στη δίοδο δεδομένων (datapath) του SG και στη συνέχεια μπορεί να παρακολουθεί και να διαβάζει την κίνηση μεταξύ έξυπνων μετρητών και πυλών για να θέσει σε κίνδυνο την ιδιωτικότητα των οικιακών χρηστών. [37],[48],[49]



Εικόνα 7 - Επίθεση αναμετάδοσης που εκτελείται από τρεις επιτιθέμενους [37]

4) Φυσικές επιθέσεις

Ένας επιτιθέμενος μπορεί να στοχεύσει στο υλικό (hardware) της μπαταρίας ενός οχήματος, σε έναν τοπικό συναθροιστή, μία πύλη ή έναν διακομιστή μεσολάβησης (proxy server) για να εκτελέσει αρκετές φυσικές επιθέσεις όπως διαφορική επίθεση (differential attack), επίθεση κακόβουλου λογισμικού (malware attack), επίθεση συμπαιγνίας (collusion attack) και επίθεση συμπερασμού (inference attack).Για την απόκτηση των δεδομένων ενός χρήστη στο SG, ένας επιτιθέμενος μπορεί να εκτελέσει μία διαφορική επίθεση. Ένας επιτιθέμενος μπορεί να εκτελέσει μία επίθεση κακόβουλου λογισμικού αναπτύσσοντας μη ανιχνεύσιμα κακόβουλα λογισμικά στο SG στοχεύοντας στην αποκάλυψη προσωπικών δεδομένων οικιακών χρηστών. Μία επίθεση συμπαιγνίας μεταξύ δύο επιτιθέμενων (συναθροιστή και ελεγκτή φόρτισης) μπορεί να χρησιμοποιηθεί για την ταυτοποίηση ενός χρήστη και τη σύνδεση αιτημάτων φόρτισης σε μία συγκεκριμένη ταυτότητα. Αν ένας επιτιθέμενος καταφέρει να αναλύσει τα χαρακτηριστικά ενός συστήματος βάσεων δεδομένων μπορεί να εκτελέσει μία επίθεση συμπερασμού.[37],[50]

3.5 Πρότυπα

3.5.1 Πρότυπα ως μέτρο ασφαλείας

Για την προστασία του SG, διάφορες λύσεις ασφαλείας μπορούν να εφαρμοστούν, συμπεριλαμβανομένων των παραδοσιακών τεχνολογιών ασφαλείας στον κυβερνοχώρο

όπως κρυπτογράφηση, έλεγχος πρόσβασης, προστασία από κακόβουλο λογισμικό (anti-malware) ή τείχη προστασίας (firewalls), καθώς και προηγμένες μέθοδοι όπως για παράδειγμα: Συστήματα Διαχείρισης Πληροφοριών και Συμβάντων Ασφαλείας (SIEM), πλατφόρμες έμπιστης υπολογιστικής (trusted computing platforms) και συστήματα επίγνωσης της κατάστασης (SANs). Οι ειδικοί για θέματα ασφαλείας συμφωνούν ότι θα έπρεπε αρχικά να χρησιμοποιηθούν λύσεις και πρακτικές που να βασίζονται στα πρότυπα (standards). Τα πρότυπα βοηθούν τους υπεύθυνους για την εισαγωγή νέων μέτρων ασφαλείας να απαντήσουν στα ερωτήματα που αφορούν την επιλογή των μεθόδων, τις προτεραιότητες υλοποίησης και την έκταση ή την επάρκεια της προσέγγισης. Λύσεις με βάση την αποκαλούμενη ¨εμπειρογνωμοσύνη¨ εργαζομένων μίας ανεξάρτητης εταιρείας ενδέχεται να υποφέρουν από περιορισμούς, ανάλογα με την εμπειρία και τις γνώσεις αυτών των ειδικών. Από την άλλη πλευρά, οι πρακτικές που συνιστώνται στα πρότυπα προσφέρουν υψηλά επίπεδα εξασφάλισης του ότι είναι συστηματικές, πλήρεις και ασφαλείς, όπως αξιολογήθηκαν από πολλούς ειδικούς σε μία μακροπρόθεσμη διαδικασία.

Οι λόγοι για την τήρηση των προτύπων είναι πολυάριθμοι. Μεταξύ αυτών, αξίζει να σημειωθεί το γεγονός ότι καθιστούν δυνατή την πιστοποίηση, καθώς συνιστούν έναν τρόπο για την απόκτηση αξιοπιστίας από τους πελάτες και τη δημιουργία ενός ανταγωνιστικού πλεονεκτήματος μεταξύ άλλων οργανισμών αυτού του τομέα. Αναφέρεται επίσης ως ένας από τους πρωταρχικούς οδηγούς που υιοθετήθηκαν. Ωστόσο, θα πρέπει επίσης να ληφθεί υπόψη ότι τα πρότυπα δεν αποτελούν ¨πανάκεια¨. Είναι συχνά γενικά κι έχουν ευρύ πεδίο εφαρμογής, που δεν επιτρέπει να προσφέρουν λεπτομερείς οδηγίες για την επίλυση ορισμένων θεμάτων. Σαν αποτέλεσμα, προσδιορίζεται η ποιότητα της εφαρμογής των συστάσεων που καθορίζονται από τα πρότυπα, η οποία συμβάλλει στα αποτελεσματικά επίπεδα ασφαλείας.[51]

3.5.2 Πρότυπα που εφαρμόζονται σε όλες τις συνιστώσες του Smart Grid

Η σειρά προτύπων *IEC 62351* στοχεύει στον καθορισμό των ιδιοτήτων ασφαλείας των πρωτοκόλλων επικοινωνίας που καθορίζονται από το IEC TC 57 (IEC 60870-5, IEC 60870-6, IEC 61850, IEC 61970 κα IEC 61968). Επιτρέπουν τη ρύθμιση διαφόρων επιπέδων πρωτοκόλλων ασφαλείας ανάλογα με το πρωτόκολλο και τις παραμέτρους που επιλέγονται για μία συγκεκριμένη υλοποίηση. Σχεδιάστηκαν για οπισθόφορη συμβατότητα και σταδιακή υλοποίηση.[52]

Τα πρότυπα *NERC CIP* καθορίζουν απαιτήσεις για ελέγχους και μέτρα προστασίας συστημάτων ηλεκτρικής ενέργειας μαζικής παραγωγής από απειλές στον κυβερνοχώρο.[53]

Το *NISTIR 7628* είναι μια έρευνα τριών τόμων που παρέχει ένα ολοκληρωμένο πλαίσιο για έξυπνες εφαρμογές οι οποίες μπορούν να χρησιμοποιηθούν για την ανάπτυξη αποτελεσματικών στρατηγικών για την ασφάλεια του κυβερνοχώρου, οι οποίες είναι προσαρμοσμένες στα ιδιαίτερα χαρακτηριστικά και ευπάθειές τους. Στον πρώτο, ορίζεται ένα λογικό μοντέλο αναφοράς του SG, το οποίο διακρίνει 22 κατηγορίες λογικών διεπαφών της αρχιτεκτονικής του SG. Ορίζονται επίσης υψηλού επιπέδου απαιτήσεις ασφαλείας που σχετίζονται με το μοντέλο αυτό. Επιπλέον, μελετά κρυπτογραφικά ζητήματα και ζητήματα διαχείρισης κλειδιών καθώς και στρατηγικές κυβερνοασφάλειας. Ο δεύτερος, ειδικεύεται στην προστασία προσωπικών δεδομένων όλων των συμμετεχόντων στο SG. Ο τρίτος, παρουσιάζει συμπληρωματικό υλικό που περιλαμβάνει για παράδειγμα κατηγορίες τρωτών σημείων του SG, ερευνητικά και αναπτυξιακά θέματα, ή βασικά θέματα χρήσης του συστήματος ενέργειας που είναι σοβαρά σε σχέση με τις απαιτήσεις ασφαλείας του SG.[6]

Το πρότυπο *NRC RG 5.71* παρουσιάζει ένα σύνολο ελέγχων ασφαλείας και καλύπτει εθνικούς κανονισμούς σχετικά με την προστασία πυρηνικών υποδομών. Οι έλεγχοι σε αυτό το πρότυπο προέρχονται από NIST SP 800-53 και NIST SP 800-82 αλλά προσαρμόστηκαν στα χαρακτηριστικά του τομέα της πυρηνικής ενέργειας. Το πρότυπο αυτό εισάγει την έννοια των κρίσιμων ψηφιακών αντικειμένων (CDA), τα οποία είναι σημαντικά για την ασφάλεια και πρέπει να προστατεύονται κατάλληλα.[54]

Το πρότυπο *Risk Management Process* δημιουργήθηκε σε συνεργασία από το US DoE, NIST και NERC, και πρόκειται για μία μεθοδολογία διαχείρισης του κινδύνου που ειδικεύεται στον τομέα της ηλεκτρικής ενέργειας. Αυτή η μεθοδολογία είναι βασισμένη στη γενικής εφαρμογής διαδικασία διαχείρισης του κινδύνου που περιγράφεται από το NIST SP 800-39.[55]

Το πρότυπο *EI RM Checklists* αποτελεί μια ολοκληρωμένη προσέγγιση διαχείρισης του κινδύνου για ενεργειακές εγκαταστάσεις μικρής και μεσαίας κλίμακας, όπως οι δημοτικές και οι ανεξάρτητες επιχειρήσεις ηλεκτρισμού ή οι αγροτικοί συνεταιρισμοί.[56]

Το πρότυπο *IEC 62541* είναι μια σειρά ανεξάρτητων συστημάτων-προτύπων διαλειτουργικότητας για ασφαλή και αξιόπιστη ανταλλαγή δεδομένων στο χώρο του βιομηχανικού αυτοματισμού και σε άλλους κλάδους. Στο μοντέλο ασφαλείας περιλαμβάνεται η περιγραφή των πιθανών απειλών στο OPC Unified Architecture (UA) και λειτουργίες ασφαλείας, με στόχο τον μετριασμό τους. Ένα σημαντικό μέρος του ειδικεύεται στο πως πληρούν τους στόχους ασφαλείας και παρέχουν προστασία ενάντια στις απειλές οι λειτουργίες ασφαλείας του OPC-UA.[57]

Το πρότυπο *RFC 6272* προσδιορίζει βασικά πρωτόκολλα διαδικτύου (IP) για χρήση στο SG. Αρκετά τμήματα του προτύπου είναι αφιερωμένα στην ασφάλεια.[58]

Στον Πίνακα 11 αναφέρονται συνοπτικά τα πρότυπα και το πεδίο εφαρμογής τους που προσδιορίστηκαν παραπάνω καθώς και ο τύπος, το εύρος αλλά και η χρονολογία δημοσίευσής τους.

Πίνακας 11 - Πρότυπα ΣΗΕ και SG που σχετίζονται με την κυβερνοασφάλεια και μπορούν να εφαρμοστούν σε όλες τις συνιστώσες του SG [51]

	Πρότυπο	**Πεδίο Εφαρμογής**	**Τύπος**	**Εύρος**	**Έτος**
1.	IEC 62351	Ασφάλεια των πρωτοκόλλων επικοινωνίας.	Τεχνικό	Παγκόσμιο	2017
2.	NERC CIP	Κυβερνοασφάλεια συστημάτων μαζικής παραγωγής ενέργειας	Γενικό	ΗΠΑ	2013
3.	NISTIR 7628	Κυβερνοασφάλεια Smart Grid	Γενικό	ΗΠΑ	2014
4.	NRC RG 5.71	Κυβερνοασφάλεια των πυρηνικών υποδομών	Γενικό	ΗΠΑ	2010
5.	EI RM Checklists	Διαχείριση κινδύνου σε μικρές/μεσαίες ενεργειακές εγκαταστάσεις	Γενικό	ΗΠΑ	2002
6.	Risk Management Process	Διαχείριση κινδύνου στον ηλεκτρικό τομέα	Γενικό	ΗΠΑ	2012
7.	IEC 62541	Μοντέλο Ασφαλείας OPC UA	Γενικό	Παγκόσμιο	2016
8.	RFC 6272	Αναγνώριση πρωτοκόλλων διαδικτύου για το Smart Grid	Τεχνικό	Παγκόσμιο	2011

3.5.3 Πρότυπα που εφαρμόζονται σε υποσταθμούς

Το πρότυπο *IEEE 1686* καθορίζει ιδιότητες, λειτουργίες και πρακτικές των ευφυών ηλεκτρονικών συσκευών (IEDs) των υποσταθμών στους τομείς όπως πρόσβαση δεδομένων, διαγνωστικά, διαμόρφωση, αναβάθμιση υλικολογισμικού ή χειροκίνητη λειτουργία. Καθορίζει βασικές απαιτήσεις ασφαλείας για τις IEDs, και ορίζει ποια μέτρα προστασίας, μηχανισμούς ελέγχου και προειδοποιητικές ενδείξεις πρέπει να παρέχονται από τους προμηθευτές αυτών των συσκευών. Επίσης, παρέχει υποστήριξη στους χρήστες

για τον καθορισμό προγραμμάτων ασφαλείας. Έχει σχεδιαστεί για να πληροί τις απαιτήσεις NERC CIP, αλλά μπορεί να εφαρμοστεί σε κάθε IED του υποσταθμού.[59]

Το πρότυπο *IEEE C37.240* περιγράφει το πρόβλημα της κυβερνοασφάλειας στον τομέα των ηλεκτρικών επιχειρήσεων και καθορίζει τις βασικές απαιτήσεις κυβερνοασφάλειας για τα συστήματα επικοινωνίας των ηλεκτρικών υποσταθμών (αυτοματοποίηση, προστασία και έλεγχος).[60]

Το πρότυπο *IEEE 1402* περιγράφει θέματα ασφαλείας που σχετίζονται με την εγκατάσταση και τη λειτουργία ηλεκτρικών υποσταθμών. Περιγράφει διαφορετικούς τύπους φυσικών εισβολών και μεθόδων προστασίας απέναντί τους, καθώς και αξιολογεί την αποτελεσματικότητα αυτών των μεθόδων.[61]

Στον Πίνακα 12 αναφέρονται συνοπτικά τα πρότυπα και το πεδίο εφαρμογής τους που προσδιορίστηκαν παραπάνω καθώς και ο τύπος, το εύρος αλλά και η χρονολογία δημοσίευσής τους.

Πίνακας 12 - Πρότυπα κυβερνοασφάλειας για ΣΗΕ και SG που εφαρμόζονται σε υποσταθμούς [51]

	Πρότυπο	**Πεδίο Εφαρμογής**	**Τύπος**	**Εύρος**	**Έτος**
1.	IEEE 1686	Κυβερνοασφάλεια	Τεχνικό	Παγκόσμιο	2007
2.	IEEE C37.240	Κυβερνοασφάλεια	Τεχνικό	Παγκόσμιο	2014
3.	IEEE 1402	Φυσική και ηλεκτρονική ασφάλεια	Γενικό	Παγκόσμιο	2008

3.5.4 Πρότυπα που εφαρμόζονται στα συστήματα αυτομάτου ελέγχου και βιομηχανικού αυτοματισμού

Τα πρότυπα *ISA99* αναπτύχθηκαν από τη Διεθνή Εταιρεία Αυτοματισμού (ISA - International Society of Automation) και διευθετούν θέματα ηλεκτρονικής ασφάλειας για συστήματα αυτομάτου ελέγχου και βιομηχανικού αυτοματισμού (IACS). Από το 2009, αυτά τα πρότυπα αφομοιώθηκαν από τη σειρά προτύπων *IEC 62443.* Οι προδιαγραφές αυτών των προτύπων περιλαμβάνουν μοντέλα και έννοιες ασφαλείας, μεθόδους μέτρησης της συμβατότητας της ασφάλειας συστημάτων, ασφάλεια του κύκλου ζωής και χρήσης, διαχείριση ενημερώσεων λογισμικού στο περιβάλλον των IACS, ασφάλεια της αξιολόγησης του κινδύνου και του σχεδιασμού του συστήματος, οδηγίες υλοποίησης για

ένα σύστημα διαχείρισης της ασφάλειας των IACS, καθώς και διάφορες απαιτήσεις που αναφέρονται σε διαφορετικές πτυχές των IACS.[62]

Το πρότυπο *ISO/IEC TR 27019* παρέχει θεμελιώδης αρχές που βασίζονται στο ISO/IEC 27002 για τη διαχείριση της ασφάλειας των πληροφοριών που εφαρμόζεται για την επεξεργασία συστημάτων ελέγχου, και χρησιμοποιείται στη βιομηχανία των εταιρειών ηλεκτρικής ενέργειας. Σκοπός του είναι να επεκτείνει το σύνολο προτύπων ISO/IEC 27000 στον τομέα της επεξεργασίας της τεχνολογίας συστημάτων ελέγχου και αυτοματισμού, επιτρέποντας έτσι στην βιομηχανία της ηλεκτρική ενέργειας να υλοποιήσει ένα τυποποιημένο σύστημα διαχείρισης της ασφάλειας των πληροφοριών (ISMS) σύμφωνα με το ISO/IEC 27001 που εκτείνεται από την επιχείρηση ως το επίπεδο της διαδικασίας του ελέγχου.[63]

Το *NIST SP 800-82* είναι μία δημοσίευση του NIST που επικεντρώνεται στην ασφάλεια των συστημάτων βιομηχανικού ελέγχου (ICS). Εισάγει και προσεγγίζει στο θέμα της ασφάλειας διάφορους τύπους ICS (SCADA, PCS και άλλα), καθώς και τυπικές τοπολογίες συστημάτων. Προσδιορίζει κοινές απειλές και ευπάθειες των ICS και προσδιορίζει συνιστάμενους ελέγχους ασφαλείας για τον περιορισμό των σχετικών κινδύνων.[64]

Το *DHS Catalog* παρουσιάζει πρακτικές που έχουν προτείνει διαφορετικοί βιομηχανικοί οργανισμοί για τη βελτίωση της ασφάλειας των συστημάτων βιομηχανικού ελέγχου (ICS). Αυτές οι προτάσεις χωρίζονται σε 19 κατηγορίες κι έχουν ευρύ πεδίο εφαρμογής ώστε να παρέχουν ένα επίπεδο ευελιξίας που επιτρέπει την ανάπτυξη υγιών προτύπων κυβερνοασφάλειας, που ειδικεύονται σε ανάγκες ατομικής ασφάλειας.[65]

Το *DHS Cyber Security Procurement Language for Control Systems* καθορίζει τις απαιτήσεις ασφαλείας για τον τομέα των προμηθευτών των συστημάτων βιομηχανικών ελέγχων (ICS).[66]

Στον Πίνακα 13 αναφέρονται συνοπτικά τα πρότυπα και το πεδίο εφαρμογής τους που προσδιορίστηκαν παραπάνω καθώς και ο τύπος, το εύρος αλλά και η χρονολογία δημοσίευσής τους.

