Electrical Power Systems Protection and Interdependencies with ICT

George M. Milis, Elias Kyriakides, and Antonis M. Hadjiantonis

KIOS Research Center for Intelligent Systems and Networks, University of Cyprus
{milis.georgios,elias,antonish}@ucy.ac.cy

Abstract. This section discusses the protection of electrical power systems (EPS) and its relation to the supporting Information and Communication Technologies (ICT) infrastructure. Several dimensions are addressed, ranging from the need of protection and available protection schemes to the identification of faults and disturbances. The challenges brought by recognizing the interdependent nature of today's and future's EPS and ICT infrastructures are also highlighted, based on the Smart Grid and the System of Systems perspectives.

Keywords: electrical power system, protection, critical infrastructures, disturbance, interdependencies.

1 Introduction

Our modern lifestyle is increasingly dependent on critical infrastructures, like the Electrical Power System, the Water Distribution Networks, the Telecommunication networks, the Transportation networks, even the Health sector, the Finance sector, and many more. The robust operation of these infrastructures is often taken for granted. But what if their operations were disrupted or even ceased? What would be the effects on our economy, our society, or on our health and safety? Around the globe, a number of communities have recognized the criticality of such infrastructures and have set their investigation and protection as a top priority, being actively engaged in research and development activities at national and international levels.

According to the European Commission [COM(2005) 576] [5] and the European Programme for Critical Infrastructure Protection (EPCIP), a "Critical Infrastructure (CI) is defined as an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social wellbeing of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions". The term Critical Infrastructure Systems (CIS) includes the public, private and governmental infrastructure assets, and interdependent cyber and physical networks. As already mentioned, due to their outmost importance to society, existing and future CIS need to be protected from disruption and destruction. Several threats need to be considered, including among others natural disasters, accidental damage, equipment failure, human error, and terrorist attacks. According to Council Directive [2008/114/EC] [6], CIS

A.M. Hadjiantonis and B. Stiller (Eds.): Telecommunication Economics, LNCS 7216, pp. 216–228, 2012.

protection should be based on an all-hazards approach, recognizing the threat from terrorism as a priority. The vast range of threats makes the protection of critical infrastructures a highly complex and interdisciplinary research domain. For example, the issue of interdependencies among critical infrastructures needs to be investigated to prevent propagation and cascading of failures between infrastructures. The research communities' understanding of interdependencies is still immature and requires the coordinated involvement of several different disciplines. On top of that, the increasing reliance on telecommunication networks and the Internet for communication, poses novel threats to critical infrastructures and there is an urgent need to prepare for cyber-attacks.

This section focuses on Electrical Power Systems (EPS) where the majority of economic activities depend upon, as well as the operation of many other infrastructures. In essence, an EPS is one of the most critical infrastructures with its protection being a priority worldwide. The section further discusses the interdependence between the EPS and the ICT infrastructures, presenting open problems and possible solutions.

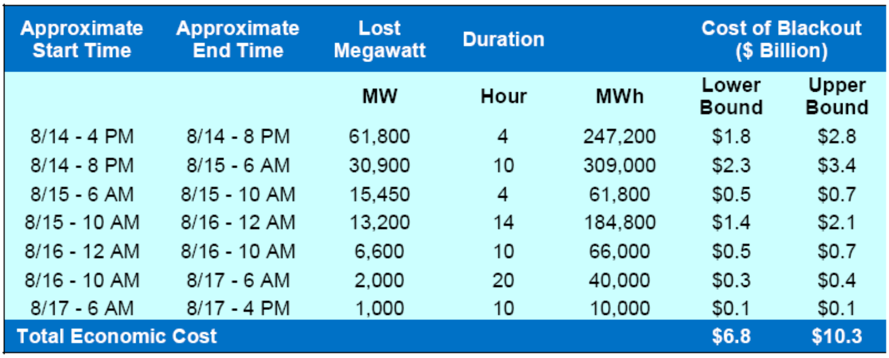
2 The Need to Protect Electrical Power Systems

