A Study on Interdependencies of Cyber-Power Networks in Smart Grid Applications

Bamdad Falahati, *Student Member, IEEE*, and Yong Fu, *Member, IEEE*

***Abstract*—A cyber-power system, a type of cyber-physical system, contains two interconnected infrastructures: a power network and a cyber network. The cyber network monitors, protects and controls the power network. Without the cyber network, the power network cannot operate efficiently or reliably. This paper studies the cyber-power interdependencies in smart grids and categorizes four types of interdependencies between cyber and power networks. The proposed classification permits the assessment of adverse effects of cyber network failures on the power network's operation. Two applications of cyber-power systems, automated substations and micro grids, are discussed in this paper, and certain cyber-power interdependencies are listed as examples.**

***Index Terms*— Cyber-power network, Interdependency, Micro grid, Smart grid, Substation automation system**

I. Introduction

In the past decade, the emergence of high-speed, reliable and smart computer systems has caused a revolution in control systems in that digital systems are replacing traditional and analogous control systems in industries. Computers analyze and process a great amount of data in a small portion of time. This advanced capability of computers has significantly increased the penetration level of cyber control systems in physical systems, such as electric power, transportation, water, and natural gas networks. A cyber-physical system contains two interconnected infrastructures: a physical network and a cyber or a computer network. Cyber networks have been employed for monitoring, protecting and controlling different types of physical systems.

In recent years, power systems have begun to take advantage of computer technologies as well. Computer networks boasting peer-to-peer communication, digital indication and protection, and automatic control are making the power system operation smarter [1]. Cyber-power systems are being studied widely in the smart grid. Phasor measurement units (PMU) are installed in the transmission sector to improve the situational awareness of power systems and to predict the system's collapse [2]. The advanced metering infrastructure with smart meters is used in the distribution sector to collect energy consumption data and to operate in a way that improves the efficiency and reliability of power distribution systems [3]. Cyber-power systems also are applied for the demand response. Volatile prices in retail markets encourage customers to consume more power in off-peak hours with a cheaper price and less power in peak hours with an expensive price. Programmable washing machines and plug-in hybrid electric vehicles (PHEV) are using smart plugs and energy management units to connect with the grid at midnight when the demand and price is less than those during the evenings [4].

Note that the efficient and reliable operation of power networks without cyber networks is actually unattainable. Analyzing power system operations requires considering the characteristics of the cyber network, as the cyber layer is vulnerable and is not failure free. It is worthwhile to pay attention to the risk of failure in cyber systems for particular reasons. First of all, an increasing usage of cyber elements in the smart grid is introducing a higher risk of failure in the cyber-power system. Second, failures in cyber elements are harder to trace than those in electrical power elements. Certain types of failures in cyber elements are hidden and will appear when a mal-operation occurs in the cyber-power system. In addition, the behaviors resulting in errors, faults, and failures in cyber systems are very complicated, thus making the modeling of cyber systems challenging. Therefore, uncertainty, unreliability and unpredictability from cyber networks adversely affect modern power systems.

Previous studies investigated critical infrastructure interdependencies. Reference [5] defined four principal classes of infrastructure interdependencies: physical, cyber, geographic and logical. In [6], general features of interactions between critical infrastructures were investigated based on the intrinsic dynamic behaviors of a failure that may cause consecutive cascade failures. For the cyber-power system study, [7] proposed a super-infrastructure containing power, computer, and communication infrastructures with close interactions and interdependencies between them. Each infrastructure has its own standards, protocols and governance by physical laws that exclusively belong to that infrastructure. Reference [8] presented a framework for an Intelligent Distributed Autonomous Power System (IDAPS), which is a specialized micro grid for managing customer-owned distributed energy resources. IDAPS has been divided into two separate layers, cyber and power. Agent-based communication was used in this paper. Reference [9]

The authors are with the Department of Electrical and Computer Engineering, Mississippi State University, Starkville, MS 39762 USA (e-mail: bf229@msstate.edu, fu@ece.msstate.edu)

978-1-4577-2159-5/12/$31.00 ©2011 IEEE

proposed a framework to analyze the extracted information in order to detect adverse effects of cyber systems on electric power infrastructures. This framework can consider intrusion attempts, file system updates on each computer system, and the anomalous changes in the status of switching devices and the setting of digital relays.

This paper focuses on the cyber-power interdependencies in smart grid applications and categorizes four types of interdependencies between cyber and power networks. The proposed classification allows for the assessment of adverse effects of failures in cyber networks on power network operation. Two applications of cyber-power systems, automated substations and micro grids, are discussed in this paper, and certain cyber-power interdependencies are listed as examples.

The rest of the paper is organized as follows. Section II describes characteristics of power and cyber layers. Section III discusses the different types of cyber-power interdependencies. The cyber-power systems in automated substations and micro grids, as applications of smart grid technologies, are discussed in Section IV. A case study about an automated substation and its results are shown in section V. Finally, the conclusion drawn from discussions in this paper is provided in Section VI.

