



**ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ**

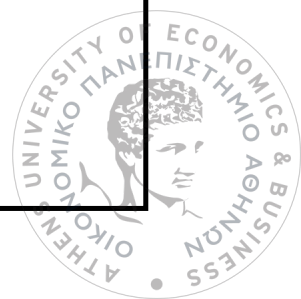
**ΜΕΤΑΠΤΥΧΙΑΚΟ ΔΙΠΛΩΜΑ ΕΙΔΙΚΕΥΣΗΣ (MSc)
στα ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ**

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«Αισθητήρες σε έξυπνα δίκτυα ηλεκτρικής ενέργειας»

**Δάλλας Κωνσταντίνος
MM4110008**

ΑΘΗΝΑ, ΣΕΠΤΕΜΒΡΙΟΣ 2013





**ΜΕΤΑΠΤΥΧΙΑΚΟ ΔΙΠΛΩΜΑ ΕΙΔΙΚΕΥΣΗΣ (MSc)
στα ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ**

**ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ
MASTER THESIS**

**«Αισθητήρες σε έξυπνα δίκτυα ηλεκτρικής ενέργειας»
«Sensors in smart grids»**

**Δάλλας Κωνσταντίνος
MM4110008**

**Επιβλέπων Καθηγητής: Αποστολόπουλος Θεόδωρος
Εξωτερικός Κριτής: Πραματάρη Αικατερίνη**

**ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ**

ΑΘΗΝΑ, ΣΕΠΤΕΜΒΡΙΟΣ 2013





Table of Contents

Table of Contents	5
Abstract.....	6
Περίληψη	12
Chapter 1: Introduction to electrical grids and the Smart Grid.....	19
1.1 Introduction	19
1.2 Brief History.....	19
1.3 Characteristics of Electrical Energy	20
1.4 How the electricity grid works	34
1.5 Limitations and problems.....	39
1.6 The Smart Grid.....	44
1.7 The importance of measurements.....	45
1.8 Security	46
1.9 Structure of this study	47
Chapter 2: The need for measurements	48
2.1 Reasons to make measurements.	48
2.2 Sensors, sensor networks and their usage in Smart Grids	58
2.3 Data characteristics and utilization.....	75
Chapter 3: Security of the Smart Grid.....	81
3.1 General issues of security in the Smart Grid.....	81
3.2 A bottom-up system security approach: identifying targets and consequences.....	88
3.3 Solutions, countermeasures and general guidelines	100
Chapter 4 : Smart Grid implementations.....	106
4.1 Case studies	106
4.2 Conclusions	113
Definitions – Acronyms.....	115
Bibliography	118



Abstract

This master thesis analyzes the usage, necessity and effects of sensors in modern smart electrical grids, emphasizing on security issues that arise. It is comprised of four chapters. The first chapter provides a mathematical background and deals with the characteristics, the functionality, the limitations and the future form of electricity grids. The second chapter presents the reasons behind the growing need for measurements, the usage of sensors in Smart grids and the qualities and usage of the produced data. The third chapter discusses general issues of security, provides a bottom-up security approach and presents solutions and security guidelines. The fourth chapter records some case studies of Smart Grid implementations from all over the world and presents overall conclusions.

Electricity, the greatest scientific achievement of the nineteenth century, was shaped to its current form by economic, political, social, and environmental factors. Faraday and Tesla were the pioneers that made large scale electricity production possible. Electric companies grew and generating facilities were interconnected to a common transmission network, thus making the grid more reliable and efficient.

The most important characteristics of electrical systems are voltage, current, impedance, power and the power factor. We are mostly concerned with electric power in a power system rather than the currents and voltages. Cosine waveforms and rotating vector diagrams are used when representing time alternating values like ac voltage. Electrical power is a complex quantity and is divided in active (real part) and reactive (imaginary part). The active power is the useful power, while the reactive does not provide any work and should be kept at lowest levels possible. The apparent or complex power is the product of the current and voltage of a circuit. The power factor is a measure of quality of the transported power. Three-phase systems are preferred over single-phase due to their ability to produce constant power and not pulsating. The per unit system was invented to simplify calculations over multiple voltage levels throughout the grid. In this system, electrical quantities are expressed as fractions of a defined base unit quantity.



An interconnected classical power system can be divided into the generation, transmission, distribution and utilization subsystems. The generation includes generators, mostly synchronous ac three-phase motors, and transformers. The transmission network transfers electric power from the generating facilities to the distribution over elevated power lines (overhead transmission) or underground cables. The part from the distribution substations to the consumer's service entrance equipment composes the distribution, while the loads of the power system in general are referred to as the utilization. The power demand varies throughout the day and can be represented with a daily demand curve diagram. The efficiency of a generating plant is assessed by the load factor, the ratio of average load over a designated period of time to the peak load occurring in that period.

Electrical power systems currently have many problems and limitations. Electricity is difficult to be stored in large scale, thus the supply of power should be continuously adjusted to balance the varying demand. Regional and national power grids are interconnected to national and international level while their supervision and control is broken down to many stakeholders due to the de-regulation. The electrical power flows to all points of a power grid and the effects of a change in transmission or generation are propagated to the whole grid and cannot be easily anticipated or controlled. The extension of transmission lines makes power delivery inefficient, while the quality of power must be maintained at high levels or else instabilities arise that could lead to blackouts.

New and efficient technologies will be introduced to resolve these problems by transforming the current electrical grids into Smart Grids. Many different definitions of the term 'smart grid' have been given worldwide. The most inclusive one is that a Smart Grid is a next-generation network that integrates communication and information technology into the existing power grid to optimize energy efficiency. Sensing and measurements are the cornerstones of this transformation, while security concerns are raised along the way.



The most important reasons to deploy sensors and take measurements in a Smart Grid are of technical - environmental and economical nature. Technical and environmental reasons include resilience and reliability, security, efficiency and the integration of emerging technologies. Resilience, the capability to withstand and recover from unpredicted actions, will be provided by sensors spread in all parts and subsystems of the grid that report their values in real-time. Security, both physical and cyber, is enforced by monitoring sensors. Greater efficiency is accomplished by measuring the qualitative characteristics of the flowing electrical power and making real-time adjustments to the grid. Integration of renewable technologies and reduction of greenhouse and toxic gas emissions is realized by being able to predict and control their fluctuating power output with the help of grid and weather sensors. Economical reasons include the elimination of the grid's over-dimensioning by reducing peaking units, the adoption of Demand Side Management, by leveraging the Advanced Metering Infrastructure and smart appliances, and the integration of cheaper, renewable resources.

Sensors are devices that measure a physical property by responding to a physical stimulus and convert it into an electrical signal. They can be categorized into active and passive, depending on their power source and into wireless and satellite, wired, optical fiber and hybrid, depending on their way of communication. They can also be grouped according to their placement inside the Smart Grid's systems to: generation, transmission, distribution and utilization system sensors. Sensors in generation are utilized by PLCs, G-SCADA and HMI systems. Sensors in transmission are used by T-SCADA, PMUs, EMS, line protection and monitoring systems. The distribution system encompasses field sensors, D-SCADA, DMS, field controllers, devices and meters forming the AMI. The utilization system takes advantage of various technologies with built-in sensing capabilities like HANs, HEMS, IHDs and BMS.

A Smart Grid can be divided into three layers, where each layer is composed of digital and non-digital technologies and systems from the domains of telecommunication, information, and energy technology. It can be viewed as an additional communication layer that is virtually overlaid on to the existing power grid and on which an application layer is built. This layered approach reduces the complexity, by creating independent components and subcomponents, leading to the creation of a system of systems.



A communication layer lies on top of the power layer but, currently, there is no end-to-end communication available because there is a communications gap between customers' premises and the rest of the components and actors in the energy chain. The AMI, or FAN, will bridge this gap by linking the existing utilities' communication networks with smart meters. Smart meter data are needed mainly by ESPs to provide innovative, value added services like sending price signals to consumers, controlling appliances and changing tariffs.

The data exchanged through Smart Grid communication systems have different behavioral characteristics, regarding the network's Quality of Service potential and can be categorized in various classes according to specific attributes. Other important aspects of the data that is generated are: its increasing volume, the preservation of consumer's and businesses' privacy and the cost effectiveness. The power grid constitutes a primary, critical infrastructure for a country, whereas its growing dependency on ICT brings along new threats and risks. Threats can be divided in intentional and unintentional. Unintentional threats can come from human-originated factors or from natural phenomena. Vulnerabilities inherited from the Smart Grid's composing elements also present a danger for security. Intentional human threats constitute a smaller threat to the power grid in total, for the time being, but are expected to increase dramatically. The capabilities of attackers have evolved and the motives behind their actions include: curiosity, notoriety, revenge or extortion, financial gain, terrorism and cyber electronic warfare. Data privacy is also a major security concern, with private data used by utilities and third parties to further increase profits.



An effort to provide a bottom-up security approach is attempted by examining the security of each individual system of the Smart Grid. The possible targets of the generation system are the individual PLCs, the SCADA systems, the HMI and the network infrastructure, with the latter posing as the greater risk. Possible targets in transmission infrastructure include: the T-SCADA and substation automation systems, the PMUs and PDCs, the line protection systems and the transformers. Here, the T-SCADA gateway serves as the most appealing target to attack. Possible targets in distribution infrastructure include: the D-SCADA and DMS systems, the field controllers, the automated field devices and the AMI. Smart meters pose a small security risk to the grid, if compromised individually, but a greater one if compromised massively. The control room is the heart of the grid's IT infrastructure and although it is well secured, faces serious emerging threats due to the interconnection with the internet.

The Smart Grid requires the highest levels of security through a continuous and standardized process. Best practices from around the world, issued by renowned organizations, are used to achieve the most important objectives: availability of the power service, integrity of the communicated data and confidentiality of the exchanged information. The best practices include: identifying what systems need to be protected, separating the systems logically into functional groups, implementing a defense-in-depth strategy around each system and controlling access into and between each group. Other practical security solutions are: the adoption of devices that have improved communication, encryption and update capabilities, the active participation and team work of all stakeholders and the use of PKI and strong encryption protocols. Smart Grid realization attempts have started throughout the globe via slow and costly upgrades of the current grids' infrastructure. The costs are enormous, so governmental support is inevitable. Italy pioneered in implementing Smart Grid technology with a project that began in 2001 by Enel. Other implementation efforts started in 2008 like in Texas, USA by Austin Energy and in Colorado by Excel Energy. The Consolidated Edison Company of New York received one of the biggest federal grants so far. Most projects include the wide deployment of smart meters which is expected to increase profits and reliability. Other attempts, worth mentioning, were made in Ontario, Canada by HydroOne, in Sacramento, USA by Municipal Utility District and in Australia by EnergyAustralia.





Περίληψη

Στην παρούσα διπλωματική εργασία αναλύεται η χρήση, η χρησιμότητα και οι επιδράσεις που έχουν οι αισθητήρες σε σύγχρονα δίκτυα ηλεκτρικής ενέργειας, με έμφαση στα ζητήματα ασφάλειας που ανακύπτουν. Η εργασία αποτελείται από τέσσερα κεφάλαια. Στο πρώτο κεφάλαιο παρέχεται το μαθηματικό υπόβαθρο και αναλύονται τα χαρακτηριστικά, η λειτουργία, οι περιορισμοί και η μελλοντική μορφή των δικτύων ηλεκτρικής ενέργειας. Στο δεύτερο κεφάλαιο παρουσιάζονται οι αιτίες πίσω από την αυξανόμενη ανάγκη για μετρήσεις, η χρήση αισθητήρων σε έξυπνα δίκτυα ηλεκτρικής ενέργειας και τα ποιοτικά χαρακτηριστικά και η χρήση των παραγόμενων δεδομένων. Στο τρίτο κεφάλαιο συζητούνται γενικά θέματα ασφάλειας, παρέχεται μια θεώρηση της ασφάλειας από κάτω προς τα πάνω και παρουσιάζονται λύσεις και γενικές κατευθύνσεις στην ασφάλεια. Στο τέταρτο κεφάλαιο καταγράφονται μερικές περιπτώσεις εγκαταστάσεων έξυπνων δικτύων ηλεκτρικής ενέργειας από όλο τον κόσμο και παρουσιάζονται τα γενικά συμπεράσματα.

Ο ηλεκτρισμός, το μεγαλύτερο επιστημονικό επίτευγμα του δέκατου ένατου αιώνα, διαμορφώθηκε στη σημερινή του μορφή από οικονομικούς, πολιτικούς, κοινωνικούς, και περιβαλλοντικούς παράγοντες. Ο Faraday και ο Tesla ήταν οι πρωτοπόροι που έκαναν δυνατή την παραγωγή ηλεκτρικής ενέργειας σε μεγάλη κλίμακα. Οι εταιρίες ηλεκτρισμού μεγάλωσαν και οι εγκαταστάσεις παραγωγής διασυνδέθηκαν σε ένα κοινό δίκτυο μεταφοράς, καθιστώντας έτσι το δίκτυο πιο αξιόπιστο και αποτελεσματικό.



Τα σημαντικότερα χαρακτηριστικά των ηλεκτρικών συστημάτων είναι η τάση, το ρεύμα, η αντίσταση, η ισχύς και ο συντελεστής ισχύος. Σε ένα ηλεκτρικό σύστημα μας ενδιαφέρει κυρίως η ηλεκτρική ισχύς παρά τα ρεύματα και οι τάσεις. Συνημιτονοειδείς κυματομορφές και διαγράμματα στρεφόμενων διανυσμάτων χρησιμοποιούνται για να αναπαραστήσουν χρονικά μεταβαλλόμενες τιμές όπως η εναλλασσόμενη ac τάση. Η ισχύς είναι μια σύνθετη ποσότητα και χωρίζεται σε ενεργό (πραγματικό μέρος) και άεργο (φανταστικό μέρος). Η ενεργός ισχύς είναι η χρήσιμη ισχύς, ενώ η άεργος δεν παράγει έργο και θα πρέπει να διατηρείται σε όσο το δυνατόν χαμηλότερα επίπεδα. Η φαινόμενη ή σύνθετη ισχύς είναι το γινόμενο του ρεύματος και της τάσης ενός κυκλώματος. Ο συντελεστής ισχύος είναι ένα μέτρο της ποιότητας της μεταφερόμενης ισχύος. Τα τριφασικά συστήματα προτιμώνται έναντι των μονοφασικών χάρη στην ικανότητά τους να παράγουν σταθερή ισχύ και όχι μεταβαλλόμενη. Το ανά μονάδα σύστημα επινοήθηκε για να απλοποιήσει τους υπολογισμούς όταν υπάρχουν πολλαπλά επίπεδα τάσης κατά μήκος του δικτύου. Σε αυτό το σύστημα, οι ηλεκτρικές ποσότητες εκφράζονται ως κλάσματα μιας καθορισμένης ποσότητας μονάδας βάσης.

Ένα κλασικό, διασυνδεδεμένο σύστημα ηλεκτρικής ισχύος μπορεί να χωριστεί στα επιμέρους υποσυστήματα: παραγωγής, μετάδοσης, διανομής και χρήσης (κατανάλωσης). Το υποσύστημα παραγωγής περιλαμβάνει γεννήτριες, ως επί το πλείστον σύγχρονους ac τριφασικούς κινητήρες, και μετασχηματιστές. Το δίκτυο μεταφοράς μεταφέρει ηλεκτρική ενέργεια από τις εγκαταστάσεις παραγωγής προς τη διανομή πάνω από υπερυψωμένες γραμμές ηλεκτρικού ρεύματος (εναέρια μετάδοση) ή υπόγεια καλώδια. Το κομμάτι από τους υποσταθμούς διανομής έως τον εξοπλισμό του καταναλωτή συνθέτει τη διανομή, ενώ τα φορτία του συστήματος ηλεκτρικής ενέργειας σε γενικές γραμμές αναφέρονται ως η χρήση. Η ζήτηση ενέργειας διαφέρει κατά τη διάρκεια της ημέρας και μπορεί να αναπαρασταθεί με ένα ημερήσιο διάγραμμα καμπύλης ζήτησης. Η αποδοτικότητα μιας μονάδας παραγωγής αξιολογείται από τον συντελεστή φορτίου, ο λόγος του μέσου φορτίου σε ένα καθορισμένο χρονικό διάστημα προς το φορτίο αιχμής που παρατηρείται στην εν λόγω περίοδο.



Τα σημερινά συστήματα ηλεκτρικής ισχύος παρουσιάζουν πολλά προβλήματα και περιορισμούς. Η ηλεκτρική ενέργεια είναι δύσκολο να αποθηκευτεί σε μεγάλη κλίμακα, οπότε η παροχή ισχύος θα πρέπει διαρκώς να προσαρμόζεται στην μεταβαλλόμενη ζήτηση. Τα περιφερειακά και εθνικά δίκτυα ενέργειας διασυνδέονται σε εθνικό και διεθνές επίπεδο, ενώ η εποπτεία και ο έλεγχός τους είναι καταναμημένα σε πολλούς ενδιαφερόμενους οργανισμούς, λόγω της απελευθέρωσης της αγοράς. Η ηλεκτρική ισχύς ρέει σε όλα τα σημεία του δικτύου ηλεκτρικής ενέργειας και οι συνέπειες μιας αλλαγής στη μετάδοση ή την παραγωγή διαδίδονται στο σύνολο του δικτύου και δεν μπορούν να προβλεφθούν εύκολα ή να ελεγχθούν. Η επέκταση των γραμμών μεταφοράς κάνει την παροχή ισχύος μη αποδοτική, ενώ η ποιότητα του ηλεκτρισμού πρέπει να διατηρείται σε υψηλά επίπεδα ειδάλλως προκύπτουν αστάθειες που μπορούν να οδηγήσουν σε εκτεταμένες διακοπές ρεύματος.

Νέες και αποτελεσματικές τεχνολογίες θα εισαχθούν για την επίλυση αυτών των προβλημάτων με τον μετασχηματισμό των υφιστάμενων ηλεκτρικών δικτύων σε Smart Grids (έξυπνα δίκτυα ηλεκτρικής ενέργειας). Πολλοί διαφορετικοί ορισμοί του « έξυπνου δικτύου » έχουν δοθεί παγκοσμίως. Η πιο περιεκτική είναι ότι ένα Smart Grid είναι ένα δίκτυο νέας γενιάς, που ενσωματώνει τις επικοινωνίες και την τεχνολογία πληροφορικής στο υπάρχον δίκτυο ηλεκτρικής ενέργειας για τη βελτιστοποίηση της ενεργειακής απόδοσης. Οι αισθητήρες και οι μετρήσεις είναι οι ακρογωνιαίοι λίθοι αυτού του μετασχηματισμού, ενώ ανησυχίες για την ασφάλεια εγείρονται κατά μήκος της διαδρομής προς τον μετασχηματισμό αυτό.



Οι πιο σημαντικοί λόγοι για την ανάπτυξη αισθητήρων και τη λήψη μετρήσεων σε ένα Smart Grid είναι τεχνικοί - περιβαλλοντικοί και οικονομικής φύσεως. Οι τεχνικοί και περιβαλλοντικοί λόγοι περιλαμβάνουν την ελαστικότητα και την αξιοπιστία, την ασφάλεια, την αποδοτικότητα και την ενσωμάτωση νέων τεχνολογιών. Ελαστικότητα, η ικανότητα ενός συστήματος να αντέχει σε απρόβλεπτες ενέργειες και να επανακτά την πρότερη του κατάσταση, θα παρέχεται από αισθητήρες καταναμημένους σε όλα τα μέρη και τα υποσυστήματα του δικτύου που θα αναφέρουν τις τιμές τους σε πραγματικό χρόνο. Η ασφάλεια, τόσο φυσική όσο και στον κυβερνοχώρο, ενδυναμώνεται από αισθητήρες παρακολούθησης. Η μεγαλύτερη αποδοτικότητα επιτυγχάνεται με τη μέτρηση των ποιοτικών χαρακτηριστικών της ρέοντος ηλεκτρικής ενέργειας και κάνοντας προσαρμογές στο δίκτυο σε πραγματικό χρόνο. Η ενσωμάτωση τεχνολογιών ανανεώσιμων πηγών ενέργειας και η μείωση των εκπομπών αερίων του θερμοκηπίου και τοξικών αερίων πραγματοποιείται με το να γίνεται εφικτό να προβλεφθεί και να ελεγχθεί η κυμαινόμενη ισχύ τους με τη βοήθεια αισθητήρων ηλεκτρικού δικτύου και καιρικών συνθηκών. Οι οικονομικοί λόγοι περιλαμβάνουν την κατάργηση της υπερ-διαστασιολόγησης του δικτύου, μειώνοντας μονάδες φορτίου αιχμής, υιοθετώντας την Διαχείριση της Ζήτησης (DSM), χρησιμοποιώντας Προηγμένες Υποδομές Μέτρησης (AMI) και έξυπνες συσκευές, καθώς και την ενσωμάτωση φθηνότερων, ανανεώσιμων πηγών ενέργειας.

Οι αισθητήρες είναι συσκευές που μετρούν μια φυσική ιδιότητα αντιδρώντας σε ένα φυσικό ερέθισμα και μετατρέποντας το σε ένα ηλεκτρικό σήμα. Μπορούν να κατηγοριοποιηθούν σε ενεργητικούς και παθητικούς, ανάλογα με την πηγή τροφοδοσίας τους και σε ασύρματους και δορυφορικούς, ενσύρματους, οπτικής ίνας και υβριδικούς, ανάλογα με τον τρόπο επικοινωνίας τους. Μπορούν επίσης να ομαδοποιηθούν ανάλογα με την τοποθέτησή τους στα συστήματα του Smart Grid σε αισθητήρες: συστήματος παραγωγής, συστήματος μεταφοράς, συστήματος διανομής και συστήματος χρήσης. Οι αισθητήρες (συστήματος) παραγωγής χρησιμοποιούνται από τα PLC, G - SCADA και HMI συστήματα. Οι αισθητήρες μετάδοσης χρησιμοποιούνται από τα T - SCADA, PMUs, EMS, τα συστήματα προστασίας καλωδίων και από τα συστήματα παρακολούθησης. Το σύστημα διανομής περιλαμβάνει αισθητήρες στο πεδίο, D - SCADA συστήματα, DMS συστήματα, στους ελεγκτές πεδίου και στις συσκευές και στους μετρητές που αποτελούν το AMI. Το σύστημα χρήσης εκμεταλλεύεται διάφορες τεχνολογίες με ενσωματωμένες δυνατότητες ανίχνευσης όπως τα συστήματα HANs, HEMS, IHDs και BMS.



Ένα Smart Grid μπορεί να χωριστεί σε τρία στρώματα, όπου κάθε στρώμα αποτελείται από ψηφιακές και μη ψηφιακές τεχνολογίες και συστήματα από τους τομείς των τηλεπικοινωνιών, της πληροφορικής και της ενεργειακής τεχνολογίας. Μπορεί να θεωρηθεί ως ένα επιπλέον στρώμα επικοινωνίας που εικονικά επικαλύπτει το υπάρχον δίκτυο ηλεκτρικής ενέργειας και στο οποίο είναι χτισμένο ένα στρώμα εφαρμογών. Αυτή η στρωματοποιημένη προσέγγιση μειώνει την πολυπλοκότητα, δημιουργώντας ανεξάρτητα συστατικά και υπο-συστατικά στοιχεία, οδηγώντας στη δημιουργία ενός συστήματος συστημάτων.

Ένα στρώμα επικοινωνίας βρίσκεται πάνω από το στρώμα ισχύος αλλά, επί του παρόντος, δεν υπάρχει διαθέσιμη επικοινωνία από άκρη σε άκρη, επειδή υπάρχει ένα χάσμα επικοινωνίας μεταξύ των εγκαταστάσεων των πελατών και των υπόλοιπων συστατικών και φορέων της ενεργειακής αλυσίδας. Οι υποδομές AMI, ή FAN, θα γεφυρώσουν αυτό το χάσμα διασυνδέοντας τα δίκτυα επικοινωνίας των υφιστάμενων επιχειρήσεων ηλεκτρισμού με τους έξυπνους μετρητές. Τα δεδομένα από τους έξυπνους μετρητές απαιτούνται κυρίως από τους παρόχους ηλεκτρικής ενέργειας (ESPs) ούτως ώστε να παρέχουν καινοτόμες υπηρεσίες προστιθέμενης αξίας, όπως είναι η αποστολή σημάτων τιμών στους καταναλωτές, ο (απομακρυσμένος) έλεγχος των συσκευών και η αλλαγή των τιμολογίων.

Τα δεδομένα που ανταλλάσσονται μέσω των συστημάτων επικοινωνίας των Smart Grids έχουν διαφορετική συμπεριφορά, όσον αφορά το δυναμικό της ποιότητας υπηρεσιών (QoS) του δικτύου και μπορούν να ταξινομηθούν σε διάφορες κατηγορίες βάσει συγκεκριμένων χαρακτηριστικών. Άλλες σημαντικές πτυχές των δεδομένων που παράγονται είναι: ο αυξανόμενος όγκος τους, η διατήρηση της ιδιωτικότητας του καταναλωτή και των επιχειρήσεων και η αποδοτικότητα/αποτελεσματικότητα κόστους.



Το δίκτυο ηλεκτρικής ενέργειας αποτελεί πρωταρχική, κρίσιμη υποδομή για μια χώρα, ενώ η αυξανόμενη εξάρτηση της από τις ΤΠΕ φέρνει μαζί νέες απειλές και κινδύνους. Οι απειλές μπορούν να χωριστούν σε εκούσιες και ακούσιες. Οι ακούσιες απειλές μπορεί να προέρχονται από ανθρώπινους παράγοντες ή από φυσικά φαινόμενα. Τα τρωτά σημεία που κληρονομούνται από τα συνθετικά στοιχεία του Smart Grid παρουσιάζουν επίσης έναν κίνδυνο για την ασφάλεια. Οι εσκεμμένες ανθρώπινες απειλές αποτελούν μικρότερη απειλή για το δίκτυο ηλεκτρικής ενέργειας, συνολικά, προς το παρόν αλλά αναμένονται να αυξηθούν δραματικά. Οι δυνατότητες των επιτιθέμενων έχουν εξελιχθεί και τα κίνητρα πίσω από τις ενέργειές τους περιλαμβάνουν: την περιέργεια, την απόκτηση φήμης, την εκδίκηση ή τον εκβιασμό, το οικονομικό όφελος, την τρομοκρατία και τον ηλεκτρονικό πόλεμο. Η προστασία των προσωπικών δεδομένων είναι επίσης μια σημαντική ανησυχία για την ασφάλεια, με τα προσωπικά δεδομένα να χρησιμοποιούνται από επιχειρήσεις ηλεκτρισμού και από τρίτα μέρη με σκοπό την περαιτέρω αύξηση των κερδών τους.

Μια προσπάθεια προσέγγισης της ασφάλειας ,από κάτω προς τα πάνω, επιχειρείται με την εξέταση της ασφάλειας του κάθε συστήματος του Smart Grid ξεχωριστά. Οι πιθανοί στόχοι (κυβερνοεπίθεσης) του συστήματος παραγωγής ηλεκτρικής ενέργειας είναι τα μεμονωμένα PLC, τα συστήματα SCADA , το HMI και οι υποδομές του δικτύου, που ενέχουν και τον μεγαλύτερο κίνδυνο (ρίσκο). Πιθανοί στόχοι στον τομέα των υποδομών μεταφοράς περιλαμβάνουν: τα T - SCADA και τα συστήματα αυτοματισμών υποσταθμού, τα PMUs και PDCs, τα συστήματα προστασίας γραμμής και οι μετασχηματιστές. Εδώ, η πύλη T - SCADA αποτελεί τον πιο ελκυστικό στόχο για μια επίθεση. Πιθανοί στόχοι στις υποδομές διανομής περιλαμβάνουν: τα D - SCADA και τα συστήματα DMS, οι ελεγκτές στο πεδίο, οι αυτοματισμοί στο πεδίο και οι AMI. Οι έξυπνοι μετρητές αποτελούν μικρό κίνδυνο για την ασφάλεια του δικτύου, εάν παραβιαστούν κατά μονάς, αλλά ένα μεγαλύτερο κίνδυνο, αν παραβιαστούν μαζικά. Η αίθουσα ελέγχου είναι η καρδιά της πληροφοριακής υποδομής της δικτύου και παρά το γεγονός ότι είναι καλά ασφαλισμένη, αντιμετωπίζει σοβαρά αναδυόμενες απειλές λόγω της διασύνδεσης της με το διαδίκτυο.



