Cyber-physical System Failure Analysis Based on Complex Network Theory

Wentao Zhu, Student Member, IEEE  
School of Electrical and Electronic Engineering  
The University of Manchester  
Manchester, UK  
wentao.zhu@manchester.ac.uk  

Jovica V. Milanović, Fellow, IEEE  
School of Electrical and Electronic Engineering  
The University of Manchester  
Manchester, UK  
milanovic@manchester.ac.uk

Abstract—Cyber-physical system studies request revolutionary methods to identify the vulnerability of the system in order to develop risk assessment and countermeasures and consequently reduce the vulnerabilities. One possible approach to analyze cyber-physical system vulnerability is to study their topology and therefore to quantify the interdependencies on the physical side and on the cyber side. This paper presents a three-dimensional Complex Network model for a coupled electric power system and information and communication technology network, where power buses and communication network routers/multiplexers are modelled as nodes while power lines and communication channels are modelled as edges. The vulnerability of each system component may vary under different system operating conditions due to the change of system’s structure. Therefore a Vulnerability-weighted Node Degree is introduced to assess the vulnerability of each component under two characteristic power system operating conditions. The most vulnerable components are identified using Vulnerability-weighted Node Degree and the consequences of failure of these components are demonstrated with Node Removal method.

Keywords—Cyber-physical Systems (CPS); Complex Networks (CN); Information and Communication Technologies (ICT), Power Distribution Systems.

I. INTRODUCTION

The rapid-growing and diverse demands, along with the escalation of intermittent and stochastic renewable energy sources (RES) create more uncertainties in Electric Power Systems (EPS). As a result, reducing the uncertainties to increase system efficiency and reliability becomes the prime impetus of integrating Information and Communication Technologies (ICT) in energy sectors. However, the interplays and interactions between the physical system and the supporting cyber network introduce cyber-physical interdependency which creates another layer of uncertainties that cannot be avoided. Physical EPS and cyber ICT form a complex interdependent System-of-Systems (SoS), where a large-scale cascading failure could be provoked by the failure of the most critical components or the interdependency links. A real-life example is the catastrophic blackout that happened in 2003 in Northwest and Midwest of the United States and Ontario in Canada, which affected 50 million people and resulted in a loss of US$7-10 billion [1].

Most of the critical infrastructure systems (CIS), are cyber-physical systems in essence (e.g. water networks, mass transportation systems, energy-efficient buildings, sensor networks etc.). With the integration of cyber network, the vulnerability of the coupled network is exacerbated. Therefore, the first step of research efforts should focus on the risk assessment of the CPS architecture by identifying the significant element of risk. Furthermore, how these elements are relying on the physical and cyber networks should also be understood in order to reduce the risks.

Physical and cyber interdependencies are introduced in this paper for the sake of clarifying the types of vulnerabilities that exist in each distinct system (especially to highlight the prominence of cyber security) and to differentiate proposed approach from traditional vulnerability studies based on single system [2-5]. Both dependency types, however, influence the reliance of one system on the other, to fulfill its own objectives. These dependencies are typically non-obvious and as such, compared to geographical interdependencies, represent a significant and hidden risk to the complete infrastructure systems [6]. A ‘power system information theory’ is introduced in [7] to combine the “physical propagation” phenomenon within power system and the underlying information theory within ICT network and to display their shared principals and accordingly facilitates the application of graph theory to study cyber-physical system as a whole.

There is a large variety of communication applications and technologies within the power grid and it is extremely challenging to define a detailed architecture. Current cyber-physical system modelling approaches are rigid and not scalable. Various methodologies and simulation tools are developed based on an industry-specific failure or attack [8-10], while few of them considered the cascading failures between cyber and physical systems holistically. Moreover, ICT, the nervous system of large complex energy networks, has evolved so quickly and differently from energy systems such as power grids that reductionist solutions fail to grasp the generality and a “theoretical” approach, maybe not a superior one but as a complementary tool, should be developed. Consequently current practice of certifying individual components should be moved to ratifying the performance of complete system.

It has been noted that physical power systems and ICT network are dissimilar from each other in network topologies; thus, this paper presents a three-dimensional (3D) reference model which describes the static topology of cyber-physical networked systems and uses a VWND to quantify the vulnerabilities and dependencies of interconnected elements. Six scenarios are then presented to illustrate the consequences of the failure of the most and least critical nodes, with the components ‘failing’ in the sense of not being able to transmit power or information.
II. COMPLEX NETWORK THEORY MODELING

A. Test System

The test system is a synthetic 14-bus distribution network with supporting ICT infrastructure, broadly based on the coupled EPS-ICT system introduced in [11]. It is modified suitably to incorporate different Distributed Generations (DGs) and loads in power grid and different ICTs in cyber network.