Electrical Power Systems comprise of large and complex machinery and assets that are responsible for the generation of electric power in sufficient quantity to meet the present and estimated future demands of the customers, its transmission to the areas where it will be consumed and its distribution within those areas to the actual demand sites. This process is synchronous and continuous and is a fundamental asset of our modern society and economy. Therefore, any disruption of its operation has huge negative effects of unforeseen size (unbalances and people reactions, disruption of economic activity, etc.) [11]. However, the EPS are subject to disturbances in their normal operation which subsequently cause 'faults', that occur either due to internal technical failures or due to external causes [15],[20]. Therefore, the protection of the EPS is defined as the effort to ensure its reliable operation within an environment with effects of disturbances, failures and events that put the system at risk. More specifically, it is necessary to ensure: i) public safety, ii) equipment protection, and iii) quality of service, by limiting the extent and duration of service interruption, as well as, minimizing the damage to the involved system components. A non-exhaustive list of EPS components that need to be protected, would include the following [10],[18]:

- Human personnel.
- EPS equipment (transmission/distribution lines, generators, transformers, motors, bus-bars).
- Customer owned equipment.
- Operational integrity of EPS (ability to deliver power, stability, power quality).
- Customer operations (e.g., large, medium and small industry, financial services, transportation services, telecommunication and other infrastructures' services).

In any case, safety of human personnel and prevention of human injury should always take priority over service continuity, equipment damage, or economic losses. It is therefore necessary to prevent or, at least, to detect and clear any faults quickly, since the longer the EPS operates under a fault, the higher that the system will become unstable and lead to cascading outages.

The cost required for having the EPS perfectly safe or perfectly reliable (by adopting components that do not fail and that require minimum maintenance) would be prohibitive. As stated in [20], risk assessment is performed to define a trade-off for the acceptable levels of risk from disruption in association with relevant costs. That is, the cost of the protection of a system determines the degree of protection that can be incorporated into it. Figure 1 provides an overview of the cost of a major blackout that occurred in the US in 2003. The estimated economic cost of $6.8-10.3 billion over three days of disruption is alarming and would justify higher investments on the protection efforts of the EPS.



Approximate Start Time	Approximate End Time	Lost Megawatt	Duration		Cost of Blackout ($ Billion)	
		MW	Hour	MWh	Lower Bound	Upper Bound
8/14 - 4 PM	8/14 - 8 PM	61,800	4	247,200	$1.8	$2.8
8/14 - 8 PM	8/15 - 6 AM	30,900	10	309,000	$2.3	$3.4
8/15 - 6 AM	8/15 - 10 AM	15,450	4	61,800	$0.5	$0.7
8/15 - 10 AM	8/16 - 12 AM	13,200	14	184,800	$1.4	$2.1
8/16 - 12 AM	8/16 - 10 AM	6,600	10	66,000	$0.5	$0.7
8/16 - 10 AM	8/17 - 6 AM	2,000	20	40,000	$0.3	$0.4
8/17 - 6 AM	8/17 - 4 PM	1,000	10	10,000	$0.1	$0.1
Total Economic Cost					$6.8	$10.3

Fig. 1. The economic cost of the Northeastern Blackout, Aug. 2003, USA [1]

3 Types of System Disturbances and Their Effects

No matter what the criticality of the investment is, it is not technically and economically feasible to design and build an EPS such as to eliminate the possibility of disturbances in service. It is therefore a fact that, infrequently, and at random locations, different types of disturbances will occur, leading to faults incurred on the system. The term ‘disturbance’ means any event, unexpected or foreseen, which requires corrective action to be taken. Sudden disturbances on EPS may occur from factors external to the system itself, such as weather or environment, or internal factors such as insulation failure on some component of the system. The following external factors of system disturbances/failures can be identified [12]:

- Weather: One of the main causes of equipment failures, according to a worldwide survey over several years in the 1980s: about 20% of failures were attributable to weather conditions.
- Sudden changes in balance between demand and generation: They can result from numerous causes: loss of transfers from/to external systems, transmission circuit

tripping, isolating parts of the system with embedded generation or demand, etc. This type of disturbance is rather frequent, as many other types of disturbances may result in some imbalance during their development.