II. Cyber and Power Networks

Electricity is generated by generators, transferred to substations through transmission lines, and then delivered to customers using the distribution network. Each sector of a power system contains two types of networks: power and cyber [9], [1]. The important prerequisite of analyzing and defining interdependencies among all constitutive elements of the cyber-power system, as a heterogeneous network, is to recognize two separate homogenous networks. The physical connection between nodes and the type of material transmitted in a connection are the two main criteria for splitting the whole system into homogeneous networks. A brief description of these two networks is presented in this section.

A. Power Networks

Electrical power networks are one of the world's most complicated and critical infrastructures. A power network is usually divided into three hierarchical levels: generation, transmission and distribution. Similar to other physical networks, a power network has its own physical laws and limitations due to its inherence. For instance, the power balance at each node and the relation between voltage and power through each line are two fundamental sets of equations that must be considered in a power system study. Also, each generation unit supplies the power within its maximum and minimum limits of generation. In addition, the overload on transmission lines and abnormal voltage at substations should be taken into account. Otherwise, they will cause destructive effects on electrical equipment and ultimately could cause the system to collapse. In recent years, blackouts have become a vital societal concern [6]. A modern power network should aim at delivering reliable, secure, and stable electricity to customers.

B. Cyber Networks

In order to operate the power system successfully, cyber networks perform a wide variety of tasks. The primary tasks of a cyber network are to monitor, protect, and control the power system. Also, a cyber network may enable time synchronization with a global positioning system (GPS), data manipulation and fault analysis, as secondary tasks.

A cyber network consists of intelligent electronic devices (IED), servers, human machine interfaces (HMI), network switches, network connections, and other apparatuses. IEDs, as interface devices between the power network and the cyber network, include measuring units, protective relays, and controllers. IEDs collect data from the electrical equipment and send them to the server; they also apply the commands received from HMIs to the electrical equipment. Network connections create paths for linking IEDs together. Network switches select paths to transfer information inside the cyber network through network connections.

Various forms of cyber networks exist in the world, and each uses different methods to transfer data between nodes. Cyber networks usually are categorized into three levels, local area networks (LAN), metropolitan area networks (MAN) and wide area networks (WAN). LANs usually are implemented in buildings with limited distances between equipment. They typically connect workstations, personal computers, printers, servers, and other devices. Ethernet is the most popular architecture of LANs in the world, and statistics show that over 95% of LANs are Ethernet [10]. Several architectures, such as star, ring and hybrid schemes, can be implemented in Ethernet networks [11], which are very common in substation automation systems and micro grids. Another type of LAN is the wireless local area network (WLAN), and its application has been extended significantly in smart grids [12]. A MAN is a large computer network that usually spans a number of buildings and interconnects a number of LANs through a high-capacity backbone technology. A WAN is a data communication network that covers a wide area, thousands of miles, and usually connects smaller MANs and LANs.

Safe and fast data transmission is of great importance. Safety and speed are directly related to each other. Greater reliability requires more time. In other words, a tradeoff is required for balancing the optimum delay and acceptable level of safety. For instance, data acknowledgement requires a returned package that decreases network efficiency and agility [13]. Furthermore, delays of network switches and connections in data transferring may deteriorate network performance [14]. Finally, the software used in cyber networks requires process time for execution and may contain bugs and errors that affect its ability to produce the desired action.

C. Comparisons between Power and Cyber Networks

Both power and cyber networks are interconnected graphs represented by nodes and branches. This common property permits a similar structure to be defined for them upon which can be applied fundamental graph theory and algorithms. Both of them are bidirectional graphs on which the electricity and data can be transferred back and forth between nodes. However, the following key differences between power and cyber networks should be considered for modeling these two networks:

- The most important difference comes from the inherent dissimilarity of data and electricity. The power flow in power systems is unintentionally based on Kirchhoff's voltage law (KVL) through loops and Kirchhoff's current law (KCL) at nodes. However, the data flow in computer networks is controllable. Based on the Rapid Spanning Tree Protocol (RSTP), manageable network switches are able to select a path for the data with priorities [15].
- Each network, whether power or cyber basically contains four essential objects: nodes, connections, source points and load points. In power systems, generation sources and demand loads are specified. However, in cyber networks, communications are bidirectional, and each pair of nodes engages in peer-to-peer communication. A digital device can act as both a destination node and as a source node, receiving and transmitting data, respectively.
- Power and cyber networks have different definitions of, reasons for, consequences of and solutions for congestions. Congestions in power networks occur when transmission lines reach their limitation. For instance, the unanticipated lack of generation in one zone forces generators in neighboring zones to provide extra power through tie lines, which may cause congestion. The high temperature caused by congestions in power networks will damage power lines. As a feasible solution, rescheduling generation and load shedding can mitigate the congestion in power systems. However, in cyber networks, congestion occurs when there is a collision in half duplex connections or queues in the output ports of switches, bridges, routers, and gateways [14]. Usually, cyber congestion will result in communication delays and data loss.
- Quantitative parameters such as current and voltage are used to evaluate the condition of power systems. However, connectivity, interoperability and synchronization are important for the assessment of cyber systems.

