Cyber-interdependency in Smart Energy Systems

Razgar Ebrahimy[1] and Zoya Pourmirza[2]
[1]*School of Computing Science, Newcastle University, Newcastle upon Tyne, U.K.*
[2]*School of Electrical and Electronic Engineering, Newcastle University, Newcastle upon Tyne, U.K.*
{*razgar.ebrahimy, zoya.pourmirza*}*@ncl.ac.uk*

Keywords: Smart Energy Systems, ICT Architecture, Complex Interdependencies.

Abstract: Critical infrastructures are highly interdependent due to the services they receive and provide to one another. These interdependencies include physical, logical, geographical and cyber. Most of these interdependencies have been studied extensively apart from the cyber interdependency which is the main focus of this paper. Critical infrastructures have cyber interdependency when the state of a physical infrastructure (energy, transport, water, waste, etc.) depends on the information transmitted through the information infrastructure. The communication network is the backbone of smart energy systems and is responsible for transmission of data from all sub-systems in both directions. Due to the complexity and combination of many sub-systems that form smart energy systems, data is generated at different levels within such systems. The data at each layer is different and has its own cyber characteristics. Knowing these characteristics and interdependencies at each layer provides the foundation for designing an appropriate ICT architecture that fits that segment (layer) rather than having an ICT architecture that is generic and designed for all layers but susceptible to risks. This paper outlines a new approach by focusing only on the cyber interdependencies in smart energy systems and how they effect the Smart Grid.

1 INTRODUCTION

Critical infrastructures are highly interdependent due to the services they receive and provide to one another. These interdependencies vary from physical, geographical and logical to cyber interdependencies (Rinaldi et al., 2001). These interdependencies could be regarded as providing both risks and opportunities to overall infrastructure system operation. In general, infrastructure systems such as power, transport and water are legacy systems that have been designed and developed during the last century and are still being developed (Ebrahimy, 2014). The availability of communication networks and digital connectivity (Oughton et al., 2016) to power systems and the benefits of data transmission have led the power sector to adopt these new technologies and integrate them into its operation in the form of Supervisory Control and Data Acquisition (SCADA) systems, which are used for controlling and monitoring.

Whilst the integration of communication network with power grid has great benefits, it is also susceptible to risks and failures due to its interdependency and reliance on external services. For instance an unplanned shut-down of a power station in Italy in 2003 led to failure of a communication node and the SCADA system (Buldyrev et al., 2010). This event resulted in further failures, causing a cascading failure in the system.

The arrival of the Smart Grid and its integration with the legacy power grid has opened new avenues to explore. This exploration must cover the expansion of already complex power systems as they become smarter and more reliant on communication technologies at the same time as integrating with the legacy systems. This all requires new approaches in defining the interdependencies and relationships with external services.

Smart Grid is the integration of traditional electrical power grid systems with information and communication technologies (ICT) (Aloula et al., 2012). This integration improves the efficiency and availability of the power system, empowers the utility providers in terms of how to operate their systems based on consumer demands, while constantly monitoring and checking the demand and supply using ICT infrastructure.

In this research we identified the lack of discussion on cyber interdependency of the Smart Grid. Since the state of the Smart Grid depends on the data transmitted through ICT architecture, the exploration of this cyber-dependency within the Smart Grid

Ebrahimy, R. and Pourmirza, Z.
Cyber-interdependency in Smart Energy Systems.
DOI: 10.5220/0006262805290537
In *Proceedings of the 3rd International Conference on Information Systems Security and Privacy (ICISSP 2017)*, pages 529-537
ISBN: 978-989-758-209-7

makes this research timely, and critical. Unlike the existing grid, the Smart Grid is comprised of distribution, intelligence, operation, system optimization, data decentralization and high dependency on communication. Smart Grid components are interdependent with bidirectional interactions which rely on predefined and correct operation of other dependant systems. Due to the complexity and collection of subsystems in Smart Grid it is important to note that the data dependency at each layer of Smart Grid has different implications on the operation of the entire system. Reliable and real-time information gathering from each layer of the Smart Grid is critical in order to minimize the impact of failures and to optimize the power flow operation in the power system.

The shift towards Smart Grid as referred to by some as an energy transition period (Jefferson, 2008) and moving away from centralized and fossil based systems to a distribution configuration that make use of low carbon alternatives highlights new opportunities and challenges that could arise. One of the key challenges that this paper addresses is the cyber interdependency in smart energy systems and the need for novel, adaptable and resilient ICT architectures that fulfils future interdependent systems.