Πίνακας 13 - Πρότυπα ΣΗΕ ή SG που σχετίζονται με την κυβερνοασφάλεια και εφαρμόζονται στα IACS [51]

	Πρότυπο	Πεδίο Εφαρμογής	Τύπος	Εύρος	Έτος
1.	IEC 62443 (ISA 99)	Κυβερνοασφάλεια IACS	Τεχνικό	Παγκόσμιο	2009
2.	ISO/IEC 27019	Κυβερνοασφάλεια IACS	Γενικό	Παγκόσμιο	2013
3.	NIST SP 800-82	Κυβερνοασφάλεια IACS	Γενικό	ΗΠΑ	2013
4.	DHS Catalog	Κυβερνοασφάλεια IACS	Γενικό	ΗΠΑ	2009
5.	DHS Cyber Security Procurement Language for Control Systems	Απαιτήσεις κυβερνοασφάλειας για τον τομέα της προμήθειας	Τεχνικό	ΗΠΑ	2008

3.5.5 Πρότυπα που εφαρμόζονται στην προηγμένη υποδομή μέτρησης (AMI)

Το *Security Profile for Advanced Metering Infrastructure* είναι μία κατευθυντήρια γραμμή που αναπτύχθηκε από την ομάδα εργασίας Advanced Metering Infrastructure Security (AMI-SEC) και δημοσιεύτηκε το 2010. Σκοπός αυτού του εγγράφου είναι η καθοδήγηση σχετικά με την ενσωμάτωση και την εφαρμογή της ασφάλειας στην υποδομή AMI. Η πλειοψηφία των ελέγχων ασφαλείας που παρουσιάζονται σε αυτό το πρότυπο έχουν υιοθετηθεί από το DHS Catalog.[67]

Το *Privacy and Security of the Advanced Metering Infrastructure* είναι ένας ολλανδικός οδηγός που παρουσιάζει τις απαιτήσεις ασφαλείας και προστασίας προσωπικών δεδομένων στην υποδομή AMI που βασίζονται στο πρότυπο ISO 27001.[68]

Το *AMI System Security Requirements* παρέχει στην βιομηχανία των ηλεκτρικών επιχειρήσεων και τους προμηθευτές ένα ευρύ σύνολο λεπτομερών τεχνικών ή οργανωτικών απαιτήσεων ασφαλείας για την υποδομή AMI, με σκοπό τη χρήση τους στη διαδικασία της προμήθειας. Ένα μεγάλο πλήθος απαιτήσεων (σχεδόν πεντακόσιες) μπορούν να χωριστούν σε τρείς κατηγορίες: 1) Βασικές υπηρεσίες ασφαλείας, 2) Υποστήριξη υπηρεσιών ασφαλείας και 3) Ασφαλιστικές υπηρεσίες.[69]

Η σειρά προτύπων *IEC 62056* είναι αφιερωμένη στην ανταλλαγή δεδομένων των ηλεκτρικών μετρητών που αφορούν την ανάγνωση, την τιμολόγηση και τον έλεγχο του φορτίου. Τα πρότυπα αυτά καθορίζουν διαφορετικές πτυχές της επικοινωνίας συμπεριλαμβανομένων των υπηρεσιών φυσικού επιπέδου, των επιπέδων μεταφοράς και εφαρμογής, της αναγνώρισης αντικειμένων και των διεπαφών. Το IEC 62056-5-3 διευθετεί θέματα ασφαλείας πληροφοριών για το πρωτόκολλο DLMS/COSEM (Device Language Message Specification/ Companion Specification for Energy Metering) που ειδικεύεται στην έξυπνη μέτρηση, έλεγχο και διαχείριση της ενέργειας.[70]

Στον Πίνακα 14 αναφέρονται συνοπτικά τα πρότυπα και το πεδίο εφαρμογής τους που προσδιορίστηκαν παραπάνω καθώς και ο τύπος, το εύρος αλλά και η χρονολογία δημοσίευσής τους.

Πίνακας 14 - Πρότυπα ΣΗΕ ή SG που σχετίζονται με την κυβερνοασφάλεια και εφαρμόζονται στην υποδομή AMI [51]

	Πρότυπο	**Πεδίο Εφαρμογής**	**Τύπος**	**Εύρος**	**Έτος**
1.	Security Profile for AMI	Κυβερνοασφάλεια	Γενικό	ΗΠΑ	2010
2.	Privacy and Security of AMI	Απαιτήσεις ασφαλείας και προστασίας προσωπικών δεδομένων	Γενικό	Ολλανδία	2010
3.	AMI System Security Requirements	Απαιτήσεις ασφαλείας για τον τομέα της προμήθειας	Τεχνικό	ΗΠΑ	2008
4.	IEC 62056-5-3	Ασφάλεια ανταλλαγής δεδομένων AMI	Τεχνικό	Παγκόσμιο	2016

3.5.6 Πρότυπα που εφαρμόζονται σε επιλεγμένες συνιστώσες του Smart Grid

Το πρότυπο *VGB-S-175* αφορά την ασφάλεια τεχνολογιών πληροφορίας για σταθμούς παραγωγής ηλεκτρικής ενέργειας και ειδικά για συστήματα μέτρησης, παρακολούθησης και ελέγχου (I&C). Αναγνωρίζει τις σχετικές απειλές και τις πηγές σφαλμάτων για τη λειτουργία των σταθμών παραγωγής και ορίζει τις τεχνικές και οργανωτικές απαιτήσεις για τη μείωση αυτών των απειλών σε αποδοτικό επίπεδο.[71]

Η σειρά προτύπων *IEC 61400-25* καθορίζει ενιαίο μοντέλο πληροφοριών και πρωτοκόλλων επικοινωνίας μεταξύ αιολικών σταθμών και βιομηχανικών συστημάτων ελέγχου. Το *IEC 61400-25-3* περιγράφει επιλεγμένες πτυχές της ασφάλειας.[72]

Η σειρά προτύπων *IEEE 2030* είναι αφιερωμένη στη συνολική διαλειτουργικότητα του SG. Καθορίζει το μοντέλο αναφοράς της διαλειτουργικότητας του έξυπνου δικτύου (SGIRM) και παρέχει σχετικές οδηγίες. Η κυβερνοασφάλεια αποτελεί ένα σημαντικό μέρος αυτής της σειράς. Περιγράφει τεχνικές ασφάλειας και προστασίας προσωπικών δεδομένων, τις βασικές αρχές της ασφάλειας, τη διαδικασία της ασφάλειας, το σχεδιασμό ασφαλών συστημάτων, τη διαχείριση κινδύνων ή κατηγοριοποίηση της ασφάλειας. Ένα τμήμα του προτύπου *IEEE 2030.2* είναι αφιερωμένο στο θέμα της ασφάλειας και προστασίας δεδομένων σε συστήματα αποθήκευσης ενέργειας. Ένα τμήμα του προτύπου *IEEE 2030.3* είναι αφιερωμένο στην ασφάλεια και την προστασία δεδομένων στο επίπεδο εφαρμογής του δικτύου επικοινωνίας.[73]

Το *ISO 15118* είναι ένα διεθνές πρότυπο που αποτελείται από τρία μέρη και καθορίζει τη διεπαφή επικοινωνίας μεταξύ μεταξύ ηλεκτρικών οχημάτων και υποδομών φόρτισης. Το δεύτερο μέρος καθορίζει απαιτήσεις πρωτοκόλλων δικτύου και εφαρμογής, συμπεριλαμβανομένης και της ασφάλειας.[74]

Η σειρά προτύπων *ISO/IEC 14543* αποτελείται από 20 πρότυπα που περιγράφουν διαφορετικά δομικά στοιχεία οικιακών συστημάτων ελέγχου συμπεριλαμβανομένης της επικοινωνίας και της διαλειτουργικότητας. Πιο συγκεκριμένα στο *ISO/IEC 14543-5-1* και ISO/IEC *14543-5-7* εξετάζονται πτυχές της ασφάλειας, όπου περιγράφονται και μηχανισμοί ασφαλείας για πρωτόκολλα IGRS.[75],[76]

Στον Πίνακα 15 αναφέρονται συνοπτικά τα πρότυπα και το πεδίο εφαρμογής τους που προσδιορίστηκαν παραπάνω καθώς και ο τύπος, το εύρος αλλά και η χρονολογία δημοσίευσής τους.

Πίνακας 15 - Πρότυπα ΣΗΕ ή SG που σχετίζονται με την κυβερνοασφάλεια και εφαρμόζονται σε επιλεγμένες συνιστώσες του SG [51]

	Πρότυπο	**Πεδίο Εφαρμογής**	**Εφαρμογογή**	**Τύπος**	**Εύρος**	**Έτος**
1.	VGB-S-175	Απαιτήσεις κυβερνοασφάλειας για σταθμούς παραγωγής	Σταθμοί παραγωγής	Τεχνικό	Γερμανία	2014
2.	IEC 61400-25	Επικοινωνία αιολικών σταθμών-IACS	Αιολικοί σταθμοί παραγωγής	Τεχνικό	Παγκόσμιο	2015
3.	IEEE 2030	Διαλειτουργικότητα συστημάτων αποθήκευσης ενέργειας	Αποθήκευση	Τεχνικό	Παγκόσμιο	2015
4.	ISO 15118	Επικοινωνία οχήματος-δικτύου	PEV και σχετικές υποδομές	Τεχνικό	Παγκόσμιο	2014
5.	ISO/IEC 14543	Ασφάλεια οικιακών ηλεκτρονικών συστημάτων	Ασφάλεια οικιακών ηλεκτρονικών συστημάτων	Τεχνικό	Παγκόσμιο	2010 2015

3.5.7 Πρότυπα και οδηγοί γενικής εφαρμογής που μπορούν να υιοθετηθούν από το Smart Grid

Η σειρά προτύπων *ISO/IEC 27000* περιλαμβάνει πρότυπα ασφάλειας πληροφοριών που παρουσιάζουν καλές πρακτικές και συστάσεις σχετικά με τη διαχείριση ασφάλειας πληροφοριών, κινδύνων και ελέγχων. Αυτά τα πρότυπα περιστρέφονται γύρω από τη δημιουργία και τη λειτουργία του συστήματος διαχείρισης ασφάλειας πληροφοριών (ISMS), το οποίο σχετίζεται με το σχεδιασμό συστημάτων διαχείρισης για τη διασφάλιση της ποιότητας και την προστασία του περιβάλλοντος. Ο επαναλαμβανόμενος κυκλικός χαρακτήρας ανταποκρίνεται στη δυναμική φύση της ασφάλειας πληροφοριών περιβάλλοντος όπου οι απειλές, οι ευπάθειες ή οι επιπτώσεις ανεπιθύμητων συμβάντων στην ασφάλεια πληροφοριών αλλάζουν με την πάροδο του χρόνου. Ένα μεγάλος αριθμός αυτών των προτύπων έχει δημοσιευθεί, ενώ κάποια βρίσκονται ακόμα σε στάδιο έρευνας.[77]

Το πρότυπο *ISO/IEC 27001*, που είναι η πρώτη δημοσίευση της σειράς *ISO/IEC 27000,* αποτελεί το πιο θεμελιώδες διεθνές πρότυπο για τη διαχείριση της ασφάλειας των πληροφοριών και εφαρμόζεται ευρέως από οργανισμούς (εμπορικούς, κυβερνητικούς, μη κερδοσκοπικούς και άλλους) διαφόρων χαρακτηριστικών και μεγέθους. Το πεδίο εφαρμογής του είναι γενικό και δεν απευθύνεται προς κάποιο συγκεκριμένο τομέα ή τεχνολογία. Καθορίζει τις απαιτήσεις για τη δημιουργία, τη λειτουργία, την εφαρμογή, την παρακολούθηση, τη συντήρηση και τη βελτίωση του ISMS εντός των πλαισίων των οργανισμών. Το *ISO/IEC 27002* παρέχει βοηθητικές και πρακτικές οδηγίες σχετικά με την υλοποίηση του *ISO/IEC 27001*.[78],[79]

Το πρότυπο *NIST SP 800-53* είναι ένα θεμελιώδες έγγραφο του NIST που είναι αφιερωμένο στη διαχείριση της ασφάλειας των πληροφοριών. Καθοδηγεί την διαδικασία επιλογής και προσδιορισμού των ελέγχων ασφαλείας για τα συστήματα πληροφοριών των ομοσπονδιακών οργανισμών. Οι οδηγίες εφαρμόζονται σε όλες τις συνιστώσες των συστημάτων πληροφοριών που είναι υπεύθυνα για τη διαδικασία της αποθήκευσης, ή της μετάδοση πληροφοριών. Το *NIST SP 800-53* ορίζει τρία είδη συστημάτων πληροφοριών ανάλογα με την επίδραση που έχουν στην εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των πληροφοριών: συστήματα μικρής, μέτριας και υψηλής επίδρασης. Για κάθε τύπο συστήματος ορίζεται ένα επίπεδο ελάχιστης ασφάλειας. Τα επίπεδα ελέγχου είναι ιεραρχικά δομημένα ανάλογα με τους ελέγχους ασφαλείας που εφαρμόζονται σε κάθε επίπεδο. Οι έλεγχοι ασφαλείας που ορίζονται από το *NIST SP 800-53* ομαδοποιούνται σε 17 κατηγορίες που καλύπτουν όλους τους τομείς της διαχείρισης της ασφάλειας των πληροφοριών (τεχνολογική, λειτουργική και άλλες). Επίσης, αυτό το πρότυπο αναφέρεται σε πτυχές της ασφάλειας, καθορίζοντας τις ελάχιστες απαιτήσεις που μπορούν να ικανοποιηθούν από διάφορους οργανισμούς και να είναι επαρκείς για τη διασφάλιση ενός καλού επιπέδου ασφαλείας. Αρχικά ειδικευόταν

για τους ομοσπονδιακούς οργανισμούς των ΗΠΑ, αλλά λόγω μεγάλου διεθνούς ενδιαφέροντος υιοθετήθηκε και εφαρμόστηκε παγκοσμίως από οργανισμούς και επιχειρήσεις. Επιπλέον είναι πλήρως συμβατό με το *ISO/IEC 27001* και τη σχετική σειρά προτύπων *ISO/IEC 27000.*[80]

Το *GB/T 22239* είναι ένα κινέζικο πρότυπο γενικού σκοπού που ειδικεύεται σε οποιουδήποτε τύπου συστήματα πληροφοριών, το οποίο δημοσιεύθηκε το 2008. Καθορίζει τις απαιτήσεις ασφαλείας για συστήματα πληροφοριών σε πέντε επίπεδα προστασίας της ασφάλειας, και πιο συγκεκριμένα εντοπίζει το βαθμό στον οποίο μπορεί ένα σύστημα να αμυνθεί απέναντι σε μία απειλή, να εντοπίσει ένα συμβάν ασφαλείας και να το επαναφέρει στην προηγούμενη κατάσταση σε περίπτωση όπου το σύστημα έχει υποστεί κάποια βλάβη. Οι απαιτήσεις διακρίνονται σε τεχνικές και διαχειριστικές.[81]

Το πρότυπο *ISO/IEC 27005* είναι μια δημοφιλής δημοσίευση της σειράς ISO/IEC 27000. Εξηγεί τη διαδικασία διαχείρισης κινδύνου, η οποία είναι κατάλληλη για οργανισμούς που υπακούν στο πρότυπο *ISO/IEC 27001*. Ένα άλλο πρότυπο που είναι αφιερωμένο στη διαχείριση κινδύνου είναι το *NIST SP 800-39,* το οποίο εξηγεί αυτή τη διαδικασία με λεπτομερή τρόπο.[82]