- Human error: errors of the personnel of a utility may occur at all stages, from planning/design to plant manufacture to plant installation to maintenance/testing to operation. In addition, members of the public may be involved in system errors unintentionally (e.g., kite flying) or consciously (e.g., illegal entry into or attack to parts of the system).

The disturbances caused by the above factors can be categorized as either faults (e.g., breakdown or burning of insulation) or abnormal operation (at local and/or system level, e.g., overload or frequency variation). Each disturbance requires protective actions and measures to minimize its impact, especially the triggering of a cascaded sequence of events.

4 Protection Measures and Devices to Minimize the Impact of Disturbances

A number of measures (including automatic mechanisms and "defense plans") should be taken in the management, planning and operation phases of EPS to minimize the effects of disturbances [13]. Protection measures often contain three main elements:

- Detect a possible disturbance and its type;
- Assess the best way to prevent it or minimize its effect at the extent possible; and
- Restore normal operation.

In general, measures are taken with the help of hardware and/or software components. However, human involvement in decision making and implementation of protection processes is equally important. The human involvement in decision making is even more important during the operational phase, particularly during the development of a disturbance. This creates a critical need for a reliable and fast communication infrastructure, which will timely convey the collected data from the equipment and distribute corrective commands to networked controllers.

4.1 Measures in the Planning, Operational, and Restoration Timescale

The system engineers are the ones defining the protection plans, as well as, what specific protective and control measures will be needed during system operation. Some of the measures (for instance, under-frequency load shedding), are addressed in the planning phase, while others (e.g. inter-tripping schemes with local impact, the necessity of which emerges at short notice) are addressed directly in the operational plan. In the event of a system disturbance, the following actions are taken, based on the operational memoranda and procedures and any special protection schemes or coordinated defense plans employed by the plant engineers: i) open breaker and under frequency relays (isolated fault), ii) switch capacitors, iii) load shedding/disconnection, iv) islanding, v) no action, vi) alarm signal, vii) generation margins adjustment, viii) demand adjustment.

As EPSs become larger and more complex, timescales for response to disturbances are shrinking, calling for the implementation of more automated measures. Effective automation requires the collection and analysis of current and voltage measurements at remote terminals of a line in order to allow remote control of equipment, thus requiring enhanced ICT infrastructure to support real-time operations.

4.2 Measures in the ICT Facilities

The EPS need very secure (physical and logical) communication links for data and speech. Such links are either system-wide or local, between substations. A way to improve the security of communications is by avoiding as much as possible the dependence on any single external provider. Usually, a utility possesses its own communication channels for connecting its equipment (e.g., power line carrier or fiber) or channels are leased from external providers, such as public communications networks or even other industries with widespread communication networks, such as railways. It is also a common practice in EPS to duplicate (at least) the SCADA (Supervisory Control and Data Acquisition) systems and the EMS (Energy Management System) within one Control Center building. In some cases, the utilities go further and provide backup of whole Control Centers in different geographic locations.

4.3 Protection System Devices and Components

In order to safeguard the robust operation of the EPS and avoid costly partial or even full blackouts, a number of sophisticated protection devices is installed and instrumented. The most important ones are mentioned below [8],[10]:

- Fuses: the most common and widely used protective device in electrical circuits. Fuses are independent, self-destructing components, aiming to isolate faulty parts of the system and save the equipment on the healthy part.
- Instrument transformers: They continuously measure the voltage and current at several locations/components of the EPS and are responsible to give feedback signals to the relays to enable them to monitor the status of the system and detect abnormal conditions in the operation.
- Circuit breakers: They are basically switches to interrupt the flow of current and they open on relay command. They are used in combination with relays, to detect and isolate faults, where fuses are unsuitable. Their important characteristics from a protection point of view are the speed of reaction and the capacity of the circuit that the main contacts are capable of interrupting.
- Tripping batteries: they give uninterrupted power source to the relays and breakers that is independent of the main power source being protected. They have an important role in protection circuits, as without them relays and breakers will not operate, making the performance of the whole network unacceptable.
- Relays: they convert the signals from the monitoring devices/instrument transformers (mostly voltages and currents) and give instructions to open a circuit

under faulty conditions or to give alarms when the equipment being protected is approaching its capacity limits. This action ensures that the remaining system remains untouched and protects it from further damage.