The remainder of this paper is organized as follows: Section 2 addresses the related work, Section 3 is about the importance of communication in Smart Grid and exploring the cyber dependency. Section 4 addresses different layers of the systems where data is generated and Section 5 analyzes the cyber characteristics of the information. Section 6 is about the differentiation of the ICT architecture and ICT infrastructure, Section 7 explains the essential requirements of Communication and Information handling. Sections 8 and 9 address cyber risks and conclusions respectively.

2 RELATED WORK

There has been intensive research on the Smart Grid from various angles by many researchers. There are many papers which focus on new developments in information and communication (Wissner, 2011), (Wu et al., 2011) and some focusing on consumers and how to involve them in active operation of power consumption management by introducing technical operation systems or providing economic incentives to facilitate their demand (Wolsink, 2012) while others focus on new challenges of dealing with risks and uncertainties in Smart Grid (Zio and Aven, 2011)(Momoh, 2012). There has also been an attempt to focus on cascading failures in interdependent Smart Grid networks and designing cascade resilient networks in Smart Grid using optimum allocation of interdependencies (Rahnamay-Naeini, 2016). As well as focusing solely on electricity there is some research which focuses on a complete set of intelligent management energy sources (Orecchini and Santiangeli, 2011) and some emphasis on market integration (Nielsen et al., 2011).

Surveys such as those conducted by (Wang et al., 2011), (Yan et al., 2013) and (Safdar et al., 2013) have studied the communication infrastructures of Smart Grids, the importance of such communication infrastructures, their challenges and requirements, and the available communication technology. However, there is lack of research on the deign of an ICT architecture, cyber Interdependency within the Smart Grid, and how this cyber interdependency affect the design on an ICT architecture for the smart power grids.

3 SMART GRID AND COMMUNICATION

The communication system is the key part of Smart Grid for data transmission (Laverty et al., 2010). As mentioned in Section 1, Smart Grid has been developed to utilize the transmitted data to deliver a better, more reliable, cost effective, secure and optimized service to consumers (Gungor et al., 2011). An Smart Grid system consists of collection of different types of data from consumer usage data to transmission and substation sensors data and control unit data.

Cyber interdependency in infrastructure (energy, transport, water, waste, etc.) as defined by (Rinaldi et al., 2001), is when a state of a physical infrastructure depends on the information transmitted through the information infrastructure. Figure 1 is a representation of an optimized energy system that is the integration of smart energy providers, smart consumers and advanced management systems with a communication network being an integral part of it.

The direction of data flow and the purpose of transmitted data from each system or sub component is very important. As can be seen from Figure 1 the type and criticality of the data depends on the transmission direction and the data generation source. For instance any data generated from the energy network is either load data or information about the status of the system which is transmitted to advanced management system.

However if the information is from the management system then the data is considered critical since it sends control data and the availability of such data is important for overall operability of the system. Again depending on the destination of the control data, the criticality varies; for instance if the control data is to send a signal to increase generation capacity or to switch load on different lines then it is regarded as critical whereas if the signal is to the consumer to manage their load, based on the demand and response management system, then it is not classed as critical since this is only a suggestion by a utility provider and there is no obligation for consumers to comply with it. In order to understand the data interaction at each layer of the system and the nature of the relationship and criticality we have structured and categorized data sources in three different layers derived from Figure 1 in section 4.

4 DIMENSION OF CYBER DEPENDENCY

Smart Grid data originates from several sources and sensors such as advanced metering systems, phasor measurement units, intelligent relays and remote terminal units. The advanced metering system is a two-way communication network consisting of smart meter, computer hardware and software, monitoring system and data management that enable the collection and redistribution of data between meters and utility providers.

A large and broad spectrum of sources that generate data and increase communication could lead to increasing vulnerability of Smart Grid with many potential points of failure and attacks to be exploited.

In smart energy systems, similar to Smart Grid, the first layer of data dependency is between the consumers (residential/commercial) and local control centres via a communication network. At this layer consumer usage and activity is reported back to a local or central control centre. Since the communication is two way, it is possible for the operator to send some signals back to consumers to suggest reduction in load or limiting their access to the services. If we call this the first layer interaction, then the absence of this information at this level is not very critical for overall operation but instead its availability helps in demand-side response and would give economic benefits to consumers.

The second layer of data dependency is between transmission substation, distribution substation, load serving entity and energy management system (EMS) which are part of modern smart energy provision. An EMS is fed from sources such RTUs, PLCs and smart relays that take system status information and load at different nodes via the communication network and then feeds the information into a state estimator to perform optimal power flow, contingency analysis and detect bad and false data received to operate the optimal power system. An EMS is also capable of receiving the transmitted data from the power network sensor readings of substation to transmission linens' and distributed and renewable energy sources to monitor the network.