III. Interdependencies between Cyber-Power Networks

Interconnected networks are mutually twisted to each other at some points. This interdependency generally means that the correct and appropriate operation of one element depends on the existence and proper function of some other elements. At first, four interactions between power and cyber networks are recognized as follows:

- Direct interaction causes the failure of or changes the behaviors of the element.
- Indirect interaction does not cause the failure of or change the behaviors of the element but will impact the performance of the element against the failure.
- Element-Element interaction refers to the interaction between elements that are physically/logically interconnected between cyber and power networks.
- Network-Element interaction evaluates the impact of the performance of one network on the element in the other network.

Therefore, four types of interdependencies are categorized in this section: Direct Element-Element Interdependencies (DEEI), Direct Network-Element Interdependencies (DNEI), Indirect Element-Element Interdependencies (IEEI), and Indirect Network-Element Interdependencies (INEI).

A. Direct Element-Element Interdependency (DEEI)

The simplest interdependency modeling is Direct Element-Element Interdependency (DEEI), which means that failures in a group of elements in one network either cause the failure of or change the specification of one element in the other network. Figure 1 presents two DEEI examples. The failure of controller C1 in the cyber network will lead to the failure of the physically connected circuit breaker CB1 in the power network.

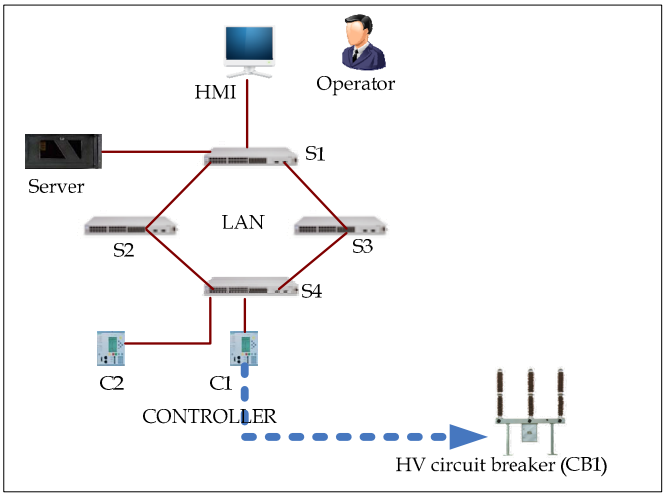

Fig. 1 Schematic drawing of a cyber-power connection in a smart grid network

B. Direct Network-Element Interdependency (DNEI)

The Direct Network-Element Interdependency (DNEI) means that the performance of one network causes the failure of or changes the specification of the element in the other network. In other words, the information regarding failures in one network is not sufficient for finding the impacts on the other network. Thus, a network study must be executed to assess its performance and find such impacts on the other network. Figure 1 also can be used to explain DNEI. The operator can successfully send a close or open command from the HMI to circuit breaker CB1 if the connectivity between HMI and controller C1 in the cyber network can be established. The failure of switch S2 in the cyber network does not mean that

the data stream cannot flow from the HMI to controller C1 because there is an alternative for the data transfer via switch S3. Therefore, the connectivity check in the cyber network should be implemented to determine the impact of the cyber network's performance on circuit breaker CB1.

C. Indirect Element-Element Interdependency

The Indirect Element-Element Interdependency (IEEI) means that failures of a group of elements in one network do not directly cause the failure of or change the behaviors of the element in the other network but will impact the performance of the element against the failure. Such interdependency may either increase the risk of new failures on the element or defer the response to the current failure on the element. For example, one of the duties of cyber networks is to monitor the power system using indicators that can report the forthcoming failure on the element in the power network. The failure on these indicators will increase the failure rate of the power element, as the operator is not able to be aware of the current situation of the element in order to make corrective actions to avoid a serious failure before it occurs. In addition, the failure of indicators will hide the failure on the power element. Thus, the repair time of the power element will increase as the failure of the indicated power element remains in the power network and will be observed until the periodical maintenance appears on it.

D. Indirect Network-Element Interdependency

The Indirect Network-Element Interdependency (INEI) means that the performance of one network does not directly cause the failure of or change the behaviors of the element in the other network but will impact the performance of the element against the failure. The protection task is an example of INEI. Distance protection, pilot protection for short lines, and circuit breaker failure protection use peer-to-peer communication between protective devices for decision making. Note that a failure in the protection system does not cause a failure on the power equipment. However, such a protection system with failures may not clear the fault that occurred in the power network. Figure 2 shows an example for INEI. Usually, there are primary and backup protections against the fault on feeder F1. Protective relay R1 will operate the primary protection, and protective relays R1, R2, R3 and R0 will communicate with each other and serve as the backup protection if the protective relay R1 fails to operate circuit breaker CB1. Therefore, if a communication problem exists on connections between R1-R2 and R2-R3, protective relay R2 will be isolated and will not receive the backup trip request from the failed R1. As a result, CB2 cannot open to isolate feeder F2 from the fault on feeder F1.

IV. Applications

In this section, two smart grid applications, automated substation and micro grid, are presented for studying the cyber-power interdependencies.