Το Smart Grid απαιτεί τα υψηλότερα επίπεδα ασφάλειας μέσω μιας συνεχούς και προτυποποιημένης διαδικασίας. Οι βέλτιστες πρακτικές από όλο τον κόσμο, που δημοσιεύονται από αναγνωρισμένους οργανισμούς, χρησιμοποιούνται για την επίτευξη των σημαντικότερων στόχων: τη διαθεσιμότητα της ενεργειακής εξυπηρέτησης, την ακεραιότητα των επικοινωνούμενων δεδομένων και την εμπιστευτικότητα των πληροφοριών που ανταλλάσσονται. Οι βέλτιστες πρακτικές περιλαμβάνουν: τον προσδιορισμό των συστημάτων που πρέπει να προστατευθούν, τον λογικό διαχωρισμό των συστημάτων σε λειτουργικές ομάδες, την υλοποίηση μιας στρατηγικής άμυνας σε βάθος, γύρω από κάθε σύστημα, και τον έλεγχο της πρόσβασης προς και μεταξύ κάθε ομάδας. Άλλες πρακτικές λύσεις ασφαλείας είναι: η υιοθέτηση των συσκευών που έχουν βελτιωμένες δυνατότητες επικοινωνίας, κρυπτογράφησης και ενημέρωσης, η ενεργός συμμετοχή και ομαδική δουλειά όλων των ενδιαφερομένων μερών και η χρήση της κρυπτογραφίας δημοσίου κλειδιού (PKI) και ισχυρών πρωτόκολλων κρυπτογράφησης.

Απόπειρες υλοποίησης Smart Grid έχουν ξεκινήσει σε όλο τον κόσμο, μέσω της αργής και δαπανηρής αναβάθμισης των υποδομών των υφιστάμενων δικτύων ηλεκτρικής ενέργειας. Τα κόστη είναι τεράστια, οπότε η κυβερνητική (οικονομική) στήριξη είναι αναπόφευκτη. Η Ιταλία ήταν πρωτοπόρος στην εφαρμογή της τεχνολογίας Smart Grid με ένα έργο που ξεκίνησε το 2001 από την Enel. Άλλες προσπάθειες υλοποίησης ξεκίνησαν το 2008, όπως στο Τέξας των ΗΠΑ από την Austin Energy και στο Κολοράντο από την Excel Energy. Η Consolidated Edison Company της Νέας Υόρκης έλαβε μία από τις μεγαλύτερες ομοσπονδιακές επιχορηγήσεις μέχρι στιγμής. Τα περισσότερα έργα περιλαμβάνουν την ευρεία ανάπτυξη των έξυπνων μετρητών που αναμένεται να αυξήσουν τα κέρδη και την αξιοπιστία. Άλλες προσπάθειες, που αξίζει να σημειωθούν, έγιναν στο Οντάριο του Καναδά από την HydroOne, στο Σακραμέντο των ΗΠΑ από την επιχείρηση ηλεκτρισμού του Δημοτικού Περιφερειακού Συμβουλίου και στην Αυστραλία από την EnergyAustralia.



Chapter 1: Introduction to electrical grids and the Smart Grid

1.1 Introduction

This master thesis analyzes the usage, necessity and effects of sensors in modern smart electrical grids, emphasizing on security issues that arise. The reader is introduced in electrical power systems and their distinct characteristics and problems. A mathematical background is provided for audience that is coming outside the electrical engineering research domain. Reasoning for the increasing adoption of measuring technologies is given and major implementations of Smart Grid technologies are recorded.

1.2 Brief History

Electricity is the greatest scientific achievement of the nineteenth century. The twentieth century is making use of electricity so extensively that it has changed the course of humanity. Electricity has become something we rely on to live our lives, but it was by no means an overnight discovery. In the past century and a half, electricity has steadily evolved from a scientific curiosity, to a luxury of the affluent, to a modern need. Along the way, it has been shaped by a variety of non-technological factors: economic, political, social, and environmental.

Static electricity was known from ancient times (Thales 640-546 B.C.) but electricity generation, as we know it, became possible in the 1820s (Meyer, 1971) by Michael Faraday. Faraday set the fundamental principles of electricity generation and his basic method, the movement of a loop of wire between the poles of a magnet, is still used today. The first central power station operated in 1881 in New York by Edison Illuminating Company and run on steam engines to produce 110 V DC power. Although transformers were invented in the 1830s, they were brought into application in the 1880s to realize ac systems. The invention of the induction motor, by Nikola Tesla in 1888, helped replace dc motors and spread the use of ac systems.



The first commercial power plant in the United States using three-phase alternating current was at the Mill Creek No. 1 Hydroelectric Plant near Redlands, California, in 1893. In the early 1900s, the development of rubber-base insulated and paper-insulated, lead covered cables allowed for underground distribution at voltages up to 5kV. The necessity for more load demand and more power over large distances led to the adoption of higher distribution voltages. Today, Extra High Voltage (EHV) has dominated the large distance power transmission methods with voltages ranging from 230 kV to 1100 kV for three phase AC and up to 800 kV DC, justified by the higher transmission capacities, more efficient use of right-of-way, lower transmission losses and reduced environmental impact.

The continuous growth of electric companies brings along the realization of economies of scale in the generating facilities, the introduction of equipment standardization and the utilization of load diversity between areas. This growth was accompanied by the interconnection of the generating facilities to a common transmission network. In this way, the probability of service interruption decreased, the total reserve capacity required to mitigate equipment-forced outages also decreased and the use of most economical units possible increased.

1.3 Characteristics of Electrical Energy

Generally, when dealing with electric power systems, we are more concerned with electric power in the circuit rather than the currents. We use a cosine representation of the waveforms, assuming that the voltage and current are sinusoidal functions derived from Fourier's harmonic analysis (Howell, 2001) and applicable to all kinds of waveforms. The value of instantaneous power flowing into an element is the product of voltage across and current through it. It seems, then, reasonable to exchange the current for power without losing any information. In treating sinusoidal steady-state behavior of circuits, some further definitions are necessary.

For a sinusoidal voltage, $v(t)$ given by

$$v(t) = V_{\max} \cos \omega t \quad (1.1)$$



The instantaneous current in the circuit is

$$i(t) = I_{\max} \cos(\omega t - \varphi) \quad (1.2)$$

In an inductive circuit the current lags the voltage by an angle φ_1 while in a capacitive circuit the voltage lags the current by an angle φ_2 .

We can also represent these characteristics by using rotating vectors known as phasors.

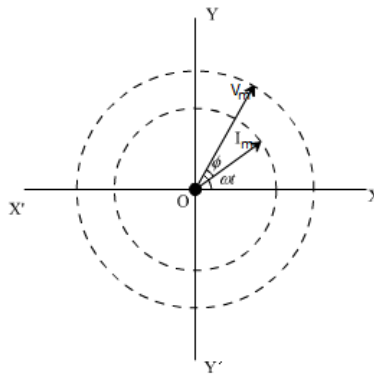


Figure 1.1. Phasor representation.

The loads, in majority, are composite and not purely resistive.

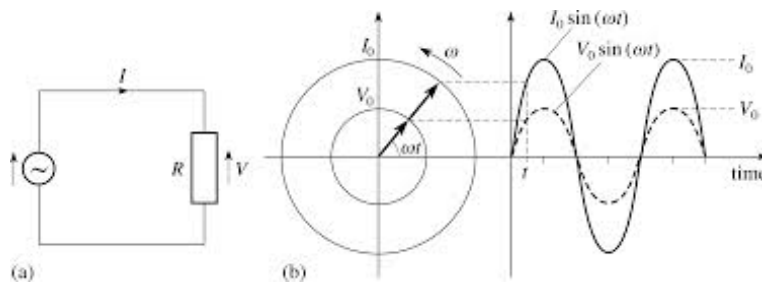


Figure 1.2. Phasor and waveform graph of a purely resistive ac circuit.

This composite resistance is called impedance (Z) and is defined as the complex ratio of the voltage to the current, in an alternating current (AC) circuit. Impedance possesses both magnitude and phase, unlike resistance, which has only magnitude.

$$Z = Z \angle \varphi \quad (1.3)$$

$$\text{and } |Z| = \frac{V_m}{I_m} \quad (1.4)$$

Derived from Ohm's law.

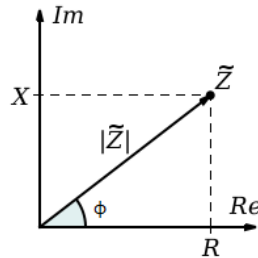


Figure 1.3. Vector representation of Impedance Z .

The instantaneous power into an element is given by :

$$p(t) = v(t)i(t) = V_m I_m [\cos(\omega t) \cos(\omega t - \phi)] \quad (1.5)$$

which reduces to:

$$p(t) = \frac{V_m I_m}{2} [\cos(\phi) + \cos(2\omega t - \phi)] \quad (1.6)$$

The average of $\cos(2\omega t - \phi)$ is zero through one cycle so this term does not contribute to the average power.

The average power p_{av} is given by :

$$p_{av} = \frac{V_m I_m}{2} \cos \phi \quad (1.7)$$

Using the effective (rms) values of voltage and current and substituting $V_m = \sqrt{2} (V_{rms})$ and $I_m = \sqrt{2} (I_{rms})$,

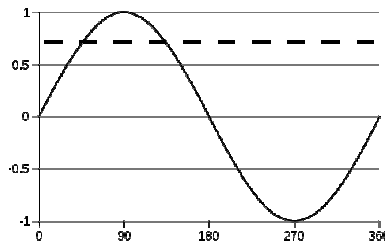


Figure 1.4. RMS value (0.707) of a sine waveform.

we get

$$p_{av} = V_{rms} I_{rms} \cos\varphi \quad (1.8)$$

For sinusoidal voltages and currents only, the power entering any network is the product of the effective values of terminal voltage and current and the cosine of the phase angle φ , which is, called the power factor (PF). When the load contains reactance and resistance, a component of the current in the circuit is engaged in conveying the energy that is periodically stored in and discharged from the reactance. This stored energy, adds to the current in the circuit but does not add to the average power.

The value of the average power consumed in a circuit is called active power P , measured in Watts, and the power that supplies the stored energy in reactive elements (represents non-active power) is called reactive power Q , measured in voltampere reactive units (var).

The instantaneous power can be written as :

$$p(t) = V_{rms} I_{rms} [\cos\varphi(1 + \cos 2\omega t)] + V_{rms} I_{rms} \sin\varphi \sin 2\omega t \quad (1.9)$$

$$p(t) = P(1 + \cos 2\omega t) + Q \sin 2\omega t \quad (1.10)$$

Thus P and Q are the average or real power and the amplitude of the pulsating power, respectively:

$$P = V_{rms} I_{rms} \cos\varphi \quad (1.11)$$

$$Q = V_{rms} I_{rms} \sin \phi \quad (1.12)$$

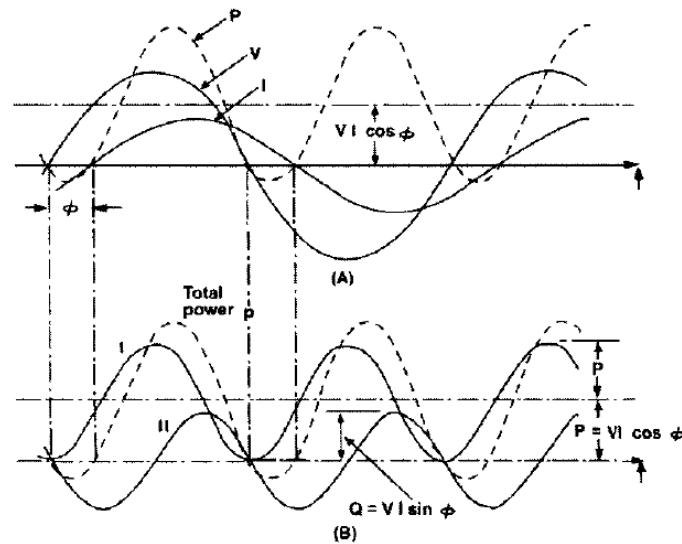


Figure 1.5. Waveform representation of active power (P), voltage (V), current (I) and reactive power (Q).

Apparent or complex power (S) is the product of the current and voltage of the circuit. Due to energy stored in the load and returned to the source, or due to a non-linear load that distorts the wave shape of the current drawn from the source, the apparent power will be greater than the real power. The apparent power is measured in voltampere units.

$$S = V I < \phi \quad (\text{rms values are implied}) \quad (1.13)$$

$$S = V I^* \quad (1.14)$$

$$S = V I e^{j\phi} \quad (1.15)$$

$$\begin{aligned} S &= V I (\cos \phi + j \sin \phi) = \\ &= P + jQ \end{aligned} \quad (1.16)$$

Consider the series circuit shown in Figure 1.6.

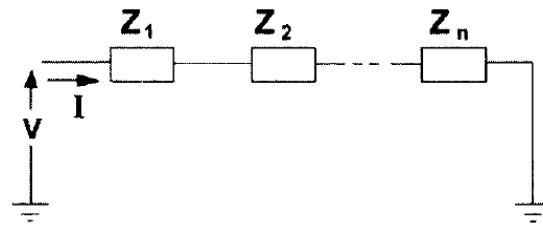


Figure 1.6. A series of complex loads.

The applied voltage to the overall arrangement is equal to the sum of the voltage drops:

$$V = I(Z_1 + Z_2 + \dots + Z_n) \quad (1.17)$$

Multiplying both sides of this relation by I^* results in

$$S = \sum_{i=1}^n S_i \quad (1.18)$$

with the individual element's complex power.

$$S_i = I_i^2 Z_i \quad (1.19)$$

Equation (1.18) is known as the summation rule for complex powers. The rule also applies to parallel circuits.

If we represent the current and voltage of an inductive circuit with phasors, the conjugate of the current will be in the first quadrant in the complex plane as shown in Figure 1.7(a). Multiplying the phasors by V , we obtain the complex power diagram shown in Figure 1.7(b).

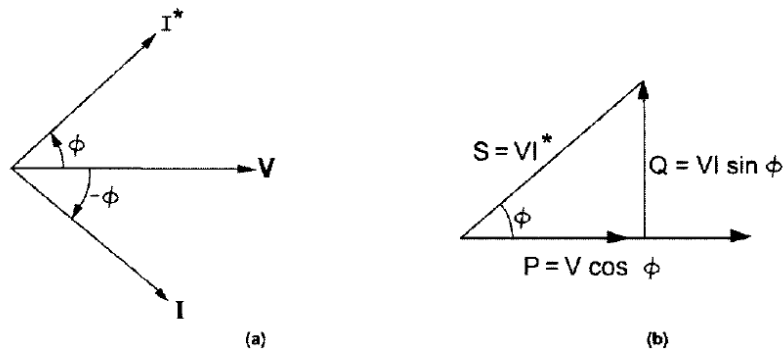


Figure 1.7. (a) Voltage-current and conjugate current vectors. (b) Complex power triangle.

From this figure and previous relations we conclude that the power factor of a circuit is :

$$\cos \phi = \frac{P}{|S|} \quad (1.20)$$

and is a dimensionless number between -1 and 1.

Three-phase systems

The majority of electric power equipment presently used in generation, transmission and distribution uses balanced three-phase systems. Three-phase operation makes more efficient use of generator copper and iron. Power flow in single-phase circuits was shown in the previous section to be pulsating and not constant (Figure 1.5). This drawback is not present in a three-phase system. Furthermore, three-phase motors start more conveniently and, having constant torque, run more satisfactorily than single-phase motors. However, polyphase systems bring more complications than three-phase ones and are not compensated for by the slight increase of operating efficiency.

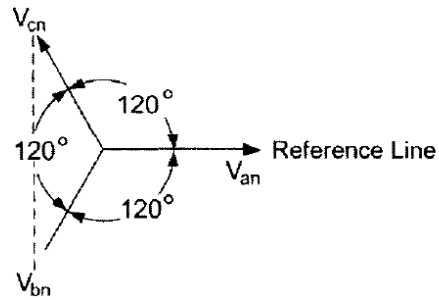


Figure 1.8. A balanced three-phase voltage system represented by rotating phasors.

A balanced three-phase voltage system consists of three single-phase voltages with the same magnitude and frequency but time-displaced from one another by 120°. The rotation or order, or phase sequence, of the voltages plays an important part for induction motors, because it determines whether the motor will turn clockwise or counter-clockwise. These three voltages can be combined in a Y connection or in a Δ connection.

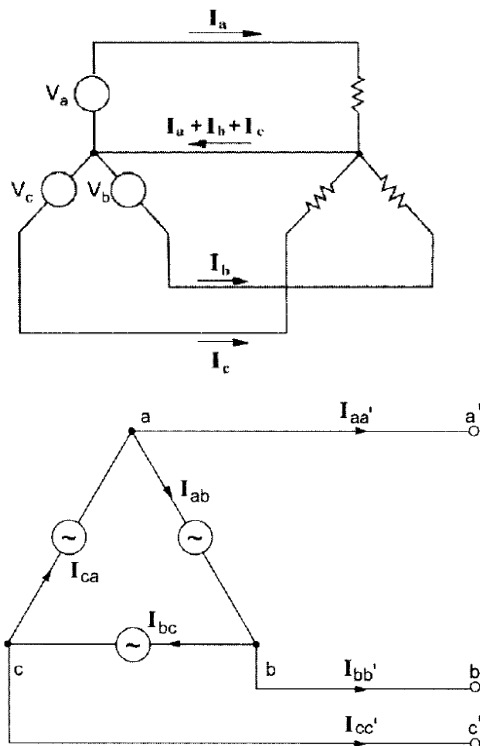


Figure 1.9. Electrical diagrams of three-phase systems connected in Y (left) and Δ(right) connection.



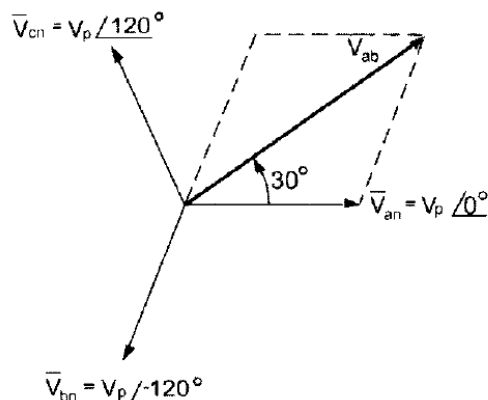
Y connection

Figure 1.10. Phasor representation of voltages in a Y connection.

As seen in Figure 1.10, the common terminal n is called the neutral or star (Y) point. The voltages appearing between any two of the line terminals a , b , and c have different relationships in magnitude and phase to the voltages appearing between any one line terminal and the neutral point n . The set of voltages V_{ab} , V_{bc} , and V_{ca} , are called the line voltages, and the set of voltages V_{an} , V_{bn} , and V_{cn} , are referred to as the phase voltages. The phase voltages have the same magnitude and each phasor is placed 120° from the other two. The voltage vector from a to b equals to the addition of voltage vectors from a to n and from n to b .

For a balanced system, each phase voltage has the same magnitude, and we define :

$$|V_{ab}| = |V_{bc}| = |V_{ca}| = V_p \quad (1.21)$$

where V_p denotes the effective magnitude of the phase voltage.

It can be shown that

$$\begin{aligned} V_{ab} &= V_p(1 - 1 \angle -120^\circ) = \\ &= \sqrt{3} V_p \angle 30^\circ \end{aligned} \quad (1.22)$$

In similar way we obtain

$$V_{bc} = \sqrt{3} V_p \angle -90^\circ \quad (1.23)$$

$$V_{ca} = \sqrt{3} V_p < 150^0 \quad (1.24)$$

The line voltages constitute a balanced three-phase voltage system whose magnitudes are $\sqrt{3}$ times the phase voltages. Thus, we write

$$V_L = \sqrt{3} V_p \quad (1.25)$$

A current flowing out of a line terminal a (or b or c) is the same as that flowing through the phase source voltage appearing between terminals n and a (or n and b, or n and c). We can thus conclude that for a Y-connected three-phase source, the line current equals the phase current. Thus,

$$I_L = I_p \quad (1.26)$$

Here I_L denotes the effective value of the line current and I_p denotes the effective value for the phase current.

Δ Connection

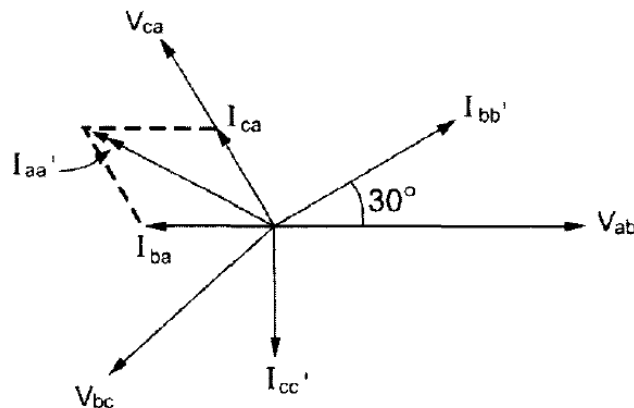


Figure 1.11. Phasor representation of currents and voltages in a Δ connection.

Three single-phase sources, connected in a triangle, form a three-phase Δ connection. The line and phase voltages have the same magnitude:

$$|V_L| = |V_p| \quad (1.27)$$

Using Kirchhoff's current law at one of the line terminals, we obtain the phase and line currents. Working in a similar way as in the Y-connected source, but now using the phase currents, we obtain:

$$I_{ab} = I_p < 0^0 \quad (1.28)$$

$$I_{bc} = I_p < -120^0 \quad (1.29)$$

$$I_{ca} = I_p < 120^0 \quad (1.30)$$

The current that flows in the line joining a to a' is denoted $I_{aa'}$ and is given by:

$$I_{aa'} = I_{ca} - I_{ab} \quad (1.31)$$

As a result, we have

$$I_{aa'} = \sqrt{3} I_p < 150^0 \quad (1.32)$$

In similar way we obtain

$$I_{bb'} = \sqrt{3} I_p < 30^0 \quad (1.33)$$

$$I_{cc'} = \sqrt{3} I_p < -90^0 \quad (1.34)$$

Note that a set of balanced three phase currents yields a corresponding set of balanced line currents that are $\sqrt{3}$ times the phase values:

$$I_L = \sqrt{3} I_p \quad (1.35)$$

where I_L denotes the magnitude of any of the three line currents.

Assuming that the three-phase generator is supplying a balanced load with the bellow three sinusoidal phase voltages:

$$v_a(t) = \sqrt{2} V_p \sin \omega t \quad (1.36)$$

$$v_b(t) = \sqrt{2} V_p \sin(\omega t - 120^0) \quad (1.37)$$

$$v_c(t) = \sqrt{2} V_p \sin(\omega t + 120^0) \quad (1.38)$$



and the currents given by:

$$i_a(t) = \sqrt{2} I_p \sin(\omega t - \varphi) \quad (1.39)$$

$$i_b(t) = \sqrt{2} I_p \sin(\omega t - 120^\circ - \varphi) \quad (1.40)$$

$$i_c(t) = \sqrt{2} I_p \sin(\omega t + 120^\circ - \varphi) \quad (1.41)$$

where φ is the phase angle between the current and voltage in each phase. The total power flowing into the load is :

$$p_{3\varphi}(t) = v_a(t) i_a(t) + v_b(t) i_b(t) + v_c(t) i_c(t) \quad (1.42)$$

Which can be condensed to:

$$p_{3\varphi}(t) = V_p I_p \{ 3\cos\varphi - [\cos(2\omega t - \varphi) + \cos(2\omega t - 240 - \varphi) + \cos(2\omega t + 240 - \varphi)] \} \quad (1.43)$$

The last three terms in the above equation are the reactive power terms and they add up to zero. Thus we obtain:

$$p_{3\varphi}(t) = 3V_p I_p \cos\varphi \quad (1.44)$$

The relationship between the line and phase voltages in a Y-connected system is

$$|V_L| = \sqrt{3}|V| \quad (1.45)$$

In terms of line quantities we obtain:

$$p_{3\varphi} = 3|V_L| |I_L| \cos\varphi \quad (1.46)$$



The value of the total instantaneous power is constant, having a magnitude of three times the real power per phase. We must not assume that the reactive power is of no importance in a three-phase system since the Q terms cancel out. This situation is analogous to the summation of balanced three-phase currents and voltages that also cancel out. Although the sum cancels out, these quantities are still very much in evidence in each phase. We thus extend the concept of complex or apparent power (S) to three-phase systems by defining

$$S_{3\phi} = 3V_p I_p^* \quad (1.47)$$

where the active power and reactive power are obtained from

$$S_{3\phi} = P_{3\phi} + jQ_{3\phi} \quad (1.48)$$

where

$$P_{3\phi} = 3|V_p| |I_p| \cos\phi \quad (1.49)$$

$$Q_{3\phi} = 3|V_p| |I_p| \sin\phi \quad (1.50)$$

and

$$P_{3\phi} = 3|V_L| |I_L| \cos\phi \quad (1.51)$$

$$Q_{3\phi} = 3|V_L| |I_L| \sin\phi \quad (1.52)$$

When specifying rated values for power system apparatus and equipment such as generators, transformers, circuit breakers, etc., we use the magnitude of the apparent power $S_{3\phi}$ as well as line voltage for specification values.

The vast length of the power grid and the multiple voltage levels used in each section make it difficult to use electrical variables in power system calculations. A solution to this problem is the per unit system ; the expression of system quantities as fractions of a defined base unit quantity. The numerical per unit value of any quantity is its ratio to a chosen base quantity of the same dimension. Thus a per unit quantity is a normalized quantity with respect to the chosen base value. The per unit value of a quantity is thus defined as:



$$\text{p.u. value} = \frac{\text{Actual value}}{\text{Reference or base value of the same dimension}} \quad (1.53)$$

The use of a per unit system leads to the following advantages:

- Similar apparatus (generators, transformers, lines) will have similar per-unit impedances and losses expressed on their own rating, regardless of their absolute size.
- Use of the constant $\sqrt{3}$ is reduced in three-phase calculations.
- Per-unit quantities are the same on either side of a transformer, independent of voltage level.

Five quantities are involved in the calculations. These are the current I , the voltage V , the complex power S , the impedance Z , and the phase angles. The angles are dimensionless; the other four quantities are completely described by knowledge of only two of them. An arbitrary choice of two base quantities will fix the other base quantities. Let $|I_b|$ and $|V_b|$ represent the base current and base voltage expressed in kiloamperes and kilovolts, respectively. The product of the two yields the base complex power in megavoltamperes (MVA):

$$|S_b| = |I_b||V_b| \text{ MVA} \quad (1.54)$$

The base impedance will also be given by

$$|Z_b| = \frac{|V_b|}{|I_b|} = \frac{|V_b|^2}{|S_b|} \text{ ohms} \quad (1.55)$$

The same megavoltampere base, usually the nominal voltage of lines and apparent power, is used in all parts of a given system. Once base voltage is chosen, all other base voltages must then be related to the one chosen by the turns ratios of the connecting transformers. From the definition of per unit impedance, we can express the ohmic impedance Z_Ω in the per unit value $Z_{p.u.}$ as



$$Z_{p.u.} = Z_{\Omega} \frac{|S_b|}{|V_b|^2} p.u. \quad (1.55)$$

where $Z_{p.u.}$ can be interpreted as the ratio of the voltage drop across Z with base current injected to the base voltage.