The generated data at this layer is critical for the operation of the system since it has direct influence on how a system should react in terms of whether to increase/decrease capacity, switch the load or disconnect a node from the grid.

The third layer of data dependency in smart energy systems is the data generated from interdependent systems which are not directly part of the Smart Grid architecture but whose inputs have direct influence and implications on how these systems operate. For instance accurate weather data could be used to forecast more realistic energy demand and prepare for sudden changes. Access to historical data about usage and weather data enables advanced advisory systems to provide more accurate and realistic predictions of energy demand in conjunction with current demand data. Although at this layer the availability of such data cannot be regarded as critical, the addition would help in better monitoring and operation of the system.

The data interdependency in smart energy systems is tight and cohesive and this is why there is a need for better understanding of layer dependencies to enable accurate measurements, performance analysis and ensure security of supply.

5 CYBER CHARACTERISTICS OF THE DATA

Within each interdependent layer the characteristics of the data and communication networks differ. For instance, depending on what data is transmitted or where it originates, the implications caused by such data on smart energy systems could vary. Figure 2 is a representation of the data that each has a source, meaning that in large complex systems such as Smart Grid there are many sources which generate information. Secondly each piece of information has a data type and finally the characteristics of the data which could be one or the collection of the set shown in Figure 2. Below are the data characteristics of the information generated, that depending on the layer and source would posses the characteristics shown in the following subsections:

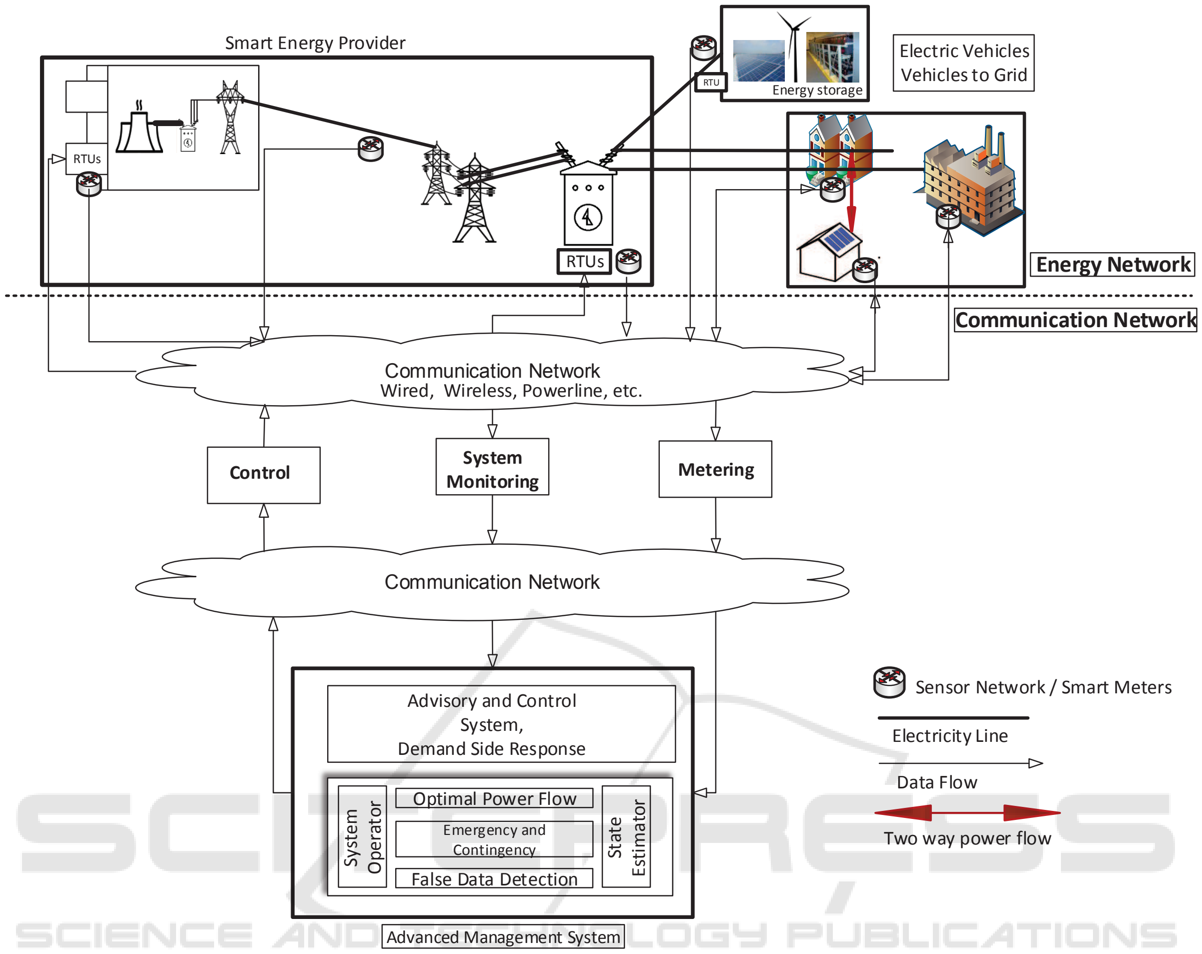


Figure 1: Energy Systems and Data Flow.