Το *ISO/IEC 15408* είναι ένα σύνολο τριών προτύπων, το οποίο περιγράφει τα κριτήρια αξιολόγησης της ασφάλειας προϊόντων τεχνολογίας πληροφοριών (υλικό και λογισμικό). Αυτά τα πρότυπα αναπτύχθηκαν στα πρότυπα κριτηρίων (Common Criteria - CC), που στοχεύουν σε έλεγχο εγκυρότητας και πιστοποίησης συστηματικών, αναγνωρίσιμων προϊόντων. Είναι πλήρως αφιερωμένα στο θέμα της αξιολόγησης της ασφάλειας όσον αφορά την ασφάλεια προϊόντων.[83]

Το πρότυπο *ISO/IEC 18045* είναι ένα συνοδευτικό έγγραφο για στα κριτήρια αξιολόγησης της ασφάλειας της τεχνολογίας πληροφοριών που ορίζονται στο πρότυπο *ISO/IEC 15408.* Καθορίζει τις ελάχιστες ενέργειες που πρέπει να εκτελεστούν από έναν εκτιμητή για τη διεξαγωγή της αξιολόγησης *ISO/IEC 15408*, χρησιμοποιώντας τα κριτήρια και τα στοιχεία αξιολόγησης που ορίζονται από αυτό το πρότυπο.[84]

Το πρότυπο *GB/T 20279* είναι ένα εθνικό κινέζικο πρότυπο που παρουσιάζει τις απαιτήσεις λειτουργίας, ασφαλείας, περιβαλλοντικής προσαρμογής και τις απαιτήσεις επιδόσεων των προϊόντων διαχωρισμού του δικτύου και των τερματικών συσκευών (network and terminal separation).[85]

Το πρότυπο *ISO/IEC 19790* καθορίζει τα προαπαιτούμενα χαρακτηριστικά ασφαλείας των κρυπτογραφικών μονάδων που χρησιμοποιούνται στα συστήματα ασφαλείας για την προστασία ευαίσθητων πληροφοριών σε υπολογιστικά και πληροφοριακά συστήματα. Ορίζει τέσσερα επίπεδα ασφαλείας για τις κρυπτογραφικές μονάδες για να έχει τη δυνατότητα να καλύψει ένα ευρύ φάσμα ευαίσθητων δεδομένων και πολλά περιβάλλοντα εφαρμογών.[86]

Το πρότυπο *NIST SP 800-64* αναπτύχθηκε για να βοηθήσει ομοσπονδιακούς οργανισμούς στην ενσωμάτωση βασικών πρακτικών ασφαλείας της διαδικασίας ανάπτυξης του κύκλου ζωής συστημάτων (SDLC) των υφιστάμενων τεχνολογιών πληροφορίας. Αυτό το πρότυπο μπορεί να εφαρμοστεί σε όλα τα ομοσπονδιακά συστήματα τεχνολογίας πληροφοριών εκτός από τα εθνικά συστήματα ασφαλείας. Πιο συγκεκριμένα, ειδικεύεται στα συστήματα της ασφάλειας όσον αφορά τη διαδικασία SDLC, παρέχοντας τους ρόλους και τις ευθύνες της ασφάλειας που απαιτείται για τη διαδικασία ανάπτυξης στα περισσότερα πληροφοριακά συστήματα, καθώς και επαρκείς πληροφορίες σχετικά με τη SDLC έτσι ώστε να μπορεί κάποιος που δεν είναι εξοικειωμένος με αυτή τη διαδικασία να κατανοήσει τη σχέση μεταξύ ασφάλειας πληροφοριών και SDLC.[87]

Το πρότυπο *NIST SP 800-124* εστιάζει στην κεντρική διαχείριση και την ασφάλεια κινητών συσκευών όπως smart phones και tablets. Παρέχει συστάσεις για την επιλογή, την εφαρμογή και τη χρήση κεντρικής διαχείρισης τεχνολογιών, και εξηγεί τα ζητήματα ασφαλείας που αφορούν τη χρήση του διαδικτύου από κινητές συσκευές δίνοντας και κάποιες προτάσεις για την ασφάλεια αυτών των συσκευών καθ' όλη τη διάρκεια των κύκλων ζωής τους.[88]

Στον Πίνακα 16 αναφέρονται συνοπτικά τα πρότυπα και το πεδίο εφαρμογής τους που προσδιορίστηκαν παραπάνω καθώς και ο τύπος, το εύρος αλλά και η χρονολογία δημοσίευσής τους.

Πίνακας 16 - Πρότυπα και οδηγοί γενικής εφαρμογής που μπορούν να υιοθετηθούν από το SG [51]

	Πρότυπο	**Πεδίο Εφαρμογής**	**Τύπος**	**Εύρος**	**Έτος**
1.	ISO/IEC 27001 και 27002	Διαχείριση IS	Γενικό	Παγκόσμιο	2013
2.	NIST SP 800-53	Διαχείριση IS	Γενικό	ΗΠΑ Παγκόσμιο	2013
3.	GB/T 22239	Διαχείριση IS	Γενικό	Κίνα	2008
4.	ISO/IEC 27005	Διαχείριση κινδύνου	Γενικό	Παγκόσμιο	2011
5.	NIST SP 800-39	Διαχείριση κινδύνου	Γενικό	ΗΠΑ	2011

6.	ISO/IEC 15408 / Common Criteria	Αξιολογήση Ασφαλείας	Τεχνικό	Παγκόσμιο	2008 2012
7.	ISO/IEC 18045 / CEM	Αξιολογήση Ασφαλείας	Τεχνικό	Παγκόσμιο	2008 2012
8.	GB/T 20279	Απαιτήσεις ασφαλείας για συσκευές διαχωρισμού του δικτύου	Γενικό	Κίνα	2015
9.	ISO/IEC 19790	Απαιτήσεις ασφαλείας για κρυπτογραφικές μονάδες	Γενικό	Παγκόσμιο	2012
10.	NIST SP 800-64	Ασφάλεια της διαδικασία της ανάπτυξης συστημάτων	Τεχνικό	ΗΠΑ	2008
11.	NIST SP 800-124	Ασφάλεια κινητών συσκευών	Γενικό	ΗΠΑ	2013

3.5.8 Θέματα προσωπικών δεδομένων στα πρότυπα που αναλύθηκαν

Το πρότυπο *NISTIR 7628* αποτελείται από τρεις τόμους, εκ των οποίων ο ένας είναι αφιερωμένος στην προστασία προσωπικών δεδομένων στο SG. Το πρότυπο αυτό εισάγει τις βασικές έννοιες του απορρήτου, περιγράφει τις νομικές πτυχές της ιδιωτικότητας στο δίκτυο, υποδεικνύει ποιες ιδιωτικές πληροφορίες μπορεί να αποκαλυφθούν στο SG και περιγράφει λεπτομερώς βασικά θέματα που αφορούν την ιδιωτικότητα στο SG, όπως η μάθηση του μοτίβου προσωπικής συμπεριφοράς ή η απομακρυσμένη επιτήρηση σε πραγματικό χρόνο. Επίσης περιγράφεται ένα αναπόφευκτο πρόβλημα στο SG, όπως είναι η πρόσβαση δεδομένων ενέργειας σε τρίτους, καθώς και θέματα ιδιωτικότητας στην επικοινωνία ηλεκτρικών οχημάτων. Για την αντιμετώπιση αυτών των θεμάτων χρησιμοποιεί υφιστάμενα εργαλεία και πρότυπα προστασίας προσωπικών δεδομένων.[6]

Στο πρότυπο *NIST SP 800-53*, το οποίο δεν αναφέρεται ειδικά στο SG αλλά είναι γενικής εφαρμογής, αφιερώνεται ένα σημαντικό μέρος του στην προστασία προσωπικών δεδομένων. Ορίζει 26 ελέγχους προστασίας προσωπικών δεδομένων που βασίζονται σε διεθνή πρότυπα και βέλτιστες πρακτικές, και τους χωρίζει σε οκτώ ομάδες. Οι έλεγχοι αυτοί μπορούν να εφαρμοστούν άμεσα για την προστασία προσωπικών δεδομένων και στο SG.[80]

Το πρότυπο *IEC 62443* διευθετεί ορισμένες πτυχές ασφαλείας της προστασίας ιδιωτικών δεδομένων που σχετίζονται με τα IACS. Αναφέρει ότι οι πληροφορίες που είναι ευαίσθητες ως προς την αποκάλυψη, πρέπει να προστατεύονται σωστά τόσο για να

διατηρηθεί το ανταγωνιστικό πλεονέκτημα όσο και για την προστασία της ιδωτικότητας των εργαζομένων. Επίσης ορίζει μετρικές ασφαλείας προσωπικών δεδομένων, όπως ο αριθμός μη εξουσιοδοτημένων αποκαλύψεων πληροφοριών του προσωπικού ιδιωτικών IACS, τον αριθμό των βλαβών για την διασφάλιση της εμπιστευτικότητας και της ακεραιότητας των αρχείων του προσωπικού ή τον αριθμό παραβιάσεων πρόσβασης για την εξαπάτηση λογαριασμών ή την πλαστογράφηση εγγράφων που οδηγούν στην αποκάλυψη δεδομένων του IACS που μπορούν να χρησιμοποιηθούν για οικονομικό όφελος. Ακόμα, προσδιορίζει την απαίτηση ασφαλείας που επιβάλλεται για την προστασία δεδομένων και ιδιωτικότητας σύμφωνα με τη νομοθεσία, τους κανονισμούς ή τις συμβατικές ρήτρες. Μια παρόμοια προσέγγιση χρησιμοποιείται και στο πρότυπο *ISO/IEC TR 27019*.[62],[63]

Το πρότυπο διαλειτουργικότητας του SG, *IEEE 2030*, σε ένα κεφάλαιο παρουσιάζει συνοπτικά το πρόβλημα της ιδιωτικότητας στο SG. Εξηγεί ότι η ιδιωτικότητα αφορά του διάφορους τρόπους χρήσης (συλλογή, πρόσβαση, διανομή και άλλα) δεδομένων προσωπικού χαρακτήρα (PII) και ότι υπάρχουν διαφορετικές ερμηνείες και ορισμοί της ιδιωτικότητας. Με τις καινούριες τεχνολογίες που διαθέτει το SG, όπως έξυπνοι μετρητές ή έξυπνες οικιακές συσκευές, προκύπτουν νέοι κίνδυνοι στην προστασία προσωπικών δεδομένων που πρέπει να αντιμετωπιστούν με κατάλληλα μέτρα όπως η εκτίμηση αντικτύπου σχετικά με την προστασία προσωπικών δεδομένων (PIA).[73]

Ο ολλανδικός οδηγός *Privacy and Security of the Advanced Metering Infrastructure* όπως αναγράφεται και στον τίτλο του, καλύπτει τόσο την ασφάλεια όσο και την προστασία προσωπικων δεδομένων της υποδομής AMI. Σύμφωνα με αυτό το έγγραφο, οι έννοιες επικαλύπτονται μερικώς. Όσον αφορά το στόχο της προστασίας, η προστασία των προσωπικών δεδομένων έχει πιο περιορισμένο πεδίο εφαρμογής διότι εστιάζει σε προσωπικά δεδομένα. Από την άλλη πλευρά, οι στόχοι της προστασίας στην ιδιωτικότητα είναι ευρύτεροι από ότι στην ασφάλεια καθώς αντιμετωπίζουν τα ζητήματα της περιττής περεταίρω επεξεργασίας πληροφοριών ή παράνομης επεξεργασίας, και ικανοποιούν νομικές απαιτήσεις που αφορούν ευαίσθητα δεδομένα. Ταυτόχρονα για να είναι δυνατή η προστασία των δεδομένων πρέπει πρώτα να εξασφαλίζεται η ασφάλεια. Ουσιαστικά, ορίζει τα δεδομένα PII και ευαίσθητες πληροφορίες απορρήτου και προσδιορίζει στόχους, κινδύνους και απαιτήσεις που σχετίζονται με την προστασία της ιδιωτικότητας.[68]

Το AMI System Security Requirements περιλαμβάνει την κατηγορία 16 απαιτήσεων που αφορούν την ιδιωτικότητα και την εμπιστευτικότητα στην υποδομή AMI. Σύμφωνα με αυτό τον οδηγό, οι στόχοι ασφαλείας στο SG πρέπει να περιλαμβάνουν την πρόληψη της παραβίασης της ιδιωτικής ζωής, ενώ ζητήματα που αφορούν την ιδιωτικότητα πρέπει να περιλαμβάνονται στην εκπαίδευση των εργαζομένων των επιχειρήσεων ηλεκτρικής ενέργειας.[69]

Το πρότυπο *NIST SP 800-82* που επικεντρώνεται στα συστήματα IACS, παρέχει καθοδήγηση και συμπλήρωση ή ενίσχυση των πληροφοριών σχετικά με την εφαρμογή των ελέγχων ασφάλειας και προστασίας προσωπικών δεδομένων του *NIST SP 800-53* στα IACS. Εξηγεί δηλαδή ότι οι έλεγχοι της ιδιωτικότητας από το *NIST SP 800-53* είναι άμεσα εφαρμόσιμοι στα IACS.[64]

Το πρότυπο *ISO/IEC 15408*, που παρέχει κριτήρια για την αξιολόγηση της ασφάλειας των προϊόντων τεχνολογίας πληροφοριών, στο δεύτερο μέρος του ορίζει μια κατηγορία (η οποία χωρίζεται σε τέσσερις οικογένειες) λειτουργικών απαιτήσεων που θεωρούν την προστασία προσωπικών δεδομένων ως προστασία των χρηστών απέναντι στην αποκάλυψη ή την εσφαλμένη χρήση της ταυτότητάς τους από άλλους χρήστες.[89]

Το πρότυπο *NIST SP 800-64*, που είναι αφιερωμένο στην ασφάλεια ανάπτυξης λογισμικού, συνιστά εκτιμήσεις αντίκτυπου σχετικά με την προστασία δεδομένων που εκτελούνται κατά τη διάρκεια της διαδικασίας κατασκευής ενός νέου συστήματος. Θα πρέπει να καθοριστεί, συνήθως κατά την κατηγοριοποίηση της ασφάλειας, εάν το σύστημα θα αποθηκεύσει ή θα επεξεργαστεί δεδομένα PII, κι έπειτα να εφαρμοστούν τα κατάλληλα μέτρα που περιλαμβάνουν τον τρόπο αντιμετώπισης περιστατικών που αφορούν πληροφορίες προσωπικών δεδομένων.[87]

Το *ISO/IEC 27001* ορίζει το στόχο ασφαλείας που αφορά την εφαρμογή κατάλληλης πολιτικής, ελέγχων και διαδικασιών για την προστασία των προσωπικών δεδομένων σύμφωνα με τη σχετική νομοθεσία, τους κανονισμούς ή τις συμβατικές ρήτρες. Ο στόχος ασφαλείας περιγράφεται πιο λεπτομερώς στο *ISO/IEC 27002*.[78],[79]

Το *Security Profile for Advanced Metering Infrastructures* κάνει αναφορά για την προστασία προσωπικών δεδομένων εξηγώντας τη λογική κάποιων πρακτικών και εντολών ελέγχου του *DHS Catalog*. Σύμφωνα με αυτό το έγγραφο, οι απαιτήσεις εμπιστευτικότητας είναι απαραίτητες για τη διασφάλιση της ιδιωτικότητας των πελατών και των πληροφοριών των επιχειρήσεων ενώ παραθέτει τις πολιτικές διαχείρισης που μπορούν να βοηθήσουν στην αποφυγή των παραβιάσεων των νόμων περί προστασίας προσωπικών δεδομένων.[67]

Στον Πίνακα 17 αναφέρονται τα πρότυπα που αφορούν θέματα προσωπικών δεδομένων καθώς και ο βαθμός σχετικότητάς τους με τον τομέα αυτό.

Πίνακας 17 - Πρότυπα που διευθετούν θέματα προσωπικών δεδομένων [51]

	Πρότυπο	**Σχετικότητα**
1.	NISTIR 7628	Υψηλή
2.	NIST SP 800-53	Υψηλή
3.	IEC 62443	Μέτρια
4.	ISO/IEC 27019	Μέτρια
5.	IEEE 2030	Μέτρια
6.	Privacy and Security of AMI	Μέτρια
7.	AMI System Security Requirements	Μέτρια
8.	NIST SP 800-82	Μέτρια
9.	ISO/IEC 15408	Μέτρια
10.	NIST SP 800-64	Μέτρια
11.	ISO/IEC 27001 και 27002	Χαμηλή
12.	Security Profile for AMI	Χαμηλή

3.6 Αντίμετρα

3.6.1 Ασφάλεια επικοινωνίας

Οι εφαρμογές της ηλεκτρικής ενέργειας απαιτούν ασφαλή υποδομή επικοινωνιών για τη διαχείριση της γεωγραφικής διασποράς των πηγών του δικτύου. Για τη μετάδοση δεδομένων συχνά χρησιμοποιείται ασύρματη επικοινωνία και μισθωμένες γραμμές που παρέχουν αυξημένη έκθεση και εισάγουν επιπλέον κινδύνους. Το δίκτυο εξαρτάται επίσης σε μεγάλο βαθμό από μία σειρά πρωτοκόλλων συστήματος ελέγχου υψηλού επιπέδου που συμπεριλαμβάνουν το Modbus, DNP3, IEC 61850, και ICCP. Αυτά τα πρωτόκολλα δεν αναπτύχθηκαν για να είναι ανθεκτικά στις επιθέσεις και δεν διαθέτουν επαρκή μηχανισμό ασφαλείας. Η κρυπτογράφηση, η αυθεντικοποίηση και ο έλεγχος πρόσβασης μπορούν να προστεθούν στις υφιστάμενες επικοινωνίας για την παροχή αυξημένης ασφάλειας.