More information about the characteristics of electricity and energy systems can be found in the works of Elgerd (2001) and M. E. El-Hawary (2008) .

1.4 How the electricity grid works

An interconnected classical power system can be divided into the following main subsystems:

- Generation
- Transmission and subtransmission
- Distribution
- Utilization

Generation

This subsystem includes generators and transformers.

Generators

The main categories of power generation sources are:

- The synchronous ac three-phase generator or alternator
- Photovoltaic panels

There are also other alternative sources such as electrochemical, piezoelectric, thermoelectric, thermionic, magnetohydrodynamic, etc that cannot currently be used for large scale generation.



Synchronous generators utilize two synchronously rotating fields to convert mechanical energy to electrical energy. A rotating magnet, called the rotor turns within a stationary set of conductors wound in coils on an iron core, called the stator. The field cuts across the conductors, generating an induced EMF (electromotive force), as the mechanical input causes the rotor to turn. The rotating magnetic field induces an AC voltage in the stator windings. The source of the mechanical power, commonly known as the prime mover, may be hydraulic turbines or wind turbines or steam turbines whose energy comes from the burning of coal, gas and nuclear fuel, gas turbines, or occasionally internal combustion engines burning oil.

Transformers

A transformer is a passive electrical device that transfers power from one voltage level to another, by inductive coupling between its winding circuits. A varying current in the primary winding creates a varying magnetic flux in the transformer's core and thus a varying magnetic flux through the secondary winding. This varying magnetic flux induces a varying voltage in the secondary winding. Step-up transformers are used to increase the voltage – and lower the current – at the side of generation of a transmission line and step-down transformers are used to reduce the voltage– and increase the current – to usable values at the distribution or utilization side.

Transmission and subtransmission

A transmission network transfers electric power from the generating facilities to the distribution system which distributes it to consumers. Neighboring utilities are also interconnected with transmission lines, allowing power to flow economically within regions, during normal conditions, or to be rerouted, during emergencies. Transmission networks can be either overhead or underground. Overhead transmission, via elevated power lines, is preferred towards underground transmission due to its economic nature. Overhead cables have no insulation, lower excavation costs and faults are easy to locate and repair. Underground cables take up less right-of-way (a right to make a way over a piece of land) than overhead lines, have lower visibility, and are less affected by bad weather. Underground transmission is limited by its low thermal capacity that in turn permits less overload than in overhead lines. Furthermore, long underground cables have higher capacitance; thus reducing the active power delivered to loads.



Standards concerning voltage levels of transmission lines are set by ETSI and ESO in Europe and ANSI in the United States. These include specifications about 69 kV, 115 kV, 138 kV, 161 kV, 230 kV, 345 kV, 500 kV, and 765 kV line-to-line transmission. Voltage levels above 230 kV are usually referred to as EHV. Lines end up in substations called high-voltage substations, receiving substations, or primary substations. Some substations are used to switch circuits in and out of service and are called switching substations. Primary substations are used to step down the voltage to more usable levels towards the load. Many very large industries are directly connected to transmission via high-voltage substations.

The subtransmission network is the part of the transmission network that connects the high-voltage substations through step-down transformers to the distribution substations. Typical voltage levels vary from 69 to 138 kV although transmission and subtransmission levels are not distinct. Some large industrial customers are directly connected to subtransmission. Capacitor banks and reactor banks are usually installed in the substations for maintaining the transmission line's quality of power.

Distribution

The part from the distribution substations to the consumer's service entrance equipment composes the distribution subsystem and the distribution lines used are called primary feeders. The voltage in this subsystem ranges from 4 to 34.5 kV and the geographical area served is well defined. Some small industrial consumers are directly connected to this subsystem.

In the secondary distribution network, the voltage is further reduced for utilization by commercial and residential consumers. Individual consumers are connected via lines and cables that do not exceed a few hundred of meters in length. Typical voltage levels of the secondary distribution network are 480V, 240V and 120V, using single-phase and three wires or three-phase and four wires either using a star (Y) or a triangle (Δ) circuit. Homes are usually served by a transformer that reduces the primary feeder voltage to 240/120 V using a three-wire line.



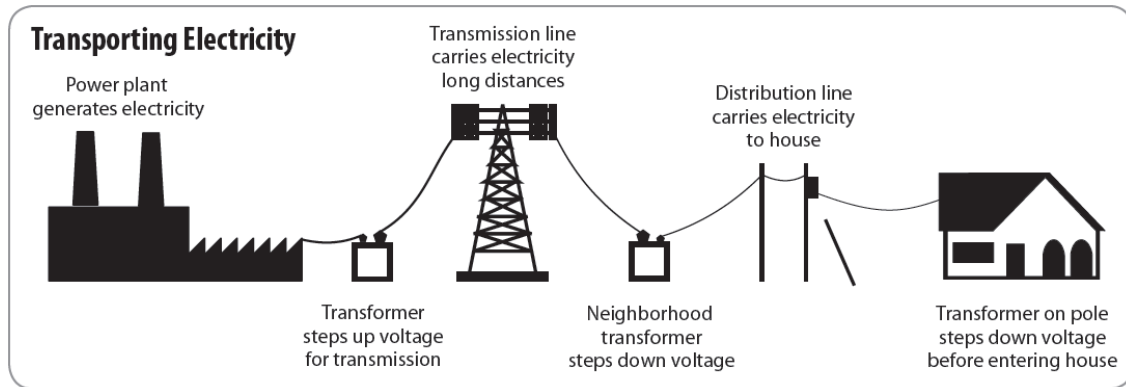


Figure 1.12. A simplified representation of how electricity is transported.

Utilization

This subsystem refers to the loads of the power system in general. Loads can be divided into three categories: industrial, commercial and residential. Industrial loads are composite and to their majority inductive, due to inductive motors. Composite loads are affected by the voltage and frequency of the flowing power and form a high portion of the system load. Commercial and residential loads consist largely of lighting, heating, and cooking. These loads are independent of frequency and consume negligibly small reactive power.

The load varies throughout the day and power generation must meet the consumers' demand at all times, with power being available to consumers on demand. At present, most consumption is time-critical and inflexible. The daily-load curve of a utility is a composite of demands made by various consumer categories. The greatest value of load during a 24-hr period is called the peak or maximum demand.

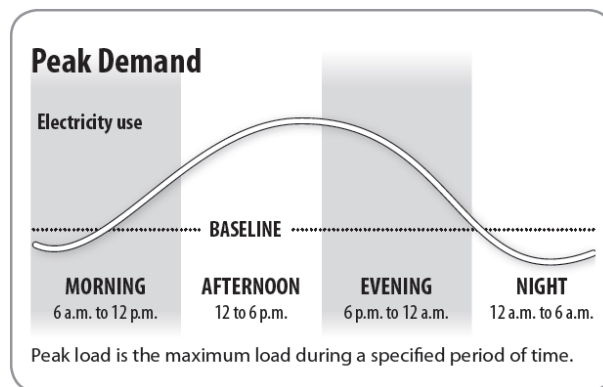


Figure 1.13. A simplified daily demand curve representation.

To assess the efficiency of a generating plant the load factor is defined. The load factor is the ratio of average load over a designated period of time to the peak load occurring in that period. Load factors may be given for a day, a month, or a year. Daily and monthly load factors are to be used in comparison to same data collected on same day or month of previous years. The yearly, or annual, load factor is the most useful since a year represents a full cycle of time. The daily load factor is

$$\text{Daily Load Factor} = \frac{\text{Average load}}{\text{peak load}} \quad (1.56)$$

Multiplying the numerator and denominator of (1.56) by a time period of 24 hr, we get :

$$\text{Daily L.F.} = \frac{\text{average load} \times 24\text{hr}}{\text{peak load} \times 24\text{hr}} = \frac{\text{energy consumed during 24hr}}{\text{peak load} \times 24\text{hr}} \quad (1.57)$$

The annual load factor is :

$$\text{Annual L.F.} = \frac{\text{total annual energy}}{\text{peak load} \times 8760\text{hr}} \quad (1.58)$$

Generally, different classes of loads have different peak load, which improves the overall system load factor. The highest system load factor is desirable for a power plant to operate economically. Typical system load factors are in the range of 55 to 70 percent. Load-forecasting at all levels is an important function in the operation, operational planning, and planning of an electric power system. To operate and protect a power system, other devices and systems are also required. Some of the protective devices directly connected to the circuits are called switchgear. They include instrument transformers, circuit breakers, disconnect switches, fuses and lightning arresters. These devices are necessary for load dispatching, either for normal operation or on the occurrence of faults.



The reliable and economic operation of a power system is monitored by a control center, called the Energy Control Center (ECC). Energy control centers, with the help of powerful computers, gather and process data from remote sensors and remotely operate the switchgear. Supervisory Control and Data Acquisition (SCADA) systems are auxiliaries to the energy control center.

1.5 Limitations and problems

Electricity is difficult to be stored in large scale and needs to be produced and consumed in real time. There is a weak balance between the generated power, also called supply, and the consumed power, known as demand. Supply and demand are balanced by adjusting supply to demand, otherwise instability arises. Rotating masses in generators act as a buffer between supply and demand. Grid frequency reflects the extent to which a balance between supply and demand exists. If the supply is higher than the demand, voltage and frequency increase, compared to their nominal values. If the supply is lower than the demand we notice voltage and frequency decrease in the grid, which needs to be handled immediately with rejection of loads.



Figure 1.14. Simplified representation of balance between power supply and demand.

To understand the grid's problems, we should start with its physical behavior. The enormous system of electricity generation, transmission, and distribution that covers North America or European interconnected countries or other countries that extend to a large geographic area, is essentially a single machine for each area.

For instance, the single network of North America is physically and administratively subdivided into three “interconnects”— the Eastern, covering the eastern two-thirds of the United States and Canada; the Western, encompassing most of the rest of the two countries; and the Electric Reliability Council of Texas (ERCOT), covering most of Texas.

Within each interconnect, power flows through ac lines, so all generators are tightly synchronized to the same 60-Hz or 50-Hz cycle for Europe. The interconnects are joined to each other by dc links, so the coupling is much looser among the interconnects than within them. (The capacity of the transmission lines between the interconnects is also far less than the capacity of the links within them.)

Before the 1990s, regional and local electric utilities were regulated, vertical monopolies. A single company controlled electricity generation, transmission, and distribution in a given geographical area and often in a whole country. Each utility generally maintained sufficient generation capacity to meet its customers’ needs, and long-distance energy shipments were usually reserved for emergencies, such as unexpected generation outages. In essence, the long-range connections served as insurance against sudden loss of power.

The system was reliable because the use of long-distance connections was limited. The physical complexities of power transmission rise rapidly as distance and complexity of interconnections grow. Power in an electric network does not travel along a set path, but rather flows like a liquid. When utility A agrees to send electricity to utility B, utility A increases the amount of power generated while utility B decreases production or has an increased demand. The power then flows from the “source” (A) to the “sink” (B) along all the paths that can connect them. This means that changes in generation and transmission at any point in the system will change loads on generators and transmission lines at every other point—often in ways not anticipated or easily controlled (Figure 1.15).



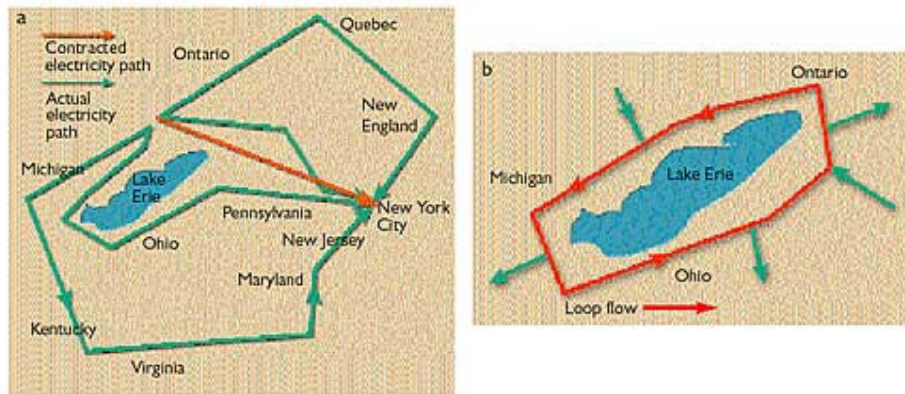


Figure 1.15. Electric power does not travel just by the shortest route from source to sink, but also by parallel flow paths through other parts of the system (a). Where the network jogs around large geographical obstacles, such as the Rocky Mountains in the West or the Great Lakes in the East, loop flows around the obstacle are set up that can drive as much as 1 GW of power in a circle, taking up transmission line capacity without delivering power to consumers (b).

A transmission line's capacity is inversely proportional to its impedance, which is governed by Ohm's law. It is affected by its material, length and the distance from adjacent lines and from the ground, for overhead cables or the thickness of insulation, for underground cables. To avoid system failures, the amount of power flowing over each transmission line must remain below the line's capacity. Exceeding capacity generates too much heat in a line, which can cause the line to sag (expand in length) or break (melt) or can create power-supply instability such as phase and voltage fluctuations (IEEE Std 1159-2009). Capacity limits vary, depending on the length of the line and the transmission voltage. The longer a line is extended, the smaller its capacity becomes.

In addition, for an ac power grid to remain stable, the frequency and phase of all power generation units must remain synchronous within narrow limits. A generator that drops 2 Hz below 60 Hz will rapidly build up enough heat in its bearings to destroy itself. Special switches, called circuit breakers, are used to trip a generator out of the system when the frequency varies too much. Much smaller frequency changes can indicate instability in the grid. In the U.S. Eastern Interconnect, a 30-mHz drop in frequency reduces power delivered by 1 GW.

A measure of the grid's quality of power is the power factor. In an ideal grid the power factor would be equal to one, which means that all loads are purely resistive. In practice, this is not the case; Non-linear loads, such as rectifiers or some kind of arc discharge devices, distort the current drawn from the system. The current in these systems is interrupted by a switching action, which leads to current containing frequency components, that are multiples of the power system frequency, called harmonics. The higher currents increase the energy lost in the system. The distortion power factor is used as a measure of how much the harmonic distortion of a load current decreases the average power transferred to the load.

If certain parts of the grid are carrying electricity at near capacity, a small shift of power flows can trip circuit breakers, which sends larger flows onto neighboring lines to start a chain-reaction failure. This happened on Nov. 10, 1965 in U.S.A., when an incorrectly set circuit breaker tripped and set off a blackout that blanketed nearly the same area as the one in August 2003. More information on the 2003 major blackout can be found in the work of Amin and Schewe(2007).

After the deregulation, electricity is treated as a commodity. Generating companies sell their power for the best price they can get, and utilities buy at the lowest price possible. For this concept to work, it is imperative to compel utilities that own transmission lines to carry power from other companies' generators in the same way as they carry their own, even if the power goes to a third party. This practice, also known as wheeling, dictates that an entity that generates power does not have to own power transmission lines: only a connection to the network or grid. The entity then pays the owner of the transmission line based on how much power is being moved and how congested the line is.

Casazza(1998) and many other experts, criticized these new rules of treating electricity as a commodity rather than as an essential service. Commodities can be shipped from point A through line B to point C, but power shifts affect the entire single-machine system. As a result, increased long-distance trading of electric power creates dangerous levels of congestion on transmission lines where controllers do not expect them and cannot deal with them.



The problems are compounded as independent power producers add new generating units, such as renewable sources, at essentially random locations determined by low labor costs, local regulations, tax incentives or climate conditions. If generators are added far from the main consuming areas, the total quantity of power flows will rapidly increase, overloading transmission lines. The system was not originally designed to handle long-distance wheeling.

System reliability is no longer accurately assessed. Data needed to predict and react to system stress—such as basic information on the quantity of energy flows—begin to disappear, treated by utilities as competitive information and kept secret. Utilities also neglect reporting on blackout statistics as well.

The separation into generation and transmission companies resulted in an inadequate amount of reactive power. Reactive power is needed to maintain voltage, and longer-distance transmission increases the need for it. However, only generating companies can produce reactive power, and with the new rules, they do not benefit from it. In fact, reactive-power production reduces the amount of deliverable power produced. In this way, transmission companies, under the new rules, cannot require generating companies to produce enough reactive power to stabilize voltages and increase system stability. The net result of the new rules was to more tightly couple the system physically and stress it closer to its capacity and at the same time, make control more diffuse and less coordinated—a prescription for blackouts.

Category	Description
Dropout	A loss of power that has a short duration, on a timescale of seconds, and is usually fixed quickly.
Brownout	The electrical power supply encounters a partial drop in voltage, or temporary reduction in electric power. In the case of a three-phase electric power supply, when a phase is absent, at reduced voltage, or incorrectly phased.
Blackout	An affected area experiences a complete loss of electrical power, ranging from several hours to several weeks.
Load shedding	An electric company either reduces or completely shuts off the available power to sections of the grid. Sometimes referred to as rolling brownouts and rolling blackouts.

Table 1.1. Power outage categories.



1.6 The Smart Grid

The current grid system is quickly becoming obsolete. This grid system will not be able to meet our future electricity demands. New, efficient technology must be introduced to solve this problem; Smart Grids will be able to efficiently handle our increasing energy demands and reduce the environmental impact by incorporating renewable resources.

Many different definitions of the term ‘Smart Grid’ have been given worldwide:

Jeju Smart Grid Project (2009)

“A Smart Grid refers to a next-generation network that integrates information technology (smart) into the existing power grid (grid) to optimize energy efficiency through a two-way exchange of electricity information between suppliers and consumers in real time.”

Climate Group (2008)

“A Smart Grid is a set of software and hardware tools that enable generators to route power more efficiently, reducing the need for excess capacity and allowing two-way, real-time information exchange with their customers for real-time Demand Side Management (DSM). It improves efficiency, energy monitoring, and data capture across the power generation and T&D network.”

Adam and Winter-steller (2008)

“A Smart Grid would employ digital technology to optimize energy usage, better incorporate intermittent "green" sources of energy, and involve customers through smart metering.”

Miller (2008)

“The Smart Grid will:

- Enable active participation by consumers
- Accommodate all generation and storage options
- Enable new products, services, and markets



- Provide power quality for the digital economy
- Optimize asset utilization and operate efficiently
- Anticipate and respond to system disturbances
- Operate resiliently against attack and natural disaster”

European Technology Platform SmartGrids (2006)

“Electricity networks that can intelligently integrate the behavior and actions of all users connected to them—generators, consumers, and those that do both—in order to efficiently deliver sustainable, economic, and secure electricity supplies.”

EPRI (2005)

“The IntelliGrid vision links electricity with communications and computer control to create a highly automated, responsive, and resilient power delivery system.”

U.S. DOE (2003)

“Grid 2030 is a fully automated power delivery network that monitors and controls every customer and node, ensuring a two-way flow of electricity and information between the power plant and the appliance, and all points in between. Its distributed intelligence, coupled with broadband communications and automated control systems, enables real-time market transactions and seamless interfaces among people, buildings, industrial plants, generation facilities, and the electric network.”

1.7 The importance of measurements

Sensing and measurements are the cornerstones of a Smart Grid. Without these, a modern power grid implementation is not feasible. Advanced sensing and measurement technologies will acquire and transform data into information and enhance multiple aspects of power system management. Some key goals that will be achieved are the evaluation of congestion and grid stability, the monitoring of equipment health, the elimination of billing estimations, emission reduction, energy theft prevention and control strategies support.

Some major quantities that need to be measured are:



- Power factor
- Power quality throughout the grid
- Phasor relationships (PMUs)
- Equipment health and capacity
- Meter tampering
- Vegetation intrusion
- Fault location
- Transformer and line loading
- Circuit voltage profiles
- Temperature of critical elements
- Outage identification
- Power consumption profiles and forecasting
- Curtailable load levels (loads that can be rejected)

Some advanced technologies to be used to acquire the above information are:

- Advanced microprocessor meters (smart meters)
- Wide-area monitoring systems(WAMS)
- Dynamic line rating (typically based on online readings by distributed temperature sensing combined with Real Time Thermal Rating (RTTR) systems)
- Electromagnetic signature analysis
- Time-of-use and real-time pricing tools
- Backscatter radio technology

1.8 Security

A first major concern about the Smart Grid is safety and reliability. The power grid is considered a critical infrastructure for modern society. This means that its service should remain unhindered and it should be robust, able to withstand extreme climate conditions, natural disasters and human malicious interference. The second major concern about the Smart Grid is the issue of cyber security.

The future grid system will be able to control and regulate electricity throughout the grid. If this powerful system falls into the hands of the wrong person, it would be catastrophic for a country. Terrorist attacks of this type are a major concern.



The cyber security of the grid is very complex. It encompasses every part of the Smart Grid, from utilities and power stations to small area networks. In the U.S.A., a group developed by the National Institute of Standards and Technology (NIST), named the Smart Grid Cyber Security Coordination Task Group (CSCTG), addresses this issue (Lee and Brewer, 2009). In Europe, the European Network and Information Security Agency (ENISA) addresses this issue with a report (ENISA Appropriate security measures for Smart Grids, 2012), stating that: “In contrast to the US’ strict regulatory path, the European approach is to allow a certain degree of ‘freedom’, where these guidelines can be tailored and combined for the needs of different actors, given the varied market.”.

1.9 Structure of this study

This study is comprised of four chapters. The first chapter dealt with the characteristics, the functionality, the limitations and the future form of electricity grids. The second chapter presents the reasons behind the growing need for measurements, the usage of sensors in Smart Grids and the qualities and usage of the produced data. The third chapter discusses general issues of security, provides a bottom-up security approach and presents solutions and security guidelines. Case studies of Smart Grid implementations from all over the world and conclusions of this study are recorded in the fourth chapter.



Chapter 2: The need for measurements

2.1 Reasons to make measurements.

An electricity grid can operate with a minimum set of basic measurements throughout its components, but a transition to becoming a Smart Grid cannot be accomplished without expanding this set of measurements and communicating it to the appropriate parties. The need for data, collected by sensors, is growing and is vital for the development of Smart Grids. We could justify this need by giving three major reasons: technical - environmental and economical.

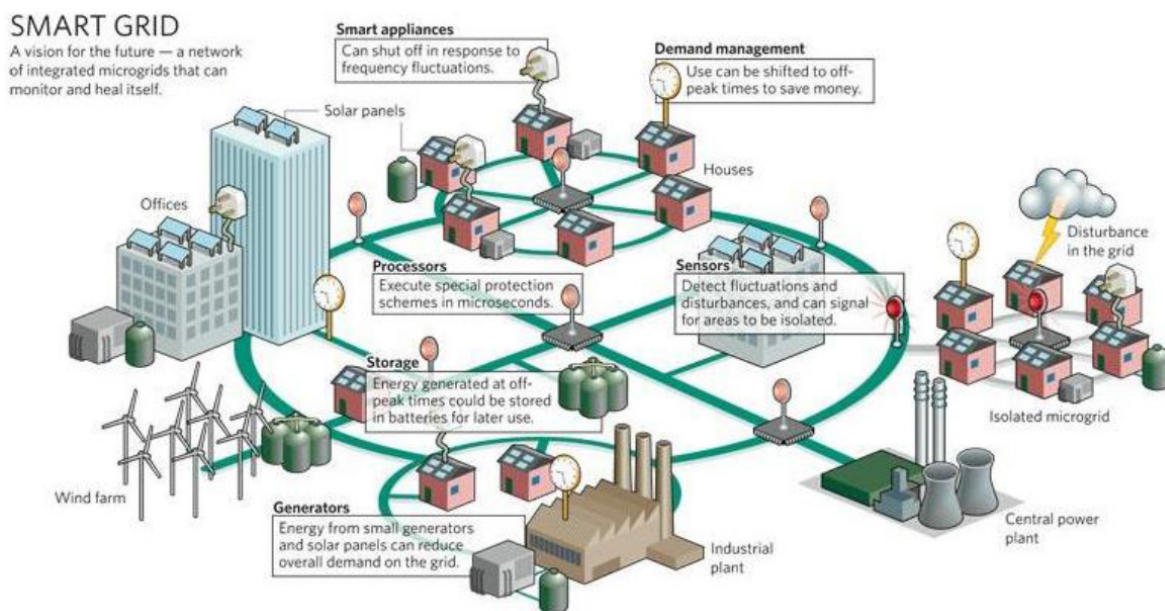


Figure 2.1. Depiction of a Smart Grid.

Technical and environmental reasons:*Grid Resilience and Reliability*

The term resilience refers to the capability of a given entity to withstand from unexpected actions, and recover very quickly thereafter. In 2004 report “Resilience of the National Electricity Network”, published by UK’s House of Commons Trade and Industry Committee, it is stated that: “UK’s electricity transmission and distribution network was built in two main periods of activity, in the late 1950s and the mid 1960s–early 1970s.

The design life of the assets used in the network was about 40 years”. From this statement is clearly understood that aging equipment is an important risk factor in electricity grids that should be taken into account. Smart Grid sensors will help mitigate this risk by providing a live status of equipment health throughout the grid’s subsystems.

At the generation subsystem, data from generators and facilities is collected, such as generator stress, resource transportation status and abundance (e.g. coal delivery or water availability). At the transmission subsystem, information about voltage and frequency is needed for line and transformer protection. Flexible Alternating Current Transmission System devices (FACTS) will help monitor the voltage on the grid in real time, thus increasing transmission distance, reducing line loss and increasing stability along the grid (Breuer et al., 2007).

At the distribution subsystem, wide-area monitoring systems (WAMS), dynamic line rating (a line’s carrying capacity can be calculated by data from sensors which monitor weather conditions and power line temperature) and electromagnetic signature measurement and analysis help identify distribution equipment problems. Superconducting cables enforce reliability by using superconductor-based fault current limiters. Superconductor-based fault current limiters “limit the amount of current flowing through the system and allow for the continual, uninterrupted operation of the electrical system” (U.S. DoE, 2009). All these lead to maintaining the integrity of the grid and preventing blackouts.



Grid security

Various sensors can provide data for the sake of physical security. Motion and pressure sensors can protect facilities and equipment until the last mile, by raising alarms and providing live image and sound. Superseding of measurements from different kinds of sensors and different communication channels can reveal cyber attacks. Manipulated readings of specific sensors and large scale cyber attacks can also be uncovered in a similar way.

A Smart Grid should be able to withstand environmental threats (both intentional and unintentional), and recover in a timely fashion. Measurements of exceeding line capacity or frequency reduction should automatically lead to load dispatching or islanding of semiautonomous parts of the grid. Meteorological data (e.g. temperature, wind velocity, humidity, etc) can provide information about climate conditions and weather forecasts about phenomena that can affect the grid's components.

Greater efficiency

Line monitoring and reactive power compensation can reduce transmission losses. Capacitor banks leveraging power factor corrections at consumer's side help improve power quality and save wasted energy. The insertion of the latest high temperature superconducting cables and HVDC systems increases the overall transmission capacity. Exceeding the capacity of lines triggers alarms and leads to automated power re-routing, thus relieving congestion, similar to telecommunication networks.

Demand-Response (DR) systems will utilize the information that new loads are about to enter the grid and commands will instantly be issued for more power generation. Commands can also be issued towards the opposite direction to dispatch non vital loads (e.g. refrigerators) that try to enter or are already serviced by the grid during peak load hours. In this way, generator backups and emergency line capacity can be reduced.

Furthermore, excessive power from renewable resources, such as wind turbines, can be stored at hydro plants (also known as hydro power storage), with reverse pumping of water, and used at a later time of high energy demand. Cutting edge energy storage technologies, also known as Distributed Energy Resources (DER), will be placed throughout the grid, making it easier for the grid to supply emergency power during a demand increase and to release congestion along the grid (Brown, 2008).