5.1 Communication Technologies

As mentioned before, a two-way communication system which includes both wired and wireless is essential for Smart Grid and smart energy systems as a whole. However based on the layer of transmission, the communication could be different. For instance, the flow of information from sensors and electrical appliances to smart meters could be via powerline or wireless communications such as ZigBee, Zwave, and others (Luan et al., 2010). The communication from smart meters to utility providers could be accomplished through mobile network or the Internet. Depending on the type of implemented technology on each layer or on each component the interactions and points of failures are different.

5.2 Margin of Error

Sometimes it is acceptable to have delay in data transmission from smart meters to utility providers, providing it is only the consumption data. The resolution of data in this case is usually not the same for each provider or similar to other countries. Usually the data is collected at discrete time slots of equal length. For instance, depending on the provider the resolution of data could vary from 1 slot a day to 48 (half hourly) (Yang et al., 2014) per day. In cases where the sensors transmit critical data such as PMUs or RTUs where the data triggers automotive decisions the margin of delay and resolution is much smaller. Therefore the source of the data is key for determining the acceptable scale of errors.

5.3 Security Measures

Security is a major concern in Smart Grid due to two-way communication in the system as modern power systems rely on information infrastructure to operate. Legacy power systems are protected by Supervisory Control and Data Acquisition (SCADA), Energy Management Systems (EMS) and Real Time Oper-

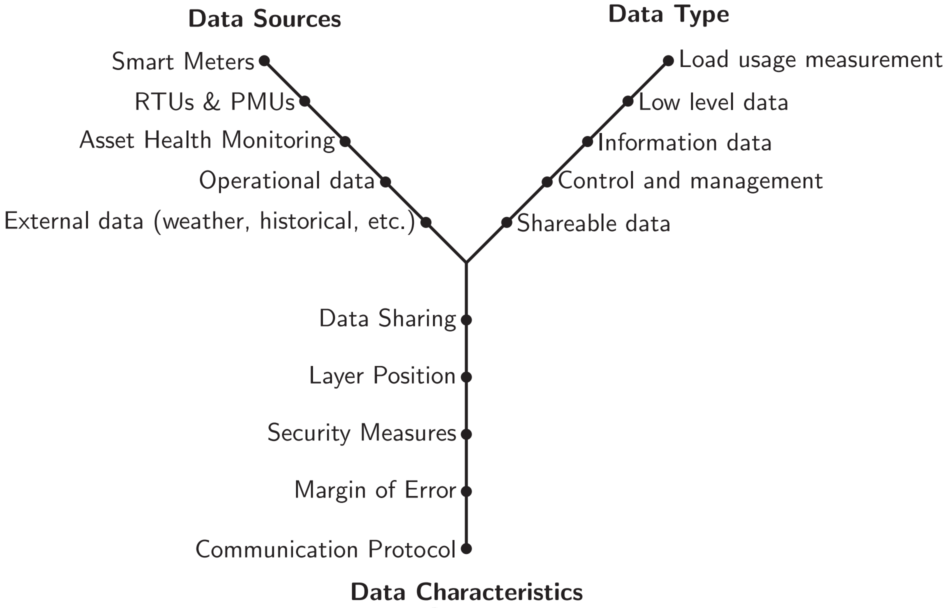


Figure 2: Data interdependency.

ating Systems (RTUS) to ensure optimal operability. To ensure the operability of the Smart Grid information infrastructure, the network and data management tools need to be secure. This is why the IEC62351 protocol was developed with the focus on authentication of data transfer (ANSI C12.22), authenticated access, intrusion detection and eavesdropping. Nevertheless there are still some concerns with bad data injection in Smart Grid systems that can not be identified by detection or state estimator (Huang et al., 2013).

5.4 Data Types

Generally there are two types of data in smart energy systems: status data and control data. Status data are generated from sensors in transmission, distribution and smart meters, etc whereas control data are generated from RTUs and management systems to trigger an event.