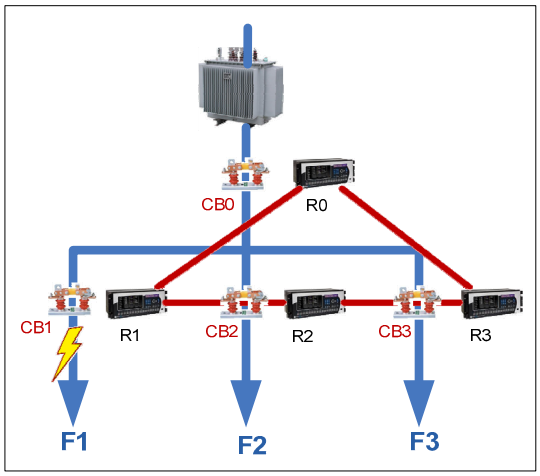

Fig. 2 Failure in protection system as an INEI between cyber and power layers in distribution grids

A. Automated Substation

An automated substation is a substation that is monitored, protected and controlled by the substation automation system (SAS). The SAS is a cyber network that collects data from the power equipment in a substation, such as incoming and outgoing feeders, transformers, circuit breakers (CBs) and disconnect switches (DSs). The data are processed in SAS, and the proper commands are released to operate the power equipment, including changing the tap of transformers and opening or closing CBs and DSs.

SAS technology is gradually superseding conventional control systems. Nowadays, the SAS integrates advanced monitoring, protection and control devices and operates as a combined and multi-task network. Fiber-optic transceivers on the power equipment, such as CBs, DSs, current transformers, and voltage transformers, are replacing the large amount of traditional copper wiring. The IEC-61850, a novel standard for communication in the substation automation, provides interoperability, reliability and agility in the communication systems [16]. As more tasks are assigned to the SAS, failures in the SAS become more critical. Any failure in SAS operation may cause failures in the power network and may even disconnect power feeders in the substation [17].

Figure 3(a) shows a substation with a typical breaker-and-a-half arrangement. Figure 3(b) shows a schematic diagram of its SAS. Power equipment transceivers are interface apparatuses between the power and cyber networks. Measurement, protection and control IEDs, such as bay control units (BCUs), protective relays and measuring units, are the main devices in the SAS and are connected together through an Ethernet network. BCUs monitor and control each bay, and peer-to-peer communication enables BCUs to share information with other cyber elements. They report all statuses and values of switchgears to other IEDs [18]. Protective relays protect the substation and all connected lines against faults. Furthermore, measuring units collect measured current and voltage and calculate powers and energies.

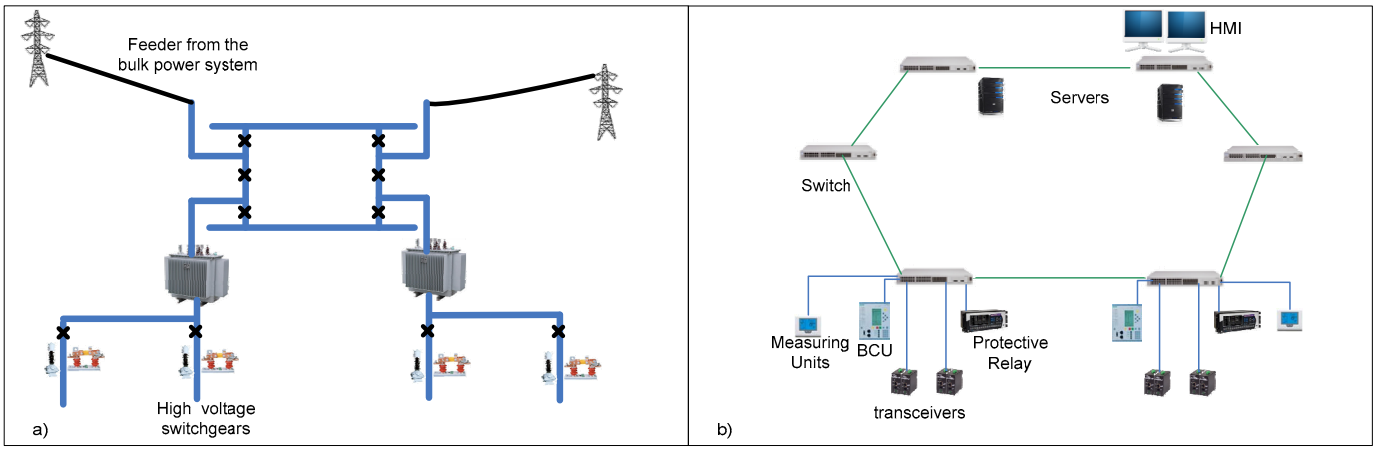

Fig. 3 a) Schematic diagram of a breaker-and-a-half substation, b) schematic diagram of substation automation systems

The measuring accuracy of CTs and VTs, and the correct status of CBs and DSs, are important concerns for the automated substation because inaccuracies in CTs and VTs, as well as false statuses from CBs and DSs, may lead to incorrect monitoring, undesirable protective trip command, or insecure control. So, the DEEI can be defined between CTs, VTs, CBs, or DSs and their corresponding BCUs and protective relays.

The DNEI defines the interactions between the cyber network and the power equipment, including transformers, CBs and DSs. The operator should be able to send a command to all of them. Problems in the connectivity, interoperability and synchronization inside the cyber network may disturb the data transfer to BCUs, which are required for changing the tap of transformers, and the status of CBs and DSs.