Energy storage technologies include: fuel cells combined with electrolyzers (Smith, 2000), ultracapacitors and batteries which will act as an uninterrupted power supply (UPS) to provide emergency power (Burke, 2000), superconducting magnetic energy storage (SMES): coils of superconducting wire able to store large amounts of circulating current indefinitely (Boyes and Clark, 2000), compressed air (Taylor and Halmes, 2010) and compressed hydrogen storage (Kelly and Briggs, 2002), flywheels (Siostrzonek et al., 2008) and thermal storage for either cooling or steam production (Vandewalle, Keyarts and D'haeseleer, 2012). The technical role and functions of Electricity Storage Systems (ESSs) can be grouped into the following categories: grid voltage support, grid frequency support, grid angular (transient) stability, load leveling / peak shaving, spinning reserve, power quality improvement, power reliability, ride through support and unbalanced load compensation (Mohd et al., 2008).

Integration of emerging technologies

By integrating more renewable energy sources into the grid, we not only increase the power we are able to supply, but also reduce the usage of fossil fuels and our impact on the environment. Integration of renewable technologies and reduction of greenhouse and toxic gas emissions can only be realized by being able to predict and control their fluctuating power output. This can be achieved by having an overall status of the grid and local weather conditions at the locations of renewable power plants. This integration of renewables will bring the reduction of need for new power plants of older, although cheaper but still polluting, technologies.

The threat of global climate change has increased the past few years and the concern about new technologies that will enhance energy security, by reducing the current dependency on carbon-based fuels, has grown. Battery Electric Vehicles (BEVs) and Plug-in Hybrid Electric Vehicles (PHEVs) solution has emerged, due to their energy efficiency, low-cost charging, and reduced petroleum usage.

PHEVs can provide a promising solution to the various energy security, power system reliability and environmental problems acting as Mobile Decentralized Storage (MDS). BEVs/PHEVs can charge their battery using electricity from an electric power grid, also referred to as “Grid-to-Vehicle” (G2V) operation, or discharge it to an electric power grid during the parking hours, also referred to as “Vehicle-to-Grid” (V2G) operation.



The G2V mode can be used to charge BEVs/PHEVs at reduced cost when the power system load is reduced and generation capacity is abundant, e.g. during night time. The V2G mode may be used when demand is high or supply is accidentally lost, since the stored electric energy can be released from BEVs/PHEVs in an aggregated way, which will offer major contributions to regulation service and spinning reserves(providing an additional generation of energy, in case a generator unit fails, within minutes), as well as load-shedding prevention (Kezunovic, 2012).

The U.S. DoE has identified and mapped key Smart Grid “Assets” to 13 “Functions” that may be enabled by Smart Grid (Table 1) (Bossart and Bean, 2011).

Smart Grid Assets	Functions												
	Fault Current Limiting Wide Area Monitoring, Visualization, and Control	Dynamic Capability Rating	Power Flow Control	Adaptive Protection	Automated Feeder Switching	Automated Islanding and Reconnection	Automated Voltage and VAR Control	Diagnosis & Notification of Equipment Condition	Enhanced Fault Protection	Real-Time Load Measurement & Management	Real-time Load Transfer	Customer Electricity Use Optimization	
Advanced Interrupting Switch									•				
AMI/Smart Meters							•					•	
Controllable/Regulating Inverter						•	•						
Customer EMS/Display/Portal												•	
Distribution Automation				•	•	•	•				•		
Distribution Management System		•		•	•	•	•			•	•		
Enhanced Fault Detection Technology								•					
Equipment Health Sensor		•						•					
FACTS Device			•										
Fault Current Limiter	•												
Loading Monitor		•						•			•		
Microgrid Controller						•							
Phase Angle Regulating Transformer			•										
Phasor Measurement Technology	•	•	•	•		•	•	•					
Smart Appliances and Equipment (Customer)												•	
Software - Advanced Analysis/Visualization	•	•											
Two-way Communications (high bandwidth)	•			•	•	•	•			•	•		
Vehicle to Grid Charging Station												•	
VLI (HTS) Cables			•										

Table 2.1. Smart Grid Assets Mapped to Functions by the U.S. DoE.



Economical reasons:

One great challenge that the electric power system faces since its origin, is the constant struggle to match energy generation to energy consumption. Added to this challenge, is the challenge of avoiding high demand peaks. Such peaks of demand impose constraints on the operation point of the network, which is one of the main causes of power supply failure. The electric power grid is typically overdimensioned in order to cope with the demand of few peak hours in a year span. Satisfying peak demands can be particularly costly, generally there exist three levels of satisfying electricity demands, and these are as follows:

- **Baseload generating units:**

Such units are intended to satisfy the base level of electricity demand.

Meeting such demand has low operating costs and is able to meet fluctuating demands (to a degree) by increasing power generation, or decrease based on demands. These large units usually need a lot of hours even days to get started or to be shutdown.

- **Intermediate units:**

To address greater fluctuations in energy demands are intermediate units.

Although they often have higher operating costs than baseload units, their ability to quickly adapt to demand fluctuations make them more appropriate to meeting higher energy demands.

- **Peaking units:**

To meet the peak demands, these units typically have the highest operating costs but are able to quickly provide a full load within a short period, as well as able to shutdown again within minutes. Due to the nature of their operations and obvious cost, the peaking units only operate for a number of days per year.



Demand Side Management (DSM) and Demand Response (DR) are the terms used to describe the wide range of programs that intend to influence the electric power demand and its usage patterns. Although sometimes they are used indistinctively, there are formal differences. DSM terminology was conceived referring to a broader scope than DR. DSM programs refer to the tools and mechanisms that influence the customer's use of energy (how much and when). DSM programs include different actions taken by the utility to modify or influence the retail customer use of electricity, with the purpose of reducing the individual user's demand, change its use in time, make a more efficient use of it, reduce the aggregated peak load, etc. DSM may be classified in two broad categories:

- **Reduce consumption:**
The end customer is motivated to save energy and use it more efficiently.
- **Shift consumption:**
The end customer is motivated to alter the time of consumption towards off peak hours and reduce consumption during peak hours.

DSM initiatives are intended to modify the consumer demand pattern, with the aim of achieving not only net energy savings but a more efficient use of the energy itself. A broad classification of DSM is summarized in Figure 2.2 by Xiao (2012).

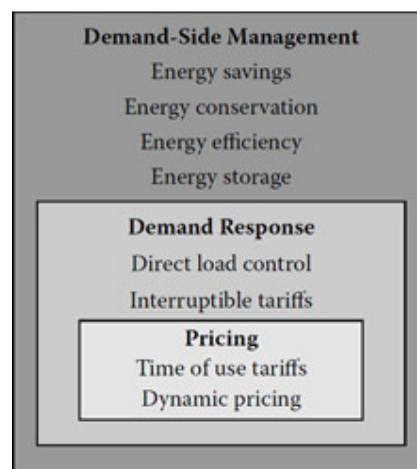


Figure 2.2. Demand side management actions/programs.

Gellings (2009) explains the load shape objectives of an energy service provider illustrated in the table below.

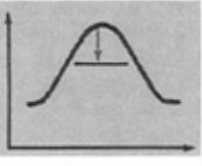
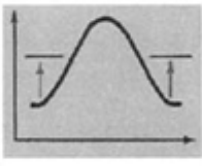



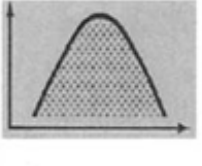
<p>Peak Clipping, or the reduction of the system peak loads, embodies one of the classic forms of load management. Peak clipping is generally considered as the reduction of peak load by using direct load control. Direct load control is most commonly practiced by direct control of customers' appliances. While many service providers consider this as a means to reduce peaking capacity or capacity purchases and consider control only during the most probable days of system peak, direct load control can be used to reduce operating cost and dependence on critical fuels by economic dispatch.</p>	
<p>Valley Filling is the second classic form of load management. Valley filling encompasses building off-peak loads. This may be particularly desirable where the long-run incremental cost is less than the average price of electricity. Adding properly priced off-peak load under those circumstances decreases the average price. Valley filling can be accomplished in several ways, one of the most popular of which is new thermal energy storage (water heating and/or space heating) that displaces loads served by fossil fuels.</p>	
<p>Load Shifting is the last classic form of load management. This involves shifting load from on-peak to off-peak periods. Popular applications include use of storage water heating, storage space heating, coolness storage, and customer load shifts. In this case, the load shift from storage devices involves displacing what would have been conventional appliances served by electricity.</p>	
<p>Energy Efficiency is the load shape change that results from programs directed at end-use consumption. Not normally considered load management, the change reflects a modification of the load shape involving a reduction in sales as well as a change in the pattern of use. In employing energy efficiency, the planner must consider what conservation actions would occur naturally and then evaluate the cost-effectiveness of possible intended programs to accelerate or stimulate those actions. Examples include weatherization and appliance efficiency improvement.</p>	
<p>Deploying new, efficient uses is the load shape change that refers to a general increase in sales beyond the valley filling described previously. This may include electrifying existing fossil uses. These new efficient uses may include the new emerging electric technologies surrounding electric vehicles, industrial process heating, and automation. These have a potential for increasing the electric energy intensity of the U.S. industrial sector. This rise in intensity may be motivated by reduction in the use of fossil fuels and raw materials resulting in improved overall productivity and a reduced impact on the environment.</p>	
<p>Demand Response is a concept related to reliability, a planning constraint. Once the anticipated load shape, including demand-side activities, is forecast over the corporate planning horizon, the power supply planner studies the final optimum supply-side options. Among the many criteria used is reliability. Load shape can be flexible – if customers are presented with options as to the variations in quality of service that they are willing to allow in exchange for various incentives. The programs involved can be variations of interruptible or curtailable load; concepts of pooled, integrated energy management systems; or individual customer load control devices offering service constraints.</p>	

Table 2.2. Load Shape Objectives.

DSM cannot be realized without feedback from the customers. This information is taken directly from customer premises, by deploying meters and communicated to the System Operator (SO) in various ways (even in old fashioned human supervising and manual recording to paper). Until recently, the employment of digital electronics in metering was typically provided only to large customers whose usage and interval measurement requirements justified the added expenses. Furthermore, meter-reading intervals have, still, not been shortened to a desired level close to real-time monitoring.

Advanced Metering Infrastructure (AMI) will improve this situation by enabling the Smart Grid to utilize advanced digital meters at all customer service locations. These meters will have two-way communication, be able to remotely connect and disconnect services, record waveforms, monitor voltage and current, and support time-of-use and real-time rate structures. In this way, the operator will eliminate billing estimations and also prevent energy theft. In addition, these meters will enable automatic DR by interfacing with smart appliances. Smart appliances such as smart refrigerators, cookers, washing machines, vacuum cleaners and plug-in electric vehicles (PEVs) will support communication both with the homeowner and the Smart Grid itself. The homeowner will be able to monitor consumption and control the smart appliances remotely (Grogan, 2012).

The utility will be able to send signals to the appliances that provide consumers with reminders to use them at periods of lower-priced energy or even switch them off during periods of high grid load, thus reducing power demand in times of excessive consumption. The residential consumer benefits from a connection to the Smart Grid in many aspects. A trend is formed, pressing the energy prices and the total energy bills downwards. The consumer is more capable and motivated to reduce consumption. Opportunities are given to reduce transportation costs by using electric vehicles instead of conventional vehicles and, furthermore, sell consumer-produced electricity back to the grid. Utilities will benefit from Smart Grid through improved operations including more accurate and automated metering and billing, better outage management, reduced electrical losses, better asset utilization, improved maintenance and improved planning processes.



2.2 Sensors, sensor networks and their usage in Smart Grids

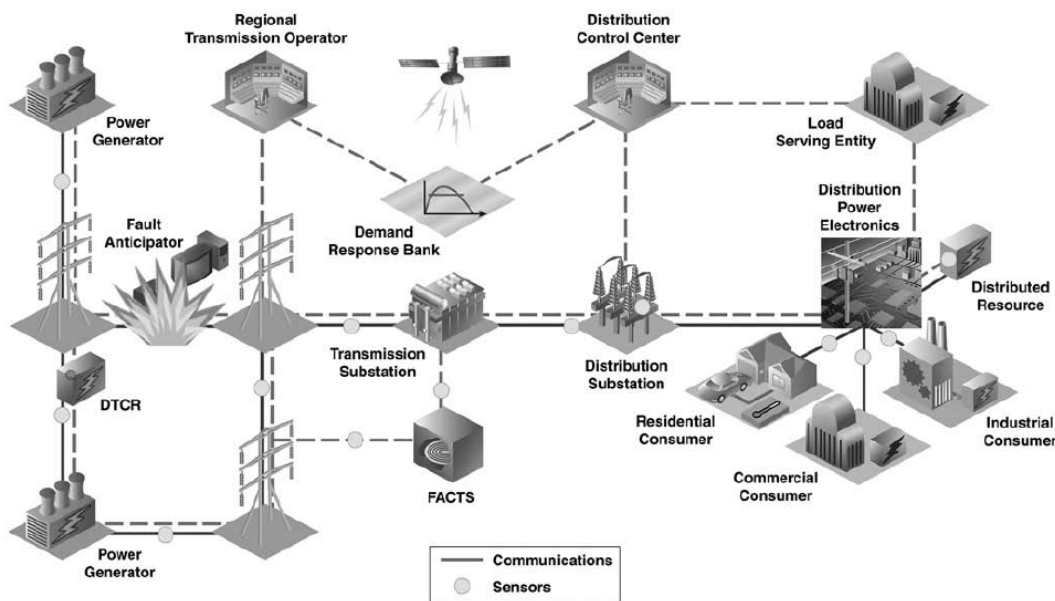


Figure 2.3. Smart grid concept by EPRI.

Sensors are devices that measure a physical property by responding to a physical stimulus, for instance: heat, light, sound, pressure, magnetism, motion, etc and convert it into an electrical signal. They perform an input function. Sensors can be divided in two large categories depending on the excitation method: Active sensors, which require an external source of excitation such as resistance temperature detectors (RTDs) and strain-gages. Passive (self-generating) sensors, which do not need an external source, like thermocouples, photodiodes and piezoelectrics. Devices which perform an output function are generally called actuators and are used to control some external device, for example an electromagnet. Both sensors and actuators are collectively known as transducers. Transducers are devices used to convert energy from one form to another. Common quantities under measurement are: light level, temperature, force or pressure, position, speed, sound, electricity and magnetism.

Table 2.4 provides examples of the main sensor types and their outputs. Further sensors include chemical sensors and biosensors but these are not dealt with in this study. Outputs are mainly voltages, resistance changes or currents. Table 2.4 shows that sensors which measure different properties can have the same form of electrical output (Wilson, 2005).

Physical property	Sensor	Output
Temperature	Thermocouple	Voltage
	Silicon	Voltage/Current
	Resistance temperature detector (RTD)	Resistance
	Thermistor	Resistance
Force/Pressure	Strain Gauge	Resistance
	Piezoelectric	Voltage
Acceleration	Accelerometer	Capacitance
Flow	Transducer	Voltage
	Transmitter	Voltage/Current
Position	Linear Variable Differential Transformers (LVDT)	AC Voltage
Light Intensity	Photodiode	Current

Table 2.4. Examples of sensor types and their outputs.

A Smart Grid sensor has four parts: a transducer, a microprocessor, a transceiver and a power source. The transducer generates electrical signals based on phenomena such as power-line voltage. The microprocessor processes and stores the sensor output. The transceiver, which can be hard-wired, wireless or optical, receives commands from a central computer and transmits data to that computer. The power for each sensor is derived from the electric utility or from a battery.

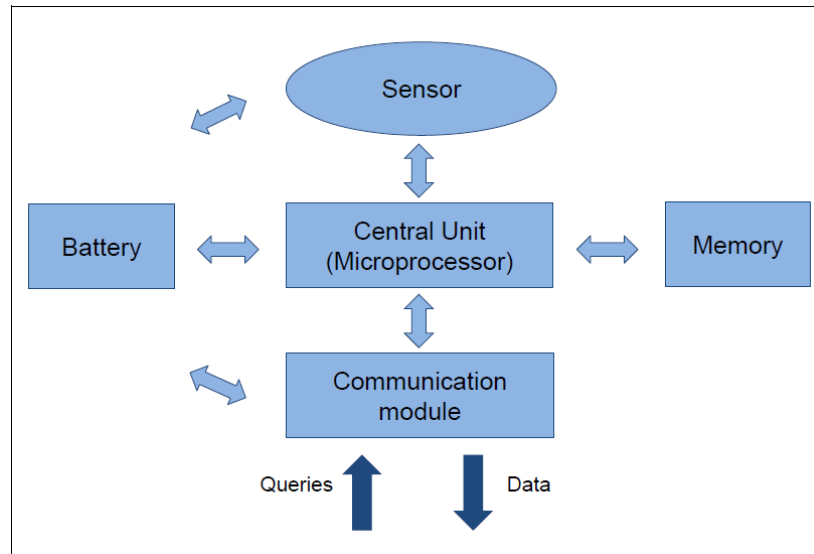


Figure 2.4. Architecture of a smart sensor.

When trying to sense and control an environment, a wireless sensor and actuator network (WSAN) deployment can be utilized. In such a network, nodes communicate with one another via wireless links. The data gathered by the different nodes is sent to a sink which either uses the data locally, through for example actuators, or is connected to other networks (e.g. the Internet) through a gateway (Verdone et al., 2008). Figure 2.5 illustrates a typical WSAN.

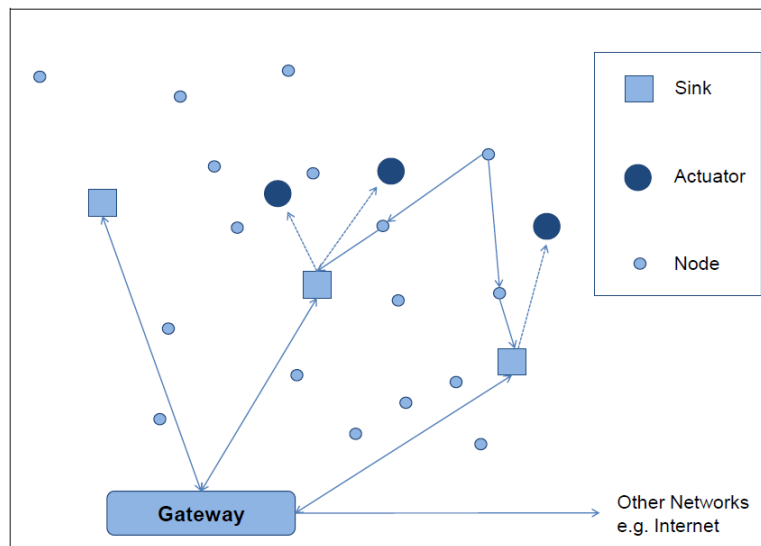


Figure 2.5. Typical wireless sensor and actuator network.

Sensor nodes are the simplest devices in the network. As their number is usually larger than the number of actuators or sinks, they have to be cheap. The other devices are more complex because of the functionalities they have to provide. To assure a sufficiently long network lifetime, energy efficiency in all parts of the network is crucial. Due to this need, data processing tasks are often spread over the network, i.e. nodes co-operate in transmitting data to the sinks (Verdone et al., 2008). Although most sensors have a traditional battery there is some early stage research on the production of sensors without batteries, using similar technologies to passive RFID chips without batteries or ambient backscatter of electromagnetic radiation (Liu et al., 2013).

Sensors can be divided into categories regarding a specific feature. Taking the type of communication technology as a criteria, sensors can be categorized as following:

- Wireless and satellite
- Wired
- Optical fiber
- Hybrid

The most common wireless technologies in use are WiFi, Bluetooth, WiMax and GPS. Wireless sensors can be subdivided into three subcategories depending on the power source and consumption.

The first subcategory is composed of sensors that have significant power available. These sensors are line powered or contain a laptop-sized battery and use technologies like WiFi or WiMax.

The second subcategory includes sensors that use medium to low power to operate. The power source can be rechargeable batteries or shorter life applications.

The third subcategory comprises of sensors that need very low power and are meant for long life operation. In this case, batteries or energy harvesting are used and specialized technologies such as Zigbee, Z-Wave and MyriaNed. Wired sensors utilize the existing power lines to communicate.



The technologies used are Power Line Communications (PLC) for industrial environments and a subset of it; Broadband over PowerLine (BPL) for buildings and homes. Power line carrier communication (PLCC) is mainly used for telecommunication, tele-protection and tele-monitoring between electrical substations through power lines at high voltages, such as 110 kV, 220 kV, 400 kV. Most PLC technologies limit themselves to one type of wires (such as premises wiring within a single building), but some can cross between two levels (for example, both the distribution network and premises wiring).

Typically transformers prevent propagating the signal, which requires multiple technologies to form very large networks. Various data rates and frequencies are used in different situations.

Fiber optic cables are currently used by utility companies for their primary system communication needs. Optical fiber communications will be used extensively in the future to support a Smart Grid's demands such as short delay, high real-time performance, rapid protection and rearrange, small bit error rate, and high reliability, at the same time, good connectivity and economy.

Optical fibers can even be used to real-time online monitoring for the power cable temperature and carrying capacity, and through carrying capacity analysis for fault diagnosis (Liuyuan et al., 2012).

A hybrid communication model makes use of multiple technologies. Many sensors embed multiple communication interfaces for redundancy or interconnection of different systems purposes. For example, data transport may primarily rely on PLC, but RF may be utilized if the PLC is unavailable. Other hybrid models may rely on RF to send data to aggregation points and then utilize PLC or Wi-Fi to transport data. Fiber-wireless (FiWi) access networks appear to be a promising technology (Ghazisaidi et al., 2009).

Sensors can also be grouped according to their placement inside the Smart Grid's systems, as follows:



Sensors in the Generation system

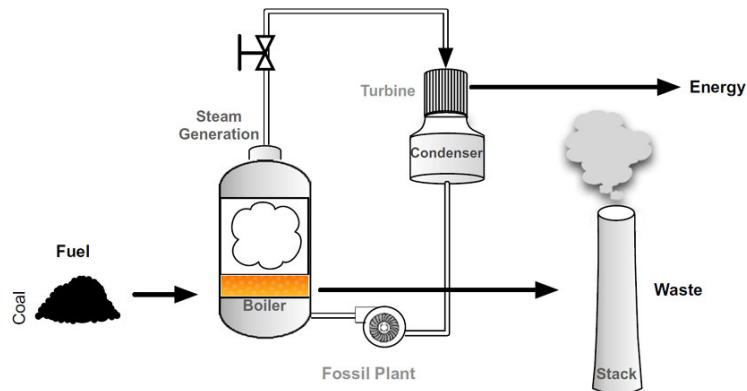


Figure 2.6. A simplified depiction of a coal fueled power plant.

A fossil fuel power plant transforms the chemical energy of fossil fuel, like coal, into electrical energy. Several processes are taking place in order to produce electrical power. The fuel is processed in various ways (purification, mincing) before it is transported and delivered to a burner. Inside the burner, the fuel is combusted with the suitable amount of air (usually preheated to the right temperature) to heat water, inside a boiler, into steam.

The steam is regulated through valves and then driven into large turbines that rotate power producing generators. The steam, having lost the greatest part of its kinetic energy, goes through condensers to be turned into water again and then back to the boiler, thus making the power production cycle more efficient due to the second law of thermodynamics. More on thermodynamics can be found in the work of Borgnakke and Sonntag.

Power plants that consume fossil fuels in other forms such as oil or natural gas differentiate only in the first phase of fuel processing and feeding it to the burner. Nuclear power plants use nuclear fuels, such as Uranium, to conserve a controlled chain reaction inside their core to heat water. The difference here is that the core's cooling system is separated from the steam generation system. Wind, hydro and solar power plants have more simple processes to produce power. Wind and hydro plants transform the raw kinetic energy of wind and flowing water, into electric energy respectively. Solar power plants convert sunlight directly into electricity or can also be used to power boilers for steam generation, replacing the coal fuel and burners with solar energy.

Other important processes of power plants include:

- The storage, transportation, and utilization of fuel.
- The storage, conditioning, and utilization of boiler feed water.
- The collection and removal of waste material.

For each function, industrial control components are used to automate a process loop, and together they make up the larger distributed control system that consists of many such process loops (Knapp, 2011).

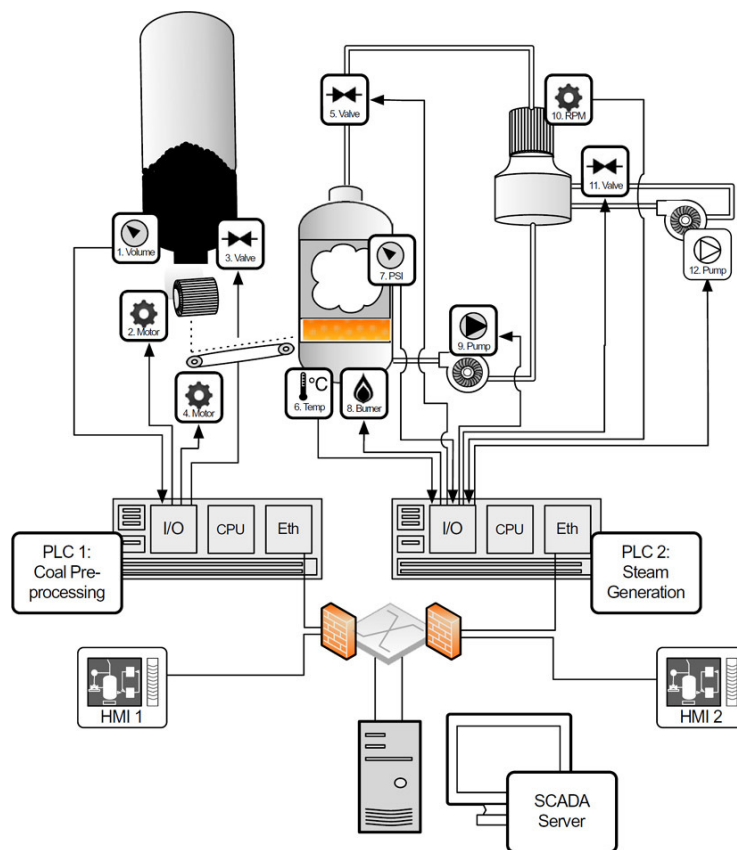


Figure 2.7. A typical electric generation system layout.

Using a coal-fired steam generator as an example in figure 2.7, we can see that the functional mechanisms map to specific designs consisting of several controllers, inputs, and outputs. For example, the fuel supply is an automated system consisting of a hopper and conveyor mechanism, while the generation itself consists of an interconnected system of burner, steam turbine, and coolant systems. There are sensors (inputs) that measure the available fuel in the hopper, as well as sensors that indicate the speed of the conveyor, the amount of fuel in the burner, the pressure in the steam system, the speed of the turbine, and many other inputs that are not illustrated here. There are also controls (outputs) that react to these inputs, such as the fuel pulverization motors, the fuel conveyor, the burner within the steam boiler, and various pumps and valves which control the pressure and rate of both the steam and coolant water.

A Programmable Logic Controller (PLC) is a digital computer used for automation of electromechanical processes, such as control of machinery. The PLCs depicted in Figure 2.7 are modular PLCs consisting of Input/Output (I/O) to the process devices, a processing module to store and execute control application, and a network interface card for Ethernet connectivity to the SCADA network, including basic control via process-specific Human-Machine-Interface (HMIs) as well as a SCADA server to manage the entire generation process. PLC 's I/O are used for fieldbus connectivity e.g. to coal preprocessors or steam regulation. HMIs provide supervision and local control of the processes for instance of coal pulverization or turbine systems.