1) Κρυπτογράφηση

Η αναβάθμιση των πρωτοκόλλων επικοινωνίας για την παροχή ασφάλειας είναι απαραίτητη για τη συνέχιση της χρήσης τους σε μη αξιόπιστους χώρους. Αυτό το επίπεδο ασφαλείας μπορεί να επιτευχθεί με την ανάπτυξη κρυπτογραφημένων εικονικών ιδιωτικών δικτύων (VPN) που προστατεύουν την κίνηση του δικτύου μέσω ενθυλάκωσης σε ένα κρυπτογραφικό πρωτόκολλο. Δυστυχώς, αυτή λύση δεν είναι πάντα εφικτή καθώς η βιομηχανία εξαρτάται σε μεγάλο βαθμό από δίκτυα που δεν ανήκουν σε IP δίκτυα. Επιπροσθέτως, οι αυστηρές απαιτήσεις διαθεσιμότητας ενδέχεται να μη μπορούν να χειριστούν τον πρόσθετο χρόνο απόκρισης του δικτύου (latency) που δημιουργείται από ένα VPN.

Η έρευνα για την κρυπτογράφηση συσκευών επικοινωνίας bump-in-the-wire (BITW) προσπαθεί να εξασφαλίσει ότι τα μηνύματα μπορούν να είναι κατάλληλα κρυπτογραφημένα και επικυρωμένα κατά τον περιορισμό του χρόνου απόκρισης που επιχειρείται. Μία τέτοια μέθοδος κρυπτογράφησης BITW μπορεί να μειώσει σημαντικά το χρόνο απόκρισης με τη μείωση της παραμονής του μηνύματος κατά τη διάρκεια της κρυπτογράφησης και της αυθεντικοποίησης. Πρόσθετη έρευνα έχει επικεντρωθεί στην αναβάθμιση παλαιών πρωτοκόλλων με κατάλληλες ιδιότητες ασφαλείας. Πολυάριθμες προσπάθειες έχουν επικεντρωθεί στην τροποποίηση των παραδοσιακών πρωτοκόλλων SCADA όπως ICCP, DNP3, και Modbus για την πρόσθετη παροχή ασφάλειας διατηρώντας παράλληλα την ενοποίηση με τα υφιστάμενα συστήματα. Οι δραστηριότητες ανάπτυξης και διαχείρισης κλειδιών εξακολουθούν να δημιουργούν δυσκολίες σε γεωγραφικά διεσπαρμένα περιβάλλοντα.

2) Αυθεντικοποίηση

Η ασφαλής απομακρυσμένη αυθεντικοποίηση παρουσιάζει μία πρόκληση που οφείλεται στις ικανότητες εκτενής ανάπτυξης και διαχείρισης περιορισμένων αλλαγών. Η έκθεση πιστοποιητικών αυθεντικοποιήσης (για παράδειγμα κλειδιά και κωδικοί) αυξάνεται καθ’ όλη τη διάρκεια ζωή τους και τα πρωτόκολλα γίνονται όλο και περισσότερο επιρρεπή σε επιθέσεις λόγω συνεχών αναθεωρήσεων της ασφάλειας και την εξέλιξη της κρυπτανάλυσης. Η ανάπτυξη ισχυρών, προσαρμοστικών και ικανοποιητικά διαθέσιμων μηχανισμών αυθεντικοποίησης αποτελεί επιτακτική ανάγκη για την αποτροπή μη εξουσιοδοτημένης πρόσβασης.

Σε ορισμένες έρευνες έχουν οριστεί αρχές σχεδιασμού που απαιτούνται για τα πρωτόκολλα αυθεντικοποίησης μέσα στο δίκτυο. Καθορίζοντας τις αρχές αυθεντικοποίησης, οι σχεδιαστές μελλοντικών συστημάτων μπορούν να εξασφαλίσουν ότι τα συστήματά τους θα πετύχουν την αποδοτικότητα και την προσαρμοστικότητα που απαιτείται για τη διαρκή ασφαλή χρήση. Επιπλέον, έρευνες για πιο ευέλικτα πρωτόκολλα αυθεντικοποίησης έχουν προταθεί για την παροχή προσαρμοστικότητας. Ένα από τα προτεινόμενα πρωτόκολλα παρέχει αλγόριθμους ανανέωσης κλειδιών (re-keying) και αναδιαμόρφωσης για προστασία απέναντι σε παραβιασμένα κλειδιά και μελλοντικές ευπάθειες των δομικών στοιχείων της αυθεντικοποίησης.

3) Έλεγχος πρόσβασης

Ενώ η κρυπτογράφηση και η αυθεντικοποίηση μπορούν να αποτρέψουν τους εξωτερικούς επιτιθέμενους, συμβάλλουν ελάχιστα στην προστασία εσωτερικών απειλών ή επιτιθέμενων που έχουν αποκτήσει ήδη κάποια εσωτερική πρόσβαση. Επιτιθέμενοι με πρόσβαση σε ένα δίκτυο επικοινωνίας μπορούν να χρησιμοποιήσουν την λειτουργικότητα διάφορων πρωτοκόλλων για την εισαγωγή κακόβουλων εντολών στις λειτουργίες ελέγχου. Η πιθανότητα μίας επιτυχημένης επίθεσης θα μπορούσε να μειωθεί σημαντικά

με τη σωστή διαμόρφωση του λογισμικού και τη χρήση πρωτοκόλλων για την απενεργοποίηση περιττής λειτουργικότητας.

Η αξιολόγηση πρωτοκόλλων βιομηχανίας για την αναγνώριση πιθανών κακόβουλων λειτουργιών αποτελεί επιτακτική ανάγκη για τη διασφάλιση των παραμέτρων του συστήματος. Μία ανάλυση του πρωτόκολλο DNP3 αναφέρει λεπτομερώς τους κωδικούς λειτουργίας και τα αντικείμενα δεδομένων που θα μπορούσαν να φανούν χρήσιμα στους επιτιθέμενους για την πρόσβαση δεδομένων, ελέγχου, ή για τον επηρεασμό της διαθεσιμότητας ενός απομακρυσμένου κέντρου ελέγχου που χρησιμοποιεί το DNP3. Από αυτή την ανάλυση προκύπτει μία βάση για την κατανόηση πιθανών φυσικών επιπτώσεων από ένα παραβιασμένο κανάλι επικοινωνίας. Πρόσθετη έρευνα σε αυτό τον τομέα μοντελοποιεί εφικτές επιθέσεις σε συστήματα ελέγχου που βασίζονται στις υφιστάμενες προδιαγραφές του πρωτοκόλλου. Πιο εξελιγμένα πρωτόκολλα που μπορούν να χρησιμοποιηθούν στο SG, όπως το ANSI C.12.22 και το IEC 61850, απαιτούν πρόσθετη ανάλυση για την ασφαλή εφαρμογή τους σε νέα συστήματα.[90]

3.6.2 Ασφάλεια Δικτύου

Α) Ανίχνευση επίθεσης για ενεργειακά δίκτυα

Λόγω της φύσης κυβερνοφυσικού συστήματος του SG και του μεγάλου αντίκτυπου των ενεργειακών συστημάτων, ο πρωταρχικός στόχος της ασφάλειας για τη λειτουργία του SG είναι η διαθεσιμότητα. Οι επιθέσεις DoS που έχουν άμεσο αντίκτυπο στη διαθεσιμότητα των συστημάτων επικοινωνίας και συστημάτων ελέγχου, χαρακτηρίζονται ως οι κύριες απειλές της ασφάλειας του δικτύου στο SG. Η ανίχνευση και η άμυνα απέναντι στις DoS επιθέσεις εξαρτώνται κυρίως από τα μέτρα ασφαλείας του δικτύου όπως κίνηση, παρακολούθηση και το φιλτράρισμα του δικτύου. Επομένως, καθίσταται απαραίτητη η παροχή αποτελεσματικών προσεγγίσεων του δικτύου απέναντι σε επιθέσεις DoS. [5]

Λόγω της αλληλεπίδρασης των δικτύων πληροφοριών και των ηλεκτρικών συσκευών στα ενεργειακά συστήματα, το SG πρέπει να μπορεί να ανιχνεύει και να εξουδετερώνει τις επιθέσεις DoS που μπορούν να εκτελεστούν οπουδήποτε στα δίκτυα επικοινωνιών. Η ανίχνευση της επίθεσης είναι το πρώτο βήμα για την παροχή αντιμέτρων κατά των επιθέσεων αυτών. Η ανίχνευση των υφιστάμενων επιθέσεων DoS μπορεί να κατηγοριοποιηθεί σε μερικά σχήματα όπως:

- **Ανίχνευση βάσει σημάτων**: Στο φυσικό επίπεδο ή επίπεδο MAC, ένας ανιχνευτής επίθεσης DoS μπορεί να μετρήσει την ισχύ της πληροφορίας του ληφθέντος σήματος (received signal strength information - RSSI) για την ανίχνευση της παρουσίας μίας

επίθεσης (για παράδειγμα wireless jamming): εάν το RSSI πολλών πακέτων είναι μεγαλύτερο από το όριο (που σημαίνει ότι δέκτης πρέπει να τα λάβει σωστά) αλλά ο αποκωδικοποιητής πακέτων δείξει σφάλματα, ο ανιχνευτής επίθεσης μπορεί σημάνει κίνδυνο για την παρουσία ενός επιτιθέμενου.

- **Ανίχνευση βάσει πακέτων:** Οι λύσεις που εμπίπτουν σε αυτή την κατηγορία μπορούν να εφαρμοστούν σε κάθε επίπεδο για τη μέτρηση του αποτελέσματος μετάδοσης κάθε πακέτου και την ανακάλυψη πιθανών επιθέσεων προσδιορίζοντας μία σημαντική αύξηση αποτυχιών των πακέτων μετάδοσης. Είναι ένα γενικό και αποτελεσματικό σχήμα ανίχνευσης δεδομένου του ότι οι επιθέσεις DoS μπορούν να οδηγήσουν σε υποβάθμιση της απόδοσης του δικτύου όσον αφορά την απώλεια ή την καθυστέρηση πακέτων.
- **Προληπτική μέθοδος:** Η βασική ιδέα είναι ο σχεδιασμός αλγορίθμων που προσπαθούν να προσδιορίσουν τις επιθέσεις DoS σε αρχικό στάδιο στέλνοντας προληπτικά πακέτα ανίχνευσης (probing packets) για τη δοκιμή ή τη μέτρηση της κατάστασης των πιθανών επιτιθέμενων.
- **Υβριδική μέθοδος:** Είναι επίσης πιθανός ο σχεδιασμός ενός σχήματος που συνδυάζει διαφορετικές ιδέες για τη βελτίωση της ακρίβειας της ανίχνευσης επιθέσεων. Για παράδειγμα ο συνδυασμός ανίχνευσης βάσει πακέτων και βάσει σημάτων για τον αποτελεσματικό εντοπισμό επιθέσεων εμπλοκής σε ασύρματα δίκτυα.

Οι περισσότεροι μέθοδοι ανίχνευσης επιθέσεων DoS ανήκουν σε παθητική ανίχνευση που παρακολουθεί την κατάσταση του δικτύου, όπως το φορτίο κίνησης (traffic load) και η αναλογία μετάδοσης πακέτων, και σημάνουν μία προειδοποίηση επίθεσης μόλις υπάρξει μία εμφανής αναντιστοιχία μεταξύ νέων δειγμάτων και ιστορικών δεδομένων. Έτσι, η υφιστάμενη μεθοδολογία για ανίχνευση επίθεσης DoS μπορεί να εφαρμοστεί άμεσα σε δίκτυα επικοινωνιών στο SG. Για παράδειγμα, οι ανιχνευτές βάσει σημάτων μπορούν εύκολα να χρησιμοποιηθούν στις ασύρματες εφαρμογές του SG και οι μέθοδοι ανίχνευσης βάσει πακέτων είναι κατάλληλες για ανίχνευση επιθέσεων DoS στα δίκτυα AMI και στους υποσταθμούς. Οι προληπτικές μέθοδοι ενδέχεται να είναι περιορισμένες σε μη-χρονικά κρίσιμα δίκτυα δεδομένου του ότι αναπόφευκτα προσθέτουν επιπλέον φόρτο στην επικοινωνία (overhead) με τη μετάδοση πακέτων ανίχνευσης.[18]

Β) Εφαρμογές μηχανισμών μετριασμού επιθέσεων στα ενεργειακά δίκτυα

Μαζί με τα σχήματα ανίχνευσης για DoS επιθέσεις, μπορούν να εφαρμοστούν μηχανισμοί μετριασμού επιθέσεων για την προστασία των κόμβων του δικτύου από τέτοιες επιθέσεις. Τα σχήματα μετριασμού των επιθέσεων DoS περιλαμβάνουν δύο προσεγγίσεις: 1) μετριασμός DoS επιθέσεων επιπέδου δικτύου (network layer) με σκοπό την εξάντληση των πόρων του στόχου και 2) μετριασμός επιθέσεων εμπλοκής φυσικού επιπέδου (physical layer) με σκοπό τη διατάραξη των ασύρματων επικοινωνιών.[18]

1) Μετριασμός επιπέδου δικτύου

Οι πιο ευρέως χρησιμοποιημένες προσεγγίσεις για το μετριασμό των επιθέσεων DoS έχουν σχεδιαστεί για το επίπεδο δικτύου και οι πιο πολλές από αυτές έχουν αποδειχθεί αποτελεσματικές για το διαδίκτυο, όπως για παράδειγμα οι ακόλουθοι μηχανισμοί:

- **Rate-limiting:** Η βασική ιδέα του των μηχανισμών rate-limiting είναι η επιβολή ενός ορίου ποσοστού σε ένα σύνολο πακέτων που έχουν χαρακτηριστεί ως πιθανώς κακόβουλα από το μηχανισμό ανίχνευσης. Συνήθως εφαρμόζεται όταν ο μηχανισμός ανίχνευσης έχει ψευδώς θετικά αποτελέσματα (false positives) ή δεν μπορεί να χαρακτηρίσει ακριβώς τη ροή της επίθεσης.
- **Filtering:** Με την υποστήριξη μεθόδων ανίχνευσης επιθέσεων, οι μηχανισμοί filtering μπορούν να συγκρίνουν την πηγή των διευθύνσεων των πακέτων με τη μαύρη λίστα που παρέχεται από τους ανιχνευτές επιθέσεων για το φιλτράρισμα όλων των ύποπτων ροών. Έτσι, αποφεύγεται η περαιτέρω προώθηση ή δρομολόγηση πακέτων στα θύματα.
- **Reconfiguration:** Προκειμένου να μετριαστεί ή επίδραση DoS επιθέσεων, μία λύση είναι η αναδιαμόρφωση της αρχιτεκτονικής του δικτύου, όπως η αλλαγή της τοπολογίας του θύματος ή του μεσάζοντος δικτύου με είτε την πρόσθεση περισσότερων πηγών στο θύμα είτε την απομόνωση των συσκευών επίθεσης.[91]

Σε σύγκριση με το διαδίκτυο που επιτρέπει αυθαίρετα τις ροές end-to-end επικοινωνίας, το SG διαθέτει χαρακτηριστικά δύο κύριων προβλέψιμων κατευθυντήριων ροών πληροφοριών: bottom-up και top-down. Αυτό στην πραγματικότητα καθιστά εύκολη για τα λογισμικά της πύλης και του δρομολογητή την εκτέλεση rate-limiting και filtering μηχανισμών για την παρεμπόδιση ανεπιθύμητων ή ύποπτων κυκλοφοριακών ροών. Γνωρίζοντας τις τυπικές συχνότητες μετάδοσης δεδομένων και τις κατευθύνσεις των πληροφοριών είναι εύκολο για τους διαχειριστές του δικτύου να προκαθορίσουν τις rate-limiting και filtering πολιτικές για τις ροές επικοινωνίας των ενεργειακών εφαρμογών για την προστασία ενάντια στις DoS επιθέσεις στο SG. Ωστόσο, η χρήση των μηχανισμών reconfiguration ενδεχομένως να μην είναι εύκολη, δεδομένου του ότι τμήματα του δικτύου του SG είναι στατικά λόγω καθορισμένης τοπολογίας των εξοπλισμών μετάδοσης και διανομής ηλεκτρικής ενέργειας.[18]

2) Μετριασμός φυσικού επιπέδου

Καθώς τα σύρματα δίκτυα χρησιμοποιούνται σε τοπικά συστήματα στο SG, το wireless jamming γίνεται η κύρια επίθεση DoS σε ασύρματα δίκτυα ενεργειακών δικτύων, ειδικά σε μερικά σενάρια που αφορούν συστήματα διανομής και μετάδοσης. Έτσι, η

ασύρματη επικοινωνία που είναι ανθεκτική σε επιθέσεις εμπλοκής, είναι πολύ σημαντική για τις εφαρμογές του SG ώστε να αντιμετωπίζουν αυτές τις επιθέσεις και να διατηρούν τη συνέχιση της μετάδοσης των πληροφοριών. Έχει σημειωθεί μεγάλη πρόοδος στην ανάπτυξη σχημάτων ασύρματων δικτύων που είναι ανθεκτικά σε επιθέσεις εμπλοκής. Τέτοια σχήματα μπορούν να σχεδιαστούν είτε συντονισμένα είτε ασυντόνιστα.