5.5 Resource and Status Sharing

Distributed energy is becoming an important part of the Smart Grid, specifically when the consumer feeds energy back to the system using solar or storage batteries. In traditional power systems in the UK, National Grid is responsible for generating electricity based on forecast figures and contingency measurements. However when consumers generate their own electricity then to track the overall generation the electricity suppliers need to have access to such data from the consumer side. This is where consumers generate data of their usage and generation, each targeting the same or different operators. This type of resource sharing in terms of data benefits both utility and grid operators.

5.6 Information Infrastructure & Big Data

Due to the complexity and integration of different systems, the amount of data that smart energy systems generate is very large scale. This is one reason that data analysis is becoming a core part of any smart system to enable the advisory systems in better decision making and optimal operation of the entire system.

6 ICT ARCHITECTURE VERSUS ICT INFRASTRUCTURE

The term infrastructure used to refer to ”the underlying foundation or basic framework (as of a system or organization)” (MA, 1993). In 1997, the term gained more importance and advanced meaning based on the work of PCCIP (US Presidents Commission on Critical Infrastructure Protection). In this new era the term infrastructure was widely used to mean the framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defence and economic security of the United

States, the smooth functioning of governments at all levels, and society as a whole. This section defines and delimits the term infrastructure in the domain of Communication and Information Technology (ICT). Additionally, it differentiates between ICT infrastructure and ICT architecture, terms which are commonly misused by researchers in a number of areas of study. Next, we will discuss how ICT architecture can influence the cyber dependency of the Smart Grid.

An ICT infrastructure describes the fundamental components such as monitoring devices, computers, controllers, software, middleware, storage, and data communication media and technologies, that offer services such as access, transmission, storage, monitoring, control, conversion of data to useful information, analysis, and finally taking action based on analysed data in a system or organization.

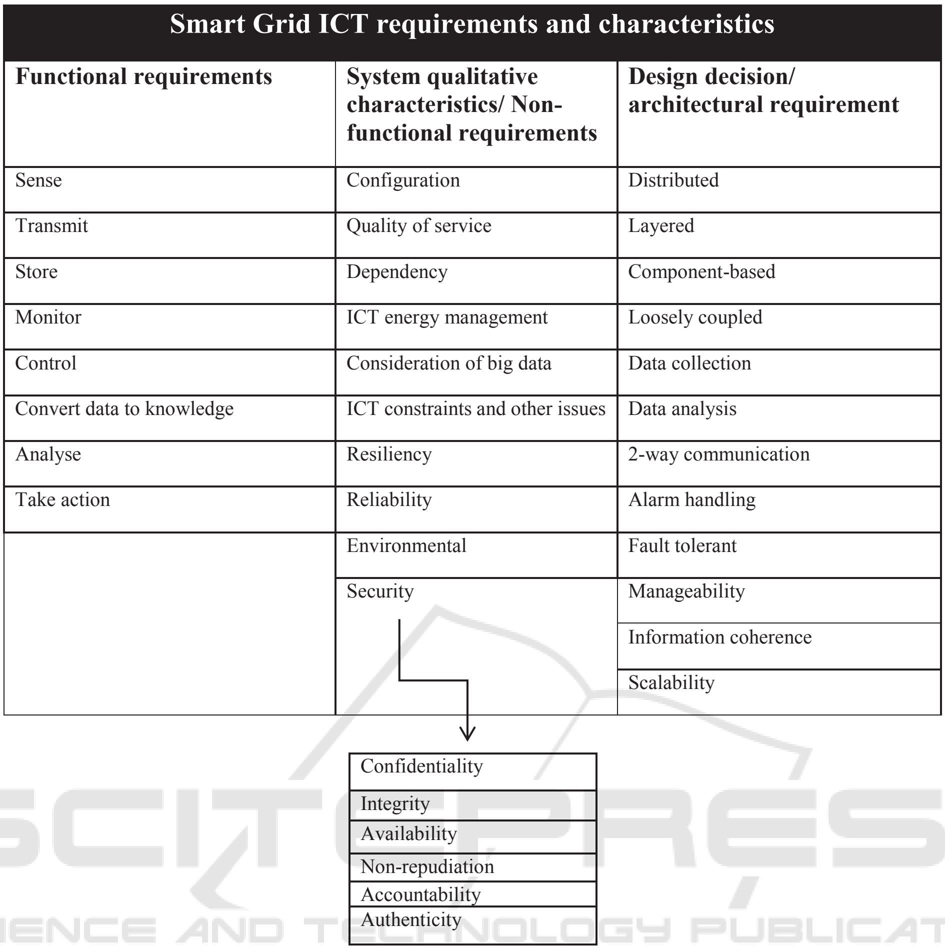
ICT infrastructure resembles the foundation or infrastructure of a building that can support a number of different building architectural styles such as Achaemenid, Ancient Chinese, Victorian, or Roman. Although different buildings might have varied architectural styles, their infrastructures are similar. Likewise, based on similar ICT infrastructure we can design and develop a number of different ICT architectures, corresponding to diverse organizational requirements.

