

# Methodology for Reliability Assessment of Smart Grid Considering Risk of Failure of Communication Architecture



# Methodology for Reliability Assessment of Smart Grid Considering Risk of Failure of Communication Architecture

Wentao Zhu, *Member, IEEE*, Mingyu Han, *Student Member, IEEE*, Jovica V. Milanović, *Fellow, IEEE*, and Peter Crossley, *Member, IEEE*

***Abstract*—This paper introduces an analytical method, based on the Complex Network Theory (CNT), to assess the risk of the Smart Grid failure due to communication network malfunction, associated with latency and ICT network reliability. Firstly, the communication architecture is modelled using a two-step CNT framework – an Operation Graph (OG) in step one and a Reliability Graph (RG) in step two. Secondly, the latency of data packets and the reliability of each communication device are incorporated into the model to identify the reliability of all operational communication paths for successful power system control purposes. Then, the risk of Smart Grid failure due to the communication network malfunction is quantified using a System Reliability Index (SRI). Next, sensitivity analysis is performed to assess the importance of each communication network component using two innovative Importance Measures (IM), namely System Reliability Advancement Worth (SRAW) and System Reliability Deterioration Worth (SRDW). Finally, the proposed approach is demonstrated on a laboratory-scale communication network.**

***Index Terms*—Complex Network Theory, Industrial Communication Technology (ICT), Reliability, Uncertainty.**

## I. Introduction

MODERN societies are more and more dependent on the secure and reliable functioning of Critical Infrastructures (CI), such as power systems, that provide the backbone of modern living. However, with widely deployed Industrial Communication Technology (ICT) networks into these CIs, for the purpose of a more observable and controllable physical environment, cyber components' failures introduced another layer of uncertainty in the assessment of the reliability (i.e., the continuity of correct service) of the CI systems, e.g., the impact of ICT failures on the monitoring [1] and control [2] of power system. In the UK, reliability has been identified as one of the most important features of the ICT network, with regards to its role played in the power transmission system [3]. Conventional well-established power system reliability evaluation techniques and industry practices and standards focus only on the physical, electrical power grid, part of the system [4-7], but neglect the impact of the failures in the auxiliary cyber environment. Recent studies based on a Cyber-physical System (CPS) framework gradually shift the research attention to the cyber domain of the ICT-Electrical Power System (EPS) to treat both systems in an integrated manner. A survey has been conducted to identify collectively the impact of imperfections of communication network on power systems, and such imperfections have been identified to arise from two aspects, namely external intrusions (e.g. cyberattacks), and internal failures (e.g. components' malfunction), which should be treated differently as security and reliability issues [8]. A cyber-constrained optimal power flow (OPF) model for smart grid emergency response is proposed in [9]. A model to assess the reliability of smart distribution network considering the reliability of its interconnected ICT infrastructure is proposed in [10]; this model, however, is incapable of quantifying the effect of latency (as stressed in [11]) when rerouting of data is considered. Other widely accepted techniques to analyze the direct cyber-to-power impact on system reliability include Markovian model [12], Reliability Block Diagram (RBD) [13, 14], fault-tree analysis [15], failure propagations studies [16], state-mapping techniques [17], and simulation approaches [18-20]. Nevertheless, these techniques require exhaustive computational effort, and the computational time grows exponentially with the size of the system being examined [21].

Another solution to this problem that has been commonly used is reliability graph [22]. Attempts have been made in the past to develop an efficient algorithm for graph-based network reliability calculations. The reliability graph is encoded into a Binary Decision Diagram (BDD) to manipulate Boolean connectivity functions, so that the storage and computation complexity in large reliability graph calculations are reduced [23]. To increase the intuitiveness of BDD- and Fault-Tree-based analyses, a method to transform the reliability graph with perfect nodes into Bayesian network with 'general gates' has been proposed in [24]. Similarly, the reliability graph with perfect edges was represented by Bayesian network with 'general gates' in [25]. Finally, optimization strategies for network reliability have been proposed with a main focus to develop a uniformly optimally reliable graph, i.e., a graph with

The authors are with the School of Electrical and Electronic Engineering, The University of Manchester, PO Box 88, Manchester, M60 1QD, UK. (email: milanovic@ manchester.ac.uk).

fixed topology that is most reliable irrespective of the change in its edges' reliabilities [26, 27]. Yet, these methods still heavily depend on cause-effect consequences and therefore, lack practicality in assessing the overall reliability of large interconnected ICT-EP systems.