The indication of transformers and the circuit breaker operation counter are two examples of IEEI. The temperature indicators of windings and the oil of transformers are monitored in substations, and any out-of-range degree activates the alarm units. A failure on these indicators increases the failure rate of the transformer, as temperature indicators cannot help to announce that the power transformer is under the hazard while failed. As another example, CBs usually have a maintenance requirement after a specified number of operations. If the HMI software for counting the number of CB operations experiences a problem, it will not report the correct operation number for scheduled maintenance. Consequently, CBs operating while ignoring their maintenance will increase the risk of damage.

In the automated substation, peer-to-peer communication is crucial for the protection task. The directional overcurrent and pilot protections are examples of operations requiring inter-substation communication, and the bus bar, circuit breaker failure, pole discordance and short zone protections are examples of operations requiring in-substation communication between relays. As an INEI example, the failure in the cyber network potentially decreases the ability of power feeders and bus bars to defend against faults.

B. Micro Grids

The concept of a micro grid developed out of the need to organize and utilize the distributed generation and renewable energy that occur in the modern distribution system. Micro grids aggregate renewable energies with conventional power systems [8]. Like other power grids, the main objective of micro grids is to supply power to local consumers from sources that are either DGs, batteries or incoming feeders from the bulk power grid. A micro grid is an application of a cyber-power system that takes advantage of computer networks in control of small power networks. The following problems should be considered in micro grids:

- Renewable energy resources are usually small [19].
- The availability of sources in micro grids depends on ambient conditions [19], [20].
- There is not a slack bus in micro grids to balance load and generation, especially when the micro grid is isolated from the bulk power system [21].

Considering the above problems, energy management units (EMU) are important devices in micro grids for managing resources to balance loads and generations. EMUs continuously run real-time optimum energy management algorithms with the objectives of maximizing benefits and minimizing load curtailments and system losses, and they make optimal decisions on the amount of generations, charging/discharging of batteries, demand response of customers, and selling to or buying from the bulk power system.

The protection of the micro grid is another important issue. The traditional protection schemes are not able to protect the micro grids appropriately because of the utilization of DGs, which changes the simple radial topology of distribution networks into meshed networks with bi-directional current flows [22]. Hence, fault management units (FMU), operating based on multi-agent technology, are the new generation of protective relays capable of peer-to-peer communication which are used for the protection of micro grids [23], [24].

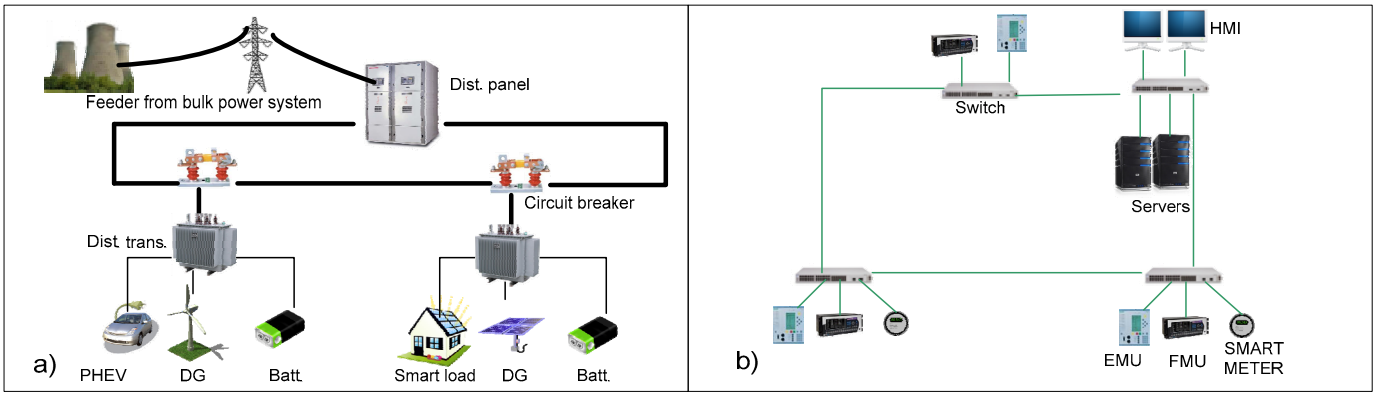

Fig.4. A schematic diagram of a micro grid a) the power network b) the cyber network

Figure 4(a) shows a schematic diagram of the power network in a micro grid. The power network includes the incoming feeder from the bulk power system, distribution transformers, renewable energy resources, distribution cables, batteries, plug-in hybrid electrical vehicle (PHEV) and smart loads. Figure 4(b) shows a schematic diagram of the cyber network of a micro grid. The cyber network includes EMUs, FMUs, servers, switches and smart meters. All devices in the power network of micro grids have data connection ports to transmit and receive signals from EMUs and FMUs. Smart meters are digital instruments that measure generated/consumed power for source and load points [25].

Because each EMU is in charge of each section in the micro grid, the insolated EMU will cause all power elements in the corresponding section to operate abnormally due to the cyber connectivity problem. Such interaction is the DNEI. Advanced power electronic technology has offered solid state transformers (SST) instead of conventional transformers. As controllable power equipment, these SSTs can be connected to the cyber network [26]. So, this interconnection between the cyber network and the SST can be also defined by DNEI.