With the advancement in digital technology, the use of microprocessors and the availability of reliable communication infrastructures, the relays became able to monitor various parameters, which give complete history of a system during both pre-fault and post-fault conditions. This led to the name of Intelligent Electronic Devices (IEDs), which is considered the component of the future protection of EPS.

4.4 Intelligent Electronic Devices (IED)

The IEDs [8] comprise the second generation of microprocessor relays that are, in addition, utilized as data acquisition units and for the remote control of the primary switchgear. This utilization of the relays has been inspired by the fact that faults do not happen so often and in all parts of a system, therefore, relays can serve other duties as well, apart from their main protection function. In addition, utilizing the protection relays also for data acquisition and control, it achieves integration and better interoperability of the various systems such as protection, supervisory control and data acquisition.

Furthermore, the use of optical fibers in digital communications allowed the exchange of information between the relay and the substation control level to be much more reliable. The following information is typically available from the relay: i) measurement data of current and voltage, ii) information stored by the relay after a fault situation, iii) relay setting values, iv) status information on the circuit breakers and isolators, v) event information. The communication link to the relay can also be used for control purposes, i.e. i) circuit breaker open/close commands, ii) remote reset of the relay or auto-reclose module, iii) changes to the protective relay settings.

The functions of a typical IED can be classified into protection, control, monitoring, metering and communications. Specifically, the communication capability of an IED is one of the most important aspects of modern EPS and protection systems. The communication can be power line carrier, microwave, leased phone lines, dedicated fiber, and even combination of these. There is a strong need to have adequate back-up in case communication is lost, e.g. as a result of a disturbance.

An efficient combination of IEDs, programmable logic controllers (PLCs) and Remote Terminal Units (RTUs) to monitor and communicate could lead to a good level of EPS substation automation in order to improve customer service. An RTU is a useful addition to record all the information about the various parts of the EPS. Adding RTUs at the substation level, further allows the built-in intelligence to be moved to the substation level. That intelligence reduces the amount of data that must be communicated between substations and the main station. For example, information can be retrieved as and when needed from databases maintained at the substation.

5 The Electrical Power System as an Interdependent Infrastructure

Today's EPS consist of several and heterogeneous components, all connected through complex electrical networks/grids [7]. The trend in recent years is that private and public EPS (utilities) operate in interconnected power grids, thus increasing the reliability of the whole system but also generating market opportunities. This interconnection evidently improves the reliability of each member utility because any loss of generation can be transparently covered by the neighbor utilities. On the other hand, this interconnection increases the complexity of the EPS. Then, the concepts of protection, security and reliability of service become much more significant, for both individual utilities and the interconnected EPS.

Moreover, the technological advances and the necessity for improved efficiency in several societal operations resulted in increasingly automated and interlinked heterogeneous infrastructures, with consequences on increased vulnerabilities to accidental and human-made disturbances. What may appear as different parts of our societies, does indeed depend on and influence each other. E.g. an apparently irrelevant event like a small social conflict, a thrown cigarette or a delayed disposal of waste can, under similar conditions, either vanish without any significant impact or trigger riots, forest fires or epidemics. Therefore, when studying complex systems, one must consider also their interdependencies with other systems.

There are four different types of interdependencies of critical infrastructure systems, as identified in [17]:

- **Physical** interdependency: arises from a physical linkage between the inputs and outputs of two infrastructures. For example, an output of one infrastructure is required as input to another infrastructure for it to operate;
- **Cyber** interdependency: the state of an infrastructure depends on information transmitted through the ICT infrastructure (computerization and automation of modern infrastructures and widespread use of supervisory control and data acquisition (SCADA) systems);
- **Geographical** interdependency: a local environmental event can create state changes in all involved infrastructures; implies close spatial proximity of the components of different infrastructures; and
- **Logical** interdependency: the state of each infrastructure depends on the state of the other via a mechanism that is not a physical, cyber, or geographic connection. For example, various policy, legal, or regulatory regimes can give rise to logical linkage among two or more infrastructures.