Conversely, an ICT Architecture refers to the design or style in which components and services of the ICT infrastructure interact. In other words, ICT infrastructure is about the components or building blocks of a system that support the ICT architecture. ICT architecture design should be based on established architectural principles and requirements of the organization. Such architecture should not only offer, but facilitate, enhance, and sustain services required by the organization. Without a proper ICT architecture design, the cyber system of an organization will not be future proof, as it may not incorporate upcoming functionalities, ideas, and changes to the system. To summarise, while ICT infrastructure is almost the same for all levels of Smart Grids, the ICT architecture varies according to a number of parameters, which will be discussed in the next section. Accordingly, ICT infrastructure does not affect the cyber-interdependency of the Smart Grid as much as the ICT architectures does. This also highlights the importance of rigorous considerations of an ICT architecture in the design phase, as it can isolate or cascade failures in such cyber-interdependent systems.

7 COMMUNICATION AND INFORMATION HANDLING REQUIREMENTS

This section identifies the ICT (Information and Communication Technology) requirements of the Smart Grid, and discusses how some of these requirements can influence the cyber-interdependency of the power grid. As mentioned earlier, in order to design a sustainable and futureproof architecture, the design team should first identify the requirements of such architecture. Since there is no one ICT architecture that can fit all the different cases (Pourmirza, 2015), the requirements and design decisions identified in this section can help ICT developers to improve and modify their designs. The ICT requirements for the Smart Grid are classified into three categories, namely functional, non-functional, and architectural requirements. Functional requirements are defined as the concrete functionalities of a system, non-functional requirements are described as the qualitative characteristics of a system which address the performance concerns (Committee and Board, 1998), and architectural requirements are defined as the design decisions which relate to the ICT architecture itself (Rohjans et al., 2012). Amongst these three categories, requirements defined under the architectural requirements or design decisions affect the degree of cyber interdependency of the power grid the most. Proper consideration of some of these parameters is critical in the design of an ICT architecture for the Smart Grid, as they can directly or indirectly cascade or isolate the fault in the system, and prevent the rest of the grid from being adversely affected. Figure 3 presents a number of requirements in each category.

The state of the Smart Grid depends on the output of its ICT architecture. Some of the parameters that highlight the cyber interdependency of the Smart Grid are as follows: distributed, layered, component-based, and loosely coupled. These parameters can affect flexibility and adaptiveness of the system in case of failure or when the system is stressed. One of the main requirements of an ICT architecture is to be a distributed system (Pourmirza and Brooke, 2013). A centralized ICT system has a single point of failure; by moving from centralized to distributed systems we can prevent this problem. Fault tolerance is one of the principles in distributed systems (Emmerich,); it is the ability to deal with the reliability of the system in the event of a fault, and it also enables the system to progress despite the presence of failure in the system. It is usually implemented by circumventing a single point of failure in the network. A distributed system can be represented by a hierarchical architecture. Hi-



Smart Grid ICT requirements and characteristics		
Functional requirements	**System qualitative characteristics/ Non-functional requirements**	**Design decision/ architectural requirement**
Sense	Configuration	Distributed
Transmit	Quality of service	Layered
Store	Dependency	Component-based
Monitor	ICT energy management	Loosely coupled
Control	Consideration of big data	Data collection
Convert data to knowledge	ICT constraints and other issues	Data analysis
Analyse	Resiliency	2-way communication
Take action	Reliability	Alarm handling
	Environmental	Fault tolerant
	Security	Manageability
		Information coherence
		Scalability

Confidentiality
Integrity
Availability
Non-repudiation
Accountability
Authenticity

Figure 3: ICT Smart Grid requirements.

erarchical systems have a tree structure such that each node is connected to several other nodes (leaves) and each of these nodes is connected to a number of different nodes, and so on. A hierarchical network is a type of network wherein processing and control functionalities are performed at different levels (Fed, 1996). These functionalities can be on top of, or below, each other or else they can be at the same level. Hierarchical systems are to some degree interdependent and partially fault tolerant. Although a failure at the leaf level may not cause huge disturbance to the whole system, their root can be considered as a single point of failure.