This oversimplified example contains two process loops (depicted in Figure 2.7) as follows:

1. PLC1 reads volume of the fuel supply from the hopper (1) of the coal pulverizer. When coal is available, it is fed through an opening (2) at a controlled rate through grinders (3) that pulverize the coal. When fuel is available (1) and the grinder is operating (3), the feed conveyor (4) delivers the powdered coal to the burner. The powder is deposited onto a conveyor that feeds the fuel burner.
2. PLC 2 controls the burner and steam generation: engaging the burner (8) in response to the temperature (6) and regulating the flow of steam using valve (5) and pump (9) in response to readings from pressure sensor (7). PLC 2 also



reads the speed of the turbine (10) to adjust the flow of coolant water using another series of valves (11) and pumps (12).

In a real generation facility, additional controllers are used to operate these and other processes, which are much more complex than represented here. There may also be other dedicated control subsystems used for specific functions like turbine control that are connected via the Ethernet network to the PLCs and SCADA server.

Sensors in Transmission

Transmission systems require wide-area communication technology to support real-time measurement of the infrastructure, and they require SCADA systems to enable the automation of real-time operations.

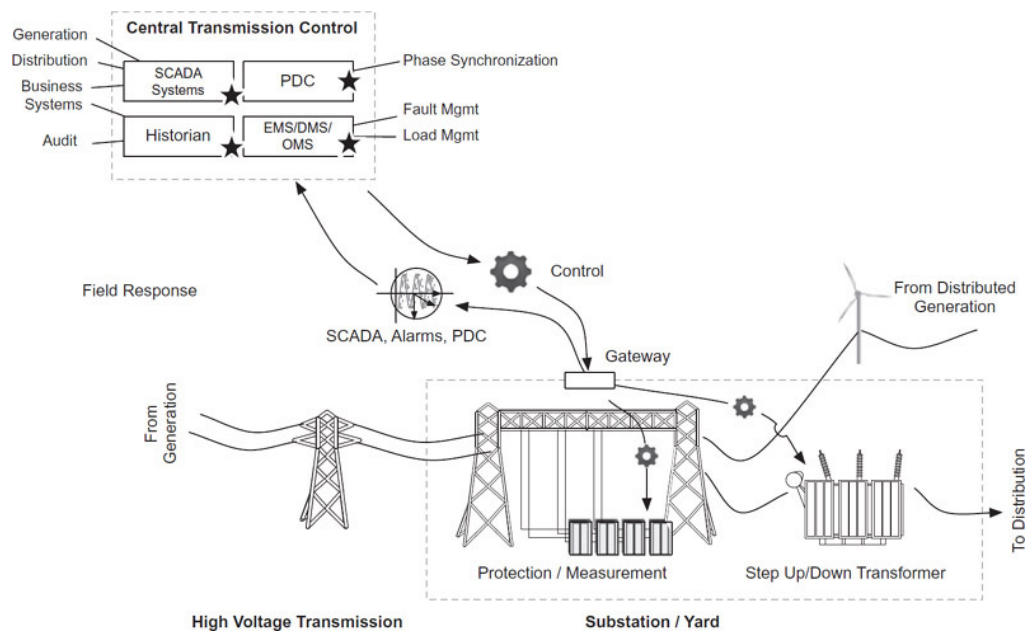


Figure 2.8. A simplified depiction of transmission architecture.

Voltage is stepped up before it enters the transmission system, by a transformer, to make it suitable for bulk and effective transmission to the grid. This typically occurs at generation facilities, but voltages may also be stepped up or down at substations where multiple lines converge, aggregate, or intersect. It will also occur more often, in the future, at distribution side due to the adoption of DG and DER. Substations or "yards" are a primary component of transmission systems. Substations also provide voltage measurement, voltage regulation, and line protection so that electricity can be transmitted as safely and efficiently as possible. The high-voltage energy is transmitted to distribution systems, including secondary and tertiary substations, where electricity is then stepped down to usable voltages and distributed to the end customer.

The transmission infrastructure includes the following important systems:

- The transmission SCADA and substation automation systems.
- The phase measurement systems and phase data concentrators.
- The line protection systems used to prevent surges and outages.
- The transformers used to shape electricity to required voltages for safe and efficient transmission.

Transmission SCADA Systems

Transmission SCADA systems, or T-SCADA, provide similar functions to transmission that generation SCADA or G-SCADA. They provide supervisory (monitoring) control (automation) and data acquisition (measurement). T-SCADA systems are typically designed to manage and control automated substation processes, in the same way that a G-SCADA system manages and controls automated generation processes.

T-SCADA systems support a combination of capabilities: measurement (or collection of measurements from device I/O), monitoring via a user console, and control (via automation logic or direct HMI). Many substation gateways combine T-SCADA functions with network communication capabilities, and act as a central nexus of information aggregation, translation, and communication in addition to SCADA functions. These gateways provide several key functions to the transmission system:



- They provide translation between multiple device and protocol messages from substation protection systems, controllers (remote PLCs or RTUs), Intelligent Electronic Devices (IEDs), synchrophasors, etc. and centralized substation management systems or Energy Management Systems (EMS).
- They provide substation control and distributed T-SCADA. The gateway, which is a computing platform (a server), executes process automation logic (such as ladder logic) much like a PLC.
- The gateway provides activity logging to the substation, where faults, events, and other data (e.g. measurements) are recorded.
- They provide communication back to the control room. Communication channels typically include communication between gateway T-SCADA and centralized T-SCADA or EMS systems (for central management) as well as communication to substation devices for remote maintenance or management of individual assets.

T-SCADA, like G-SCADA, is responsible for monitoring inputs and outputs: Inputs might include phasor measurement, line voltages, frequency, transformer settings, load, faults, while outputs might include capacitance, load adjustments, (step-up/step-down controls), protection/breaker controls.

To effectively transmit electricity throughout the transmission system, it is necessary to have an overview of the voltage and phase angle at key locations in the grid, because electricity flows from higher voltages to lower voltages and from higher phase angles to lower phase angles. A Phasor Measurement Unit (PMU) is a device that measures these electrical characteristics on the grid and then communicates them back to a Phasor Data Concentrator (PDC) and ultimately to T-SCADA systems.

Phasor Measurement Units

PMUs are often called synchrophasors because modern PMUs synchronize multiple phasor measurements from different points on the grid to a common time source, typically using IRIG-B, a GPS-based time synchronization protocol.

Latest advances in high speed packet switching has made time synchronization over packet networks, using the traditional packet method like Network Time Protocol (NTP) or emerging synchronization solutions based on the IEEE 1588 Precision Time Protocol (PTP), an attractive solution too (Aweya and Al Sindi, 2013).



A synchronized PMU or synchrophasor is able to accurately measure the quality of the grid, both in terms of voltage and in terms of current, at any given time across all measurement points. Understanding distributed phasor measurements allows the grid to be utilized more efficiently, by adjusting load throughout the grid to the maximum dynamic limits of the transmission system, at any given point. The result is more efficient, reliable and safe transmission, because available transmission lines are able to transmit the maximum amount of power, while surges or ebbs in load can be reduced or eliminated.

Synchrophasors consist of measurement, synchronization, and logging functions. Typical PMUs will provide multiple measurements up to 30 times per second, as specified by the IEEE Synchrophasor Standard, C37.118–2005. These readings are time-stamped to the synchronized time source and collected by the PDC, which samples the data logging mechanisms of the PMU in real time. The centralized and synchronized measurements are then utilized by T-SCADA and EMS to adjust transmission rates, manage outages, and other functions. Many automation devices include phasor measurement capabilities, just as many synchrophasors support remote management and control, enabling transmission quality to be automated.

Line Protection and Monitoring Systems

Line protection systems prevent undercurrent and overcurrent of powerlines and combine metering and measurement with protection mechanisms. Typically, line protection consists of breakers that will trip to prevent a potentially hazardous fault—much like a home circuit breaker will trip in response to a power surge, in order to prevent a fire or other hazard. Modern protection systems combine line monitoring with automation logic to allow appropriate and efficient responses to a variety of line conditions, overcurrent protection, power swing protection, and recovery, including under-frequency load correction, breaker fault detection and isolation, and synchronization loss detection and recovery (IEEE report, 2005).

Line protection systems are highly dependent of line monitoring, including current, voltage, frequency, power, energy, and phasor measurement. The measurement functions of a protection system overlap with phasor measurement units, and therefore, many protection systems include PMU capabilities (according to IEEE C37.118) or integrate with external PMUs.



Line monitoring is also important for the detection of various abnormal conditions that might indicate equipment failure (or imminent equipment failure). Proactive maintenance of substation devices such as transformers and breakers can extend their life, thus saving expenses and enable failing equipment to be safely repaired or replaced prior to an incident or outage (McDonald, 2012).

Transformers

Transformers typically communicate to protection systems and/or substation automation systems over IEC 61850. There may be a direct communication to a centralized T-SCADA system, or an indirect communication to centralized T-SCADA via substation automation systems in PMUs, gateways, and protection systems.

More on transmission sensing can be found in the work of Phillips, Bose and Rogers (2010).

Sensors in Distribution

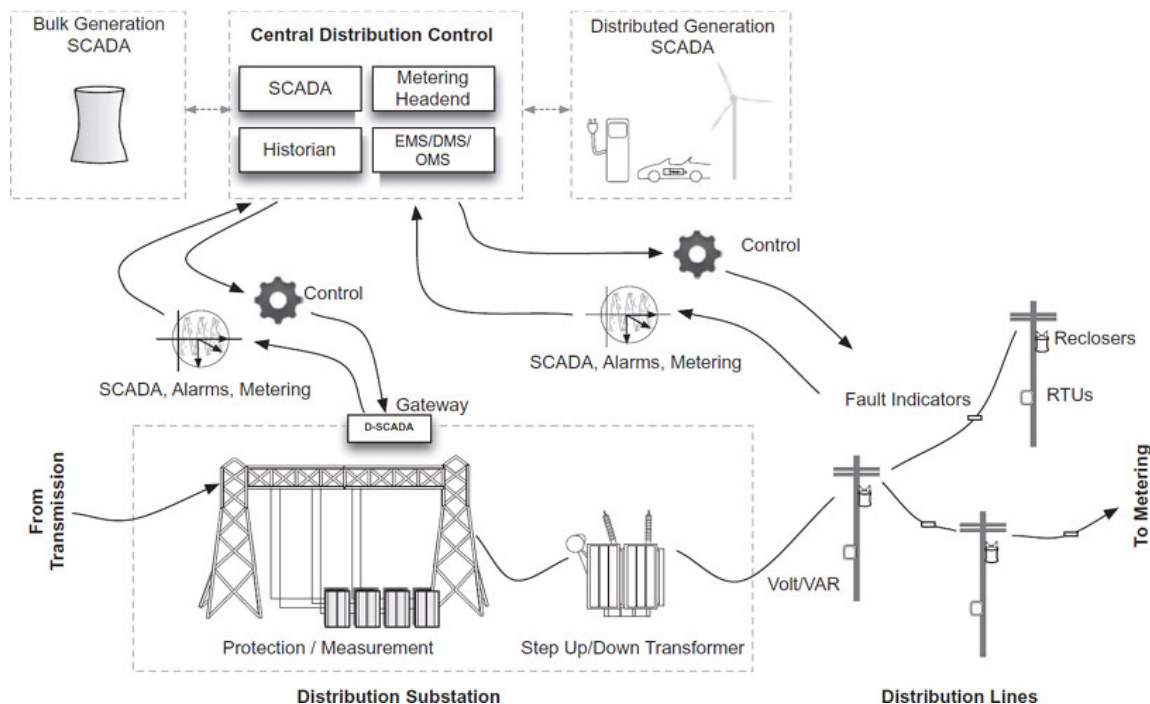


Figure 2.9. A simplified depiction of distribution architecture.

The distribution part of the grid extends from the end of the transmission part (the last substation towards the load) until the meter outside a home or a business. Typically, transformers are used, again, to step down the voltage to usable levels by the metering infrastructure and the end consumer. Distribution lines are numerous and usually support many end users: from city blocks, to suburbs and neighborhoods.

Substations are utilized by distribution systems for energy conditioning, monitoring, protection, and automation. Similar to transmission systems, distribution systems communicate back to a centralized SCADA Master Terminal Unit (MTU), Distribution Management Systems (DMS), Outage Management Systems (OMS), and a variety of back-office systems located in a data center or central control facility. Line measurement and protection systems are, again, vital to effectively manage energy usage, monitor and respond to outages, etc.

The distribution systems are smaller, more numerous, and operate at lower voltages than the primary and secondary substations used in the transmission system. The specific functions of a distribution system have small differentiations. Transmission systems focus more on generation control, delivery, condition management, energy storage/reserve management, interchange management.

On the other hand, distribution focuses more on load management and modeling, two-way power flow, risk analysis and outage management, and Dynamic Feeder Reconfiguration (DFR), islanding and to isolate, bypass or otherwise avoid outages (Sorebo and Echols, 2011).

The distribution architecture is shown in Figure 2.9, and consists of several important systems:

- Field sensors and monitoring.
- SCADA and DMS systems.
- Field controllers and automated field devices.
- Metering and AMI



Distribution SCADA and DMS

Distribution SCADA or D-SCADA systems are responsible for the control of distribution operations, including manual and automated control of load management and DFR. D-SCADA systems, within the substation, control the distribution substation automation, similar to transmission substation automation. They are often included in a gateway device, which communicates back to a larger D-SCADA system in a central control center. Remote D-SCADA servers will typically offer similar features and capabilities as those used in transmission.

These servers are communication gateways that provide: the network communications capability to substation devices (LAN, serial) and to centralized systems (WAN); data concentration functions to collect and aggregate substation data from other systems; automation capability through programmable logic (i.e. a controller); metering functions; fault recording and alerting; and transformer monitoring and control.

Field controllers and automated field devices.

A field controller is a Remote Terminal Unit (RTU), IED or other distributed controller used throughout the distribution system, outside of the substation. It differs from a PLC because it is more suitable for wide geographical telemetry, often using wireless communications, while PLCs are more suitable for local area control (plants, production lines, etc.) where the system utilizes physical media for control. Automated field devices include auto-reclosers, breakers, volt/VAR regulators and capacitors.

Advanced Metering Infrastructure

In legacy power systems, analog meters measured usage at the demarcation of the home or business. Analog meters lack any advanced communication capability and require human intervention for the extraction of readings. Smart Grids add considerable sophistication to metering, and as such they utilize new "smart meters" that not only measure energy utilization, but can also be used to remotely connect or disconnect meters. Smart meters are able to receive commands and communicate utilization to and from a centralized system, eliminating the need for a human meter reader.



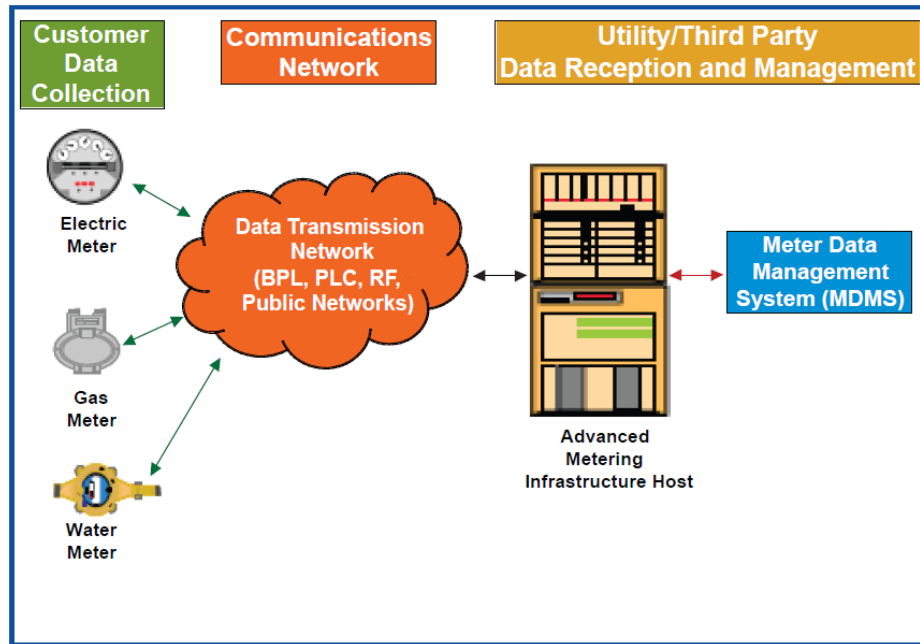


Figure 2.10. AMI building blocks by EPRI.

Advanced Metering Infrastructure (AMI) provides this infrastructure. AMI systems are utilized by many energy, water, and gas utilities. AMI architecture consists of three primary components: smart meters, a communication network, and an AMI server or headend (EPRI, 2007).

The smart meter is a digital meter consisting of the below key elements:

- A solid-state meter for real-time data collection
- A microprocessor and local memory to store and transmit digital meter measurements.
- A communication network often including a home network connection for home automation and other advanced in-home services.

Smart metering also requires interconnectivity of smart meters, which may be deployed by the millions. As such, a highly scalable communication network is required. A variety of network technologies are used in AMI systems, including Broadband over Power Line (BPL), Power Line Communications (PLC), radio networks, or telecommunications (landline, cellular, paging, etc.) networks. Smart meters communicate, ultimately, to the AMI headend.

A headend usually consists of an AMI server, which is primarily responsible for collection of meter data, and a Meter Data Management System (MDMS), which manages that data and shares it with demand response systems, historians, billing systems, and other systems.

Sensors in Utilization

The utilization part of the grid is the final segment, behind the meter, inside the consumer's premises. The most important aspects are presented below:

- Home Area Networks (HANs) represent any in-home communication. Like a Local Area Network (LAN), Wide Area Network (WAN), or Metropolitan Area Network (MAN), a HAN defines the scope of the network itself rather than the devices it interconnects. Various communication technologies are used such as WiFi, Bluetooth and Power Line Communications.
- Home Energy Management Systems (HEMS) provide a system to monitor, manage, and automate in-home energy usage. HEMS interface with In-Home Devices (IHDs) via the HAN, the AMI, and even distribution and utility back-office systems. HEMS may be located in-home as an end-user operated server, but are commonly managed Web interfaces or cloud-based systems.
- Building Management Systems (BMS) are computer-based control systems installed in buildings that control and monitor the building's mechanical and electrical equipment such as heating, ventilation, lighting, power systems, fire systems, and security systems. Numerous sensors are utilized and even more communication protocols, mostly proprietary, to interconnect them with the management system.
- Smart appliances and IHDs imbue residential appliances both large and small with intelligence, allowing HEMS to monitor and control in home power usage.
- Private generation, such as residential solar or wind generation, can be considered extremely small-scale instances of distributed generation. Electric vehicle charging stations may also have the ability to sell power back to the grid and can be considered an in-bound energy source to the larger grid.



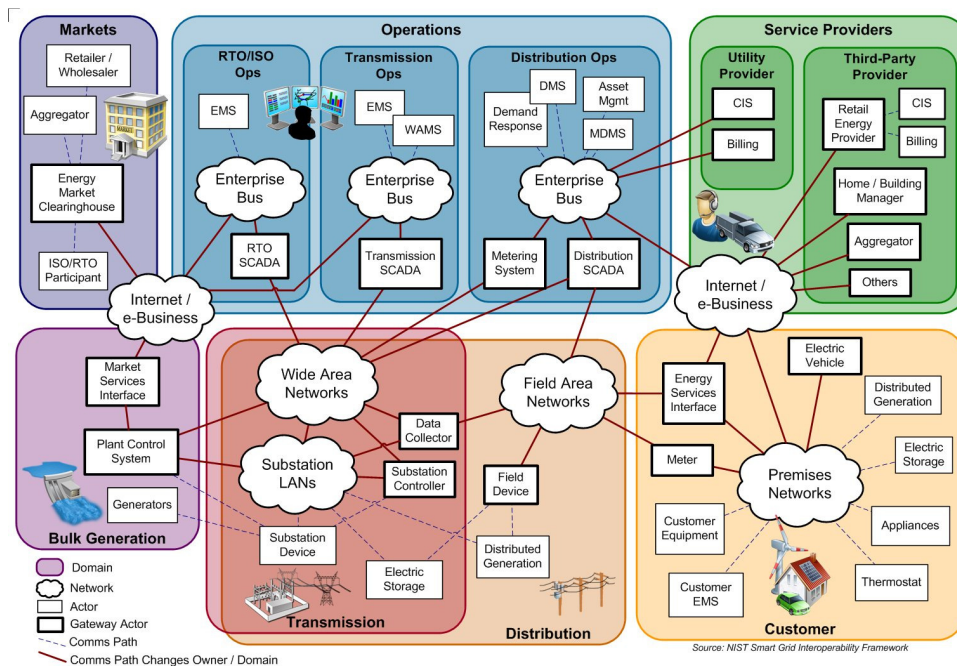


Figure 2.11. A Smart Grid services and technologies overview by the U.S. N.I.S.T.

2.3 Data characteristics and utilization

A Smart Grid can be divided into three layers, concerning its technological aspects. Each layer is composed of digital and non-digital technologies and systems from the domains of telecommunication, information, and energy technology as seen in Figure 2.12. From an architectural perspective, a Smart Grid can be viewed as an additional communication layer that is virtually overlaid on to the existing power grid and on which an application layer is built (Kranz and Picot, 2011).

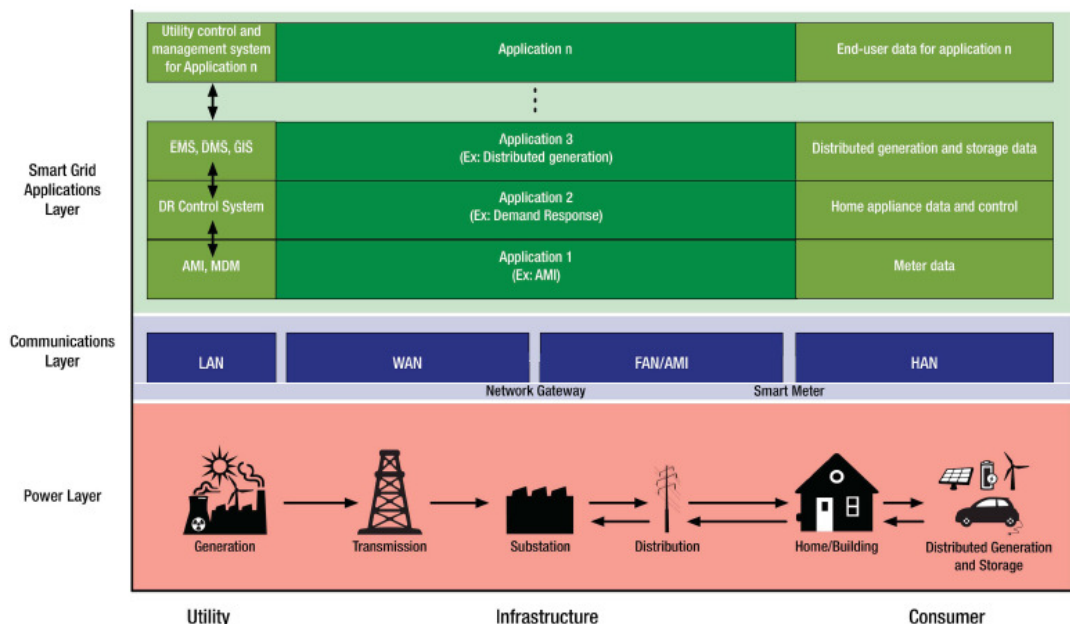


Figure 2.12. Smart Grid layers by the NRRI.

This layered approach reduces the complexity by creating independent components and subcomponents. This interconnection of formerly isolated components, actors, networks, and technologies, leads to the creation of a system of systems (NIST 2009). These components need to be compatible and have well-defined interfaces with their upper layer. The components of each layer provide specific services to the above layer and utilize the services of the layer below them, resembling to the internet's original design principle by employing an end-to-end architectural approach: components and actors can send and receive data without knowing the network's structure (Economides and Tag, 2009).

A communication layer lies on top of the power layer but, currently, there is no end-to-end communication available. Utilities have interconnected parts of their infrastructure with SCADA systems in order to manage grid operations but a link is missing: there is a communications gap between customers' premises and the rest of the components and actors in the energy chain.

The AMI, also referred to as Field Area Network (FAN), will bridge this gap by linking the existing utilities' communication networks with smart meters. Smart meters also serve as the central gateway to in-house devices such as BMSs and home appliances inside a HAN. This gateway can be viewed as an analogous to the last mile in telecommunications. On the communication layer's one end, the AMI connects smart meters, while on the other end, it interfaces with the backhaul network that aggregates and transports the data to the WAN, as illustrated in Figure 2.13 (NIST 2009).

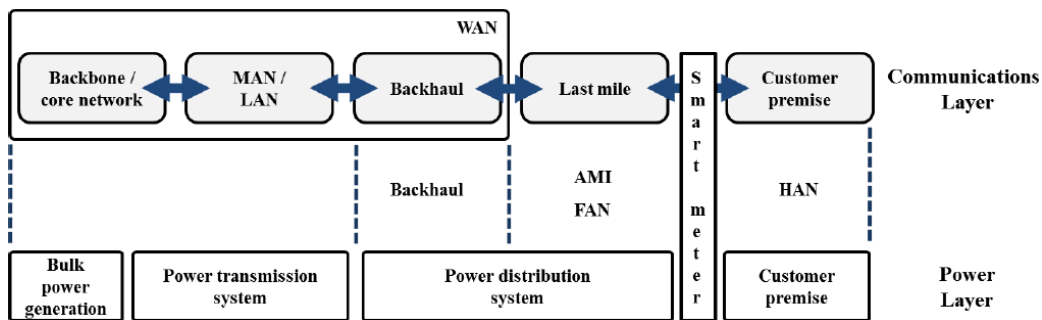


Figure 2.13. Smart grid communications architecture mapping by the US NIST.

Smart meter data are needed by many authorized actors apart from the utility. These actors are mainly market actors, such as Energy Service Providers (ESPs). Actors will be able to utilize two-way communications with the meters so as to provide innovative, value added services like sending price signals to consumers, controlling appliances and changing tariffs (ERGEG 2007). Table 2.5 provides an overview of the market actors and their respective data needs.

Actors	Use of Data
DSO	Grid operation, ES billing, forecasting, loss detection, and customer service process automation, customer switching, power quality monitoring
Supplier	Billing, tendering, forecasting, and trading
Generation (distributed)	Plant operation, fulfillment of supply contracts
Customer	Information, usage control, decision making
ESPs and other third parties	Using energy efficiency measures, input to home and building automation, aggregation of supply and demand data for electronic electricity markets
Government Body or Regulators	Monitoring power quality, statistics, and disaster management

Table 2.5. Actors and their data needs (based on ERGEG 2007).

End-to-end communications inside the Smart Grid face problems of interoperability, due to the plethora of used protocols and problems of security, due to needed compliance to national security and privacy requirements. Literally dozens of protocols are used, routable and non routable, enabling communication within a subsystem but impeding communication between subsystems. Therefore, the development of open and non-proprietary communication protocols and standards is crucial (NIST, 2012).

The data exchanged through Smart Grid communication systems have different behavioral characteristics, regarding the network's Quality of Service (QoS) potential. Taft and Ahmed (2009) categorize the data in three classes: a) operational data that tends to be constant in volume and timing and may be the same in terms of bandwidth and latency requirements, b) non-operational or telemetry-type data and c) asynchronous event messages generated by Smart Grid devices in reaction to grid physical events.



They note that these messages come in unpredictable bursts and floods that need to be transmitted and processed with very low latency. The North American Synchro-Phasor Initiative network (NASPInet) accommodates five classes of data services for supporting different types of applications named from A to E with descending performance requirements (NASPInet, 2009). Jeon (2011) groups these five classes into two groups: real-time streaming data and historical data. Realtime streaming data may be real-time control and visualization applications, such as closed-loop voltage control and feed-forward remedial action control.