As shown in Figure 1, the physical power system includes 14 buses, 17 power lines, 7 DGs (Photovoltaic Generators, Wind Generators, Fuel Cells), 9 loads (domestic, commercial and industrial), and 3 HV/MV transformers. The generation from DGs (except for Fuel Cells) and consumption of electricity vary with time during the year, and the variation which creates a time-dependent power flow is modelled using corresponding daily loading curves and production curves simulated in DlgsILENT. The overall micro-grid could both import and export electric power from/to the external grid.

The supporting ICT network consists of 3 routers and 5 multiplexers, 23 communication channels based on Ethernet, Optical Fiber and Wireless communication technologies. The power line 2-23 also acts as an information exchange channel between router 23 and power bus 2, which utilizes Power over Ethernet (PoE) technology. The ICT network, allowing for bidirectional information flow through its channels, plays a vital role in monitoring and controlling the power distribution system.

B. Graphical Representation

Based on Complex Network Theory, the graphical representation of the test network is presented in Figure 2. Power system buses and ICT routers/multiplexers are modelled as nodes (V_e and V_i to represent the set of electric nodes and ICT nodes respectively), and power lines and information channels are modelled as edges $E_e$ and $E_i$ to represent the set of electric edges and ICT edges respectively. PoE link 2-23 is modelled as a power line and a cyber link to display its dual functionalities in both physical and cyber domains. Overall, the 3D model is composed of an upper layer describing EPS, a lower layer describing ICT and the interactions between both systems. Power flow within EPS layer and power supply to ICT network are presented as red unidirectional solid lines and red unidirectional dash dot lines respectively, while the information exchange within the ICT layer and the transmission of sensory/control data between EPS layer and ICT layer are represented as blue solid lines and blue dashed lines respectively. Due to the variation in general production and consumption of electricity, the power flow directions within each power transmission line may alter with time; therefore as an illustrative example, the undirected lines in the EPS layer represent the power lines with reverse power flows under maximum and minimum loading conditions throughout the year.

!!! Fig. 1. 14-bus test system [11]!!!

III. VULNERABILITY ASSESSMENT

A. Complex-valued Adjacency Matrix

An $n \times n$ complex-valued adjacency matrix $A$ is the first step to convert system topology to mathematical forms to allow hidden system properties to be studied. The connections in the 3D graph are classified into the following four categories corresponding to the type of topological relationship [11].

Category 1: The power flow from an electric node to another electrical node.

Category 2: The information flow from an ICT node to another ICT node.

Category 3: The electric energy supply from an electric node to an ICT node.

Category 4: The sensory data/control command from/to an electric node to/from an ICT node.

The electric and ICT connections within the 3D model are presented as complex-number entries $a_{ij}^e$ and $a_{ij}^i$ respectively based on the rules described in (1) and (2), where ‘$i$’ is the imaginary component representing a cyber element.

\[
A_e = \begin{cases} 
1 & \text{if } (i,j) \text{ belongs to category 1} \\
1+i & \text{if } (i,j) \text{ belongs to category 3} \\
0 & \text{otherwise} 
\end{cases} 
\]  
(1)

\[
A_i = \begin{cases} 
 i & \text{if } (i,j) \text{ belongs to category 2} \\
1+i & \text{if } (i,j) \text{ belongs to category 4} \\
0 & \text{otherwise} 
\end{cases} 
\]  
(2)

Consequently, the complex-valued adjacency matrices for physical and cyber layers can be formed. Figure 3 presents the adjacency matrices for CPS under power system maximum loading condition.

!!! Fig. 2. 3D model (base case) !!!

!!! Fig. 3. Complex-valued adjacency matrices a) EPS layer; b) ICT layer !!!
B. Complex-valued Node Degree

Node degree (ND) $k_i$ has been widely exploited to quantify the topological importance of a node $i$. It represents the number of nodes a focal node is incident with. Cascading failures within an interdependent network have been found to have a close relation with the disabling of highly connected nodes [12]. In order to describe the directions and types of dependency, the node degree has been divided into an in-degree and an out-degree with real part and imaginary part. They are calculated according to (3) and (4) [13].

\[ k_i^{in} = \sum_{j \in V} \alpha_{ij}^{in} + i \cdot k_i^{out} \]  
\[ k_i^{out} = \sum_{j \in V} \alpha_{ij}^{out} + i \cdot k_i^{in} \]  

Figure 4 presents the results of coupled system’s cyber and physical node degree frequency distribution. Figure 4 a) identifies the existence of well-connected nodes within both systems. Figure 4 b) shows that the power distribution system is well supported by ICT network.