- Τα συντονισμένα πρωτόκολλα είναι συμβατικά ενάντια σε επιθέσεις εμπλοκής της μετάδοσης σχήματα που έχουν ήδη διερευνηθεί στον τομέα των ασύρματων επικοινωνιών. Μπορούν να κατηγοριοποιηθούν ως διασπορά φάσματος με άμεση ακολουθία (DSSS), διασπορά φάσματος με εναλλαγή συχνοτήτων (FHSS) και διασπορά φάσματος με ολίσθηση συχνότητας (CSS). Ωστόσο, το ζήτημα που σχετίζεται με τα συντονισμένα πρωτόκολλα είναι ότι το μυστικό, όπως η απευθείας ακολουθία στο DSSS και το μοτίβο εναλλαγής στο CSS, θεωρείται εμπιστευτικό στους άλλους (για παράδειγμα στου επιτιθέμενους). Μια τέτοια υπόθεση δεν ισχύει για πρότυπα ανοικτής επικοινωνίας, όπως το WiFi και τα κυψελωτά δίκτυα. Έτσι, τα συντονισμένα πρωτόκολλα είναι ευάλωτα σε σκόπιμες επιθέσεις με γνώσεις των πληροφοριών του πρωτοκόλλου.
- Τα ασυντόνιστα πρωτόκολλα έχουν προοπτικές για τη διασφάλιση των ασύρματων επικοινωνιών σε κατανεμημένα περιβάλλοντα. Τα ασυντόνιστα πρωτόκολλα δε χρειάζονται τον πομπό και το δέκτη να μοιράζονται ένα εκ των προτέρων γνωστό μυστικό μεταξύ τους. Δημιουργούν τυχαία ένα μυστικό (για παράδειγμα το μοτίβο εναλλαγής στο FHSS) για κάθε μετάδοση και αποτρέπουν τις επιθέσεις από την απόκτηση επαρκών γνώσεων για τη διατάραξη της επικοινωνίας. Το συμβατικό FHSS και DSSS, έχουν απροσδιόριστα ισοδύναμα UFHSS και UDSSS αντίστοιχα.

Τόσο τα συντονισμένα όσο και τα ασυντόνιστα πρωτόκολλα μπορούν να χρησιμοποιηθούν στο SG για την επίτευξη ανθεκτικών ασύρματων επικοινωνιών ενάντια στις επιθέσεις εμπλοκής. Σε σύγκριση με τα συντονισμένα πρωτόκολλα, τα ασυντόνιστα πρωτόκολλα είναι πιο ασφαλή και πιο ανθεκτικά σε σκόπιμες επιθέσεις, καθώς δε μοιράζονται ένα εκ των προτέρων γνωστό μυστικό μεταξύ πομπού και δέκτη. Ωστόσο, το κόστος των ασυντόνιστων πρωτοκόλλων από την άλλη πλευρά , είναι η καθυστερημένη εκτέλεση δεδομένου του ότι χρειάζεται να διαπραγματευτούν ένα μυστικό πριν ξεκινήσουν την επικοινωνία δεδομένων. Αυτά τα σχήματα καθώς και άλλα υφιστάμενα σχήματα όπως το DEEJAM και Timing-channel (TC), μπορούν εύκολα να εφαρμοστούν σε ασύρματα δίκτυα AMI και οικιακά δίκτυα όπου η κίνηση της επικοινωνίας είναι μη-χρονικά κρίσιμη. Παρ’ όλα αυτά, εξακολουθεί να είναι ασαφές εάν μπορούν να χρησιμοποιηθούν αποτελεσματικά σε συστήματα διανομής και μεταφοράς, όπου η εκτέλεση της επικοινωνίας σε επίπεδο χιλιοστών του δευτερολέπτου είναι απαραίτητη.[18]

3.6.3 Κρυπτογράφηση για ασφάλεια δεδομένων

Οι μηχανισμοί κρυπτογράφησης αποσκοπούν στη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της μη-αποποίησης των δεδομένων. Υπάρχουν δύο τύποι κρυπτογράφησης: η συμμετρική και η ασύμμετρη. Οι πιο χρησιμοποιημένοι αλγόριθμοι στη συμμετρική κρυπτογράφηση είναι το πρότυπο κρυπτογράφησης δεδομένων (DES) και το προηγμένο πρότυπο κρυπτογράφηση (AES). Από την άλλη πλευρά, η ασύμμετρη κρυπτογράφηση, χρησιμοποιεί δύο κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση δεδομένων: ένα ιδιωτικό κλειδί (private key) και ένα δημόσιο κλειδί (public key). Ο RAS (Rivest–Shamir–Adleman) είναι κρυπταλγόριθμος ασύμμετρου κλειδιού. Στο SG, συνυπάρχουν διαφορετικά στοιχεία με διαφορετικές υπολογιστικές δυνατότητες. Ως εκ τούτου, μπορούν να χρησιμοποιηθούν τόσο η συμμετρική όσο και η ασύμμετρη κρυπτογράφηση κλειδιού, και η επιλογή εξαρτάται από διάφορους παράγοντες, συμπεριλαμβανομένης της κρισιμότητας των δεδομένων, των χρονικών περιορισμών και των υπολογιστικών πόρων.

Η αυθεντικοποίηση ορίζεται ως η ενέργεια επαλήθευσης ότι η ταυτότητα ενός αντικειμένου είναι έγκυρη, όπως η χρήση ενός κωδικού πρόσβασης. Ένα αντικείμενο μπορεί να είναι ένας χρήστης, μία έξυπνη συσκευή ή οποιοδήποτε στοιχείο συνδεδεμένο στο δίκτυο του SG. Η αυθεντικοποίηση πολυεκπομπής (multicast) είναι ένας ιδιαίτερος τύπος αυθεντικοπίησης και οι εφαρμογές της χρησιμοποιούνται ευρέως στο SG. Τρεις μέθοδοι για την επίτευξη αυθεντικοποίησης για εφαρμογές πολυεκπομπής είναι: η ασυμμετρία μυστικής πληροφορίας, η ασυμμετρία χρόνου και η υβριδική ασυμμετρία.

Η διαχείριση κλειδιών είναι μία κρίσιμη προσέγγιση για την κρυπτογράφηση και την αυθεντικοποίηση. Η διαχείριση δημόσιων κλειδιών ή η διαχείριση κοινών μυστικών κλειδιών μπορεί να χρησιμοποιηθεί για την εξασφάλιση της αυθεντικότητας για την επικοινωνία μεταξύ των δικτύων. Στην υποδομή δημόσιου κλειδιού (PKI), οι ταυτότητες των δύο οντοτήτων αποθηκεύονται από ένα πιστοποιητικό που έχει εκδοθεί από μία τρίτη οντότητα που ονομάζεται αρχή πιστοποίησης (Certification Authority - CA). Ο μηχανισμός αυτός γίνεται πριν τη δημιουργία οποιασδήποτε σύνδεσης μεταξύ των δύο οντοτήτων. Στη διαχείριση κοινού μυστικού κλειδιού, χρησιμοποιούνται τέσσερα βήματα για τη διατήρηση της ασφάλειας της επικοινωνίας: δημιουργία κλειδιού, διανομή κλειδιού, αποθήκευση κλειδιού και ενημέρωση κλειδιού. Λόγω της κατανεμημένης φύσης του SG, θα πρέπει να εξεταστούν ορισμένες ειδικές απαιτήσεις για το σχεδιασμό διαχείρισης κρυπτογραφικού κλειδιού. Βασικές αλλά σχετικές απαιτήσεις του σχήματος διαχείρισης κλειδιών αποτελούν η αποδοτικότητα, η ικανότητα ανάπτυξης, η επεκτασιμότητα και η ασφαλής διαχείριση. Επιπλέον, έχουν προταθεί διάφορα πλαίσια διαχείρισης κλειδιών ειδικά για τα συστήματα ηλεκτρικής ενέργειας, όπως για παράδειγμα: μοναδικό κλειδί (single-key), εγκαθίδρυση κλειδιού για συστήματα SCADA (SKE), αρχιτεκτονική διαχείρισης κλειδιού για συστήματα SCADA (SKMA), προηγμένη αρχιτεκτονική

διαχείρισης κλειδιού (ASKMA), ASKMA+ και κλιμακωτή μέθοδος διαχείρισης κρυπτογραφικού κλειδιού (SMOCK). Η επιλογή ενός πλαισίου βασίζεται σε διαφορετικά κριτήρια, συμπεριλαμβανομένης της επεκτασιμότητας, της ικανότητας των υπολογιστικών πόρων και της υποστήριξη πολυεκπομπής. Έρευνες έχουν διεξαχθεί για τη σύγκριση μεταξύ των σχημάτων διαχείρισης κλειδιών που αναφέρθηκαν παραπάνω. Η σύγκριση βασίστηκε στην επεκτασιμότητα, την υποστήριξη πολυεκπομπής, την ανθεκτικότητα στην παραβίαση κλειδιών και την εφαρμογή σε συστήματα ηλεκτρικής ενέργειας. Το ASKMA+ και το SMOCK παρουσίασαν ενδιαφέροντα αποτελέσματα. Το ASKMA+ είναι ένα αποτελεσματικό σχήμα διαχείρισης κλειδιών που υποστηρίζει την πολυεκπομπή, αλλά εξακολουθεί να υποφέρει από επεκτασιμότητα. Το SMOCK από την άλλη, παρουσιάζει καλή επεκτασιμότητα, ωστόσο έχει κάποιες αδυναμίες όπως η μη υποστήριξη πολυεκπομπής και η χαμηλή υπολογιστική αποδοτικότητα.[92]

3.6.4 Έμπιστη υπολογιστική και ασφάλεια συσκευών

Λαμβάνοντας υπόψη το απίστευτο μέγεθος της απειλής της κυβερνοασφάλειας και τις σοβαρές συνέπειες από κυβερνοεπιθέσεις, η προστασία της κυβερνοασφάλειας στο SG πρέπει να πληροί σε μεγάλο βαθμό τις απαιτήσεις της κυβερνοασφάλειας. Η επικοινωνία στο SG απαιτεί ένα ολοκληρωμένο σχέδιο που περιλαμβάνει σχεδόν όλες τις πτυχές των λειτουργιών του SG. Ένα μέρος ενός τέτοιου σχεδίου περιλαμβάνει την έμπιστη υπολογιστική (trusted computing). Τέτοιες πλατφόρμες και σχετικοί μηχανισμοί χρησιμοποιούνται για τη διασφάλιση της αποφυγής της εισόδου κακόβουλου λογισμικού στις συσκευές επεξεργασίας λογισμικού. Ο κύριος στόχος του σχεδίου είναι η υλοποίηση ενός ουσιαστικού και άρα εύχρηστου, σταθερού και αξιοποιήσιμου πυρήνα ασφαλείας (security kernel) για τις συμβατικές πλατφόρμες υλικού (hardware platforms), διακομιστές (servers), ενσωματωμένα συστήματα (embedded systems) και κινητές συσκευές (mobile devices) όπως PDAs και smartphones. Όλες οι απαιτήσεις πληρούνται με την εξαγωγή κρίσιμων για την ασφάλεια λειτουργιών και δεδομένων στον πυρήνα ασφαλείας.

Υπάρχουν δύο κατηγορίες συσκευών για τις οποίες πρέπει να λαμβάνονται υπόψη τα προβλήματα προστασίας από κακόβουλο λογισμικό: ενσωματωμένα υπολογιστικά συστήματα και υπολογιστικά συστήματα γενικού σκοπού. Τα ενσωματωμένα συστήματα είναι υπολογιστικά συστήματα που είναι σχεδιασμένα για την εκτέλεση εργασίας ή μίας σειρά εργασιών. Έχουν ως σκοπό την εκτέλεση του λογισμικού που παρέχεται από την κατασκευή. Αντίθετα, τα συστήματα γενικού σκοπού προορίζονται για την υποστήριξη άλλου λογισμικού που αγοράστηκε από ένα συγκεκριμένο καταναλωτή που διαθέτει το σύστημα. Ένα καλό παράδειγμα συστημάτων γενικού σκοπού αποτελεί ο υπολογιστής, Ένας φούρνος μικροκυμάτων ή ένας αποκωδικοποιητής καλωδιακής τηλεόρασης είναι παραδείγματα ενσωματωμένων συστημάτων. Το πρόβλημα της προστασίας από κακόβουλο λογισμικό πρέπει να εξετάζεται χωριστά για κάθε κατηγορία.

Για ενσωματωμένα συστήματα το πρόβλημα της προστασίας απέναντι στην εγκατάσταση κακόβουλων λογισμικών μπορεί να λυθεί με υψηλό βαθμό διαβεβαίωσης. Πρώτα από όλα, οι κατασκευαστές πρέπει να εφαρμόσουν ασφαλείς διαδικασίες ανάπτυξης λογισμικού. Έχουν καθοριστεί πολλά πρότυπα μοντέλα για τέτοιες διαδικασίες. Δεύτερον, αν η συσκευή προορίζεται για να είναι αναβαθμίσιμη, οι κατασκευαστές πρέπει να παρέχουν μία ασφαλή λύση αναβάθμισης λογισμικού. Η επικρατέστερη μέθοδος για να γίνει αυτό είναι η κατασκευή του υλικού μέρους του ενσωματωμένου συστήματος (hardware) με ασφαλή αποθήκευση περιέχοντας υλικό κρυπτογράφησης (keying material) για την επικύρωση λογισμικού. Συνήθως, το hardware πρέπει να έχει διαμορφωθεί με το δημόσιο κλειδί ενός διακομιστή με ασφαλή υπογραφή από τον κατασκευαστή. Με αυτό το κλειδί η συσκευή μπορεί να επικυρώσει όλα τα πρόσφατα λογισμικά πριν την εκτέλεσή τους. Συνήθως μια τέτοια προληπτική προσέγγιση πρέπει να παρέχει υψηλά επίπεδα διαβεβαίωσης από αυτά που παρέχει μία αντιδραστική προσέγγιση όπως ένα πρόγραμμα για τον εντοπισμό ιών.[93]

Για συσκευές που προορίζονται να λειτουργούν για μεγάλες χρονικές περιόδους χωρίς εκκίνηση (booting), είναι χρήσιμο να υπάρχει μία μέθοδος εκτέλεσης ασφαλούς επικύρωσης λογισμικού στον κώδικα που εκτελείται. Είναι δυνατό να υπάρχουν στο παρασκήνιο εργασίες που να εκτελούν περιοδικά τέτοιες λειτουργίες χωρίς να διαταράσσουν τις λειτουργίες της συσκευής. Είναι επιπλέον δυνατή η σύζευξη τέτοιων σταδίων επικύρωσης στο παρασκήνιο με άλλες λειτουργικές πτυχές της συσκευής όπως ότι αν διαπιστωθεί ότι η συσκευή βρίσκεται σε κίνδυνο, το ασφαλές hardware στη συσκευή θα αποτρέψει την τοπική συσκευή από το να δημιουργήσει και να διατηρήσει συσχετίσεις ασφαλείας (security associations) με τις απομακρυσμένες οντότητες. Μία πολλά υποσχόμενη νέα προσέγγιση για την απομακρυσμένη επαλήθευση κώδικα είναι μία τεχνολογία που ονομάζεται επιβεβαίωση (attestation) . Η επιβεβαίωση κώδικα (code attestation) επιτρέπει σε μία εξωτερική οντότητα να εξετάζει το λογισμικό που εκτελείται σε ένα σύστημα με τέτοιο τρόπο που να αποτρέπει την απόκρυψη κακόβουλου λογισμικού. Δεδομένου του ότι η επιβεβαίωση αποκαλύπτει μία υπογραφή του κώδικα εκτέλεσης, ακόμα και εάν ένα κακόβουλο λογισμικό είναι άγνωστο, θα τροποποιεί αυτή την υπογραφή και έτσι μπορεί να ανιχνευθεί. Σε διάφορες μελέτες έχουν περιγράφει μέθοδοι για την απομακρυσμένη επιβεβαίωση συσκευής (remote device attestation). Η επιβεβαίωση βάσει λογισμικού (software-based attestation) είναι μία προσέγγιση που δε βασίζεται σε εξειδικευμένο hardware, αλλά δημιουργεί κάποιες αξιώσεις ότι η οντότητα που εκτελεί την επιβεβαίωση μπορεί να επικοινωνεί με μοναδικό τρόπο με τη συσκευή που βρίσκεται υπό επιβεβαίωση. Επίσης, σε κάποιες μελέτες έχει παρουσιαστεί η εφαρμοσιμότητα αυτής της προσέγγισης σε συσκευές SCADA.[24]

Η κατάσταση γίνεται ακόμα χειρότερη με την ταχεία υιοθέτηση του υπολογιστικού νέφους (cloud computing) και των εξελιγμένων εφαρμογών που βασίζονται στο διαδίκτυο, που έχουν οδηγήσει στην ευρεία χρήση τεχνολογιών mobile code. Το mobile code είναι ο κώδικας που κατεβαίνει και εκτελείται στον υπολογιστή, συνήθως από κάποιο πρόγραμμα

περιήγησης, χωρίς τη γνώση των χρηστών. Παραδείγματα του mobile code περιλαμβάνουν ActiveX, Flash animation, Java, JavaScript, PDF, Postscript και Shockwave. Ο όρος αναφέρεται συνήθως σε κακόβουλο περιεχόμενο καθώς το mobile code δημιουργεί διάφορους βαθμούς βλαβών στον υπολογιστή και το σύστημα.