Modeling the interdependencies among interlinked infrastructures and assessing their impacts on the ability of each system to provide resilient and secure services are of high importance. Specifically for the case of the EPS, following such interdependency analysis is of utmost importance so as to take steps to mitigate any identified vulnerabilities and protect the system's operation from any internal or external threat.

The first step in analyzing interdependencies is identifying them. The case presented below offers an illustration of the type of obvious and not so obvious interdependencies between the EPS and the ICT infrastructure.

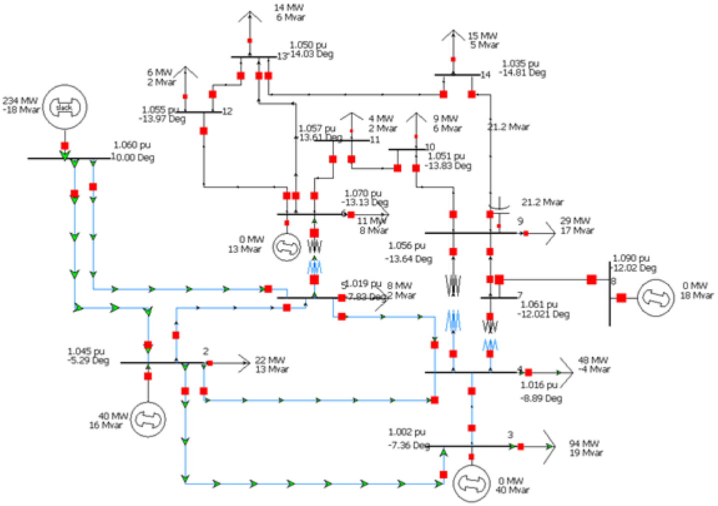


Fig. 2. The IEEE 14 bus test system

The IEEE 14 Bus Test System is a reference EPS which is extensively used in the literature for examining new concepts in a comparable way. Though not a realistic EPS, it is a miniature of real systems useful for educational purposes. It includes 14 buses, i.e. points of electric power exchange, 5 generators and several loads, i.e., the consumers of power. For illustration purposes, the 14 bus system is reorganized and characterized in seven geographic areas, and overlaid with eleven Remote Terminal Units (RTUs) to control equipment on all buses. RTUs are the computerized front-ends of IEDs and are connected using communications infrastructure with the primary control center for Supervisory Control and Data Acquisition (SCADA). The SCADA system is the communications backbone of every modern EPS.

As seen in Figure 3, a wide geographic area is considered where the EPS operates and in Figure 4 a possible network topology of communication links between RTUs in those areas is illustrated. This imaginary case assumes the EPS operator owns the communication links at the bottom half of the figure (operator network, red lines), e.g., a private optical fiber network. The six RTUs, as well as the primary and secondary control centers are directly controlled by the EPS operator. For resilience, the EPS operator leases a number of communication links from a carrier (shown with dashed red lines). The remaining five RTUs are assumed to be located in residential and industrial areas, out of the reach of the private optical fiber network of the EPS operator. Therefore, their RTUs are connected with the SCADA system using an ISP's access network.