As a result, a scalable yet practical tool to evaluate the risk of failure of interconnected system due to ICT system reliability, and to identify the critical cyber components, needs to be developed.

The main contributions of this paper include 1) the establishment of a two-step model based on Complex Network Theory (CNT), for the assessment of the structural importance of the ICT components within a Supervisory Control and Data Acquisition (SCADA) system; 2) the introduction of a novel System Reliability Index (SRI) to quantify the reliability level of the system; 3) the development of System Reliability Advancement Worth (SRAW) and System Reliability Deterioration Worth (SRDW) to rank the criticality of each ICT component for the overall system reliability. The fundamentals of the proposed approach are illustrated on a laboratory-scale communication network used in the IEC 61850-based substations.

## II. Complex Network Model

### A. Operation Graph and Reliability Graph

The first step to evaluate the risk of misoperation of ICT network structure is to identify the event to be analyzed and its consequences. To comprehensively analyze the risk of the ICT network, all faulty or hazardous events should be considered. For demonstration purposes, this paper considers only one event at a time, and all consequences equal to one. It can equally be applied though, to include the possibilities of occurrence of other events and associated consequence values. A quantitative definition of risk is given as the product of the probability of the occurrence of undesired events and their consequences, as given in (1).

$$Risk = \sum_i p(E_i) \times C(E_i) \qquad (1)$$

where $p(E_i)$ is the probability of the occurrence of undesired event $E_i$ and the $C(E_i)$ is its related consequences.

Subsequently, the structure of the ICT network is mapped onto an Operation Graph (OG) $G_O$, which is a pair of sets ($V_O$, $E_O$), and a Reliability Graph (RG) $G_R$, which is a pair of sets ($V_R$, $E_R$). Let $V_O \equiv \{v_{o1}, v_{o2}, \ldots, v_{om}\}$ and $V_R \equiv \{v_{r1}, v_{r2}, \ldots, v_{rn}\}$ be the node sets for $G_O$ and $G_R$, respectively, in which $m$ and $n$ are the number of nodes in $G_O$ and $G_R$, respectively. Let also $E_O \equiv \{e_{o1}, e_{o2}, \ldots, e_{op}\}$ and $E_R \equiv \{e_{r1}, e_{r2}, \ldots, e_{rq}\}$ be the edge sets for $G_O$ and $G_R$, respectively, where $p$ and $q$ are the number of edges in $G_O$ and $G_R$ respectively. As shown in Fig. 1, based on the time constraints of a power system control action, critical paths can be identified in the OG. The number affiliated with each edge is edge weight $W_e$, and the number associated with each vertex is vertex weight $W_v$, which represent the latency (or "delay") that occurs at each communication channel and node, respectively. For example, by specifying the latency threshold of a successful power system control action (e.g. load shedding, $t_\theta$=1s), possible routing strategies between a source node (e.g., Remote Terminal Unit (RTU) node), and a target node (e.g., Control Center node), can be identified. The most efficient path that is most critical to the operation of power system in the example network is highlighted in Fig.1 with dashed green lines. Consequently, all available routes that meet the latency criteria $t_\theta$ are reflected on the RG where communication channels are assumed to be perfect, while ICT nodes are subject to failures, and the possibility of failures are denoted by failure rates.

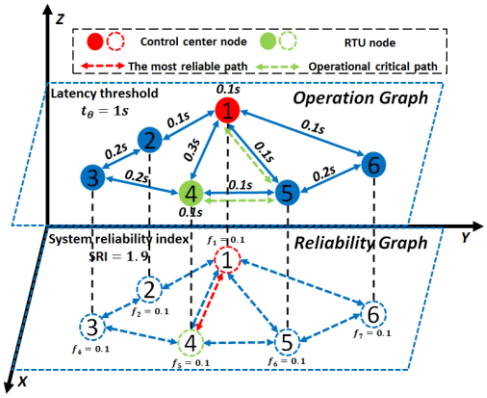


Fig. 1. Illustration of the operation graph and reliability graph (the numerical values shown are for the illustration purposes only)

The reliability of an $N$-node route from a source node to a target node (see Fig. 2) is the product of the reliability of each node along the route, assuming each node fails independently with a failure rate $f_{s_n}$, as given in (2).

$$R = \prod_{n=1}^{N} r_{s_n} = \prod_{n=1}^{N} (1 - f_{s_n}) \qquad (2)$$

in which $r_{s_n}$ and $f_{s_n}$ are the reliability and failure rate of node $s_n$, respectively.