The indication of battery level is an example of the IEEI because the lack battery power can increase the risk of a power outage in the micro grid while the battery is operated as a source.

The demand response (DR) potentially prevents the power network from critical outages by curtailing voluntary customers or shifting loads instead of generating [27]. The DR is applied by the cyber network between all customers. The failure of the cyber network to implement the DR does not cause any consequent failures in the operation of the micro grid. However, the failure in the operation of the DR reduces the reserve margin and the sustainability of the micro grid, accordingly increasing the risk of load curtailment. In other words, if the failed DR is not able to curtail voluntary customers or unimportant loads when an outage occurs in the power network, the other essential loads will be forced to leave the power system. Therefore, the DR can be regarded as an example of INEI.

C. Summary

Table I summarizes the study on interdependencies of cyber-power networks for two applications, automated substation and micro grid.

V. Case Study

In this case study, the impact of direct and indirect interdependencies is considered in the reliability of a substation.

A. Information about the case study

1) Power network

The power network is a 400/63 kV substation in that the higher voltage has a breaker and a half arrangement and the lower voltage has a single busbar. Each 400 kV incoming feeder is connected to a 400/63 kV transformer.

Each 400/63 kV transformer has a 600 MW capacity, and each outgoing feeder feeds an area with a 200 MW load.

A reliability assessment is performed based on LOLP and EENS indices, indicating the probability of loss load, ignoring the amount of load curtailed, and the expected value of energy not supplied, respectively.

2) Cyber Network

A cyber network consists of two levels, the station level and the bay level. The cyber network has a star-wired, ring topology. Controllers of 400 kV busbars are connected to SWITCH1, and those of F10 and F20 busbars are connected to SWITCH2 and SWITCH3, respectively.

The ring topology provides an acceptable level of reliability with a redundant path for data transmission. Two redundant servers automatically control the substation, saving and analyzing the data surrounding the substation.

Figure 5 shows the schematic diagram of both the cyber and power network in the substation.

TABLE I
SUMMARY OF SAS AND MICRO GRID AS TWO PARADIGMS OF CYBER-POWER SYSTEMS

	Power Elements	Cyber Elements	Examples for interdependencies	
Automated Substation	Incoming feeders Circuit breakers (CB) Power transformers	Bay control units (BCU) Protective relays Measuring units Servers Switches Fiber optic cables, UTP cables	DEEI	BCUs to circuit breakers
			DNEI	Servers to circuit breakers
			IEEI	Indicator of oil and winding temperature of power transformers
			INEI	Protection network
Micro Grid	Renewable energy resources Battery (Storage devices) Incoming feeder(s) from bulk power Circuit breakers (CB) Solid state transformers (SST)	Energy Management Units (EMU) Fault Management Units (FMU) Smart meters Switches Fiber optic cables, UTP cables	DEEI	EMUs to circuit breakers
			DNEI	Switches to circuit breakers Control of SST
			IEEI	Battery level indicator
			INEI	Demand response (DR)

B. Scenarios

In the first evaluation, a classic reliability assessment is performed, in that the cyber network is assumed to be sufficiently dependable to experience no failure. Therefore, the reliability indices would belong to the power network alone.

In the second scenario, the control system of the cyber network is modeled as direct interdependency between the cyber and power networks. Losing control of each bay will lead to power outages in the corresponding bay. A redundant control system is not assumed in the SAS.

In Scenario 3, monitoring and indication is included as indirect interdependencies between networks.

This means that if any failure blocks the monitoring and indication IEDs from operating correctly, the failure rate of monitored equipment will increase consequently.

Finally, the fourth scenario simulates the impact of failure in both control and monitoring IEDs.

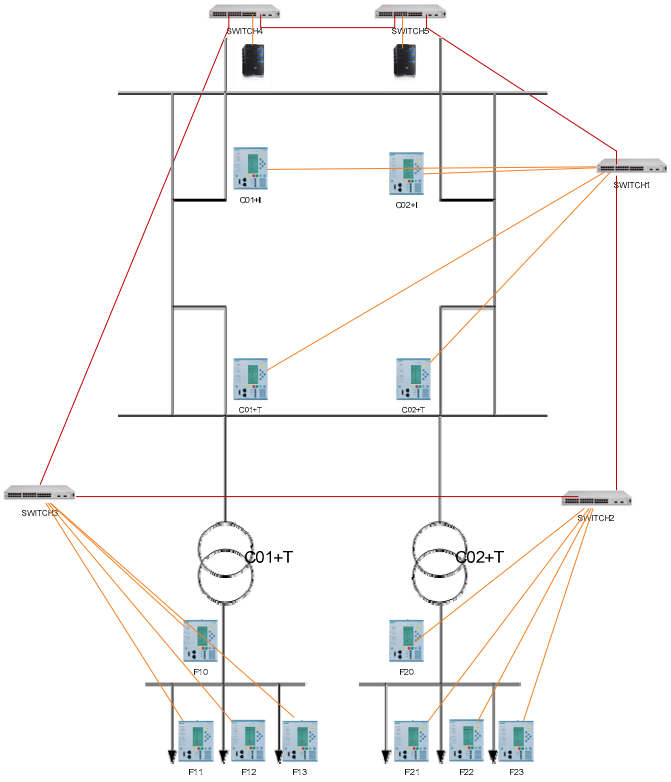

Fig. 5. Power and cyber configuration of a 400/63 kV substation

C. Results

In all scenarios, power network elements have constant failure rates, but the failure rate of cyber elements gradually increases from 0 to 1 occurrence/year.