Για την αντιμετώπιση αυτού του ζητήματος, προτείνεται η υιοθέτηση και η προσήλωση σε αυστηρά πρότυπα πιστοποίησης υπογραφής κώδικα (code signing) από τους προμηθευτές και τους διαχειριστές του SG. Μηχανισμοί για την επιβολή τέτοιων προτύπων σε υπολογιστές γενικής χρήσης, όπως οι προσωπικοί υπολογιστές, έχουν τεθεί από το Trusted Computing Group και είναι καλά τεκμηριωμένοι. Τέτοια πρότυπα πρέπει να καλύπτουν όλες τις σημαντικές συσκευές που περιλαμβάνουν μονάδες που χρησιμοποιούνται στον τομέα του SG, όπως RTU και IED, συσκευές δικτύου όπως δρομολογητές, μεταγωγείς και τείχη προστασίας, και εξοπλισμός κέντρου ελέγχου όπως διακομιστές και κονσόλες χρηστών. Τα πρότυπα πρέπει να καλύπτουν τα ενσωματωμένα συστήματα, καθώς και υπολογιστές γενικής χρήσης, λειτουργικά συστήματα, οδηγούς συσκευής, εφαρμογές καθώς και mobile codes. Δηλαδή, δεν πρέπει να επιτρέπεται η εκτέλεση κανενός mobile code σε κρίσιμο υπολογιστή ή διακομιστή που δεν έχει πιστοποιηθεί από μία αρχή που είναι ικανή να προσδιορίσει την αξιοπιστία του κώδικα. Θεωρώντας ότι είναι βέβαιο ότι τα στοιχεία υλικού και λογισμικού των κρίσιμων συνιστωσών του SG θα προέρχονται από διαφορετικούς παρόχους, είναι πιθανό ότι θα πρέπει να δημιουργηθεί για το SG ένα πλαίσιο διαχείρισης εμπιστοσύνης (trust management). Αυτό το πλαίσιο θα απαιτεί πιθανώς τη θέσπιση ενός συνόλου κριτηρίων που πρέπει να πληρούνται από τους προμηθευτές που επιθυμούν να πουλήσουν σημαντικά εξαρτήματα στους διαχειριστές του SG. Επιπλέον, είναι πιθανό ότι θα πρέπει να συσταθεί ένας ή περισσότεροι οργανισμοί διαπίστευσης για τον έλεγχο των προμηθευτών ώστε να διαπιστωθεί ότι πληρούν τα καθορισμένα κριτήρια.[93]

Το σύστημα πρέπει να είναι σχεδιασμένο έτσι ώστε αν ένας επιτιθέμενος εκτελέσει επίθεση πλαστοπροσωπίας σε ένα μετρητή, το πεδίο επιρροής του να περιορίζεται στην επίδραση του μηνιαίου λογαριασμού που σχετίζεται με αυτό τον μετρητή. Πολλοί έχουν αναφέρει την πιθανότητα ότι ένας επιτιθέμενος μπορεί να καταστήσει το δίκτυο ως μη διαθέσιμο με επίθεση πλαστοπροσωπίας ή χακάροντας ένα μετρητή, ως ένα λόγο για αναβαθμίσιμες κρυπτογραφικές υλοποιήσεις στο μετρητή. Μία καλύτερη προσέγγιση θα ήταν ο σχεδιασμός ενός συστήματος που θα προσφέρει θεμελιωδώς προστασία απέναντι σε τέτοιες επιθέσεις. Ένας μετρητής θα πρέπει να είναι σε θέση να στέλνει πακέτα σε ένα ¨σημείο συλλογής δεδομένων μετρητών¨ και ένα ¨διαχειριστή μετρητών¨, ο οποίος με τη σειρά του μπορεί να επικοινωνεί με συγκεκριμένα σχεδιασμένες συσκευές για συγκεκριμένα σχεδιασμένες υπηρεσίες. Ένας μετρητής δε θα πρέπει να είναι ποτέ σε θέση να στείλει πακέτα σε αυθαίρετα εξαρτήματα του συστήματος όπως IED ή επεξεργαστές κατανεμημένου ελέγχου που βρίσκονται στον υποσταθμό.

Πρέπει να εφαρμοστούν διάφορες μέθοδοι για να επιτευχθεί αυτό. Πρώτα, όλες οι συσκευές πρέπει να γνωρίζουν με ποιον επικοινωνούν, και με ποιον πρέπει να επικοινωνούν. Αυτό επιτυγχάνεται με τεχνικές αμοιβαίας αυθεντικοποίησης όπως το πρωτόκολλο TLS ή IPSec. Κατά τη διάρκεια της αμοιβαίας αυθεντικοποίησης, παράγονται μοναδικά συμμετρικά κλειδιά τα οποία χρησιμοποιούνται για την παροχή αυθεντικοποίησης και ακεραιότητας του μηνύματος για μεταγενέστερη κίνηση. Δεύτερον, πρέπει να απομονωθούν τα τμήματα του λογικού δικτύου (logical network segments). Οι έλεγχοι πρέπει να είναι εγκατεστημένοι στο δίκτυο AMI για να διασφαλιστεί ότι η κίνηση του μετρητή δεν μπορεί να φτάσει σε έναν υποσταθμό, ή κάποια αυθαίρετη διεύθυνση του δικτύου. Επίσης, οι έλεγχοι πρέπει να είναι εγκατεστημένοι στον υποσταθμό ή στο κέντρο ελέγχου, για να διασφαλίζουν ότι η κίνηση εγκρίνεται από εξουσιοδοτημένες πηγές. Μία τέτοια προσέγγιση άμυνας χρησιμοποιείται σε δίκτυα επιχειρήσεων για χρόνια. Η φυσική απομόνωση του δικτύου AMI από άλλα δίκτυα θα μπορούσε να αποτελεί την καλύτερη λύση. Ωστόσο, πρέπει να σημειωθεί ότι τα λειτουργικά έξοδα θα ωθήσουν τις εταιρείες ηλεκτρισμού στη χρήση πόρων κοινόχρηστου δικτύου (shared network) για διάφορους σκοπούς. Συνεπώς, οφείλει να διασφαλιστεί η αρχιτεκτονική του SG ώστε να μπορεί να υποστηρίξει τη λογική απομόνωση των λογικά ανόμοιων δικτύων που μοιράζονται κοινούς πόρους.[94]

3.6.5 Διαχείριση και ενημερότητα ασφαλείας

Η αυξημένη επίγνωση του κινδύνου της ασφαλείας και η κατάλληλη διαχείριση των πληροφοριών που σχετίζονται με την ασφάλεια παρέχουν εξίσου σημαντικό ρόλο στη διατήρηση μίας αξιόπιστης υποδομής. Στη συνέχεια εξετάζονται μία σειρά δραστηριοτήτων και εργαλείων ασφαλείας όπως η ανάλυση ψηφιακών πειστηρίων (Digital Forensics) και η διαχείριση περιστατικών/συμβάντων ασφαλείας (security incident/event management).

1) **Ανάλυση ψηφιακών πειστηρίων:** Η ικανότητα να εκτελείται ακριβής ανάλυση ψηφιακών πειστηρίων μέσα στο SG είναι απαραίτητη για τον εντοπισμό αποτυχιών ασφαλείας και την αποφυγή μελλοντικών περιστατικών. Οι δυνατότητες για τέτοιες αναλύσεις είναι επίσης απαραίτητες κατά τη διερεύνηση γεγονότων για τον καθορισμό της αιτίας ή της έκτασης της βλάβης που προκλήθηκε από μία επίθεση. Ενώ η ανάλυση ψηφιακών πειστηρίων των παραδοσιακών συστημάτων τεχνολογίας πληροφοριών τυγχάνει κατάλληλης έρευνας, ο μεγάλος αριθμός ενσωματωμένων συστημάτων και συσκευών παλαιού τύπου στο δίκτυο δημιουργεί νέες προκλήσεις. Σε κάποιες έρευνες έχει προταθεί η ανάπτυξη πρακτόρων για την ανάλυση ψηφιακών πειστηρίων σε όλη την υποδομή του κυβερνοχώρου για τη συλλογή δεδομένων σχετικά με τις πιθανές επιθέσεις. Στις πληροφορίες που συλλέγονται από αυτούς τους πράκτορες μπορεί να δοθεί προτεραιότητα που βασίζεται στην ικανότητά τους να επηρεάζουν αρνητικά τις λειτουργίες του δικτύου. Η επέκταση των δυνατοτήτων

αυτών των αναλύσεων στα ενσωματωμένα συστήματα, συμπεριλαμβανομένων των μετρητών και των IEDs, είναι απαραίτητη για τη διασφάλιση της ακεραιότητας σε αυτούς τους κρίσιμους πόρους. Επιπλέον, τα λειτουργικά συστήματα μπορεί να μην είναι κατάλληλα για ανάλυση ψηφιακών πειστηρίων και η έρευνα με μεθόδους online ανάλυσης να χρειάζεται σε αυτές τις περιπτώσεις.

2) **Διαχείριση περιστατικών και συμβάντων ασφαλείας:** Η ανάπτυξη τεχνολογιών για τη συλλογή και την ανάλυση πηγών δεδομένων όπως αρχεία καταγραφής συστήματος, αποτελέσματα συστημάτων ανίχνευσης εισβολής και πληροφορίες ροής δικτύου, είναι απαραίτητες για να διασφαλιστεί ότι τα δεδομένα είναι σωστά οργανωμένα και διαθέτουν την κατάλληλη προτεραιότητα. Σε μία μελέτη διερευνάται η ενσωμάτωση διαφόρων πηγών δεδομένων κυβερνοασφάλειας σε ένα σύστημα ελέγχου και αποδεικνύεται η ικανότητά της για ανίχνευση επιθέσεων. Αυτή η μελέτη ένωσε εργαλεία οπτικοποίησης για την κατανόηση της κατάστασης του δικτύου σε πραγματικό χρόνο στους διαχειριστές. Η προσαρμογή αυτής της τεχνολογίας για την παροχή αποτελεσματικής ανάλυσης του δικτύου θα δώσει μία ώθηση στις προειδοποιήσεις του συστήματος ελέγχου, καθώς παρέχει πληροφορίες για τις πιθανές φυσικές επιπτώσεις που προκαλούνται από επιθέσεις στον κυβερνοχώρο. Τα περιστατικά και τα συμβάντα εντός του SG θα διαφέρουν σημαντικά από τα αντίστοιχα των τεχνολογιών πληροφορίας, επομένως οι μέθοδοι ανάλυσης θα πρέπει να συσχετίζονται με τη γνώση του φυσικού συστήματος για τον προσδιορισμό ανωμαλιών. Οι αλγόριθμοι συνάθροισης και ανάλυσης ενδέχεται να χρειάζονται προσαρμογή για περιβάλλοντα με μειωμένα ποσοστά συμβάντων λόγω μικρότερων βάσεων χρηστών και διαχωρισμένων δικτύων. [90]

3.6.6 Σχήματα προστασίας της ιδιωτικότητας στο Smart Grid

Υπάρχουν πολλά σχήματα για την προστασία της ιδιωτικότητας που αναπτύχθηκαν ή εφαρμόζονται στο πλαίσιο του SG. Η διαδικασία υλοποίησης ενός σχήματος για την προστασία της ιδιωτικότητας για το SG βασίζεται σε επτά βήματα: 1) ορισμός του μοντέλου επικοινωνίας και συστήματος (για παράδειγμα αρχιτεκτονική Vehicle-to-grid (V2G), αρχιτεκτονική marketing του S.G και άλλα), 2) ορισμός του μοντέλου ιδιωτικότητας (για παράδειγμα το απόρρητο της τοποθεσίας, το απόρρητο της ταυτότητας και άλλα), 3) ορισμός του μοντέλου των επιθέσεων (για παράδειγμα επιθέσεις κλειδιού, επιθέσεις δεδομένων και άλλες), 4) επιλογή αντιμέτρων (για παράδειγμα μέθοδοι κρυπτογράφησης), 5) πρόταση βασικών φάσεων του σχήματος (για παράδειγμα αρχική ρύθμιση, διαδικασίας εγγραφής και άλλα), 6) ανάλυση ασφάλειας χρησιμοποιώντας προσεγγίσεις θεωρίας παιγνίων (για παράδειγμα αποδείξεις μηδενικής γνώσης) και 7) αξιολόγηση της απόδοσης (για παράδειγμα όρους που σχετίζονται με το κόστος αποθήκευσης και την πολυπλοκότητα του υπολογισμού). Στο Σχήμα 4 φαίνεται μία κατηγοριοποίηση των σχημάτων προστασίας της ιδιωτικότητας στο SG σε πέντε κατηγορίες βάσει μοντέλων επικοινωνίας και συστήματος συμπεριλαμβανομένου:

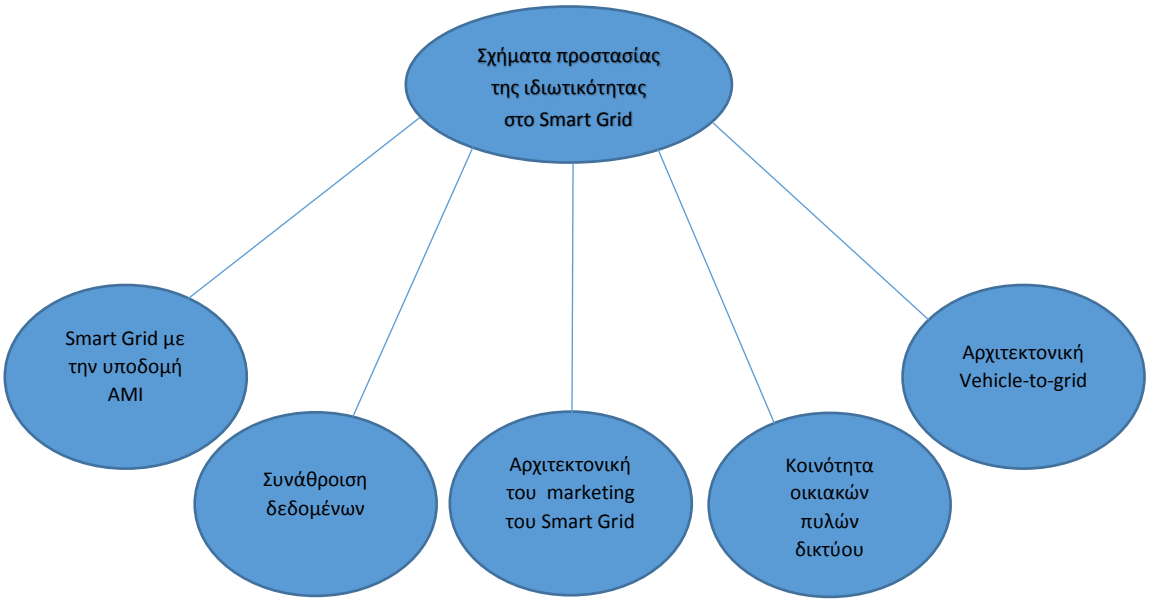
1)Smart Grid με την υποδομή AMI, 2) συνάθροιση δεδομένων, 3) αρχιτεκτονική του marketing του Smart Grid, 4) ¨έξυπνη¨ κοινότητα οικιακών πυλών δικτύου και 5) αρχιτεκτονική Vehicle-to-grid. Επιπλέον, τα σχήματα αυτά μπορούν κατηγοριοποιηθούν σε πολλαπλά μοντέλα προστασίας της ιδιωτικότητας, ωστόσο η κατηγοριοποίηση τους με βάση το μοντέλο δικτύου τους μπορεί να προφέρει μία πιο γενική εικόνα.

1) Smart Grid με προηγμένη υποδομή μέτρησης

Υπάρχουν πολλά σχήματα προστασίας της ιδιωτικότητας για το SG με την προηγμένη υποδομή μέτρησης (AMI). Η υποδομή AMI εξαρτάται από εξελιγμένες συσκευές μέτρησης που αποκαλούνται έξυπνοι μετρητές. Ένα παράδειγμα υποδομής AMI βασίζεται σε τρία μέρη, δηλαδή ένα έξυπνο σπίτι, μία συσκευή επικοινωνίας με την εταιρεία ηλεκτρισμού και ένα γραφείο της εταιρείας για παροχή υπηρεσιών.

2) Συνάθροιση δεδομένων

Μεγάλο πλήθος σχημάτων για την προστασία της ιδιωτικότητας στο SG χρησιμοποιεί συνάθροιση δεδομένων κατά τη διάρκεια της επικοινωνίας. . Οι τεχνικές συνάθροισης σε ασύρματα δίκτυα αισθητήρων έχουν προταθεί σε πολλές έρευνες. Η βασική ιδέα αυτών των τεχνικών βασίζεται στην χρήση ενός συναθροιστή και μίας έμπιστης αρχής (trusted authority). Ωστόσο, το ιδιωτικό απόρρητο της συνάθροισης δεδομένων παρουσιάζει πολλές ερευνητικές προκλήσεις όσον αφορά την προστασία της ιδιωτικότητας στο SG.