Historical data may be non-real-time applications, such as post-disturbances analysis and off-line studies. Alcatel-Lucent (Deshpande et al., 2011) gathered some of the most important Smart Grid applications and their qualitative network requirements in the following Table (2.6).

APPLICATION	DATA RATE/VOLUME (AT ENDPOINT)	LATENCY ALLOWANCE (ONE-WAY)	RELIABILITY	SECURITY
Smart metering	Low/Very low	High	Medium	High
Inter-site rapid response (for example, Teleprotection)	High/Low	Very low	Very high	Very high
SCADA	Medium/Low	Low	High	High
Operations data	Medium/Low	Low	High	High
Distribution automaton	Low/Low	Low	High	High
Distributed energy management and control (DER, storage, PEV)	Medium/Low	Low	High	High
Video surveillance	High/Medium	Medium	High	High
Mobile workforce (Push to Talk)	Low/Low	Low	High	High
Corporate data	Medium/Low	Medium	Medium	Medium
Corporate voice	Low/Very low	Low	High	Medium

Table 2.6. Network requirements for Smart Grid applications by Alcatel-Lucent.

Another important aspect of the data that is generated is its increasing volume. Economical and environmental factors are driving the evolution of the power grid from its current static state towards becoming a dynamic and real time system.

The effort to match fluctuating supply (due to increasing penetration of renewable resources) to continuously increasing demand, leads to the deployment of millions of sensors throughout the grid. The most important types of sensors, like PMUs and smart meters, can generate a huge amount of data in real time.



For example, PMUs can produce a measurement every tens of milliseconds. Smart meters report meter data at the interval of 5-15 minutes, with a future tendency to decrease the interval to one minute or less. These data must be collected, ingested and delivered to analytics applications to generate control decision in almost real time. An analysis system that supports such huge amount of data, aiming at a diverse set of applications must fulfill the fundamental requirements of: scalability, real time performance, high reliability, enforced security and low cost (Yin et al., 2013).

The system must be scalable so as to support future sensor deployments and grid expansions. Its performance is of vital importance because data concerning the stability of the grid must be processed in real time while historical data are kept and used in statistical analysis.

Partial failures of the large number of hardware and software components are unavoidable, thus, the system should be able to withstand these without service interruption. The preservation of business sensitive and consumer private data is also a challenge. Finally all of the above should be offered at a reasonable cost. High costs could stall investments or discourage selection from consumers.



Chapter 3: Security of the Smart Grid

3.1 General issues of security in the Smart Grid

The power grid constitutes a primary, critical infrastructure for a country. National security and economic vitality depend on the grid's reliable and continuous operation. A disruption or destruction of electricity grids would have a serious impact on societal functions, reaching even to a global scale. The incorporation and application of Information and Communication Technologies (ICT) has led to higher efficiency and flexibility to the grid. Unfortunately, this growing dependency on ICT brings along new threats and risks as well. Intentional and unintentional threats are a reality and tend to multiply.

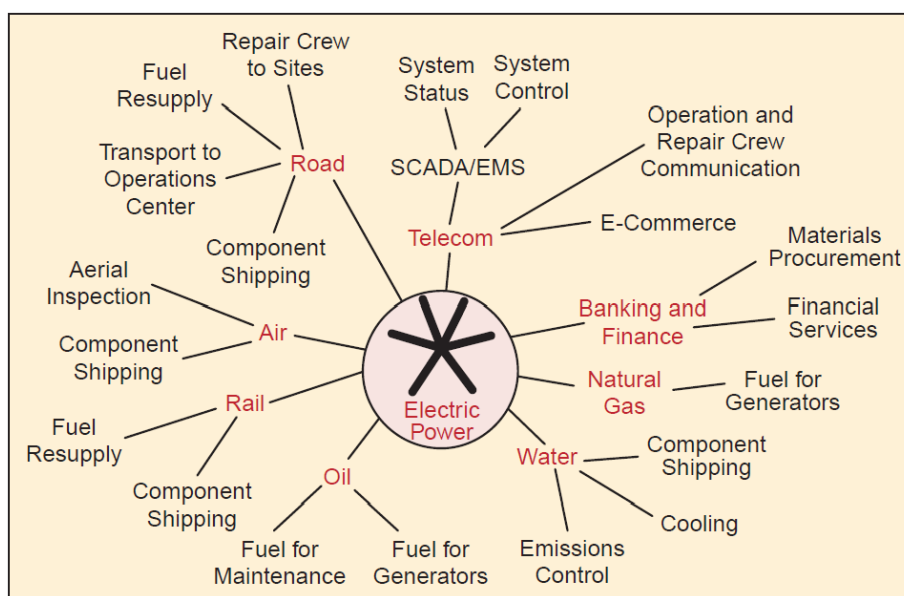


Figure 3.1. Electric power infrastructure dependencies example by Rinaldi et al (2012).

Not all threats are intentional or originating from human intervention. Unintentional threats can come from various factors. Human-originated unintentional threats include human error or lack of action (usually due to inexperience or inadequate training), such as neglected maintenance of hardware or unprecedented peak demands, and security limits violation, such as profit driven actions that jeopardize the grid's stability.

Naturally occurring threats include extreme weather conditions, such as storms, typhoons, tornados, tsunamis, floods or even persistent drought affecting hydro-plants, and natural disasters, such as earthquakes and solar electromagnetic storms.

A study from the North American Reliability Corporation (NERC) (2009) reported 104 disturbances in the bulk electric system of United States and Canada during the first three quarters of 2009. As illustrated in Figure 3.2, natural threats are the major cause of these disturbances. It is obvious that the world climate change, that is ongoing, will bring even more extreme weather phenomena posing as one of the greatest challenges power grids have to face.

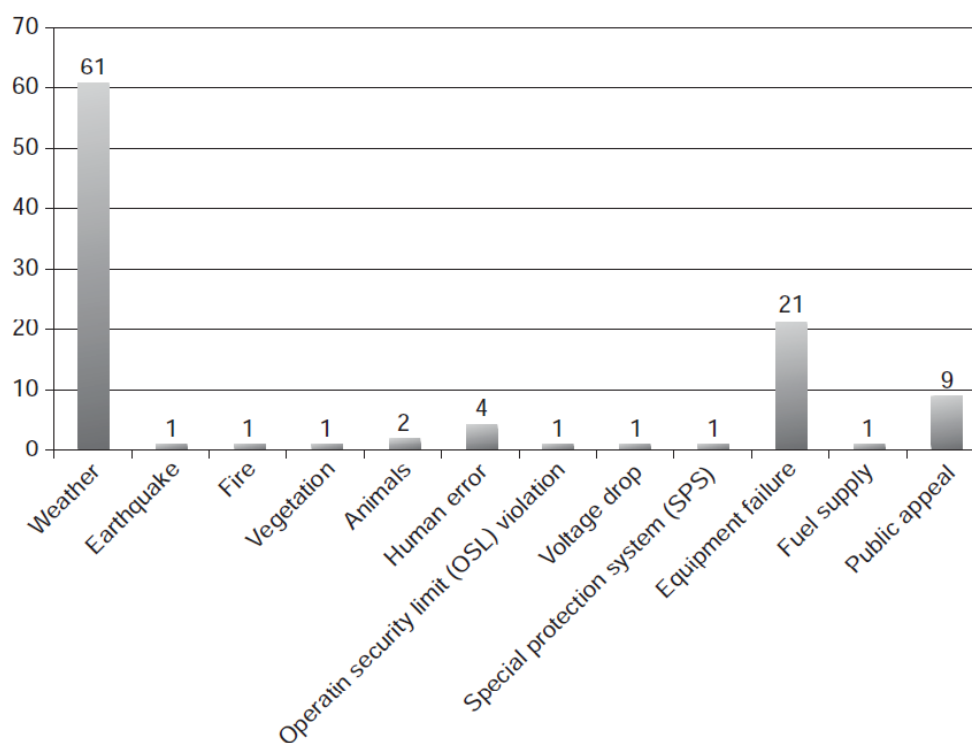


Figure 3.2. Major causes of disturbances according to NERC (2009).

Before discussing intentional human threats, a small reference to the inherent vulnerabilities of Smart Grids should be made. All systems inherit minor or greater vulnerabilities from their composing elements. This is also the case in a Smart Grid where communication technology lies at the heart, while the system was not originally designed to take this complex form but rather evolved by adding various technologies.

It can be considered as a System of Systems (SoS) in which component-systems attempt to: a) fulfill valid purposes in their own right and continue to operate to fulfill those purposes if disconnected from the overall system, and b) are managed in part for their own purposes rather than the purposes of the whole (Maier and Rechtin, 2000), (Chandy et al., 2010). In such cases, it is very difficult to determine the effect on one part of the system that results from a disturbance introduced at another part because of the non-linearity of interdependent subsystems (Asprou et al., 2012).

According to Rinaldi et al. (2001) there are four different types of interdependencies of critical infrastructure systems: physical and geographical (obvious), cyber and logical (not so obvious). Moreover, the high complexity incommodes an overall overview of the grid in real-time. Although this digital transparency and accessibility is desirable it is also a major vulnerability. Access to and compromise of one subsystem could lead to an overall compromise or a total interruption of power supply.

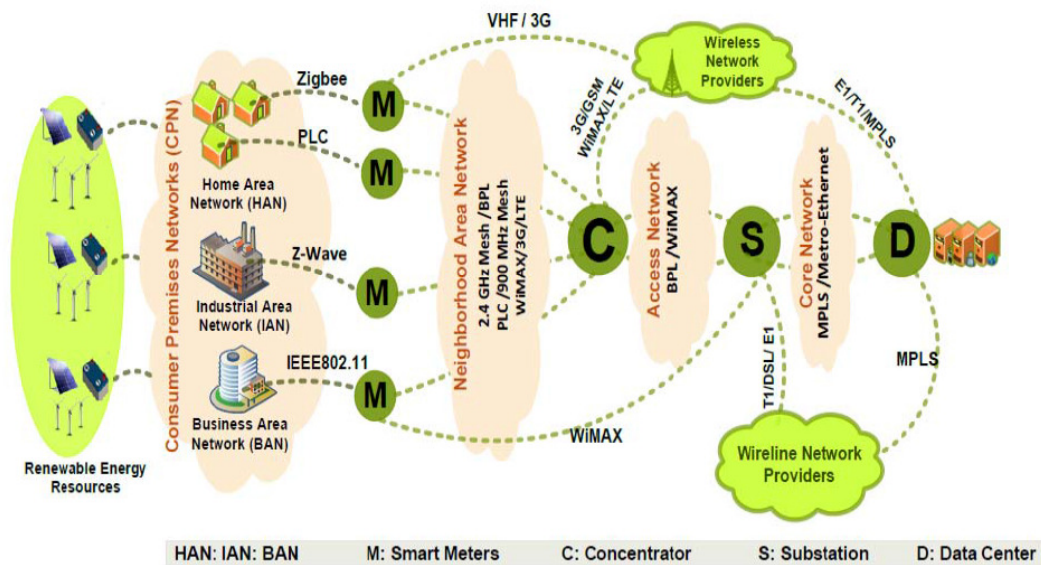


Figure 3.3. Smart Grid architecture and network options by Al-Omar (2012).



Other serious vulnerabilities are given by Clements and Kirkham (2010) and summarized by Aloul et al (2012):

- Customer security: smart meters and their functioning as gateways for enormous amount of consumer data.
- The great number of intelligent devices: devices managing supply and demand are deployed in massive numbers (estimated 100 times larger than the Internet) and may act as attack entry points.
- Physical security: many components are outside the utilities' premises, making physical access easier.
- The lifetime of power systems: there is an inconsistency between classical power systems, designed for long duration and relatively short-lived IT systems.
- The implicit trust between traditional power devices: device-to-device communication is prone to data spoofing.
- Different teams' background: inefficient communication between teams can lead to bad decisions.
- Using Internet Protocol (IP) and commercial off-the-shelf hardware and software: IP and commercial technologies carry their inherent vulnerabilities e.g. Denial of Service.
- More stakeholders: more people participating leads to greater probability of insider threat and sensitive data leakage.

Intentional human threats constitute a smaller threat to the power grid in total, for the time being, compared to naturally occurring ones, but are definitely not negligible. Vulnerabilities in Smart Grid technologies may not currently present significant risk to national security because Smart Grid technologies are not widely deployed yet (Flick and Morehouse, 2011). The spreading of critical information and the increasing addiction to technology and electricity give rise to abnormal behaviors in cyberspace and encourage cybercrime. Apart from great knowledge concentration, the capabilities of attackers have evolved as well. The motives behind their actions vary and are influenced by socioeconomic conditions.



The most common motives behind cyberattacks, in an impact ascending order, are:

- Curiosity
- Notoriety
- Revenge or extortion
- Financial gain
- Terrorism
- Spying and cyber electronic warfare

Curiosity is a very common motive usually among young people fascinated with technology. Smart meters will be installed and accessible in almost every house, providing young hackers with a new challenge at easy reach. Deep understanding of Smart Grid functions is not an issue for “script kiddies” (unskilled adolescent attackers), since many tools for ICT exploits, like Backtrack and Metasploit, are freely available on the internet.

Notoriety motivates hackers who have the experience and skills to perform massive attacks, usually for activism reasons or attraction of publicity. These hackers can cause a lot of damage, mostly financial, because their next hit always has to be greater than the previous one, targeting global recognition. It can also motivate script kiddies. Revenge or extortion are not usual motives but whenever this is the case the impact of the attack can be considerable. An ex-employee that wants to strike her, or his, old company for personal reasons or a frustrated partner or an outraged consumer matches this profile. For instance a utility’s IT employee who loses her, or his, job has enough inside information to harm the organization’s equipment and operations, causing a disturbance to the power supply of a whole region. Personal differences could also drive attempts to blackout specific buildings or neighborhoods.

Financial gain is the most common and greatest motive for attackers. A home user could try to manipulate the meter’s readings to transmit lower consumption than the actual to the service operator or to make it worse, also tamper a neighbor’s meter to report both houses’ consumption and charge the neighbor for both.



Producers could tamper the meter to over-report produced power to receive higher benefits, thus threatening the stability of the grid since the falsely reported supply would be shorter than the real demand. Other electricity market stakeholders could also try to manipulate DR real-time reported data to benefit from the stock-market resembling transactions. Industrial espionage is also present in the electric power industry. An employee could also try to sell strategic blueprints to a competitor company or cause operational damage to her, or his, company under the instructions of the competitor.

Terrorism motives mobilize extremist religious or nationalist groups of people. Such a group, targeting a specific geographical region or country, would first attempt to attack its critical infrastructure in physical or cyber space. Terrorist groups could assault lightly guarded equipment such as remote substations or long transmission lines (also serving as backbone communications via coexisting optical fibers) to cause a total interruption of power delivery to the load. Again, financial incentives could be given to hired cybercriminals to assist in remote cyber attacks.

Spying was always a common practice between countries, especially neighboring ones. Cyber electronic warfare refers to politically motivated cyberattacks of a country to conduct sabotage and espionage towards another country, impacting its economy and psychology. What started as cyberwar movie fiction became a reality in the last decade with the discovery of Night Dragon virus and Stuxnet worm.

The McAfee antivirus company discovered that in November 2009 coordinated covert and targeted cyberattacks, originating from China, have been conducted against global oil, energy, and petrochemical companies (McAfee, 2011). The Stuxnet worm was at first identified by the security company VirusBlokAda in mid-June 2010 and is believed to have been created by the United States and Israel to attack Iran's nuclear facilities (Keizer, 2010).



Finally, an important issue of security that affects end users and market participants is data privacy. Smart meters measure energy consumption in a higher resolution than traditional meters and could also integrate or work together with gas, water and heat meters in the future. They will also act as communication gateways for appliances and devices within future ‘smart-homes’. Quinn (2008) has pointed out that by analyzing high resolution energy usage data, the following information can be inferred: the specific type of electrical appliance that was used by its load signature (depicted in Figure 3.4), patterns and personal habits of the residents such as wake up time, time of absence and time of PHEV charging, or even the resident’s age and social status.

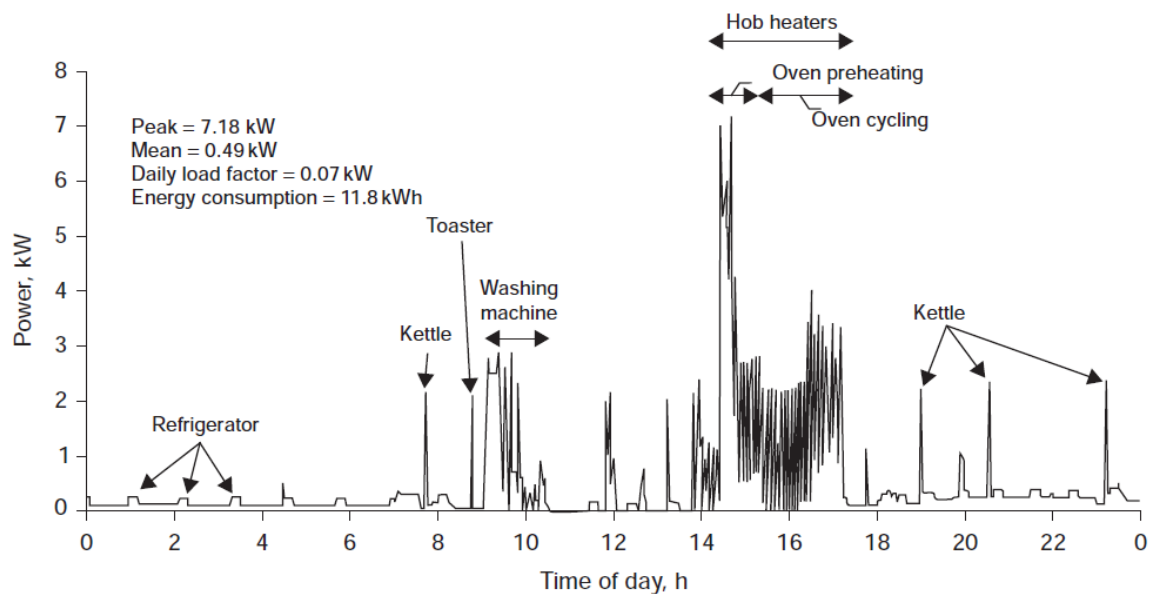


Figure 3.4. Inference of used appliance via analysis of the daily power load.

Utilities may take advantage of such ‘assets’ by selling collected usage information to marketing agencies or other interested parties, following an internet advertising-like scheme. Some businesses may aggressively pursue this information such as efficiency consultants that could use collected smart metering data to identify possible clients, as well as identify efficiency holes that could be plugged to save consumers’ energy costs.

Robust privacy policies are needed to regulate usage of Smart Grid data but certain privacy aspects of smart metering data could be better protected by design (Kalogridis et al., 2011). Generally, all these processes of mass data exchange increase the attack surface and the probability of consumer data and business sensitive information leakage as well, because information can also be inferred from the data that are transferred to a third party.

3.2 A bottom-up system security approach: identifying targets and consequences

The Smart Grid constitutes a system of interconnect and interdependent systems, thus, its security cannot be approached only from a single point of view. Nevertheless, an effort to provide a bottom-up approach will be attempted by examining the security of each individual system.

Generation system

Common concepts are used in generation facilities, regardless of the generation method, concerning information generation, utilization, and automation. Information and automation systems attacks or manipulations can be identified by examining the specific areas that are vulnerable to potential exploitation. Some general areas of risk are illustrated in Figure 3.5.

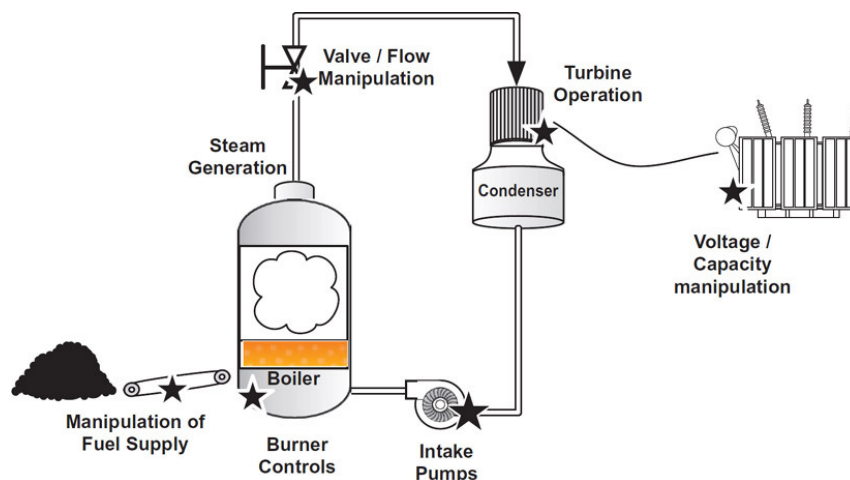


Figure 3.5. A depiction of generation architecture and possible targets.

In principle, any system that is controlled by a microprocessor or that is controlled by any device that contains a microprocessor and an operating system can be compromised. Areas of interest, illustrated here, are as follows: the mechanism(s) used to feed fuel into the burner; the mechanisms of the burner itself that control rate of combustion, regulate temperature via steam pressure, etc.; the mechanisms used to control the intake and flow of water/steam that is used to drive the turbine; the turbine generator; and the mechanisms used to transform the generated energy to the appropriate voltages and frequencies for transmission and distribution. While the accessibility to these various mechanisms will vary, the manipulation of any one mechanism can influence the generation process as a whole.

Specific components that constitute attack or manipulation targets are:

- Individual Programmable Logic Controllers (PLCs)
- The SCADA systems
- The Human-Machine Interface (HMI)
- The network that interconnects all of the above

The primary target of an attack would be the network used to interconnect all actuators and sensors. This is usually an Ethernet network using IP protocols or a legacy serial bus network. Although the physical access to an industrial network is well protected, once an intruder gains access, it is fairly easy to overhear, manipulate or inject data due to the unsafe protocols utilized. Fieldbus protocols such as Distributed Network protocol (DNP3), Modicon Communication Bus (Modbus), Inter Control Center Protocol (ICCP), PROFIBUS/PROFINET, Common Industrial Protocol (CIP), etc. are designed following a common architecture of request and respond: a "master" device, such as an HMI, sends commands to subordinate "slave" devices, such as a PLC, to retrieve data (reading inputs) or apply control (writing to outputs).



Many of these protocols lack authentication, encryption, or other basic security measures, therefore, a malicious actor or attacker could utilize the "request and respond" system as a mechanism for "command and control" like functionality (Knapp, 2011). Some specific security concerns regarding industrial control protocols include: network or transport failure that could cause protocol failure and the availability of various commands that could harm, manipulate, disable or extract information from the slave devices. Network attacks could include man-in-the-middle (MITM), network replay, or denial-of-service attacks.

The HMI and SCADA systems are also key targets. They could be used to establish a command and control (C2) channel outside of the control room, to enable data theft and/or further attacks remotely. A compromised HMI could: misrepresent measurements of other compromised PLC or SCADA to hide the breach from human operators, present false measurements (otherwise accurate) to trick the human operator into mal adjusting an output, crash itself so that no view and control of the plants processes is possible. PLCs have built in communications ports, usually 9-pin RS-232, but optionally EIA-485 or Ethernet. Modbus, BACnet or DF1 is usually included as one of the communications protocols. Other options include various fieldbuses such as DeviceNet or Profibus. Network connectivity to SCADA servers is mostly done via Ethernet and TCP/IP while the device I/O is typically via the fieldbus protocol. They are built using common hardware and a commercially available operating system like Windows, while many utilize an embedded operating system (OS) or a real time operating system like VxWorks.

PLC programs are typically written in a special application on a personal computer and then downloaded by a direct-connection cable or over a network to the PLC. The program is stored in the PLC either in battery-backed-up RAM or some other non-volatile flash memory. Most PLCs utilize Ladder Logic Diagram Programming, a model which emulates electromechanical control panel devices (such as the contact and coils of relays).



Langner (2011) showed that Stuxnet malware exploited publicly announced flaws from Idaho National Laboratory (INL) and Siemens, concerning Siemens' PLCs, at a Chicago conference in 2008. He proved that manipulation of PLC logic is not limited to the alteration of existing logic, but can be used to introduce entirely new logic, replacing or appending legitimate code to almost any end. All these make the PLC vulnerable, in the way that an attacker could gain access via the network and exploit a known OS vulnerability.

The attacker's target would be to:

- Alter the flow of a whole process via changing set points, timing or other variables in the PLC.
- Insert new commands.
- Remove specific commands, e.g. bypass safety restrictions.
- Copy and extract commands to steal intellectual property (industrial espionage).

The manipulation of a single process can affect the whole generating process and eventually bring it to a stop. For example, in Figure 2.7 an extreme, though not impossible, scenario would be to manipulate PLC2 logic that controls steam generation to overheat steam, bypass temperature safety limits and shut the valve 5, resulting in an explosion of the heater.

Transmission system

Transmission systems are highly distributed, with power lines extending up to thousands of kilometers, covering large geographic areas. Unlike generation systems, transmission systems have easier physical access. A generation plant is typically behind closed walls, protected with strict access controls and physical security mechanisms. On the other hand, remote substations represent a physical access risk, as they can be relatively easy targets since their physical security is minor. While transmission substations are physically secured to a certain degree, the lines themselves are easily accessible.



Possible targets in transmission infrastructure include:

- The transmission SCADA and substation automation systems.
- The Phase Measurement Systems (PMSs) and Phase Data Concentrators (PDCs).
- The line protection systems, used to prevent surges and outages.
- The transformers, used to shape electricity to desired voltage levels.

Transmission SCADA systems, or T-SCADA, have similar functionality to generation SCADA, or G-SCADA. Their provided functions to transmission are: supervisory (monitoring, via a user console), control (automation, via automation logic or direct HMI) and data acquisition (measurement or collection of measurements from device I/O). Many substation gateways combine T-SCADA functions with network communication capabilities to provide: a) translation between multiple device and protocol messages from substation protection systems, controllers (remote PLCs or RTUs), intelligent electronic devices (IEDs), synchrophasors, etc. and centralized substation management systems or energy management systems (EMS), b) substation control (acting like a PLC) and distributed T-SCADA, c) activity, fault, event and other data logging to the substation, d) communication back to the control room.

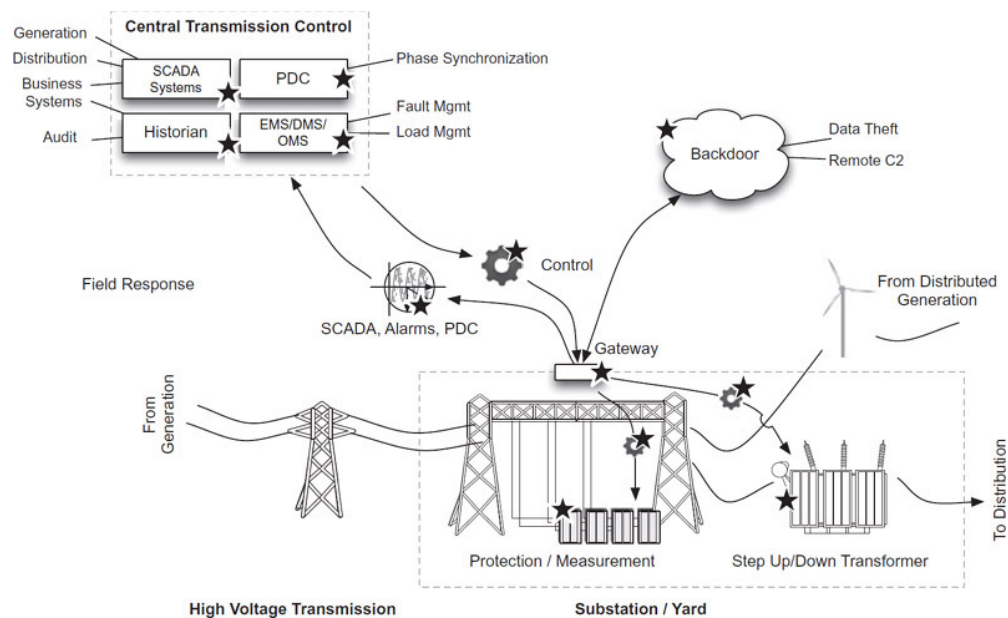


Figure 3.6. A depiction of transmission architecture and possible targets.