The other requirement of an ICT architecture is to be a layered system (Pourmirza, 2015). Hierarchical relations can also be represented through use of layers. As defined by the National Communications System Technology and Standards Division in the US (Emmerich,), layering in a communication system is referred to as a group of related functions that are performed in a given level in a hierarchy of related functions. Layering addresses how different sections of the ICT of the Smart Grid are connected, and how the information passes between each section. A strictly layered hierarchical architecture is an interdependent system, if one layer fails, the whole architecture will fail. This is because an entity in each layer can only interact with an entity in its own layer, or with the layer directly below, because the upper layer asks for services or data from layers below.

The next requirement of an ICT architecture is to be a component-based system (Pourmirza, 2015). A component has been defined by the National Communications System Technology and Standards Division (Fed, 1996) as a part of a system that is essential for the operation of a bigger system and is a direct sub-division of the system to which it belongs. Some of the components that result from a sub-division of the ICT architecture are: smart meters, WSNs, monitoring devices in the substations, databases and visualization tools. Accordingly, some of these components can also be sub-divided into other components.

For example, monitoring devices in the substations can be componentized into other components, namely cRIOs, data storage, a control unit and a router. Since these components are interdependent, failure to pass correct or updated data to another component may cause a fault in the system. Therefore, what happens to one layer or component can directly and indirectly affect the rest of the system, and finally impact the operation of the whole power grid.

The other main requirement for the design of the an ICT architecture is loose coupling which falls under the architectural requirement category. Infrastructures can be tightly or loosely coupled. Tight coupling addresses the strong dependency of one layer or component on another one in a cyber system. Cascading failures are usually caused by tightly coupled systems, as disturbances in one section can affect the other sections to which they are tightly coupled. In cyber infrastructure, loose coupling allows for flexibility of design of the ICT architecture. In a layered ICT architecture a loosely coupled system has a little or no knowledge about the internal details of the other layers and communication between layers is based on abstractions. This will affect their operational performance, and flexibility to deal with failures and changes in the system.

Overall, ICT requirements such as distributed, layered, component-based, and loosely coupled can influence the degree of cyber-dependencies of the Smart Grid.

8 CYBER RISKS

Due to the nature, complexity and interdependency of the Smart Grid it is essential to consider security objectives in its communication systems. These objectives are confidentiality, integrity and availability which are required for control management and monitoring and must operate within acceptable risk level (Zhang et al., 2010). Since the emergence of different Smart Grid technologies, standards and techniques have been developed by the community. However there is still a lack of a widely accepted protocol which includes all the elements of Smart Grid such as smart meters, smart devices and household appliances and the integration of renewable energy. One of the reasons for the lack of full deployment of Smart Grid is regional policy making and the definition of Smart Grid in that region or country. Nowadays power systems are much more susceptible to failures and blackouts due to increase in connectivity to information infrastructure than when power systems were operating in isolation. This means the whole system needs to be more resilient and secure by implementing new security measurements and in most cases there is a need to change the ICT architecture that fits the system and satisfies the new requirements.

9 CONCLUSION

Smart Grid and smart energy systems are interdependent and highly dependent on communication networks. In addition there is high dependency on the information and data generated by these systems which are critical for the operation of dependent systems. This paper has presented a top down approach to represent the data and communication interdependencies between legacy power systems, Smart Grid and smart energy systems individually and as a whole. It has also shown how important it is to design and develop an ICT architecture that facilitates such systems using the existing ICT infrastructure.

Additionally, it has demonstrated how a number of design decisions while developing an ICT architecture affects the cyber interdependency of the Smart Grids. Having an ICT architecture that fits the requirement of each discrete system enables the overall systems to be more reliable, resilient and secure against any threats and failures.

ACKNOWLEDGEMENTS

The research reported in this paper was partially supported by of the STRATA; Layers for Structuring Trustworthy Ambient Systems funded by the Engineering and Physical Sciences Research Council under Programme Grant EP/N023641/1.

The authors also would like to thanks Cliff Jones for his feedbacks and guidance on this paper.

REFERENCES

(1996). Telecommunications: Glossary of telecommunication terms.

Aloula, F., Al-Alia, A., Al-Dalkya, R., Al-Mardinia, M., and El-Hajj, W. (2012). Smart grid security: threats, vulnerabilities and solutions. *International Journal of Smart Grid and Clean Energy*, 1(1):1–6.

Buldyrev, S. V., Parshani, R., Paul, G., Stanley, H. E., and Havlin, S. (2010). Catastrophic cascade of failures in interdependent networks. *Nature*, 464(7291):1025–1028.

Committee, I. C. S. S. E. S. and Board, I.-S. S. (1998). Ieee recommended practice for software requirements specifications. Institute of Electrical and Electronics Engineers.