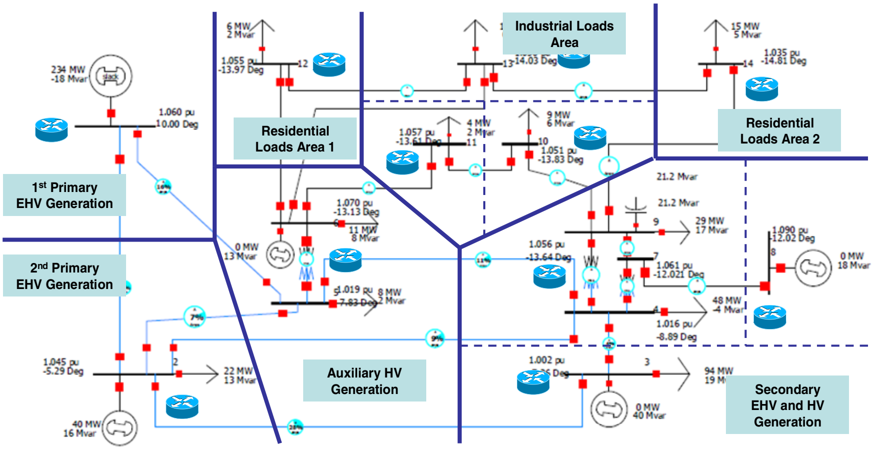


Fig. 3. Illustration of geographic areas based on IEEE 14 bus test system

Physical and **Geographical** interdependencies are relatively straightforward to identify, but require a thorough knowledge of all infrastructures involved. Since information exchange between infrastructure operators is limited, several Physical and Geographical interdependencies go unnoticed until a disruptive event occurs. A recent event in Ireland highlights such hidden interdependencies. In this case, a single transformer fault at the local EPS utility brought down the "cloud infrastructure" of two major ICT infrastructure providers all over Europe[1]. In the above simple case, the reliance of the EPS operator to external communication networks obviously creates a **cyber interdependency**, which needs to be carefully engineered to avoid future contingencies. Although the provisioning of leased communication lines from a carrier network may be tied to strict contractual agreements for availability, these agreements remain private contracts. EPS operators have expressed concerns that these agreements may not be sufficient to guarantee public safety, especially in the event of major catastrophes and natural disasters. The type of **logical** interdependencies are harder to identify and even harder to protect from. They may involve business interests and regulatory conformance of one infrastructure, which may indirectly affect the operation of another. For example, company policies may prevent a fixed-access ISP to announce performance degradation events, such as temporary network congestion. Although the EPS operator could benefit from this knowledge and proactively enable alternative communication means for isolated RTUs (e.g., via GPRS/3G data links), the lack of information exposes the EPS operator to the possibility of communication degradation and sudden disruption.

In the presented test case, the simplicity of the EPS and ICT network immediately reveals their interdependencies. However, in real EPS grids with hundreds of busses, the complexity of the interconnected ICT networks and their dependencies are

[1] See `https://www.datacenterknowledge.com/archives/2011/08/07/lightning-in-dublin-knocks-amazon-microsoft-data-centers-offline/`

daunting. As discussed in the next subsection, the advent of the Smart Grid is amplifying communication requirements for modern EPS, further increasing the importance to investigate them in parallel to a resilient ICT infrastructure.