Σχήμα 4 - Κατηγοριοποίηση των σχημάτων προστασίας της ιδιωτικότητας στο SG [37]

3) Αρχιτεκτονική του marketing του Smart Grid

Ορισμένα σχήματα για την προστασία της ιδιωτικότητας χρησιμοποιούν την αρχιτεκτονική του marketing του SG. Η ενσωμάτωση των συστημάτων SCADA στο SG επιτρέπει σε έναν διαχειριστή της εταιρείας ηλεκτρισμού να παρακολουθεί και να ελέγχει απομακρυσμένα δίκτυα όπως HAN, BAN, IAN, NAN, FAN και WAN. Τα κακόβουλα δεδομένα σε ένα σύστημα SCDA διαταράσσουν την ομαλή λειτουργία της διαχείρισης αυτών των δικτύων.

4) ¨Έξυπνη¨ κοινότητα οικιακών πυλών δικτύου

Κάποια άλλα σχήματα για την προστασία της ιδιωτικότητας επικεντρώνονται την ¨έξυπνη¨ κοινότητα οικιακών πυλών του δικτύου. Μία τέτοια κοινότητα είναι ένα εικονικό περιβάλλον που αποτελείται από δικτυωμένα έξυπνα σπίτια που βρίσκονται σε μία τοπική έξυπνη περιοχή. Σε μία ¨έξυπνη¨ κοινότητα βασίζεται σε τρία μέρη: τους έξυπνους μετρητές, την τοπική πύλη και το κέντρο ελέγχου.

5) Αρχιτεκτονική του Vehicle-to-grid

Μερικά σχήματα προστασία της ιδιωτικότητας στο SG βασίζονται στην αρχιτεκτονική Vehicle-to-grid. Το V2G είναι ένα σχέδιο ενσωμάτωσης των οχημάτων στο SG που λειτουργούν ως κατανεμημένες πηγές-φορτίο και συσκευές παραγωγής αποθήκευσης. Ένα παράδειγμα μίας τέτοιας αρχιτεκτονικής βασίζεται σε πέντε μέρη: ηλεκτρικά οχήματα, υπηρεσία hotspot σε έξυπνο σταθμό φόρτισης, πύλη δικτύου επιπέδου γειτονιάς (NAN), πύλη κτιριακού δικτύου (BAN) και κέντρο ελέγχου. Το δίκτυο V2G αποτελεί μία από τις πιο σημαντικές αρχιτεκτονικές του SG, όπου τα ηλεκτρικά οχήματα (EV) επικοινωνούν με τους παρόχους υπηρεσιών μέσω συναθροιστών ή άλλων δικτύων.[37]

ΚΕΦΑΛΑΙΟ 4

ΣΥΜΠΕΡΑΣΜΑΤΑ

Τρεις κυριότεροι παράγοντες που επηρεάζουν τα μελλοντικά ηλεκτρικά συστήματα του κόσμου: κυβερνητικές πολιτικές, ανάγκες καλύτερης απόδοσης από τους πελάτες και νέες ευφυείς τεχνολογίες υλικού και λογισμικού υπολογιστών. Επιπλέον, οι περιβαλλοντικές ανησυχίες οδηγούν ολόκληρο το ενεργειακό σύστημα στην αποδοτικότητα, τη συντήρηση και τις ανανεώσιμες πηγές ηλεκτρικής ενέργειας. Οι πελάτες γίνονται πιο ενεργητικοί και μπορούν να συμμετέχουν σε αποφάσεις ενεργειακής κατανάλωσης που επηρεάζουν την καθημερινή τους ζωή. Ταυτόχρονα οι ενεργειακές ανάγκες συνεχώς αυξάνονται. Για παράδειγμα, η συμμετοχή των καταναλωτών θα περιλαμβάνει σύντομα εκτεταμένη χρήση ηλεκτρικών οχημάτων, απομακρυσμένο έλεγχο οικιακών συσκευών για περισσότερη εξοικονόμηση ενέργειας, κατανεμημένη παραγωγή από ολοένα και περισσότερες ανανεώσιμες πηγές και διαχείριση της αποθήκευσης ηλεκτρικής ενέργειας για την τοπική προσαρμογή της προσφοράς στη ζήτηση. Η διαθεσιμότητα των νέων τεχνολογιών, όπως οι κατανεμημένοι αισθητήρες, η ασφαλής αμφίδρομη επικοινωνία, το προηγμένο λογισμικό διαχείρισης δεδομένων, και οι ευφυείς και αυτόνομοι ελεγκτές έχουν δημιουργήσει νέες ευκαιρίες για την αλλαγή του ενεργειακού συστήματος. Για παράδειγμα, ενώ οι τεχνολογίες και τα συστήματα δικτύωσης έχουν ενισχυθεί σημαντικά, το SG αντιμετωπίζει προκλήσεις όσον αφορά την αξιοπιστία και την ασφάλεια τόσο σε ενσύρματα όσο και σε ασύρματα περιβάλλοντα επικοινωνίας. Οι έξυπνες οικιακές συσκευές αντιπροσωπεύουν ένα σημαντικό μέρος του SG, το οποίο στοχεύει στην αύξηση της ενεργειακής απόδοσης. Για την επίτευξη αυτού του στόχου, πρέπει οι οικιακές συσκευές να επικοινωνούν με άλλες οντότητες και φορείς του SG μέσω οικιακών δικτύων. Επομένως, το ηλεκτρικό σύστημα του μέλλοντος θα πρέπει να μπορεί να αντιμετωπίσει όλες τις ανάγκες και τις ανησυχίες χρησιμοποιώντας νέες τεχνολογίες για τη δημιουργία ενός πιο έξυπνου, αποδοτικότερου και βιώσιμου δικτύου.

Ενώ λοιπόν το SG υπόσχεται πολλαπλά οφέλη, παράλληλα δημιουργεί πολλές νέες προκλήσεις που αφορούν την ασφάλεια και την προστασία της ιδιωτικότητας. Με την εκτεταμένη χρήση δικτυακών συσκευών για την παρακολούθηση και τον έλεγχο του δικτύου, καθίσταται ευκολότερη για τους επιτιθέμενους η εύρεση τρωτών σημείων, συμπεριλαμβανομένων νέων έξυπνων συσκευών, για πρόσβαση σε διάφορα τμήματα του δικτύου με αποτέλεσμα την αύξηση πεδίου δράσης τους. Επίσης, οι νέες λειτουργίες που παρέχονται από τις νέες συσκευές, όπως η δυνατότητα απομακρυσμένης σύνδεσης που παρέχεται από πολλούς έξυπνους μετρητές, μπορεί να εκμεταλλευθεί από τους επιτιθέμενους με αποτέλεσμα σημαντικούς κινδύνους για την ασφάλεια του συστήματος. Μία επίσης πολύ σημαντική πρόκληση για την ασφάλεια πηγάζει από το γεγονός ότι το

SG είναι ένα κυβερνο-φυσικό σύστημα όπου η δυναμική του φυσικού κόσμου συνδέεται στενά με τα στοιχεία της τεχνολογίας πληροφοριών.

Η διασφάλιση του SG αποτελεί ένα δύσκολο έργο και απαιτεί κοινές προσπάθειες από τους προμηθευτές, τις επιχειρήσεις ηλεκτρικής ενέργειας, τους καταναλωτές (οικιακούς και εμπορικούς), τους παρόχους υπηρεσιών και τις κυβερνητικές οργανώσεις. Η βασικότερη απαίτηση είναι ότι οι προμηθευτές και οι πάροχοι έχουν ακολουθήσει τις βέλτιστες πρακτικές της βιομηχανίας για την ασφάλεια των πληροφοριών. Αυτές περιλαμβάνουν την αξιολόγηση του κινδύνου και τη μοντελοποίηση των απειλών, τη διασφάλιση των πρακτικών και της επανεξέτασης του κώδικα, την προστασία (έλεγχος πρόσβασης και κρυπτογράφηση), την πολιτική και τους μηχανισμούς ανίχνευσης και απόκρισης στις παραβιάσεις της ασφάλειας με κατάλληλους μηχανισμούς ελέγχου και καταγραφής για την υποστήριξη της ανάλυσης ψηφιακών πειστηρίων, την αξιολόγηση και τον έλεγχο των ευπαθειών.

Εκτός από τις βέλτιστες πρακτικές ασφαλείας, οι εφαρμογές του SG πρέπει να εξετάσουν τις πρόσθετες πρακτικές απαιτήσεις που επιβάλλονται στα συστήματα συμπεριλαμβανομένων της ενσωμάτωσης παλαιών συσκευών, της εκτεταμένης χρήσης ενσωματωμένων συστημάτων, (με δισεκατομμύρια συσκευές συνδεδεμένες στο δίκτυο), της κεντρικής διαχείρισης πολλών συσκευών, της ανάγκης για αξιόπιστη λειτουργία των συσκευών των κρίσιμων υποδομών και των ενσωματωμένων συστημάτων χαμηλού κόστους. Παρόλο που ορισμένες από αυτές τις απαιτήσεις μπορούν να αντιμετωπιστούν κατάλληλα, ορισμένες αποτελούν σήμερα ενεργά ερευνητικά πεδία.

Είναι επίσης σημαντικό το σχέδιο για ενδεχόμενα σφάλματα. Τα πολύπλοκα συστήματα λογισμικού πρόκειται να έχουν πολλά εκμεταλλεύσιμα σφάλματα. Η βιομηχανία των εταιρειών ηλεκτρικής ενέργειας πρέπει να συνεργαστεί με τους προμηθευτές για να αναπτύξει ολοκληρωμένες στρατηγικές αποκατάστασης. Αυτά τα σχέδια πρέπει να επιτρέπουν την επιδιόρθωση λογισμικού και την ταχεία αναγνώριση και απομόνωση των παραβιασμένων συστημάτων.

Υπάρχουν επίσης πολλά οργανωτικά προβλήματα που μπορούν να αντιμετωπιστούν με οικονομικά κίνητρα, νέες κρατικές οργανώσεις και πιθανούς νέους κανονισμούς. Επιπρόσθετα στα τεχνικά και οργανωτικά προβλήματα, η φύση κυβερνο-φυσικών συστημάτων του SG παρέχει νέες προκλήσεις και ερευνητικές ευκαιρίες που πρέπει να διερευνηθούν περαιτέρω. Οι τρέχουσες προσεγγίσεις για την ασφάλεια των υποδομών στον κυβερνοχώρο εφαρμόζονται σίγουρα για τη διασφάλιση των κυβερνο-φυσικών συστημάτων: τεχνικές για διαχείριση κλειδιού, ασφαλή επικοινωνία (μυστικότητα, αυθεντικοποίηση και διαθεσιμότητα), ασφαλή εκτέλεση κώδικα, ανίχνευση εισβολών και άλλα. Δυστυχώς αυτές οι προσεγγίσεις δε γνωρίζουν σε μεγάλο βαθμό τις

φυσικές πτυχές των κυβερνο-φυσικών συστημάτων. Η κυβερνοασφάλεια στο SG είναι ένας νέος τομέας έρευνας που έχει προσελκύσει ραγδαίως αυξανόμενη προσοχή στην κυβέρνηση, τη βιομηχανία και τον ακαδημαικό κόσμο.

Οι νέες τεχνολογίες που χρησιμοποιούνται στα έξυπνα δίκτυα βασίζονται σε μία ευρεία συλλογή δεδομένων του χρήστη, συμπεριλαμβανομένης της κατανάλωσης ενέργειας , η οποία μπορεί να αποκαλύψει προσωπικές πληροφορίες. Οι τεχνολογίες του SG μπορούν να χρησιμοποιηθούν για την εξαγωγή συμπερασμάτων σχετικά με την τοποθεσία και τη συμπεριφορά των χρηστών όπως το αν βρίσκονται στο σπίτι, την ποσότητα ενέργειας που καταναλώνουν και το είδος των συσκευών που χρησιμοποιούν. Με την αύξηση της συλλογής πληροφοριών για τους καταναλωτές, νέες μορφές επίθεσης καθίστανται δυνατές. Τα τελευταία χρόνια υπάρχει αυξημένη ανάγκη για αποτελεσματικά σχήματα προστασίας της ιδιωτικότητας στο SG. Αυτό οφείλεται κυρίως στην αυξημένη ανάγκη που έχει η βιομηχανία ηλεκτρικής ενέργειας για αυξημένη προστασία της ιδιωτικότητας και των προσωπικών δεδομένων. Υπάρχουν ακόμα αρκετοί ερευνητικοί τομείς (για παράδειγμα ανίχνευση και αποφυγή νέων επιθέσεων, αρχιτεκτονικές συστημάτων ανίχνευσης εισβολών που ενισχύουν την προστασία της ιδιωτικότητας στο SG, νέες μετρικές ιδιωτικότητας, SG που βασίζονται στο διαδίκτυο των πραγμάτων και ιδιωτικότητα στο διαδίκτυο ενέργειας) που μπορούν επίσης να αναλυθούν περαιτέρω στο εγγύς μέλλον.

Επίσης αναφέρθηκε ένας μεγάλος αριθμός προτύπων σχετικά με την ασφάλεια του SG. Αυτές οι δημοσιεύσεις ποικίλουν ως προς το πεδίο εφαρμογής, από το γενικό, που αναλύει θέματα υψηλού επιπέδου χωρίς να παρέχει λεπτομέρειες για συγκεκριμένη εφαρμογή, έως το αυστηρά τεχνικό. Ένα μέρος αυτών είναι αποκλειστικά αφιερωμένο στις πτυχές της κυβερνοασφάλειας, ενώ άλλα αναφέρονται στην κυβερνοασφάλεια που αντιμετωπίζει διάφορα προβλήματα στο SG. Επιπλέον, δεν υπάρχουν πρότυπα που να είναι αποκλειστικά αφιερωμένα στο SG, αλλά υποδεικνύονται ως εφαρμόσιμα ή προτείνονται για το SG. Επίσης, κάποια από αυτά περιγράφουν θέματα ιδιωτικότητας στο SG. Η πλειονότητα των προτύπων παρουσιάζει γενικές μεθόδους και αρχές προσαρμοσμένες σε συγκεκριμένες περιοχές του SG σύμφωνα με κάποιες ιδιόκτητες γνώσεις. Μία πιθανή κατεύθυνση μελλοντικών εξελίξεων είναι να συμπεριληφθούν λύσεις που βασίζονται σε πρακτικές εμπειρίες από προηγούμενες εφαρμογές.

Στα κεφάλαια που προηγήθηκαν, παρουσιάστηκε μία ευρεία σύνοψη του έξυπνου δικτύου με έμφαση στα θέματα της ασφάλειας και της ιδιωτικότητας. Παρόλο που έχει σημειωθεί μεγάλη πρόοδος για τη διασφάλιση της τρέχουσας αλλά και της μελλοντικής υλοποίησης του έξυπνου δικτύου, εξακολουθούν να υπάρχουν πολλές προκλήσεις που πρέπει να αντιμετωπιστούν. Η ασφάλεια και η ιδιωτικότητα στο έξυπνο δίκτυο θα βασίζονται ουσιαστικά στην προώθηση της χρήσης των καλύτερων πρακτικών ασφαλείας των πληροφοριών στην υλοποίηση και την ανάπτυξη νέων πρωτοβουλιών για το έξυπνο

δίκτυο. Οι συνεργασίες στη βιομηχανία και η κρατική στήριξη είναι απαραίτητες για τη δημιουργία οντοτήτων για τη διαχείριση, το συντονισμό και τη διάδοση πληροφοριών σχετικά με τα περιστατικά, τις ευπάθειες, τα προβλήματα και τις λύσεις στην ασφάλεια και την ιδιωτικότητα στο έξυπνο δίκτυο. Ιδιαίτερη προσοχή πρέπει να δοθεί στην ιδιωτικότητα των καταναλωτών και στη σύσταση οντοτήτων που να προασπίζονται τα δικαιώματα της ιδιωτικής ζωής των καταναλωτών.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] M. Abrar, M. A. Tahir, R. Masroor and H. U. Hamid, "Real time smart grid load management by integrated and secured communication," in *2018 International Conference on Innovative Trends in Computer Engineering*, 2018.

[2] H. Gharavi and R. Ghafurian, "Smart Grid: The Electric Energy System of the Future," *Proceedings of the IEEE,* vol. 99, no. 6, pp. 917 - 921, 2011.

[3] X. Fang, S. Misra, G. Xue and D. Yang, "Smart Grid — The New and Improved Power Grid: A Survey," *IEEE Communications Surveys & Tutorials,* vol. 14, no. 4, pp. 944 - 980, 2011.

[4] M. M. Kumbhar, P. R. Narvekar, A. B. Nandgaonkar and S. Nalbalwar, "Smart Grid: Advanced Electricity Distribution Network," *IOSR Journal of Engineering,* vol. 6, no. 2, pp. 23-29, 2012.

[5] National Institute of Standards and Technology, "NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0," 2014. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1108r3.pdf.

[6] National Institute of Standards and Technology, "Guidelines for Smart Grid Cybersecurity," 2014. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf.

[7] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati and G. P. Hancke, "Smart Grid Technologies: Communication Technologies and Standards," *IEEE Transactions on Industrial Informatics,* vol. 7, no. 4, pp. 529 - 539, 2011.

[8] R. Rajkumar, I. Lee, L. Sha and J. Stankovic, "Cyber-physical systems: The next computing revolution," in *Design Automation Conference*, 2010.