Figure 3.6 illustrates some possible targets in transmission. A compromise of T-SCADA can lead to manipulation of phase measurement and synchronization, power conditioning, load, etc. While not so obvious, G-SCADA and distribution SCADA systems can also be manipulated through this compromise since they use data from T-SCADA to ensure proper loads are being generated and delivered to the distribution systems.

Historians, and through them, real-time business intelligence systems are also affected due to their input of falsified or manipulated data from T-SCADA. Generally, the gateway (illustrated in Figure 3.7) is the perfect target for a cyber attack towards transmission: It is reachable via both the wide area network (TCP/IP) and the device network (serial bus protocols), it supports both control and data acquisition aspects of SCADA, it is responsible for messaging to and from the control room, and (typically) it runs a commercially available OS.

An attacker could then directly manipulate all communications to and from the substation—including the command and control capability of centralized T-SCADA or EMS. T-SCADA servers or substation gateways control the routing of power and the protection of transmission lines by connecting and disconnecting them from the grid. An attacker could inject SCADA protocol traffic to or from the substation to cause an unnecessary disconnection resulting to a power outage.

Other vulnerabilities in the gateways include email (SMTP) and web interface (HTTP) support that require certain open ports and could be taken advantage of to materialize MITM attacks, DoS, data theft and covert communications between a compromised substation and other substations in the network.



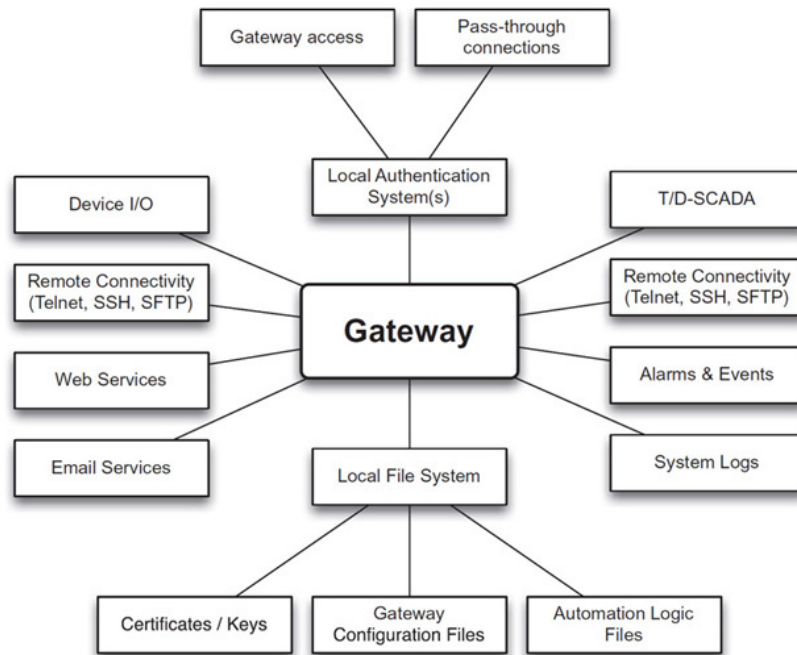


Figure 3.7. T-SCADA gateway services.

Substations communicate with the control room via WAN connections. This communication also poses a possible target. In the Open Systems Interconnection (OSI) physical layer, wireless and fiber optic technologies are commonly used. Wireless communications are more vulnerable while optical fiber communication is more secure. In the presentation OSI layer, Secure Socket Layer (SSL) and Transport Layer Security (TLS) protocols are mostly used in WAN communications under the International Electrotechnical Commission (IEC) 61850 standards. TLS and its predecessor, SSL, are secure enough protocols but there are still some vulnerabilities that can be used to launch MITM and DoS attacks that can result in eavesdropping or data manipulation and communication blocking respectively (Fender, 2009), (Fisher, 2001).

T-SCADA and EMS servers can also be comprised. Such compromise would result in reliability and safety jeopardy similar to G-SCADA discussed earlier. An attacker, after taking over a T-SCADA server, could: misrepresent values sent to SCADA console, to data historians and to other services in the back office systems, insert new logic to controllers like IEDs and RTUs and manipulate secure communication channels towards substation gateways or other substation assets.

PMUs and synchrophasors nowadays include remote management and control capabilities that automate transmission quality. Unfortunately, this brings the same vulnerabilities as in other SCADA system components. They bare network interfaces, Ethernet and serial, support multiple protocols, like HTTPS for management access, DNP3 and Modbus and utilize commercial operating systems, typically Windows. A possible compromise would have impacts that range from minor scale, like inefficient transmission, to major scale, like a total disruption of delivered power. Manipulation of a PMU's measurements could result in: loss of line condition supervision (when a PMU is disabled), erroneous load reports leading to improper load management, unnecessary activation of recovery action systems and line protection systems, leading to instabilities.

Line protection and monitoring systems rely on measurements received from PMUs and are usually integrated within them. Their objective is to protect the transmission lines by tripping circuit breakers. Similarly, they bare network interfaces like Ethernet, serial and USB, support industrial protocols like IEC 61850 and DNP3 and commercial protocols like TFTP and HTTPS and web services like NTP, all these built on top of commercial OSs. Event, measurement and alarm logging is provided as well. A successful attack could lead to disruption of service, impacting whole regions, or causing of damage to generation equipment by opening and closing a breaker out of synchronism, also known as the Aurora vulnerability (Zeller, 2011).

Transformers pose a small risk in the security of transmission. Their communication is limited to protection systems and T-SCADA, from which they receive external control via IEC 61850 protocol. Nevertheless, an attacker could use them as an entry point to gain access to other interconnected systems like substation automation and protection systems. A manipulation of a transformer could result in excessive voltage levels that would deteriorate the transformer's hardware and overload transmission lines, while reporting normal measurements back to monitoring systems.



This broad range of access methods and their geographical proximity to urban area make these systems a key target for attacks. Successful attacks would not only impact substation automation but would serve as a launching point for attacks to other interconnected systems, thus propagating the threat. Via a compromised D-SCADA, an attacker could gain access and breach outage management systems, the AMI or even G-SCADA systems all the way back to generation facilities.

Field controllers and automated field devices like RTUs and IEDs present a considerable risk. RTUs contain multiple communication interfaces like Ethernet and serial via various technologies like WiMax, GSM and satellite. Support for multiple protocols like IEC 61850, DNP3 (serial and TCP) and Modbus (serial and TCP) is provided, as well as, automation logic and physical interfaces like USB and removable memory cards for data extraction and firmware updates.

Field devices like reclosers and Volt/VAR systems encompass fewer communication capabilities. Network interfaces are often limited to serial interface, used protocols include IEC 61850, DNP3 (mostly serial), and/or Modbus (mostly serial). Automation logic is limited and interconnected only to the field RTU or IED. A compromise of field devices or controllers could have minor to major impacts but limited to a specific region.

Minor impacts would be inefficiencies in operations and inaccurate reported data, while an area's blackout would be a major impact. An attacker could manipulate a protective recloser to trip unnecessarily, creating a cascading effect throughout the distribution system. A complete compromise of an RTU could allow an attacker to insert malicious logic into the controller that could cause failures, while reporting normal conditions back to DMS and central D-SCADA systems.

Smart meters pose a small security risk to the Grid, if compromised individually, but a greater one if compromised massively. Their most common features are: communications, via optical or serial ports, via wireless, like GSM and ZigBee and diagnostics, via infrared ports or short-range wireless like Bluetooth, which can be used for meter readings as well.



Through these features, remote management and configurations capabilities are provided, usually via proprietary dedicated software, that includes: remote meter configuration, utilization and demand assessment, load profiling, remote disconnection of power supply and others. An attacker has easy physical access and could manipulate its function to report smaller consumption or access the board memory via available ports and interfaces.

Krebs (2012) pointed out that it is very easy to hack a meter via the optical diagnostics port, using inexpensive hardware. A massive hacking of meters to manipulate reported consumption could lead to hundreds of millions of dollars in losses for utilities. A DoS attack could also be utilized, to prevent communication to the AMI, via RF jamming or readily available tools like Metasploit Framework.

AMI headends, collection and MDMS systems can introduce a major risk for the Grid. They typically run on Windows and are located at the utility's premises. Most MDMS systems utilize commercial Relational Database Management Systems (RDBMS).

Vulnerabilities are often in commercial OSs and database systems, while their expected lifetime is long and patching is difficult in real-time operation environments. A successful exploit of a MDMS server would provide unauthorized control over all aspects of AMI, including the representation of AMI data to other systems and the messaging and communication of AMI. By manipulating the AMI communications, an attacker could manipulate AMI data passing through, inject false data and block legitimate data. This could result in readings altering, prevention of power disconnection of a rogue meter or targeted disconnection of power to specific buildings or facilities. An unauthorized access to a database could lead to manipulation of historical or readings information, but could also be used as an entry point to AMI components or to propagate to other databases such as billing and customer management systems. This poses a serious threat for customers' privacy since usage profiles, billing information and other sensitive information could be exposed.



The control room

The control room lies at the heart of the IT infrastructure and is typically secured and heavily guarded. Physical access is highly controlled and the risk of intrusion is minor. Cyber access is also well guarded concerning external networks, utilizing firewalls, IDSs and IPSs.

Emerging threats, though, cannot be overlooked. The traditional "air gap" separation of SCADA and ICS systems from other private and public networks is now called into question. The US Department of Energy's Industrial Control Systems Cyber Emergency Response Team (ICSCERT) issued an alert in response to growing trends in both control system accessibility and the emergence of ICS exploitation tools, "that increase the risk of control systems attacks.

These elements include Internet accessible ICS configurations, vulnerability and exploit tool releases for ICS devices, and increased interest and activity by hacktivist groups and others." The availability of publically released tools, targeting PLCs or industrial protocols put any accessible control system at risk. At the same time, "The ERIPP and SHODAN search engines can be easily used to find Internet facing ICS devices, thus identifying potential attack targets.

These search engines are being actively used to identify and access control systems over the Internet. Combining these tools with easily obtainable exploitation tools, attackers can identify and access control systems with significantly less effort than ever before." (ICSCERT, 2012).

Other very important threats are social engineering and insider threats. The impacts of a possible compromise could be disastrous. A successful penetration could end up in business and private data theft or a regional blackout cascading to a national or even international level, depending on the attacker's motivation.



3.3 Solutions, countermeasures and general guidelines

As a critical infrastructure element, Smart Grid requires the highest levels of security. Security, in general, should be considered as a continuous process and not a onetime product. According to EPRI (2009) “every aspect of the Smart Grid must be secure. Cyber security technologies are not enough to achieve secure operations without policies, on-going risk assessment, and training. The development of these human-focused procedures takes time—and needs to take time—to ensure that they are done correctly.”.



Figure 3.9. A holistic view of security by EPRI.

The NIST Smart Grid Interoperability Panel (2010) issued a guideline for Smart Grid cyber security where an overall Smart Grid cyber security strategy is described in steps. The proposed steps are as follows:

1. Selection of use cases with cyber security considerations.
2. Performance of a risk assessment.
3. Specification of high-level security requirements.
4. Development of a logical reference model and Assessment of Smart Grid standards.
5. Conformity Assessment.

The high level objectives that need to be met are:

- **Availability:** Ensuring timely and reliable access to and use of information is of the most importance in the Smart Grid. This is because a loss of availability is the disruption of access to or use of information, which may further undermine the power delivery.
- **Integrity:** Guarding against improper information modification or destruction is to ensure information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information and can further induce incorrect decision regarding power management.
- **Confidentiality:** Preserving authorized restrictions on information access and disclosure is mainly to protect personal privacy and proprietary information. This is in particular necessary to prevent unauthorized disclosure of information that is not open to the public and individuals.

Availability and integrity are the most important objectives, concerning the Grid's reliability. Confidentiality is the least critical for system reliability but starts to become more important in systems that handle customer data like AMI and DR.

According to Flick and Morehouse (2011) a utility company that operates or initiates an information security program has two major frameworks to choose from; either the ISO/IEC 27000 series or the Information Security Forum's of Good Practice (SoGP).

The ISO/IEC 27000 standards provide organizations with a set of international best practices for information security that focuses on risk assessment and control implementation. The SoGP provides organizations with a documented set of best practices that should be implemented to develop and maintain an effective information security program, and is available to all free of charge.

Knapp (2011) states that these best practices are extremely important and can be divided into four steps: a) identifying what systems need to be protected, b) separating the systems logically into functional groups, c) implementing a defense-in-depth strategy around each system, and d) controlling access into and between each group. The identification of systems that need to be protected can be performed by following available international standards like International Society of Automation's ISA-99 that will separate devices in two categories: critical assets and non-critical assets.



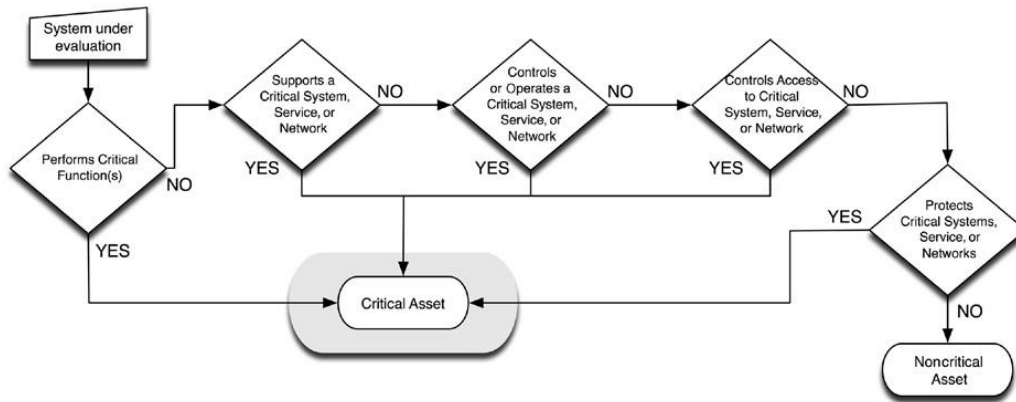


Figure 3.10. Process Diagram for Identifying Critical Cyber Assets.

The aggregation of assets under common domains allows uncontrolled information to flow and increases the attack surface. In order to reduce this exposure, the separation of assets into functional groups is needed. In this way, specific services like web services and email are tightly locked and controlled.

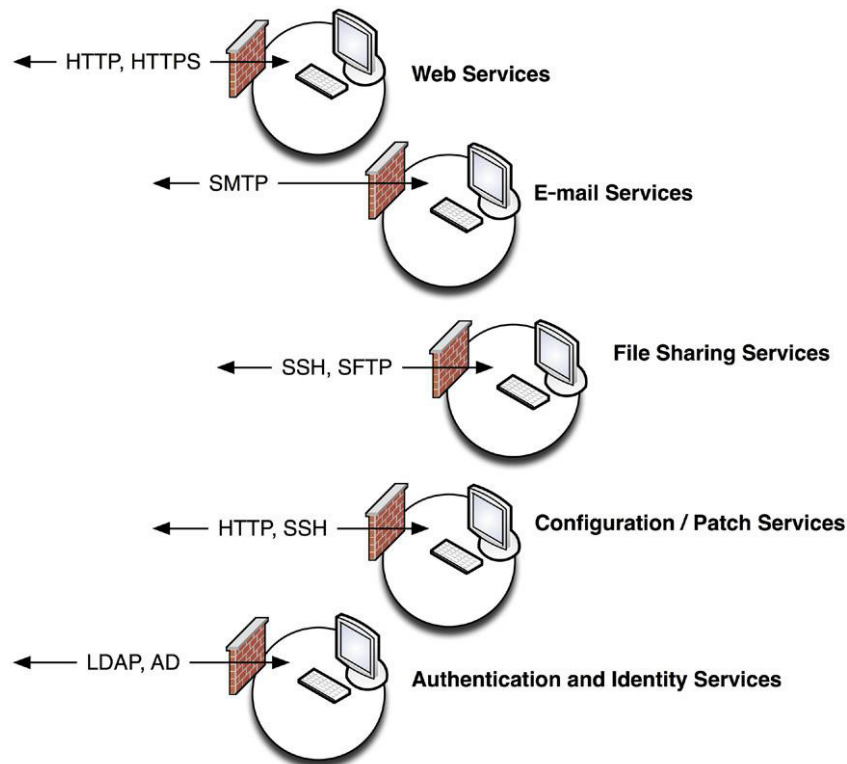


Figure 3.11. Example of asset separation into functional groups.



These isolated functional groups, or enclaves, are secured using various methods: by dedicated firewalls, intrusion detection and prevention devices, application content filters, access control lists or other controls.

An in depth defense strategy is proposed by all standards organizations. By “in-depth defense”, a philosophy of a layered or tiered defensive strategy is implied. The corresponding layers vary from OSI layers to policy layers, depending on the context.

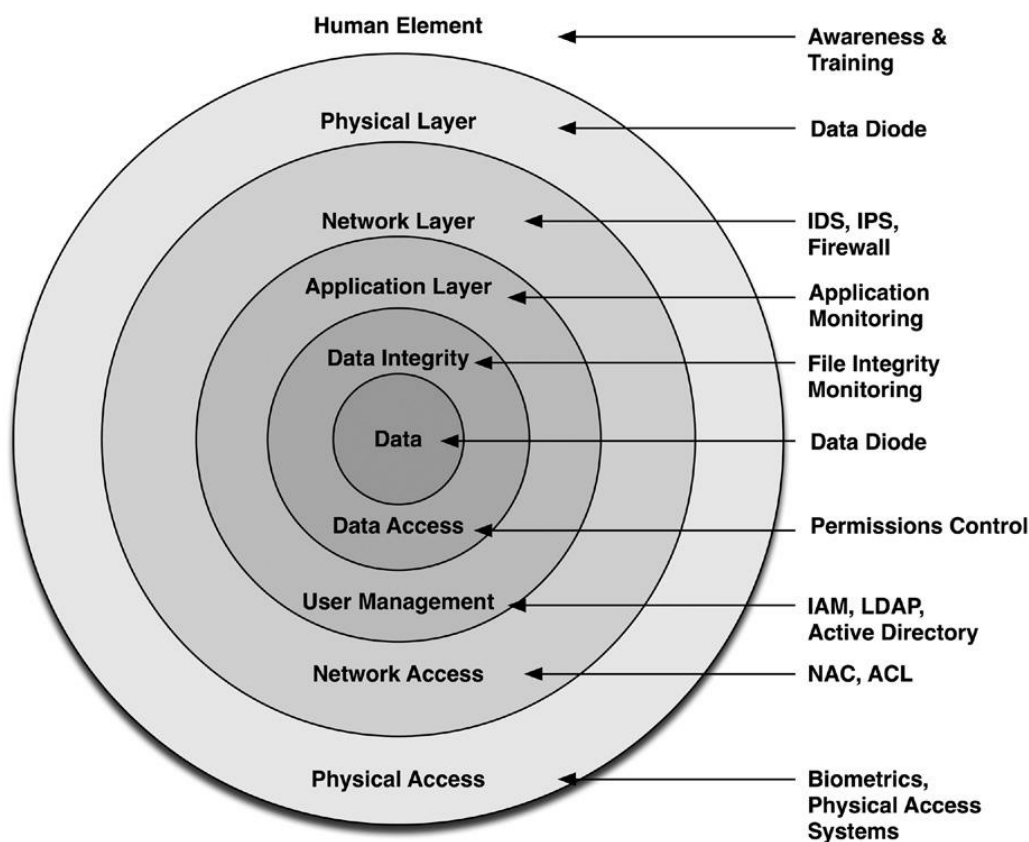


Figure 3.12. In-Depth defense with corresponding protective measures.

To make things more difficult for an attacker, a further lock down of services to specific users or groups is needed. Access control is a difficult, nonetheless, essential task. There are many technologies that enforce access control like Network Access Control (NAC) or authentication services, but a successful implementation is impeded by the complexity of managing users and their roles and mapping them to the specific devices and services. Nevertheless, the more layers of complexity applied to the rules of user authentication and access, the more difficult it will be for an attacker to gain unauthorized access.

Other practical security solutions include (Aloul et al., 2012), (Wang and Lu, 2013), (Clements and Kirkham, 2010):

- Authentication of identity for all network devices. An implicit deny policy should be applied by organizations, such that access to the network is granted only through explicit access permissions.
- Embedded malware protection for all devices. The manufacturers are required to embed in their products a secure storage that contains keying material for software validation during upgrades or patching. Using a key, the system can validate any newly downloaded software prior to running.
- Vulnerability assessments and penetration testing must be performed at least annually to make sure that elements that interface with the perimeter are secure.
- Awareness and continuous training programs should be put in place to educate the network users about security best practices for using network tools and applications.
- Devices must support mutual authentication techniques using Transport Layer Security (TLS) or Internet Protocol Security (IPSec), Virtual Private Network (VPN) architectures and Public key Infrastructure (PKI) for secure communication. Additionally, an enhanced security function that should be used is device attestation. Device attestation techniques provide a method to securely ascertain if a device has been tampered with, as well as the true identity of a device (prior to any on-site provisioning) (Metke and Ekl, 2010).
- Utilities should only collect the data needed to achieve their goals, in order to minimize possible data leakages and information theft.



- Various teams in the organization should cooperate smoothly and be equally involved in securing the Smart Grid network.
- The life cycle of the Smart Grid is longer than that of the IT systems involved, therefore, all IT technologies should have the ability to be upgraded.
- The development of a robust authentication protocol is needed for communications between Smart Grid parties. The protocol must operate in real-time offering minimum computational cost, low communication overhead, and robustness to attacks, especially Denial-of-Service attacks.

Generally, security must be part of the Smart Grid design.



Chapter 4 : Smart Grid implementations

4.1 Case studies

Smart Grid realization attempts have started throughout the globe. The transition is slow and mostly focuses in current grids' infrastructure upgrades. The costs are enormous, so governmental support is inevitable. USA has given a high priority in their electrical grid's evolution by issuing at least 100 public grants worth \$3.4 billion (The White House's Office of the Press Secretary, 2009). The funded companies have also contributed an equal amount. Some of the most important implementations worldwide are presented below.

Boulder, Colorado USA - SmartGridCity from Excel Energy

Xcel Energy started a Smart Grid project in 2008 at Boulder, Colorado. The \$100 million Boulder Smart Grid project was named SmartGridCity. SmartGridCity is a "fully integrated Smart Grid community with what is possibly the densest concentration of these emerging technologies to date". SmartGridCity was the first of its kind in the world. Boulder's Smart Grid includes updated substations, transformers, and feeders. The Boulder Smart Grid uses a fiber-optic loop that encircles the city. This network allows for households and utilities to communicate with each other.

The Boulder Smart Grid also has the ability to reroute power during an outage. Participating customers in Boulder have in-home smart meters such as smart thermostats and smart plugs.

These smart meters communicate with the Smart Grid network and allow customers to access their usage information online. Consumers will be able to program their appliances online and choose which energy source to use. In addition to in-home monitoring, Xcel Energy has chosen a few homes to act as small power plants.

One example of the Smart Grid technologies being placed in these test homes is the placement of solar panels on the roof. The panels are connected to a battery, providing backup energy for the consumer's homes and for the grid as well.



Xcel Energy is also pioneer in launching dynamic pricing pilots, offering participants different tariffs as an incentive to shift electricity consumption from on-peak to off-peak periods. Three pricing options are being tested: Time-Of-Use (TOU) rate, Critical Peak Pricing (CPP) rate and Peak Time Rebate (PTR) rate. The TOU rate will break the day into two periods (on-peak and off-peak). CPP Rate will add a third interval to the TOU rate when system capacity/economic conditions require reduced energy usage; and PTR rate which allows customers paying the standard residential rate and at the same time offers a rebate if the electricity consumption is reduced during critical peak times.

Austin, Texas USA

Austin, Texas, started its Smart Grid project in December 2008, called the Pecan Street Project. This project is run by Austin Energy and involves several high-tech companies, including IBM, Semiconductor, GridPoint, and GE Energy.

Austin Energy chose the Mueller development in Austin to execute the Smart Grid project, a 700-acre development on the former site of the Robert Mueller Municipal Airport. The Mueller community is comprised of new, green, efficient homes and businesses that run off of an on-site power plant.

The first phase of the project, entitled Smart Grid 1.0, is a 440-square-mile system that includes over 500,000 devices and involves roughly 100 terabytes of data which measure minute-to-minute consumer energy use down the appliance level, solar panel generation, electric vehicle charging, transformer impacts and even natural gas and water use for hundreds of households. This Smart Grid includes approximately 1 million consumers and 43,000 businesses.

Since April 2013, the Pecan Street Research Institute has opened membership in its research consortium to university students, faculty and researchers from around the world. Upon sign-up, new members receive a free sample data set of home electricity use that appears to be the largest ever made available to university researchers. The free data set available to research consortium members includes seven days of disaggregated, time-stamped, one-minute interval electricity use data for 10 homes participating in Pecan Street's research in Austin.



The data set includes electricity use, voltage and apparent power readings for the whole home, and disaggregated electricity and apparent power readings for 12 circuits within the home. Data for three homes with solar panels and two homes with a Level 2 electric car charger is also included. The data set is also provided in 15-minute intervals.

Sacramento, California USA

The Sacramento Municipal Utility District's (SMUD) SmartSacramento Project was federally financed in 2012 for a system-wide deployment of an advanced metering system integrated with existing enterprise and information technology systems as well as a partial deployment of advanced distribution grid assets that equip distribution circuits with automated control and operation capabilities.

The project also includes customer systems and a field test of plug-in electric vehicle charging stations. Smart Grid Features Communication infrastructure includes wireless systems that provide two-way communication for smart meters, customer devices, and distribution automation equipment. A new backhaul communications network, meter data relay network, and front-end data management system are being deployed throughout the SMUD service territory. Software platforms for meter data management and analysis are being installed to organize, integrate, summarize, and make data accessible from the smart meters.

These systems provide SMUD with expanded capabilities to link customer information, electric distribution operations, and system-level reliability information. Advanced Metering Infrastructure (AMI) includes the deployment of approximately 600,000 smart meters covering SMUD's entire service territory. This system provides automated meter reading, improved meter accuracy, enhanced outage response and notification, and improved theft detection.

More detailed and timely data on peak electricity usage improves load forecasting and capital investment planning. Time-based rate programs include time of use, critical peak pricing, and time of use with critical peak pricing. Customers with smart meters selected to receive the new program rates can keep their existing rates or enroll in the new program.



The aim is to evaluate the relative merits of these programs in terms of load impacts, customer acceptance, and cost effectiveness. SMUD expects to provide customers with greater control over their electricity bills and limit capital investment and emissions that result from adding peak generation capacity.

Advanced electricity service options include enhanced Web portal services and tools for customer information and energy management, control, and automation; the installation of up to 10,000 residential and small commercial Home Area Network devices to provide customers with options to conveniently control or manage their energy use based on lifestyle or operating choice; and the implementation of advanced energy management control systems with automatic demand response (AutoDR) capability at customer facilities.

In combination with time-based rates, these service options provide customers with greatly enhanced tools to manage overall energy, reduce peak electricity demand, or shift their consumption from on to off-peak periods. Direct load control devices include programmable communicating thermostats and other devices that support load reduction or load shifting for air conditioners and other appliances and equipment during peak demand periods.