Fig. 2. Simple reliability route

### B. Operation Matrix and Reliability Matrix

Let matrix $C$ be the mathematical representation of the topology of a graph. Its entry $c_{hj}$ = 1 if there is a link between node $h$ and $j$; otherwise if $c_{hj}$ = 0, node $h$ and $j$ have no direct connections. Figure 3 a) shows the connectivity of the example graph of Fig. 1 represented by blue dots (i.e. "1s"). Fig. 3 b) shows the corresponding operation matrix $O$, where the entry $o_{hj}$ is represented by blue circles whose sizes correspond to the latency of the connection – the larger the size, the larger the latency. Fig. 3 c) presents the reliability matrix $R$ of the example graph. Similarly, the size of the diamond in Fig. 3 c) corresponds to the reliability value of the link represented by entry $r_{hj}$. Symmetric patterns can be observed between the upper part and the lower diagonal matrix in each of these matrices, as it is assumed in this paper that all communication

technologies used in the ICT network are full-duplex, and the forward and backward latencies between two nodes are identical.

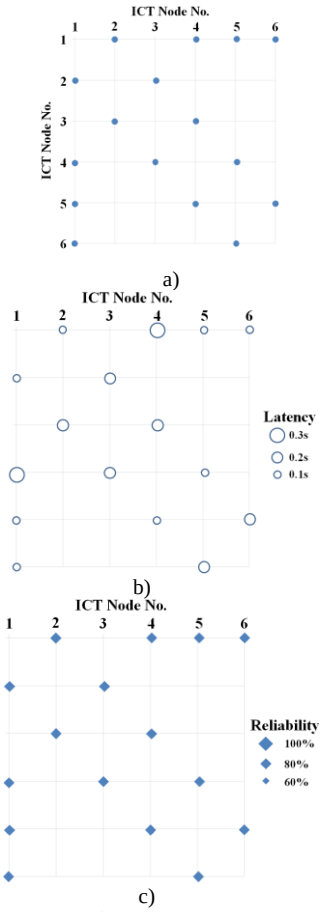


Fig. 3. Matrix representation of the example graph a) Connection matrix; b) Operation matrix; c) Reliability matrix

## III. Risk Evaluation

### A. The Operational Path and The Most Reliable Path

Although research efforts have been made in reliability-related analysis to simplify RBD, or Complex Network, based network topology [14, 28], it is still less practical in large network analysis due to the excessive computational power required. Some exploratory findings based on exhaustive search for shortest paths between source and target nodes using Dijkstra's algorithm have been presented in [29]. Taking advantage of the shortest path algorithms, the most reliable path can be identified by manipulating the path reliability into its logarithmic form [30]. A CNT-based reliability efficiency measure is proposed in [31], to facilitate the quantification of the nontrivial criticality of system components within a large complex network. However, the most reliable paths and the operational paths may not be the same, as shown in Fig. 1, and the 'shortest paths' may not be adequate to quantify the level of reliability of the system.

### B. System Reliability Index (SRI)

To effectively address this issue, therefore, a novel CNT-based index, System Reliability Index (SRI) is introduced in this paper, and its calculation procedure is presented in Fig. 4. First, the depth first search (DFS) is applied to find all available routes between source(s) and target(s) for a complete power system monitoring and control action. Then, paths that meet the latency criteria required for a specific type of power system application are screened out, denoted as $n_c$. Next, the sum of the natural logarithm of the reliability value of each cut $r_{hj}$ within the path $n_x$ is calculated for all $n_x \in n_c$. Finally, the SRI of the system is calculated by (3).

$$SRI = \frac{1}{N(N-1)} \sum_{x=1}^{M} \frac{1}{\sum_{h,j \in V_R, h \neq j} -\ln r_{hj}} \quad (3)$$

where $M$ is the number of operational paths that meet the latency criteria and $N$ is the total number of ICT components.