The results of four scenarios are shown in Pictures 6 and 7. Both charts show a nearly linearly increment of LOLP and LOLE while increasing the failure rate. The Scenario 3, considering only indirect interdependencies between cyber and power networks, has more non-linear behavior than other scenarios.

Comparing Scenario 4 with scenarios 3 and 2, overlapping between Direct and Indirect interdependencies is obvious, because some elements have both control and monitoring tasks.

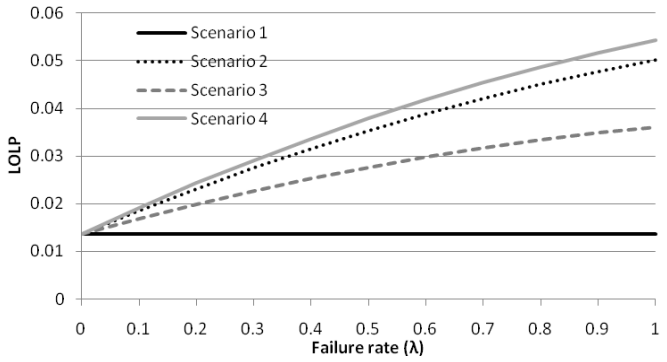

Fig.6. LOLP of the cyber-Physical network

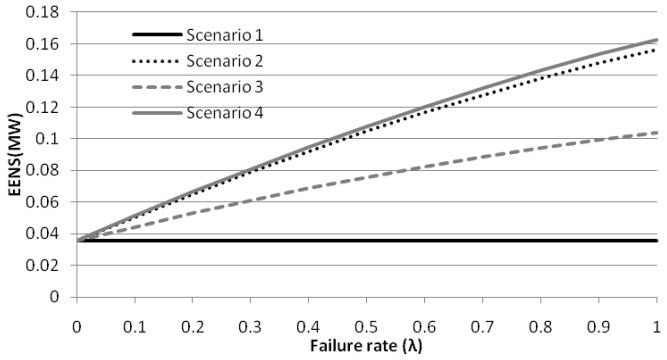

Fig.7. EENS of the cyber-Physical network

VI. CONCLUSION

This paper describes a cyber-power system in smart grid applications and studies the interdependencies between cyber and power networks. In this study, Direct, Indirect, Element-Element, and Network-Element, as fundamental interactions

between two networks, are introduced, and four categories of interdependencies, DEEI, DNEI, IEEI, and INEI, are defined. In this paper, two applications, automated substation and micro grid, are discussed, and certain interdependencies are investigated and categorized. Based on this study, the mathematical model will be developed for quantitatively evaluating the effects of interdependencies in the cyber-power system.

The results of the case study show that the power system's reliability may be affected by the failure in control and monitoring devices of the cyber network in two different ways: Direct and Indirect interdependencies.

VII. References

[1] H. Farhangi, "The Path of the Smart Grid," *IEEE Power & Energy Magazine*, Vol. 8, No. 1, Jan./Feb. 2010, pp. 19-28.

[2] D. Karlsson, M. Hemmingsson, and S. Lindahl, "Wide area system monitoring and control," *IEEE Power Energy*, vol. 2, no. 5, pp. 68–76, Sep./Oct. 2004.

[3] S. Massoud Amin and B.F. Wollenberg, "Toward a smart grid: power delivery for the 21st century," *IEEE Power and Energy Magazine*, Vol. 3, No. 5 Sept.-Oct. 2005, pp. 34-41.

[4] F.Rahimi and A.Ipakchi, "Demand Response as a Market Resource Under the Smart Grid Paradigm," *IEEE Transactions on Smart Grid*, vol.1, no.1, pp.82-88.

[5] S.M. Rinaldi, J.P. Peerenboom, T.K. Kelly, "Identifying, understanding and analyzing critical infrastructure dependencies," *IEEE Control Systems magazine*, vol. 21, no 6, December 2001, pp. 11-25.

[6] D.E. Newman, B. Nkei, B.A. Carreras, I. Dobson, V.E. Lynch, and P. Gradney, "Risk Assessment in Complex Interacting Infrastructure Systems," *System Sciences, 2005. HICSS '05. Proceedings of the 38th Annual Hawaii International*, pp. 63c- 63c.

[7] M.G. Adamiak, A.P. Apostolov, M.M. Begovic, C.F. Henville, K.E. Martin, G.L. Michel, A.G. Phadke, and J.S. Thorp,"Wide Area Protection—Technology and Infrastructures," *IEEE Transactions on Power Delivery*, Volume 21, Issue 2, April 2006.