C. Efficiency and Vulnerability

The concept efficiency was introduced to quantify how efficiently the network components exchange information with each other. It is defined in (5), where $d_{ij}$ is the total shortest path length between node $i$ and $j$, and $n$ is the number of nodes in the network.

\[ E = \frac{1}{n(n-1)} \sum_{i<j} \frac{1}{d_{ij}} \]  

The concept of vulnerability of a(n) node/edge is introduced by assessing the efficiency drop of the system after removing that node/edge out of the system. It is denoted by $V(n)$ and is calculated as in (6) where $E(Y)$ is the normal state system efficiency and $E(Y-1)$ is the efficiency after the removal of that node/edge.

\[ V(n) = \frac{E(Y) - E(Y-1)}{E(Y)} \]  

Figure 5 presents vertices vulnerability results. The vulnerability results obtained from the interconnected system operating under maximum loading condition identify electric nodes 2, 5 and 8 to be the most vulnerable buses in power system. Moreover, in terms of the reliability of power supply, ICT node 15 and 23, are potentially vulnerable due to the reason that a failure initiated within power system could easily pass down through critical power bus 2 (as bus 2 is the critical bus passed by many optimal power flow paths), which will result in the destabilization or cut off of the power supply links 2-15 and 2-23. Within the ICT network, the removal of nodes 20, 19 and 16 caused the highest impact on the system efficiency.

D. Vulnerability-weighted Node Degree (VWND)

The canonical forms of CNT-based criticality and vulnerability analysis exhibit effectiveness to some extent. However, they have intrinsic deficiencies in studying coupled networks. For instance, degree based assessment underestimates the importance of topologically centralized nodes with fewer connections. Vulnerability index identifies system’s boundary spanners that are noncritical in single system but critical in interconnected system, by attributing a great amount of centralities to these nodes/edges. However, it cannot discriminate dependency and impact of a component to its own or the other infrastructure. Consequently, a new index should be developed to address the above deficiencies. The complex-valued adjacency matrices introduced in Figure 3 are utilized to compute the VWND for each node.

Representing $i$ as physical system node and $k$ as cyber system node, VWND is calculated in (7) – (10).

\[ D_i^{in} = D_i^{in} + D_i^{out} = \sum_{j \in V} \alpha_{ji}^{in} \cdot V_{e_{ij}^{in}} + i \cdot \sum_{k \in V} \alpha_{ik}^{out} \cdot V_{e_{ik}^{out}} \]  
\[ D_i^{out} = D_i^{out} + D_i^{in} = \sum_{j \in V} \alpha_{ij}^{out} \cdot V_{e_{ij}^{out}} + \sum_{k \in V} \alpha_{kj}^{in} \cdot V_{e_{kj}^{in}} + i \cdot \sum_{k \in V} \alpha_{ik}^{in} \cdot V_{e_{ik}^{in}} \]  
\[ D_k^{in} = D_k^{in} + D_k^{out} = i \cdot \left( \sum_{j \in V} \alpha_{ji}^{in} \cdot V_{e_{ij}^{in}} + \sum_{k \in V} \alpha_{kj}^{out} \cdot V_{e_{kj}^{out}} \right) \]  
\[ D_k^{out} = D_k^{out} + D_k^{in} = i \cdot \left( \sum_{j \in V} \alpha_{ij}^{out} \cdot V_{e_{ij}^{out}} + \sum_{k \in V} \alpha_{kj}^{in} \cdot V_{e_{kj}^{in}} \right) \]  

VWND not only associates the degree of a node with its incident edges’ vulnerabilities, but also with the physical and cyber components adopted from Complex-valued ND analysis, it differentiates the dependency/importance from/to each system. Figure 6 presents the variation of cyber/physical dependency/importance of each component under maximum and minimum loading conditions. It can be concluded from Figure 6 a) 6 c) that the alteration of loading conditions creates a significant impact on physical and cyber systems’ inner-dependences (e.g. power bus 3, central ICT router 19). While...
comparing Figure 6 b) and 6 d), the noticeable increase of electrical importance and decrease of cyber importance within EPS can be observed from maximum loading condition to minimum loading condition. Particularly, central router 19 has the least electrical dependence and yet, its normal cyber functioning is both critical and strictly reliant on the normal functioning of the ICT systems.

![Node criticality variation under maximum and minimum loading conditions](image)

**Fig. 6.** Node criticality variation under maximum and minimum loading conditions. a) Electrical dependence; b) Electrical importance; c) Cyber dependence; d) Cyber importance (NB: Solid bars represent a higher criticality under maximum loading condition; otherwise criticalities are higher under minimum loading condition).