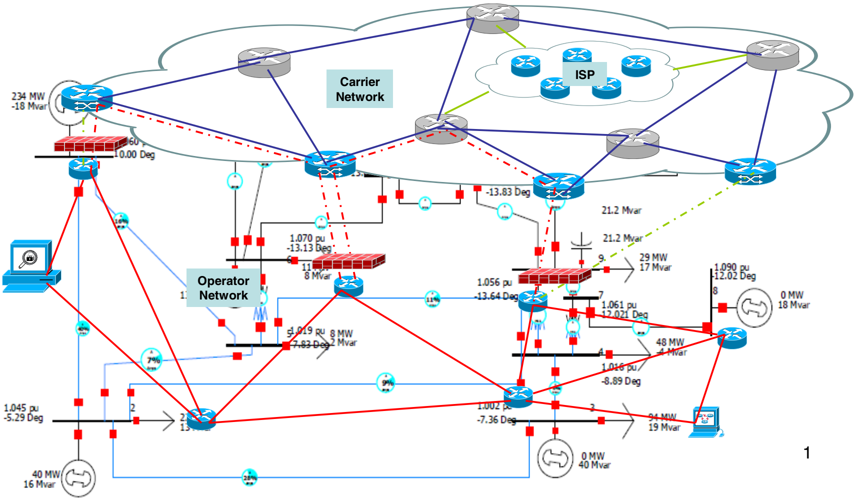


Fig. 4. SCADA system's interdependent ICT infrastructure

6 The Smart Grid and the Systems of Systems Perspective

The previous subsection presented the interdependent nature of the EPS and the need to model all types of interdependencies in order to ensure effective monitoring, control and thus protection of the infrastructure and its objectives. This fact became much more evident with the emergence of the Smart Grid concept and technologies [1], which brings the interdependencies between the EPS and the ICT infrastructures in the forefront. It has been already made clear that to ensure the effective protection of the EPS, the following three elements are considered fundamental: measurements (data defining the state of the system), data processing, and control [8]. Evidently, these elements are tightly interconnected with the ICT infrastructure, which, as seen, is increasingly employed to provide the necessary two-way communication between EPS elements, as envisioned for the Smart Grid. According to IEEE, the Smart Grid is seen as a large and complex system where different domains are expanded into three foundational layers: (i) the Power and Energy Layer, (ii) the Communication Layer and (iii) the IT/Computer Layer. Layers (ii) and (iii) are enabling infrastructure platforms of the Power and Energy Layer that makes the grid "smarter" [9].The viewpoint of IEEE is representative of the awareness around the interdependent nature of the EPS and the ICT infrastructure.

The Smart Grid calls for computers, communication, sensing, and control technologies to operate in parallel towards enhancing the reliability, minimizing the costs and facilitating the inter-connection of new sources in the EPS. The mobilization of the above ICT-enabled technologies needs to happen across broad temporal, geographical and industry scales, so as to close loops where they have never been closed before. The following is a non-exhaustive list of advantages promised by the Smart Grid technologies while being employed in the EPS:

- Self-healing from power disturbance events
- Enabling active participation by consumers in the response of the system (effective demand management)
- Operating resiliently against physical and cyber attacks
- Accommodating all generation and storage options (integration of intermittent renewable energy sources)
- Optimizing of assets and efficient operation (secure and real-time two-way power and information flows)

However, the optimization of EPS operations and resources comes with the cost of increased risk from cyber-attacks, which signifies the need to employ full cyber-security. For example, smart meters (the new metering devices that are deployed in customers' premises) are an attractive part for attacks. Malicious access to the communication channels could cause catastrophic effects on the EPS by driving decisions based on inaccurate data [16],[19].

Beyond the security threats, other aspects that need to be carefully addressed by the introduction of two-way communication are some key privacy concerns. That is, the "smart infrastructure" will require storing personal profiles of customers, to enable the determination of consumer energy behavioral patterns. Moreover, the energy consumption will be recorded remotely and in real-time, thus generating information on whether people use specific facilities.

6.1 System of Systems Architectures

A way forward to achieve real control over the operation of the EPS, thus meeting the needs of the uncertain future, seems to be the driving of the evolution in Systems of Systems (SoS) architectures [3]. An SoS is defined as a collaborative set of systems in which component-systems i) fulfill valid purposes in their own right and continue to operate to fulfill those purposes if disconnected from the overall system, and ii) are managed in part for their own purposes rather than the purposes of the whole [14].

As mentioned earlier, the Smart Grid evolves to include devices that were not previously considered, such as distributed energy sources, storage, electric vehicles and appliances. Such devices comprise heterogeneous systems that serve as integrated components of the emerging EPS and that have different characteristics, requirements for security, requirements or fault detection, protection and metering. Therefore, the traditional architectures turn to be inefficient due to the increasing demand for greater control of energy usage. The challenge is to build the grounds for an evolving SoS architecture, which will be based on open standard services mechanisms. Such architecture will avoid any hard assumptions made at the design phase, allowing a loose coupling for:

- Components to be added, replaced or modified individually in case of malfunctions, without affecting the remainder of the system;
- Components to be distributable; and
- Defining interfaces using standard metadata for application developers for use in replacing components.

The evolution of the EPS as a SoS, with the emergence of clear interfaces among component-systems and processes is expected to enhance the ability of controlling and protecting the EPS. Knowing the components and their interactions will definitely increase our ability to detect problems (created by accidental or malicious intervention), characterize them and address them quickly and efficiently.