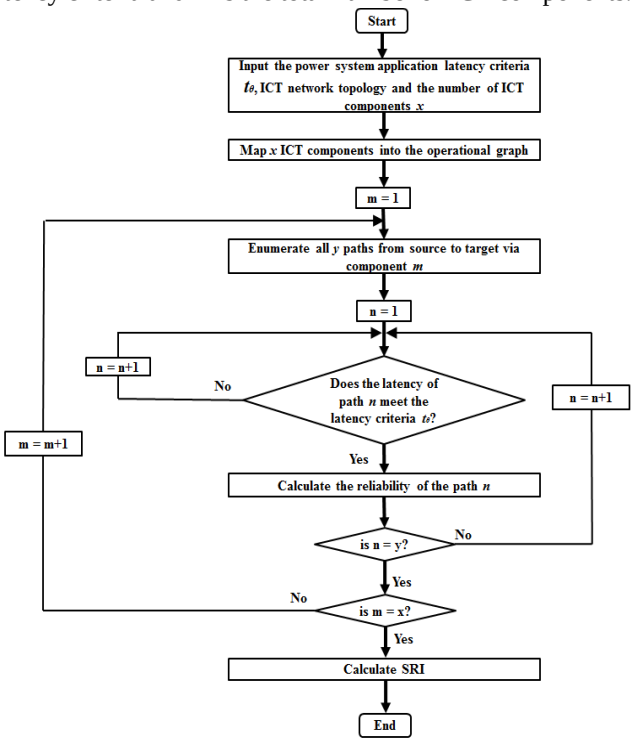


Fig. 4. Scheme of the proposed method

TABLE I. Operational Paths of the Example Network

| Path | | | Path | | |
|---|---|---|---|---|---|
| **Forward** | **Backward** | **Latency** | **Forward** | **Backward** | **Latency** |
| 4-1 | 1-4 | 0.9s | 4-5-1 | 1-6-5-4 | 0.9s |
| 4-5-1 | 1-5-4 | 0.7s | 4-5-1 | 1-2-3-4 | 1s |
| 4-5-6-1 | 1-6-5-4 | 1.1s | 4-5-6-1 | 1-4 | 1s |
| 4-3-2-1 | 1-2-3-4 | 1.3s | 4-5-6-1 | 1-5-4 | 0.9s |
| 4-1 | 1-5-4 | 0.8s | 4-5-6-1 | 1-2-3-4 | 1.2s |
| 4-1 | 1-6-5-4 | 1s | 4-3-2-1 | 1-4 | 1.1s |
| 4-1 | 1-2-3-4 | 1.1s | 4-3-2-1 | 1-5-4 | 1s |
| 4-5-1 | 1-4 | 0.8s | 4-3-2-1 | 1-6-5-4 | 1.2s |

By assuming the control center has a processing time of 1s, and the data collection time and command execution time of RTUs are both 1s, while other nodes handle signal instantly, the

routing strategies and their total latencies are presented in Table I. The SRI of the example network is therefore calculated to be 1.9.

## IV. IMPORTANCE MEASURE

In order to reveal the risks embedded in the ICT system, the impact of the cyber components' failures, as well as the impact of the improvement of their reliabilities, on the overall system performance needs to be analyzed. Sensitivity analysis techniques, including Birnbaum's Importance Measure (BIM) [32] and Fussell-Vesely (FV) factor [33], have been implemented and advanced significantly to study a single component's criticality with respect to the reliability of a complex system with time-dependent uncertainties [34-39]. These Importance Measures (IMs) consider mainly two sources contributing to the criticality of the components, namely, the reliability of the component itself [40, 41], and the topological position of the component (i.e. the structural importance) [42, 43]. In this section, the structural importance is further divided into two aspects – an application specific aspect, and a non-application specific aspect. The results obtained from these two aspects are discussed in order to emphasize the significance of using the OG.

### A. Topological Criticality

The topological criticality of a component is quantified by its contribution to the network's global efficiency. The global efficiency $E_{glob}$ is defined in (4) [44], and the topological criticality $C_t$ of node $i$ is simply the ratio of the difference between $E_{glob}(N)$ and $E_{glob}(N\text{-}1)$, each are the global efficiency of the network with and without node $i$, to $E_{glob}(N)$.

$$E_{glob} = \frac{1}{N(N-1)} \sum_{i,j \in V_A, i \neq j} \frac{1}{d_{ij}} \quad (4)$$

$$C_t = \frac{E_{glob}(N) - E_{glob}(N-1)}{E_{glob}(N)} \quad (5)$$

where $N$ is the number of nodes in the network, and $d_{ij}$ is the length of the geodesic (the shortest path) between node $i$ and node $j$.

The results of the topological criticality of the components in the example network are presented in Table II.