[9] X. Yu and Y. Xue, "Smart Grids: A Cyber–Physical Systems Perspective," *Proceedings of the IEEE,* vol. 104, no. 5, pp. 1058 - 1070, 2016.

[10] V. Gunes, S. Peter, T. Givargis and F. Vahid, "A Survey on Concepts, Applications, and Challenges in Cyber-Physical Systems," *KSII Transactions on Internet and Information Systems,* vol. 8, no. 12, pp. 4242-4268, 2014.

[11] F. B. Beidou, W. G. Morsi, C. P. Diduch and L. Chang, "Smart grid: Challenges, research directions and possible solutions," in *The 2nd International Symposium on Power Electronics for Distributed Generation Systems*, 2010.

[12] A. Mohd, E. Ortjohann, A. Schmelter, N. Hamsic and D. Morton, "Challenges in integrating distributed Energy storage systems into future smart grid," in *2008 IEEE International Symposium on Industrial Electronics*, 2008.

[13] P. McDaniel and S. McLaughlin, "Security and Privacy Challenges in the Smart Grid," *IEEE Security & Privacy,* vol. 7, no. 3, pp. 75 - 77, 2009.

[14] M. Amin, "Challenges in reliability, security, efficiency, and resilience of energy infrastructure: Toward smart self-healing electric power grid," in *2008 IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century*, 2008.

[15] A. Cardenas and R. Safavi-Naini, "Security and Privacy in the Smart Grid," in *Handbook on Securing Cyber-Physical Critical Infrastructure*, 2012, pp. 637-654.

[16] U. S. G. A. Office, "ELECTRICITY GRID MODERNIZATION: Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed," 2011. [Online]. Available: https://www.gao.gov/new.items/d11117.pdf.

[17] F. Aloul, A. R. Al-Ali, R. Al-Dalky, M. Al-Mardini and W. El-Hajj, "Smart Grid Security: Threats, Vulnerabilities and Solutions," *International Journal of Smart Grid and Clean Energy,* vol. 1, no. 1, 2012.

[18] W. Wang and Z. Lu, "Cyber security in the Smart Grid: Survey and challenges," *Computer Networks,* vol. 57, no. 5, pp. 1344-1371, 2013.

[19] R. K. Pandey and M. Misra, "Cyber Security Threats - Smart Grid Infrastructure," in *2016 National Power Systems Conference*, 2016.

[20] V. Lamba, N. Šimková and B. Rossi, "Recommendations for smart grid security risk," *Cyber-Physical Systems,* vol. 5, no. 2, p. 92–118, 2019.

[21] E. McCary and Y. Xiao, "Smart Grid Attacks and Countermeasures," *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems,* vol. 2, no. 2, 2015.

[22] A. Dagoumas, "Assessing the Impact of Cybersecurity Attacks on Power Systems," *Energies,* 2019.

[23] A. Hansen, J. Staggs and S. Shenoi, "Security analysis of an advanced metering infrastructure," *International Journal of Critical Infrastructure Protection,* vol. 18, pp. 3-19, 2017.

[24] Y. Mo, T. H.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig and B. Sinopoli, "Cyber–Physical Security of a Smart Grid Infrastructure," *Proceedings of the IEEE,* vol. 100, no. 1, pp. 195 - 209, 2012.

[25] A. O. Otuoze, M. W. Mustafa and R. M. Larik, "Smart grids security challenges: Classification by sources of threats," *Journal of Electrical Systems and Information Technology,* vol. 5, no. 3, pp. 468-483, 2018.

[26] D. Wei, Y. Lu, M. Jafari, P. Skare and K. Rohde, "An integrated security system of protecting Smart Grid against cyber attacks," in *2010 Innovative Smart Grid Technologies*, 2010.

[27] J. Liu, Y. Xiao, W. L. S. Li and C. L. P. Chen, "Cyber Security and Privacy Issues in Smart Grids," *IEEE Communications Surveys & Tutorials,* vol. 14, no. 4, pp. 981 - 997, 2012.

[28] A. R. Metke and R. L. Ekl, "Security Technology for Smart Grid Networks," *IEEE Transactions on Smart Grid,* vol. 1, no. 1, pp. 99 - 107, 2010.

[29] S. Zhongwei, H. Sitian, M. Yaning and S. Fengjie, "Security mechanism for smart distribution grid using Ethernet Passive Optical Network," in *2010 2nd International Conference on Advanced Computer Control*, 2010.

[30] U.S. Department of Energy Office of Electricity Delivery and Energy Reliability, "Study of security attributes of smart Attributes of Smart Grid Systems – Current Cyber Security Issues," 2009. [Online]. Available: https://www.hsdl.org/?abstract&did=15524.

[31] V. O. K. Li, F. F. Wu and J. Zhong, "Communication Requirements for Risk-Limiting Dispatch in Smart Grid," in *Communication Requirements for Risk-Limiting Dispatch in Smart Grid*, 2010.

[32] F. Alsiherov and T. Kim, "Secure SCADA Network Technology and Methods," in *Proceedings of the 12th WSEAS International Conference on AUTOMATIC CONTROL, MODELLING & SIMULATION*, 2010.

[33] M. Kezunovic, "Automated fault analysis in a smart grid," in *2009 Transmission & Distribution Conference & Exposition: Asia and Pacific*, 2009.

[34] S. D. Warren and L. D. Brandeis, "Harvard Law Review: The Right to Privacy," 1890. [Online]. Available: http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm.

[35] R. Clarke, "What's Privacy?," 2006. [Online]. Available: http://www.rogerclarke.com/DV/Privacy.html.

[36] F. Siddiqui, S. Zeadally, C. Alcaraz and S. Galvao, "Smart Grid Privacy: Issues and Solutions," in *2012 21st International Conference on Computer Communications and Networks*, 2012.

[37] M. AmineFerrag, L. A.Maglaras, HelgeJanicke, J. Jiang and LeiShu, "A systematic review of data protection and privacy preservation schemes for smart grid communications," *Sustainable Cities and Society,* vol. 38, pp. 806-835, 2018.

[38] L. R. Knudsen and V. Rijmen, "Known-Key Distinguishers for Some Block Ciphers," in *A Simple Variant of the Merkle-Damgård Scheme with a Permutation*, 2007, pp. 315-324.

[39] S. Blake-Wilson and A. Menezes, "Unknown Key-Share Attacks on the Station-to-Station (STS) Protocol," in *Second International Workshop on Practice and Theory in Public Key Cryptography*.

[40] F. G. Mármol, C. Sorge, O. Ugus and G. M. Pérez, "Do not snoop my habits: preserving privacy in the smart grid," *IEEE Communications Magazine,* vol. 50, no. 5, pp. 166 - 172, 2012.

[41] N. Saxena, B. J. Choi and R. Lu, "Authentication and Authorization Scheme for Various User Roles and Devices in Smart Grid," *IEEE Transactions on Information Forensics and Security,* vol. 11, no. 5, pp. 907 - 921, 2016.

[42] B. Wu, J. Chen and J. W. Cardei, "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks," in *Wireless Network Security*, 2007, pp. 103-135.

[43] W. Jia, H. Zhu, Z. Cao, X. Dong and C. Xiao, "Human-Factor-Aware Privacy-Preserving Aggregation in Smart Grid," *IEEE Systems Journal,* vol. 8, no. 2, pp. 598 - 607, 2014.

[44] J. F. Barrera, C. Vargas, M. Tebaldi and R. Torroba, "Chosen-plaintext attack on a joint transform correlator encrypting system," *Optics Communications,* vol. 283, no. 20, pp. 3917-3921, 2010.

[45] R. Canetti, S. Halevi and J. Katz, "Chosen-Ciphertext Security from Identity-Based Encryption," in *Advances in Cryptology - EUROCRYPT 2004*, 2004, pp. 207-222.

[46] M. Conti, P. Gasti and M. Teoli, "A lightweight mechanism for detection of cache pollution attacks in Named Data Networking," *Computer Networks,* vol. 57, no. 16, pp. 3178-3191, 2013.

[47] M. Conti, N. Dragoni and V. Lesyk, "A Survey of Man In The Middle Attacks," *IEEE Communications Surveys & Tutorials,* vol. 18, no. 3, pp. 2027 - 2051, 2016.

[48] C. Lai, H. Li, R. Lu, R. Jiang and X. Shen, "LGTH: A lightweight group authentication protocol for machine-type communication in LTE networks," in *2013 IEEE Global Communications Conference*, 2013.

[49] E. Ayday, "Secure, intuitive and low-cost device authentication for Smart Grid networks," in *2011 IEEE Consumer Communications and Networking Conference*, 2011.

[50] M. Pazos-Revilla, M. Baza, M. Nabil and A. Sherif, "Privacy-Preserving and Collusion-Resistant Charging Coordination Schemes for Smart Grid," 2019. [Online]. Available: https://arxiv.org/pdf/1905.04666.pdf.

[51] R. Leszczyna, "Cybersecurity and privacy in standards for smart grids – A comprehensive survey," *Computer Standards & Interfaces,* vol. 56, pp. 62-73, 2018.

[52] IEC, "IEC/TS 62351-1: Power systems management and associated information exchange - Data and communications security - Part 1: Communication network and system security - Introduction to security issues," 2007. [Online]. Available: https://webstore.iec.ch/publication/6903.

[53] North American Electric Reliability Corporation, "NERC CIP Standards," 2013. [Online]. Available: https://www.symantec.com/content/en/us/enterprise/other_resources/b-nerc_cyber_sercurity_standard_21171699.en-us.pdf.

[54] NRC, "NRC RG 5.71 Cyber Security Programs for Nuclear Facilities," 2008. [Online]. Available: https://www.nrc.gov/docs/ML0903/ML090340159.pdf.

[55] DOE, NIST, NERC, "Electricity Subsector Cybersecurity Risk Management Process," 2012. [Online]. Available: https://www.energy.gov/ceser/downloads/cybersecurity-risk-management-process-rmp-guideline-final-may-2012.

[56] DoE, "Energy Infrastructure Risk Management Checklists for Small and Medium Sized Energy Facilities," 2002. [Online]. Available: https://www.hsdl.org/?view&did=446053.

[57] IEC, "IEC TR 62541-2:2016 OPC unified architecture - Part 2: Security Model," 2016. [Online]. Available: https://webstore.iec.ch/preview/info_iec62541-2%7Bed2.0%7Den.pdf.

[58] F. Baker and D. Meyer, "RFC 6272 – Internet protocols for the smart grid," 2011. [Online]. Available: https://tools.ietf.org/html/rfc6272.

[59] IEEE, "1686-2007 - IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities," 2007. [Online]. Available: https://ieeexplore.ieee.org/document/4453853.

[60] IEEE, "C37.240-2014 - IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems," 2014. [Online]. Available: https://ieeexplore.ieee.org/document/7024885.

[61] IEEE, "1402-2000 - IEEE Guide for Electric Power Substation Physical and Electronic Security," 2000. [Online]. Available: https://ieeexplore.ieee.org/document/836296.

[62] ISA, "ISA99, Industrial Automation and Control Systems Security," 2017. [Online]. Available: https://www.isa.org/isa99/.

[63] ISO/IEC, "ISO/IEC TR 27019:2013: Information technology — Security techniques — Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry," 2013. [Online]. Available: https://www.iso.org/standard/43759.html.

[64] NIST, "NIST SP 800-82 Guide to Industrial Control Systems (ICS) Security Revision 2," 2015. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf.

[65] DHS, "Recommendations for Standards Developers," 2010. [Online]. Available: https://www.us-cert.gov/sites/default/files/documents/CatalogofRecommendationsVer7.pdf.

[66] DHS, "Cyber Security Procurement Language for Control Systems Version 1.8," 2008. [Online]. Available: https://www.hsdl.org/?abstract&did=465486.

[67] Advanced Security Acceleration Project, "Security Profile for Advanced Metering Infrastructure," 2010.

[68] Netbeheer Nederland, "Privacy and Security of the Advanced," 2010. [Online]. Available: https://www.smart-energy.com/regional-news/europe-uk/ami-security-and-privacy-requirements-released-in-netherlands/.

[69] AMI-SEC Task Force, "AMI System Security Requirements v1.01," 2008. [Online]. Available: https://www.smartgrid.gov/files/AMI_System_Security_Requirements_200808.pdf.

[70] IEC, "IEC 62056-5-3:2016 Electricity metering data exchange - The DLMS/COSEM suite - Part 5-3: DLMS/COSEM application layer," 2016. [Online]. Available: https://webstore.iec.ch/p-preview/info_iec62056-5-3%7Bed2.0%7Db.pdf.

[71] VGB, "VGB-S 175 – IT Security for Generating Plants," 2014. [Online]. Available: https://www.vgb.org/shop/s-175e-ebook.html.

[72] IEC, "IEC 61400-25-3:2015: Wind turbines - Part 25-3: Communications for monitoring and control of wind power plants - Information exchange models," 2015. [Online]. Available: https://webstore.iec.ch/preview/info_iec61400-25-3%7Bed2.0%7Db.pdf.

[73] IEEE Standards Coordinating Committee 21, "IEEE Guide for the Interoperability of Energy Storage Systems Integrated with the Electric Power Infrastructure," 2015. [Online]. Available: https://ieeexplore.ieee.org/document/7140715.

[74] ISO, "ISO 15118-2:2014 Road vehicles – Vehicle-to-Grid Communication Interface – Part 2: Network and application protocol," 2014. [Online]. Available: https://www.iso.org/standard/55366.html.

[75] ISO/IEC, "ISO/IEC 14543-5-1:2010: nformation technology — Home electronic system (HES) architecture — Part 5-1: Intelligent grouping and resource sharing for Class 2 and Class 3 — Core protocol," 2010. [Online]. Available: https://www.iso.org/standard/44391.html.

[76] ISO/IEC, "ISO/IEC 14543-5-7:2015: Information technology — Home electronic system (HES) architecture — Part 5-7: Intelligent grouping and 3 resource sharing — Remote access system architecture," 2015. [Online]. Available: https://www.iso.org/standard/64274.html.

[77] ISO/IEC, "ISO/IEC 27000-series," [Online]. Available: https://en.wikipedia.org/wiki/ISO/IEC_27000-series.

[78] ISO/IEC, "ISO/IEC 27001:2013: Information technology — Security techniques — Information security management systems — Requirements," 2013. [Online]. Available: https://www.iso.org/standard/54534.html.

[79] ISO/IEC, "ISO/IEC 27002:2013: Information technology — Security techniques — Code of practice for information security controls," 2013. [Online]. Available: https://www.iso.org/standard/54533.html.

[80] NIST, "NIST SP 800-53 Rev. 4 Recommended Security Controls for Federal Information Systems and Organizations," 2013. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

[81] GB/T, "GB/T 22239:2008 – Information Security Technology – Baseline for Classified Protection of Information System Security," 2008. [Online]. Available: https://www.chinesestandard.net/PDF/Sample.aspx/GBT22239-2008.

[82] ISO/IEC, "ISO/IEC 27005:2011: Information technology — Security techniques — Information security risk management," 2011. [Online]. Available: https://www.iso.org/standard/56742.html.

[83] ISO/IEC, "ISO/IEC 15408-1:2009: Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model," 2009. [Online]. Available: https://www.iso.org/standard/50341.html.

[84] ISO/IEC, "ISO/IEC 18045:2008: Information technology — Security techniques — Methodology for IT security evaluation," 2008. [Online]. Available: https://www.iso.org/standard/46412.html.

[85] GB/T 20279, "GB/T 20279-2015 – Information Security Technology – Security Technical Requirements of Network and Terminal Separation Products," 2015. [Online]. Available: https://www.chinesestandard.net/PDF/English.aspx/GBT20279-2015.

[86] ISO/IEC, "ISO/IEC 19790:2012: Information technology — Security techniques — Security requirements for cryptographic modules," 2012. [Online]. Available: https://www.iso.org/standard/52906.html.

[87] NIST, "NIST SP 800-64 Rev. 2 Security Considerations in the System Development Life Cycle," 2008. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-64r2.pdf.

[88] NIST, "NIST SP 800-124 Rev. 1 - Guidelines for Managing the Security of Mobile Devices in the Enterprise," 2013. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf.

[89] ISO/IEC, "ISO/IEC 15408-2:2008: Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components," 2008. [Online]. Available: https://www.iso.org/standard/46414.html.

[90] S. Sridhar, A. Hahn and M. Govindarasu, "Cyber–Physical System Security for the Electric Power Grid," *Proceedings of the IEEE,* vol. 100, no. 1, pp. 210 - 224, 2012.

[91] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS Defense mechanisms," *ACM SIGCOMM Computer Communication Review,* vol. 34, no. 2, pp. 39-54, 2004.

[92] Z. E. Mrabet, N. Kaabouch, H. E. Ghazi and H. E. Ghazi, "Cyber-security in smart grid: Survey and challenges," *Computers & Electrical Engineering,* vol. 67, pp. 469-482, 2018.

[93] Y. Yan, Y. Qian, H. Sharif and D. Tipper, "A Survey on Cyber Security for Smart Grid Communications," *IEEE Communications Surveys & Tutorials,* vol. 14, no. 4, pp. 998 - 1010, 2012.

[94] A. R. Metke and R. L. Ekl, "Security Technology for Smart Grid Networks," *IEEE Transactions on Smart Grid,* vol. 1, no. 1, pp. 99 - 107, 2010.