[8] S. Rahman, M. Pipattanasomporn and Y. Teklu, "Intelligent Distributed Autonomous Power Systems (IDAPS)," *In Proc. 2007 the IEEE PES Annual General Meeting*, Tampa, Florida, 8pp.

[9] Ten Chee-Wooi, Liu Chen-Ching, and M. Govindarasu, "Anomaly extraction and correlations for power infrastructure cyber systems," Systems*,IEEE International Conference on Man and Cybernetics*, 2008, pp.7-12.

[10] C. Hoga and G.Wong. "IEC 61850: Open Communication in Practice in Substations," *In Proc. IEEE Power Systems Conf.and Exposition*, pages 618–623, 2004.

[11] S.S. Tarlochan, Y. Yujie, "Modelling and Simulation for Performance Evaluation of IEC61850-Based Substation Communication Systems," *IEEE Transactions on Power Delivery*, 2007, pp. 1482-1489.

[12] P.P Parikh, M.G. Kanabar, T.S. Sidhu, "Opportunities and challenges of wireless communication technologies for smart grid applications," *Power and Energy Society General Meeting*, 2010 IEEE , pp.1-7.

[13] Michael Duck and Richard Read, *Data Communications and Computer Networks for Computer Scientists and Engineers.* Second Edition, 2003, Pearson, Prentice Hall.

[14] F. Gebali*, Analysis of Computer and Communication Networks* . Springer Science Business Media, LLC, New York, 2008.

[15] R. Pallos, J. Farkas, I. Moldován and C. Lukovszki, "Performance of Rapid Spanning Tree Protocol in Access and Metro Networks," *AccessNets 2007*, Ottawa, Canada, August 22-24, 2007.

[16] *Communication networks and systems in substation*, International Standard, IEC 61850-9-1, First edition, 2003-05.

[17] M. Ingram, R. Ehlers, "Toward effective substation automation," *IEEE Power and Energy Magazine*, Vol. 5(3) , pp. 67-73. 2007.

[18] L. Anderson, C. Brunner, and F. Engler, "Substation automation based on IEC 61850 with new process-close technologies," *in IEEE PowerTech Conference*, vol. 2, Bologna, Italy, June 2003, p. 6.

[19] S. R. Bull, "Renewable energy today and tomorrow," *Proc. IEEE*, vol. 89, no. 8, pp. 1216–1226, Aug. 2001.

[20] N. Jayawarna , X. Wut , Y. Zhangt , N. Jenkins , M. Barnes, "Stability of a MicroGrid," *Proc. of the 3rd IET Int. Conf. on Power Electronics, Machines and Drives*, Dublin, Ireland, March 2006.

[21] P. Ledesma, J. Usaola, and J. L. Rodriguez, "Transient stability of a fixed speed wind farm*," Renewable Energy*, vol. 28, pp. 1341-1355, 2003.

[22] Lim Seong-Il Lim, Choi Myeon-Song, and Lee Seung-Jae, "Adaptive protection setting and coordination for power distribution systems," *Power Systems Conference, 2006. MEPCON 2006. Eleventh International Middle Eas*t , vol.1, pp.129-134.

[23] I.H. Lim, S.J. Lee, M.S. Choi, P. Crossley, "Multi-Agent System-based Protection Coordination of Distribution Feeders," Intelligent Systems Applications to Power Systems, 2007. ISAP 2007., pp.1-6.

[24] Hui Wan, K.K.Li and K.P.Wong, "Multi-Agent Application of Substation Protection Coordination with Distributed Generators," *European Transactions on Electrical Power*, Vol.16, Issue 5, September, 2006, pp. 495-506.

[25] P.K Lee, LL. Lai, "Smart Metering in Micro-Grid Applications," *in Proc. of the IEEE Power and Energy Society General Meeting*, July 2009.

[26] Madhav D. Manjrekar, Rick Kiefemdorf, etc, "Power Electronic Transformers for Utility Applications," *Trans Of China electrotechnical society*, vol.16, no.5, pp35-39.

[27] F. Katiraei, R. Iravani, N. Hatziargyriou, and A. Dimeas, "Microgrids Management," *IEEE Power and Energy Magazine*, vol. 6, no. 3, pp. 54-65, May/June 2008, 2008.

VIII. Biographies

Bamdad Falahati (S'08) received the B.S. and M.S. degrees in electrical engineering from Sharif University of Technology, Iran, in 1999 and 2008, respectively. He currently is working toward the Ph.D. degree at Mississippi State University, Starkville. From 2004 to 2008, Bamdad was with Moshanir Co. as an R&D Engineer. His research interests include substation automation systems, power system reliability, distribution grid management and micro grids.

Yong Fu (M'05) received his B.S. and M.S. in electrical engineering from Shanghai Jiaotong University, China, in 1997 and 2002, respectively, and his Ph.D. degree in electrical engineering from the Illinois Institute of Technology, USA, in 2006. From 2006 to 2009, he was a senior research associate in the Electric Power and Power Electronics Center at the Illinois Institute of Technology. Presently, he is an assistant professor in the department of electrical and computer engineering at Mississippi State University. His research interests include power system optimization and economics, and critical infrastructure interdependency.