7 Conclusions

Evidently, the operation of the EPS affects our everyday life, across many dimensions, from economical to societal. Therefore, electric utilities allocate a justifiable part of their budget for installing, operating and maintaining a sophisticated protection layer. As shown, the protection system undergoes significant evolutionary changes through the years, namely the technological advances utilized in protection devices, the algorithms that allow for the orchestration of the protection devices become more intelligent, and the protection processes become more and more automated, utilizing the ICT infrastructure. At the same time, the complexity of the resulting system drastically increases due to the amplified impact of the EPS to other critical infrastructures in our society, as well as, due to the increase of the impact of other infrastructures to the operation of the EPS. The challenge for the academia and industry is to join forces and make sure they find the necessary balance, to keep the operation of the system reliable and with high quality of service.

References

1. Amin, M., Wollenberg, B.F.: Toward a smart grid: power delivery for the 21st century. IEEE Power and Energy Magazine 3(5), 34–41 (2005)
2. Bansari, S.: The Economic Cost of the Blackout-An issue paper on the Northeastern Blackout. ICF Consulting, Fairfax, VA, August 14 (2003)
3. Chandy, K.M., Gooding, J., McDonald, J.: Smart Grid System-of- Systems Architectures: Systems Evolution to Guide Strategic Investments in Modernizing an Electric Grid
4. Chiaradonna, S., Di Giandomenico, F., Lollini, P.: Interdependency Analysis in Electric Power Systems. In: Setola, R., Geretshuber, S. (eds.) CRITIS 2008. LNCS, vol. 5508, pp. 60–71. Springer, Heidelberg (2009)
5. Commission of the European Communities, Green Paper on a European Programme for Critical Infrastructure Protection, COM (2005) 576 Final (November 2005)
6. Council Directive 2008/114/EC, On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Official Journal of the European Union (December 2008)
7. CRUTIAL: European Project CRUTIAL - critical utility infrastructural resilience (contract n. 027513)
8. Hewitson, L.G., Brown, M., Balakrishnan, R.: Practical Electrical Power Systems Protection. Elsevier, Burlington (2004)

9. IEEE Smart Grid Conceptual Model, accessed online, `http://smartgrid.ieee.org/ieee-smart-grid`
10. Johnson, B.K.: Electrical power system Protection and Relaying. In: Lectures of ECE525-Electrical Power System Protection and Relaying at the Department of Electrical and Computer Engineering, University of Idaho, Moscow (2010)
11. Knight, U.G.: Disturbances in Electrical power systems and Their Effects. In: Electrical Power Systems in Emergencies - From Contingency Planning to Crisis Management. John Wiley & Sons (2001)
12. Knight, U.G.: The Natural Environment-Some Disturbances Reviewed. In: Electrical Power Systems in Emergencies - From Contingency Planning to Crisis Management. John Wiley & Sons (2001)
13. Knight, U.G.: Measures to Minimize the Impact of Disturbances. In: Electrical Power Systems in Emergencies - From Contingency Planning to Crisis Management. John Wiley & Sons (2001)
14. Maier, M.W., Rechtin, E.: The Art of Systems Architecting, 2nd edn. CRC Press, London (2000)
15. McLean, I.: Certificate in Electrical power system Protection. IDC Technologies, USA, Rep. on training courses (2010)
16. Mohajerin, E.P., Vrakopoulou, M., Margellos, K., Lygeros, J., Andersson, G.: A Robust Policy for Automatic Generation Control Cyber Attack in Two Area Power Network. In: IEEE Conference on Decision and Control, Atlanta, Georgia, USA (December 2010)
17. Rinaldi, S., Peerenboom, J., Kelly, T.: Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. IEEE Control Systems Magazine, 11–25 (December 2001)
18. Soman, S.A.: Electrical power system Protection. In: Lectures of Electrical Power System Protection at the Department of Electrical Engineering, IIT Bombay
19. Teixeira, A., Amin, S., Sandberg, H., Johansson, K.H., Sastry, S.S.: Cyber-security analysis of state estimators in electric power systems. In: IEEE Conference on Decision and Control (March 2010)
20. Wall, R.W.: Introduction to Practical Electrical power system Protection. In: Lectures of EE526: Protection of Electrical Power Systems II, Department of Electrical Engineering, University of Idaho, Moscow (2005)
21. Zima, M.: Special Protection Schemes in Electric Electrical power systems, Swiss Federal Institute of Technology, Literature survey (2002)