**E. Failure Scenarios**

Assuming backup communication channels (e.g. ICT links 22-12, 22-13, 22-14 are backed up with 20-12, 20-13, 20-14) can be configured to monitor and control electric buses for a sufficient length of time under branch breakdown contingency, the worst scenario case studies are carried out under different failure scenarios to demonstrate the criticalities of the most important nodes as identified using VWND. Efficiency is only used to quantify the topological connectedness of the network and therefore power line overload constraints are not considered for simplicity.

![Different failure scenarios in CPS](image)

**Fig. 7.** Different failure scenarios in CPS – maximum loading condition: a) Normal State; b) Removal of most critical EPS node; c) Removal of least critical EPS node; d) Removal of the most critical ICT node; e) Removal of least two critical ICT nodes; f) Removal of most critical EPS and ICT nodes.

Figure 7 a) presents the complete, undisturbed CPS under maximum loading condition of power distribution system (EPS efficiency 0.1697, ICT efficiency 1.2296).

Figure 7 b) shows the impact of the removal of node 2, the dramatic decrease of output from the whole micro-distribution network. Furthermore, because node 2 is the only electric energy supplier of ICT nodes 15 and 23, the failure of node 2 will cause the LAN-Giga network to go blind, which further causes the controlled electrical buses to be unobservable and uncontrollable (EPS efficiency 0.1044, 38.5% drop; ICT efficiency 0.9214, 25.1% drop).

Figure 7 c) demonstrates the impact of the removal of the least critical EPS node. Disconnecting node 1, the external grid component, will have minimum impact to the internal micro-distribution network as it acts merely as an end-receiver in the system (EPS efficiency 0.1697, 0% drop; ICT efficiency 1.2296, 0% drop).

Figure 7 d) demonstrates the impact of the failure of the most central router, node 19. Although node 19, the heart of the system-of-systems, does not directly control any power buses, it takes the role to centrally process the information and dispatch the controlling commands to its ‘child’ node (ICT nodes 20, 18, 17, 21), which are further connected with other
ICT components to coordinate the information transmission and are directly controlling more than half of the EPS buses including nodes 3, 4, 5, 7, 8, 9, 12, 13, 14 (EPS efficiency 0.0079, 95.3% drop; ICT efficiency 0.0714, 94.2% drop).

Figure 7 e) shows the scenario of the failure of two least critical ICT nodes 15 and 22. These two nodes are identified as least ‘important’ using VWND due to the fact that their distributed control channels are backed up with redundancies and therefore the network traffic can be easily redistributed through the backup links under node failures (EPS efficiency 0.1697, 0% drop; ICT efficiency 1.0386, 15.5% drop).

Figure 7 f) presents the sequence of the concurrent breakdown of the most critical EPS node and the most critical ICT node. The breakdown of both nodes directly and indirectly causes the complete collapse of the cyber network. While the switch-off of output gate node 2 will raise significantly the potential of overloaded power lines, the whole distribution network is in addition unobservable and uncontrollable (EPS efficiency 0, 100% drop; ICT efficiency 0, 100% drop).

As can be concluded from the 6 scenarios, the failure of a key node, especially a cyber node, could cause large-scale breakdown of the whole network. Although the standalone structure of the Lan-Giga network avoided the single point of failure (SPOF) that could have been caused by node 19’s failure, the concurrent failure of node 2 put the whole CPS under risk of complete failure. In general, this interconnection model demonstrated how cascading failure effects could propagate between two interconnected systems, not only within one single system. The main purpose of using Complex Network Theory is to identify the most vulnerable components that could initiate such an effect. ‘Efficiency’ quantifies this vulnerability from a loss of accessibility angle (in terms of the effect of a failure of the focus node on operation of different interconnected systems) by comparing the system efficiency under normal condition and after the removal of the focal node.

IV. CONCLUSIONS

This paper presented a topological approach to evaluate the vulnerability of cyber-physical system. Complex network theory is adopted to model a 14-bus EPS-ICT system, and system interdependencies are analyzed under different loading conditions. The importance of key nodes is further demonstrated using failure scenarios and quantified by efficiency drop in each individual system.

The main limitation of the proposed method is that it is based on purely topological criterion and that it is purely static, in the sense that dynamic phenomena are not considered. Nevertheless, complex network theory is an active research area and with the integration of other methods the said limitation can be overcome.

With the wide deployment of ICT in energy sectors, the control theory can be developed based on the global modeling of CPS, which deserves more research efforts.

ACKNOWLEDGEMENT

This work was partly inspired by and built on research by Dr. José Libardo Sanches Torres at the G2ELAB laboratory at the University of Grenoble.

REFERENCES