Ebrahimy, R. (2014). Investigating SCADA failures in interdependent critical infrastructure systems. *CoRR*, abs/1404.7565.

Emmerich, W. Distributed system principles.

Gungor, V. C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., and Hancke, G. P. (2011). Smart grid technologies: Communication technologies and standards. *IEEE Transactions on Industrial Informatics*, 7(4):529–539.

Huang, Y., Esmalifalak, M., Nguyen, H., Zheng, R., Han, Z., Li, H., and Song, L. (2013). Bad data injection in smart grid: attack and defense mechanisms. *IEEE Communications Magazine*, 51(1):27–33.

Jefferson, M. (2008). Accelerating the transition to sustainable energy systems. *Energy Policy*, 36(11):4116–4125.

Laverty, D. M., Morrow, D. J., Best, R., and Crossley, P. A. (2010). Telecommunications for smart grid: Backhaul solutions for the distribution network. In *IEEE PES General Meeting*, pages 1–6.

Luan, W., Sharp, D., and Lancashire, S. (2010). Smart grid communication network capacity planning for power utilities. In *IEEE PES T D 2010*, pages 1–4.

MA (1993). *MerriamWebsters Collegiate Dictionary*, volume 10th ed. Springfield.

Momoh, J. (2012). *Smart grid: fundamentals of design and analysis*, volume 63. John Wiley & Sons.

Nielsen, S., Sorknæs, P., and Østergaard, P. A. (2011). Electricity market auction settings in a future danish electricity system with a high penetration of renewable energy sources–a comparison of marginal pricing and pay-as-bid. *Energy*, 36(7):4434–4444.

Orecchini, F. and Santiangeli, A. (2011). Beyond smart grids–the need of intelligent energy networks for a higher global efficiency through energy vectors integration. *International Journal of hydrogen energy*, 36(13):8126–8133.

Oughton, E. J., TRAN, M., JONES, C. B., and EBRAHIMY, R. (2016). 9 digital communications and information systems. *The Future of National Infrastructure: A System-of-Systems Approach*, 1995(2000):181.

Pourmirza, Z. (2015). *An ICT architecture for the neighbourhood area network in the Smart Grid*. PhD thesis, University of Manchester.

Pourmirza, Z. and Brooke, J. M. (2013). A realistic ict network design and implementation in the neighbourhood area of the smart grid. *Smart Grid and Renewable Energy*, 4(6):436–448.

Rahnamay-Naeini, M. (2016). Designing cascade-resilient interdependent networks by optimum allocation of interdependencies. In *2016 International Conference on Computing, Networking and Communications (ICNC)*, pages 1–7.

Rinaldi, S. M., Peerenboom, J. P., and Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems*, 21(6):11–25.

Rohjans, S., Dnekas, C., and Uslar, M. (2012). Requirements for smart grid ict-architectures. In *2012 3rd IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe)*, pages 1–8.

Safdar, S., Hamdaoui, B., Cotilla-Sanchez, E., and Guizani, M. (2013). A survey on communication infrastructure for micro-grids. In *2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC)*, pages 545–550.

Wang, W., Xu, Y., and Khanna, M. (2011). A survey on the communication architectures in smart grid. *Computer Networks*, 55(15):3604–3629.

Wissner, M. (2011). The smart grid–a saucerful of secrets? *Applied Energy*, 88(7):2509–2518.

Wolsink, M. (2012). The research agenda on social acceptance of distributed generation in smart grids: Renewable as common pool resources. *Renewable and Sustainable Energy Reviews*, 16(1):822–835.

Wu, Y.-n., Chen, J., and Liu, L.-r. (2011). Construction of china's smart grid information system analysis. *Renewable and Sustainable Energy Reviews*, 15(9):4236–4241.

Yan, Y., Qian, Y., Sharif, H., and Tipper, D. (2013). A survey on smart grid communication infrastructures: Motivations, requirements and challenges. *IEEE Communications Surveys Tutorials*, 15(1):5–20.

Yang, L., Xue, H., and Li, F. (2014). Privacy-preserving data sharing in smart grid systems. In *Smart Grid Communications (SmartGridComm), 2014 IEEE International Conference on*, pages 878–883.

Zhang, R., Zhao, Z., and Chen, X. (2010). An overall reliability and security assessment architecture for electric power communication network in smart grid. In *Power System Technology (POWERCON), 2010 International Conference on*, pages 1–6.

Zio, E. and Aven, T. (2011). Uncertainties in smart grids behavior and modeling: What are the risks and vulnerabilities? how to analyze them? *Energy Policy*, 39(10):6308–6320.