Participating customers receive financial incentives in return for SMUD gaining the ability to turn off, or turn down, major appliances during times of system need. SMUD is installing the software platform for a demand response management system to provide more effective and centralized administration of direct load control operations and to enable a more robust two-way communication and feedback loop with its customers.

Distribution automation systems include advanced automated equipment to improve the performance of distribution systems. SMUD is deploying automated switches, automated capacitor banks, remote fault indicators, and feeder monitors integrated with our energy management system on 102 distribution circuits. This equipment automatically responds to power disturbances and provides voltage regulation and isolates interrupted circuits. SMUD expects to reduce service interruptions and the frequency and duration of outages and the need for truck visits to maintain the distribution grid. Distribution automation assists the grid integration of solar and wind power installed on or near residences and commercial buildings.



Queens, New York USA - Consolidated Edison Company (Con Ed)

The Consolidated Edison Company of New York, Inc. (Con Edison) received a federal grant of \$136 million in 2010 to enhance electric distribution planning and operations. The project is deploying various types of distribution automation equipment such as substation and feeder monitors, automated switches, and capacitor automation devices on 850 feeder lines to improve operational efficiency and control, combined with the integration of distribution management systems and supervisory control and data acquisition (SCADA) systems.

Communications infrastructure includes an upgrade of existing radio sites for the SCADA system. The upgrade enables increased capacity and enhanced security through encryption and allows for automated communication and control of the auto loop reclosers.

The project upgrades existing radio sites and complies with the North American Electric Reliability Council Critical Infrastructure Protection Requirements for data authentication and encryption. Distribution automation systems include the deployment of automated sectionalizing switches with SCADA control. The switches allow for rapid restoration of electricity loss to sections of the grid affected by an outage as well as reduced restoration time as faults are easier to locate.

Additionally, Con Edison is deploying approximately 6,800 transformer condition-monitoring devices that use the power line communications infrastructure to alert Con Edison of any problems with the distribution equipment. The sensors enable maintenance crews to perform targeted preventative maintenance, thus reducing the number of equipment failures and outages. The automated sectionalizing switches and the equipment condition monitors help to increase reliability while reducing operations and maintenance costs.

Distribution system energy efficiency improvements involve the integration of capacitor automation and a power quality monitoring system. The enhancements are being made to the 4kV portion of the grid (the 4kV portion of the grid consists of the primary feeders that deliver power to homes, such as the overhead wires seen in residential neighborhoods) and are aimed at improving the power quality of the grid and reducing operations and maintenance costs.



The capacitors improve voltage control, power quality, and increase distribution capacity through grid efficiency. Distributed energy resources interface involves the deployment of secure two-way wireless communication to approximately 180 network type distribution transformers. The cyber secure communication system allows for distributed generation to be fed into the grid without causing safety issues, reliability issues, or damage to the grid. When the project is completed, distributed generation integration will allow for distributed resources such as solar and combined heat and power to come online.

Ontario, Canada - HydroOne

Canada's Hydro One in Ontario operates Smart Grid technology on a much larger scale than Boulder, CO, and Austin, TX. Hydro One's goal is to create an intelligent communications network to lower costs and raise efficiency. The Hydro One project was started in response to the energy crisis facing Ontario. By 2025, Ontario will have to replace 80% of its current grid system. Hydro One will rebuild the Ontario grid by utilizing Smart Grid technology. Hydro One will use a two-way self-healing mesh radio network to communicate with devices in the network. These devices include in-home meters. Hydro One had installed over 700,000 meters by December 2008 and planned to install 1.3 million meters by the end of 2010. In 2013, phase 1 release 2 investments will include:

The upgrade of the DMS and pilot of DG control and power quality monitoring, the integration of the DMS with energy storage systems, the installation of voltage regulating devices integrated with the DMS on the distribution system to pilot Conservation Voltage Reduction, the integration of a demand response system with the AMI (smart meter) network, the integration of the AMI with the DMS and the Outage Management System through an Operational Service Bus to optimize outage response and the implementation of the Energy Theft Analytic system.

Italy – Enel

Italy pioneered in implementing Smart Grid technology. The project was begun in 2001 by Enel, Italy's largest power company. In 2006, Italy made it mandatory for all electricity providers to use smart meters.



Since then, 85% of Italian homes have Enel smart meters. Enel designed and developed all of its own smart meters. Enel uses these meters to relay usage information back to its central office and to offer real-time pricing to customers. Enel reportedly has saved \$750 million annually since the implementation of the meters. These meters have been successful in reducing costs for consumers as well.

Australia – Smart Grid, Smart City – EnergyAustralia

The Australian government has committed to investing \$100M in Smart Grids in 2009. The intention is to increase customer awareness and engagement in energy usage and establish distributed demand management and distributed generation management. EnergyAustralia, announced as the lead utility in the federally sponsored consortium to study Smart Grid in Australia, will build the Smart Grid over five sites in New South Wales with partners IBM, Grid Net, a San Francisco-based energy software company, and GE Energy.

The WiMAX-based Smart Grid will support such applications as Substation Automation and plug-in hybrid electric vehicles (PEV), ultimately supporting 50,000 Smart Meters and 15,000 IHDs as well. Smart Grid trials include:

- Active Volt Var Control: Use Smart Grid technology to manage voltage delivery across the network to more efficiently manage the power supply.
- Fault Detection Isolation & Restoration (FDIR): Installing equipment to better pinpoint location of faults and isolate them to restore power faster.
- Substation and Feeder Monitoring (SFM): Leveraging communications platforms to reduce the cost of getting vital asset information, including from high voltage underground cables.
- Wide Area Measurement (WAM): Using integrated Phasor Measurement Devices to better predict system state and possibly prevent network interruptions across a large area.



Chicago, Illinois USA - Building Owners and Managers Association of Chicago (BOMA/Chicago) & Korean Smart Grid Association

Through a partnership with the Korean Smart Grid Association, a handful of buildings in downtown Chicago, Illinois, are launching a Smart Grid pilot program aimed to reduce overall electric consumption and lower bills through customized “demand-response” strategies that respond to wholesale electricity market rates.

The Building Owners and Managers Association of Chicago (BOMA/Chicago) hopes to expand the program to 80% of buildings in the business district and ultimately cut 200 megawatts of peak demand, equivalent to the output of a mid-sized coal-powered generating facility.

4.2 Conclusions

Classic electricity grids face many problems that need to be addressed by technology. Limitations and problems of the past will be resolved by a technological evolution of the grid into a Smart Grid.

The benefits are multiple and range from financial and technical to environmental and societal. Measurements and sensors play an important role for Smart Grid operation, maintenance, monitoring and security. Sensors are deployed at every possible point of the power system: in generation facilities, in transmission, in distribution and even inside consumer’s premises.

The data produced and communicated have distinct characteristics and requirements and their volume is expected to increase dramatically in the following years. Electricity supply is vital for today’s digitized world and the power infrastructure is the most critical for a country. Security concerns about intentional and unintentional threats are justified.

The integration of ICT with the power systems brings along new risks for consumers and organizations. Countermeasures and remedies already exist for most of the vulnerabilities and research to mitigate the rest is ongoing.



A combined effort of all involved stakeholders, private and government, is crucial for the achievement of a more secure Smart Grid. The deployment of Smart Grid technologies has already started in costly efforts across the globe, but there is still a long distance to be covered till the ideal Smart Grid is reached.



Definitions – Acronyms

AC	Alternating Current
AMI	Advanced Metering Infrastructure
AutoDR	Automatic Demand Response
BEVs	Battery Electric Vehicles
BMS	Building Management Systems
BOMA/Chicago	Building Owners and Managers Association of Chicago
BPL	Broadband over PowerLine
C2	Command and Control
CIP	Common Industrial Protocol
Con Ed	Consolidated Edison Company
CPP	Critical Peak Pricing
CSCTG	Cyber Security Coordination Task Group
DER	Distributed Energy Resources
DFR	Dynamic Feeder Reconfiguration
DMS	Distribution Management Systems
DNP3	Distributed Network Protocol 3
DR	Demand-Response
DSM	Demand-Side Management
ECC	Energy Control Center
EHV	Extra High Voltage
EMF	Electromotive Force
EMS	Energy Management Systems
ENIS	A European Network and Information Security Agency
ERCOT	Electric Reliability Council of Texas
ESPs	Energy Service Providers
ESSs	Electricity Storage Systems
FACTS	Flexible alternating current transmission system
FAN	Field Area Network
FDIR	Fault Detection Isolation & Restoration
FiWi	Fiber-wireless
G2V	Grid-to-Vehicle
HANs	Home Area Networks



HEMS	Home Energy Management Systems
HMIs	Human-Machine-Interface
I/O	Input/Output
ICCP	Inter Control Center Protocol
ICSCERT	Industrial Control Systems Cyber Emergency Response Team
IEC	International Electrotechnical Commission
ICT	Information and Communication Technologies
IEDs	Intelligent Electronic Devices
IEEE	Institute of Electrical and Electronics Engineers
IHDs	In-Home Devices
INL	Idaho National Laboratory
IP	Internet Protocol
IPSec	Internet Protocol Security
LAN	Local Area Network
MAN	Metropolitan Area Network
MDMS	Meter Data Management System
MDS	Mobile Decentralized Storage
MITM	Man-In-The-Middle
Modbus	Modicon Communication Bus
MTU	Master Terminal Unit
MVA	Megavoltamperes
NAC	Network Access Control
NASPInet	North American Synchro-Phasor Initiative network
NERC	North American Reliability Corporation
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OMS	Outage Management Systems
OS	Operating System
OSI	Open Systems Interconnection
PDC	Phasor Data Concentrator
PEV	Plug-in hybrid Electric Vehicles
PF	Power Factor
PHEVs	Plug-In Hybrid Electric Vehicles
PKI	Public key Infrastructure



PLC	Power Line Communications
PLC	Programmable Logic Controller
PLCC	Power line carrier communication
PMSs	Phase Measurement Systems
PMUs	Phaser Measurement Units
PTP	Precision Time Protocol
PTR	Peak Time Rebate
QoS	Quality of Service
RDBMS	Relational Database Management Systems
RTDs	Resistance temperature detectors
RTTR	Real time thermal rating
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SFM	Substation and Feeder Monitoring
SMES	superconducting magnetic energy storage
SMUD	Sacramento Municipal Utility District's
SO	System Operator
SoGP	Information Security Forum's of Good Practice
SoS	System of Systems
SSL	Secure Socket Layer
TLS	Transport Layer Security
TOU	Time-Of-Use
UPS	Uninterruptible Power Supply
V2G	Vehicle-to-Grid
VPN	Virtual Private Network
WAM	Wide Area Measurement
WAMs	Wide Area Monitoring System
WAN	Wide Area Network
WSAN	Wireless Sensor and Actuator Network



Bibliography

Adam, R. and Wintersteller, W. 2011. From Distribution To Contribution Commercializing The Smart Grid. Booz&Company.

Al-Omar, B., Al-Ali, A.R., Ahmed, R., Landolsi, T. 2012. Role of Information and Communication Technologies in the Smart Grid. Journal of Emerging Trends in Computing and Information Sciences (CIS), vol. 3, No 5.

Aloul, F., Al-Ali, A.R., Al-Dalky, R., Al-Mardini, M., El-Hajj, W. 2012. Smart Grid Security: Threats, Vulnerabilities and Solutions. International Journal of Smart Grid and Clean Energy.

Asprou, M., Hadjiantonis, A.M., Ciornei, I., Milis, G. 2012. On the complexities of interdependent infrastructures for wide area monitoring systems. Complexity in Engineering (COMPENG).IEEE.

Aweya, J., Al Sindi, N. 2013. Role of Time Synchronization in Power System Automation and Smart Grids. 2013 IEEE International Conference on Industrial Technology (ICIT).

Bevis, T., Hacker, B., Edrington, C.S., Azongha, S. 2009. A review of PHEV grid impacts. North American Power Symposium (NAPS), 2009. IEEE. DOI: 10.1109/NAPS.2009.5483995

Borgnakke, C., Sonntag R.E. 2013. Fundamentals of Thermodynamics, 8th Edition SI Version. Wiley. ISBN: 978-1-118-32177-5

Bossart, S.J., Bean, J.E. 2011. Metrics and benefits analysis and challenges for Smart Grid field projects. Energytech, 2011 IEEE. DOI: 10.1109/EnergyTech.2011.5948539

Boyes, J.D., Clark, N.H. 2000. Technologies for energy storage. Flywheels and super conducting magnetic energy storage. Energy Storage Program, Sandia Nat. Labs., USA. IEEE.



Breuer, W., Povh, D., Retzmann, D., Urbanke, Ch., Weinhold, M. 2007. Prospects of Smart Grid Technologies for a Sustainable and secure Power Supply. The 20th World Energy Congress & Exhibition, Rome, Italy. Web.

<http://www.worldenergy.org/documents/p001546.pdf>. [accessed July 2013].

Brown, R. E. 2008. Impact of Smart Grid on Distribution System Design. Power and Energy Society General Meeting—Conversion and Delivery of Electrical Energy in the 21st Century, 2008. IEEE.

Burke, A. 2000. Ultra capacitors: why, how, and where is the technology. Journal of Power Sources, ELSEVIER SCIENCE 91 pp. 37-50, 2000.

Casazza, J. A. 1998. Blackouts: Is the Risk Increasing?. Electrical World, vol. 212 (4), 62–64.

Casazza, J. A., Delea, F. 2003. Understanding Electric Power Systems: An Overview of the Technology and the Marketplace. Wiley.

Chandy, K. M., Gooding, J., McDonald, J. 2010. Smart Grid System of Systems Architectures: Systems Evolution to Guide Strategic Investments in Modernizing an Electric Grid. Grid-Interop Proceedings, Chicago, IL-USA, pp. 1-11.

Clements, S., Kirkham, H. 2010. Cyber-security considerations for the smart grid. Power and Energy Society General Meeting, IEEE.

Department of Energy, United States (DoE). 2003. Grid 2030 – A Vision for Electricity’s Second 100 Years.

Deshpande, J., Locke, A., Madden, M.. 2011. Smart Choices for the Smart Grid. Technology White Paper, Alcatel/Lucent. http://www.smartgrids-cre.fr/media/documents/Alcatel-Lucent_ChoicesSmartGridTechnology.pdf [accessed August 2013].



Economides, N., Tåg, J. 2009. Net Neutrality on the Internet: A Two-Sided Market Analysis. NET Institute Working Paper No. 07-45; NYU Law and Economics Research Paper 07-40; NYU Working Paper No. 2451/26057. http://www.stern.nyu.edu/networks/Economides_Tag_Net_Neutrality.pdf [accessed August 2013].

Efthymiou, C., Kalogridis, G. 2010. Smart Grid Privacy via Anonymization of Smart Metering Data. First IEEE International Conference on Smart Grid Communications (SmartGridComm).

Electric Power Research Institute (EPRI). 2005. IntelliGridSM – Smart Power for the 21st century, www.epri-intelligrid.com/intelligrid/docs/Intelligrid_6_16_05.pdf. [accessed July 2013].

Elgerd, O.I. (2001). Electric Energy Systems Theory : An Introduction. TMH. 2nd Edition. Tata McGraw-Hill Education.

El-Hawary, M. E. 2008. Introduction to Electrical Power Systems. Wiley-IEEE Press
EPRI. 2007. Advanced metering infrastructure (AMI). http://www.ferc.gov/eventcalendar/Files/20070423091846-EPRI_-_Advanced_Metering.pdf [accessed July 2013].

EPRI. 2009. Report to NIST on Smart Grid interoperability standards roadmap. www.nist.gov/smartgrid/upload/Report_to_NIST_August10_2.pdf [accessed September 2013].

ERGEG. 2007. Smart Metering with a Focus on Electricity Regulation. http://www.energy-regulators.eu/portal/page/portal/EER_HOME/EER_PUBLICATIONS/CEER_ERGEG_PAPERS/Customers/2007/E07-RMF-04-03_SmartMetering_2007-10-31_0.pdf [accessed August 2013]. Ref: E07-RMF-04-03. European Regulators' Group for Electricity and Gas.



European Commission. 2011. Cyber Security of the Smart Grids. Summary Report. Expert Group on the Security and Resilience of Communication Networks and Information Systems for Smart Grids.

http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1761 [accessed August 2013].

Fender, S. 2009. PhoneFactor Team Discovers Vulnerability in SSL Authentication. Phonefactor blog. <http://blog.phonefactor.com/2009/11/06/phonefactor-team-discovers-vulnerability-ssl-authentication/>. [accessed August 2013].

Fisher, D. 2001. Attack tool released to exploit SSL DoS issue. Threat post. http://threatpost.com/en_us/blogs/attack-tool-released-exploit-ssl-dos-issue-102411 [accessed August 2013].

Flick, T., Morehouse, J. 2011. Securing the Smart Grid Next Generation Power Grid Security. Elsevier Inc. Syngress. ISBN: 978-1-59749-570-7

Gellings, C. W. 2009. The Smart Grid: Enabling Energy Efficiency and Demand Response. The Fairmont Press, Inc. ISBN-10: 0-88173-623-6

Ghazisaidi, N., Maier, M., Assi, C.M. 2009. Fiber-wireless (FiWi) access networks: A survey. Communications Magazine, Volume:47 , Issue: 2. IEEE.

Grogan, A . 2012. Smart appliances. Engineering & Technology. Volume:7 , Issue: 6. IEEE.

House of commons Trade and Industry Committee. London, UK. 2004. Resilience of the National Electricity Network.

Howell, K. B. 2001. Principles of Fourier Analysis. CRC Press.

IEEE Power System Relaying Committee Working Group D6. 2005. Power swing and out-of-step considerations on transmission lines. IEEE.



IEEE Standard 1159-2009 (Revision of IEEE Std 1159-1995). Recommended Practice for Monitoring Electric Power Quality.

IEEE Standard C37.118-2005. IEEE Standard for Synchrophasors for Power Systems. 2006.

Kalogridis, G., Cepeda, R., Denic, S.Z., Lewis, T. 2011. ElecPrivacy: Evaluating the Privacy Protection of Electricity Management Algorithms. IEEE Transactions on Smart Grid, Volume:2, Issue: 4.

Kalogridis, G., Cepeda, R., Denic, S., Lewis, T., Efthymiou, C. 2011. ElecPrivacy: Evaluating the privacy protection of electricity management algorithms. IEEE Transactions on Smart Grid, vol. 2, no. 4.

Keizer, G. 2010. Is Stuxnet the 'best' malware ever?
<http://www.infoworld.com/print/137598> [accessed September 2013].

Kelly, M., Briggs, A. 2002. Methods of Hydrogen Storage for Standby Power Units. Telecommunications Energy Conference, 2002. INTELEC. 24th Annual International. IEEE. DOI: 10.1109/INTLEC.2002.1048676

Kezunovic, M. 2012. BEVs/PHEVs as Dispersed Energy Storage in Smart Grid. Innovative Smart Grid Technologies (ISGT), 2012 IEEE PES. DOI: 10.1109/ISGT.2012.6175569

Knapp, E. 2011. Industrial network security: securing critical infrastructure network for Smart Grid, SCADA, and other industrial control systems. Waltham, MA. Syngress.

Knapp, E., Samani, R. 2013. Applied Cyber Security and the Smart Grid—Implementing Security Controls into the Modern Power Infrastructure. Elsevier Inc. ISBN: 978-1-59749-998-9



Kranz, J.J., Picot, A. 2011. Toward an End-to-End Smart Grid: Overcoming Bottlenecks to Facilitate Competition and Innovation in Smart Grids. http://www.nrri.org/web/guest/home?p_auth=JB8c3Fh3&p_p_auth=sfZLkml3&p_p_id=20&p_p_lifecycle=1&p_p_state=exclusive&p_p_mode=view&_struts_action=%2Fdocument_library%2Fget_file&_groupId=317330&_folderId=0&_name=5476 National Regulatory Research Institute (NRRI). U.S.A. [accessed July 2013].

Krebs, B. 2012. FBI: smart meter hacks likely to spread. KrebsOnSecurity. <http://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/> [accessed September 2013].

Langner, R. 2011. A time bomb with fourteen bytes. <http://www.langner.com/en/2011/07/21/a-time-bomb-with-fourteen-bytes/#more-1028> [accessed September 2013].

Lee, A. and Brewer, T. 2009. The Cyber Security Coordination Task Group. Smart Grid Cyber Security Strategy and Requirements. U.S. DoC

Liu, V., Parks, A., Talla, V., Gollakota, S., Wetherall, D., Smith, J.R. 2013. Ambient Backscatter: Wireless Communication Out of Thin Air. University of Washington.

Maier, M. W., Rechtin, E. 2000. The Art of Systems Architecting, 2nd edition. CRC Press, London.

Massoud, A., Schewe, P. F. 2007. Preventing Blackouts. Scientific American, vol. 296, no. 5, pp. 60-67

McAfee Foundstone Professional Services and McAfee Labs. 2011. Global Energy Cyberattacks: “Night Dragon”. White paper. <http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf> [accessed September 2013].



McDonald, J.D. 2012. Substation automation basics—the next generation. Electric energy online.com .

http://www.electricenergyonline.com/?page=show_article&mag=43&article=321

[accessed July 2013].

Metke A.R., Ekl, R.L. 2010. Security Technology for Smart Grid Networks. IEEE Transactions on Smart Grid vol. 1, No. 1.

Meyer, H. W. 1971. A History of Electricity and Magnetism. MIT Press.

Miller, J. 2008. The Smart Grid – How Do We Get There?. Smart Grid News online journal.

Mohd, A., Ortjohann, E., Schmelter, A., Hamsic, N. 2008. Challenges in integrating distributed Energy storage systems into future smart grid. IEEE International Symposium on Industrial Electronics, 2008.

NASPInet. 2009. Phasor Gateway Technical Specifications for North American Synchro-Phasor Initiative Network (NASPInet).

http://wiki.gridtrak.com/wiki/images/1/12/Naspinet_phasor_gateway_final_spec_20090529.pdf [accessed August 2013]. U.S. DoE, NETL.

NIST. 2009. The Role of the Internet Protocol (IP) in AMI Networks for Smart Grid.

<http://www.ietf.org/mail-archive/web/smartpower-interest/current/docFn1Z5XcFuW.doc>

[accessed August 2013]. National Institute of Standards and Technology. U.S.A.

NIST. 2010. NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1_NISTIR. <http://www.nist.gov/el/smartgrid/sgridcoord.cfm>

[accessed August 2013].

NIST. 2012. NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2_NISTIR.

http://www.nist.gov/customcf/get_pdf.cfm?pub_id=910824 [accessed August 2013].



North American Electric Reliability Corporation (NERC). 2009 First third quarter NERC DAWG number of disturbances by region. American Electric Reliability Corporation.

<http://www.nerc.com/pa/rrm/ea/System%20Disturbance%20Reports%20DL/2009SystemDisturbance.pdf> [accessed August 2013].

Phillips, A. 2010. Staying in shape: Advanced sensor technologies can help keep aging transmission and distribution systems in good condition. *Power and Energy Magazine*, Volume: 8, Issue: 2. IEEE

Phillips, A., Bose, S., Rogers, B. 2010. Sensing the Future. *IEEE Power and Energy magazine*. DOI 10.1109/MPE.2010.938519

Quinn, E. L. 2008. Privacy and the New Energy Infrastructure. *Social Science*

Research Network (SSRN). Center for Energy and Environmental Security (CEES) working paper No. 09-001.

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1370731 [accessed June 2013]

Rinaldi, S. M., Peerenboom, J. P., Kelly, T. K. 2001. Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems*, vol. 21, no. 6, pp. 11-25.

Saponara, S., Bacchillone, T. 2012. Network Architecture, Security Issues, and Hardware Implementation of a Home Area Network for Smart Grid. *Journal of Computer Networks and Communications* Volume 2012. Article ID 534512. <http://dx.doi.org/10.1155/2012/534512> [accessed August 2013].

Siostrzonek, T., Pirog, S., Baszynski, M. 2008. Energy storage systems the flywheel energy storage. *IEEE*.

Smith, W. 2000. The Role of Fuel Cells in Energy Storage. *Journal of Power Sources* 86(1-2): 74–83, 2000. DOI: 10.1016/S0378-7753(99)00485-1.



Sorebo, G.N., Echols M.C. 2011. Smart Grid security: an end-to-end view of security in the new electrical Grid. CRC Press.

Taft, J., Ahmed, S. 2009. Networks for High Performance: The Journey to Smart Grid Communications Infrastructure.

<http://www.energycentral.com/gridtandd/gridoperations/articles/2156/Networks-for-High-Performance-The-Journey-to-Smart-Grid-Communications-Infrastructure>

[accessed August 2013].

Taylor, J., Halnes A. 2010. Analysis Of compressed air energy storage. PCIC Europe 2010 Conference Record, Oslo.IEEE

Ten, C.W., Manimaran, G., Liu, C.C. 2010. Cybersecurity for Critical Infrastructures: Attack and Defense Modeling. IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans, vol. 40, No. 4.

The NETL Modern Grid Initiative. 2007. A Systems View of the Modern Grid. National Energy Technology Laboratory, Department of Energy Office of Electricity Delivery and Energy Reliability, U.S.A.Web.

http://www.netl.doe.gov/smartgrid/referenceshelf/whitepapers/ASystemsViewoftheModernGrid_Final_v2_0.pdf [accessed June 2013]

The Smart Grid Interoperability Panel. 2010. Cyber Security Working Group, Guidelines for smart grid cyber security, NISTIR 7628. www.nist.gov/smartgrid/upload/nistir-7628_total.pdf [accessed September 2013].

The White House's Office of the Press Secretary. 2009. President Obama Announces \$3.4 Billion Investment to Spur Transition to Smart Energy Grid. <http://www.whitehouse.gov/the-press-office/president-obama-announces-34-billion-investment-spur-transition-smart-energy-grid> [accessed September 2013].

U.S. Department of Energy. (DoE). 2009. Fault Current Limiters (FCL) Fact Sheet. Superconducting & Solid-State Power Equipment: Plugging America into the Future of Power. Web. <http://energy.gov/oe/downloads/fault-current-limiters-fcl-fact-sheet> [accessed September 2013].



US Department of Energy. Industrial Control Systems Cyber Emergency Response Team (ICSCERT). Increasing Threat to Industrial Control Systems (Update A). <https://ics-cert.us-cert.gov/alerts/ICS-ALERT-12-046-01A> [accessed September 2013].

Vandewalle, J., Keyarts, N., D'haeseleer, W. 2012. The role of thermal storage and natural gas in a smart energy system. IEEE 9th International Conference on the European Energy Market (EEM), 2012

Verdone, R., Dardari, D., Mazzini, G., Conti, A. 2008. Wireless Sensor and Actuator Networks. Academic Press/Elsevier, London.

Wang W., Lu Z. 2012. Cyber security in the Smart Grid Survey and challenges. Computer Networks journal, Elsevier.

Wilson, J. S. 2005. Sensor Technology Handbook. Elsevier Inc. ISBN: 0-7506-7729-5

Xiao, Y. 2012. Communication and Networking in Smart Grids. Auerbach Publications. ISBN:9781439878736

Yin, J., Sharma, P., Gorton, I., Akyoli, B. 2013. Large-Scale Data Challenges in Future Power Grids. IEEE

Yuan, L., Tao, L., Zhihui S., Chang, W. 2012. Application of distributed optical fiber temperature system in online monitoring and fault diagnosis of smart grid. Power and Energy Engineering Conference (APPEEC), 2012 Asia-Pacific. IEEE.

Zeller, M. 2011. Myth or Reality – Does the Aurora Vulnerability Pose a Risk to My Generator? A&M Conference for Protective Relay Engineers, Texas. IEEE. <https://www.selinc.com/WorkArea/linkit.aspx?LinkIdentifier=id&ItemID=8504> [accessed August 2013]