TABLE II. TOPOLOGICAL CRITICALITY OF THE TEST NETWORK COMPONENTS

| Node No. | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| $C_t$ | 43.38% | 30.88% | 29.41% | 36.76% | 35.29% | 29.41% |

### B. System Reliability Advancement Worth (SRAW) and System Reliability Deterioration Worth (SRDW)

Two commonly used criticality measures in industrial practices for Nuclear Power Plants are Risk Reduction Worth (RRW) [45] and Risk Achievement Worth (RAW) [46], to evaluate the significance of a system component's failure, and the influence of the improvement of the component's reliability to one to the overall system reliability, respectively. The calculation of both indices is given by (6) and (7), respectively.

$$RRW = R/R(0_c) \quad (6)$$

$$RAW = R(1_c)/R \quad (7)$$

where $R$ is the general risk of the system, and $R(0_c)$ is the reduced risk assuming the risk contributor is vanished, and $R(1_c)$ is the increased risk assuming the risk contributor is deemed to exist.

Similarly, the System Reliability Advancement Worth (SRAW) and System Reliability Deterioration Worth (SRDW) are defined, by (8) and (9).

$$SRAW = SRI/SRI(0_f) \quad (8)$$

$$SRDW = SRI(1_f)/SRI \quad (9)$$

where $SRI$ is the System Reliability Index of the system in normal state, and $SRI(0_f)$ and $SRI(1_f)$ are the SRI when the failure rate of the component is zero (i.e., the component is 100% reliable), and one (i.e., the component is failed), respectively.

Consequently, the criticality of the component $i$ is quantified in two aspects, SRAW and SRDW, as presented in (10) and (11), where $SRI(0_i)$ and $SRI(1_i)$ are the SRI when the failure rate of the component $i$ is zero and one, respectively.

$$C_{SRAW}^{G_R}(i) = (SRI(0_i) - SRI)/SRI \quad (10)$$

$$C_{SRDW}^{G_R}(i) = (SRI - SRI(1_i))/SRI \quad (11)$$

As illustrated in Section II.A, the Reliability Graph $G_R$ mirrors the topology of the Operation Graph $G_O$ after the latency requirement is applied. Therefore, the SRAW and SRDW introduced above should only be assessed with respect to specified latency criteria determined by power system applications. For better illustration purposes, the latency requirement of the example network is set to 1s, and the SRAW criticality and SRDW criticality of the components are calculated and presented in Table III.

TABLE III. SRAW CRITICALITY AND SRDW CRITICALITY OF THE EXAMPLE NETWORK

| Node No. | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| $C_{SRAW}^{G_R}$ | 64.44% | 2.78 % | 2.78 % | 64.44% | 38.89 % | 5.56% |
| $C_{SRDW}^{G_R}$ | 100.00 % | 5.56 % | 5.56 % | 100.00 % | 44.44 % | 11.11 % |

Comparing the results presented in Table II and Table III, conclusions can be drawn that systematic measures $C_{SRAW}^{G_R}$ and $C_{SRDW}^{G_R}$ are better than pure topological index $\boldsymbol{C_t}$ in differentiating the role of important components. Despite the fact that both SRAW and SRDW report the same sequence in ranking nodes' criticalities, SRDW places more emphasis on the substance of the system's functionality, while SRAW is more useful in determining the room of improvement in components' reliabilities. In the next section, a substation Ethernet network architecture is used to demonstrate the effectiveness of the proposed method.

Because of the complexity of real communication network structure and the inherent uncertainty in communication delays, as well as the inaccuracy in single-value estimate of reliability, a more descriptive "low-level" model should be developed to incorporate the engineering details of the ICT system. This model should be able *a)* to adequately capture the uncertainty of ICT network latency (including processing delay, propagation delay, transmission delay, and queuing delay) uncertainties in the ICT network; *b)* to differentiate the functional layers in a large ICT network (e.g., a national-scale SCADA system); *c)* to effectively model the routing strategies in a complex ICT network when the variation of data traffic is taken into account; *d)* to practically assess the importance of each ICT component with regard to different power system applications; *e)* to effectively quantify the inaccuracy of the reliability estimation of each ICT component; and *f)* to comparatively analyze the risks of ICT networks with different topological configurations. However, due to space limitation, all these factors not presented in this paper but will be discussed in a subsequent paper.

## V. Case Study

### A. Test Network

A laboratory test network is used in this section to demonstrate the application of the proposed method. Modern substation secondary system is constructed according to IEC 61850 which is a series of guidelines used to standardize the engineering process in order to enable intelligent electronic devices (IEDs) from various vendors to communicate with each other. IEC 61850 defines three levels in the substation automation system (SAS) architecture, namely process level, bay level, and station level. The data exchange between different levels is realized using a station bus and a process bus (Ethernet communication links).

In an IEC 61850 based substation that uses the process bus, the analogue voltage and current measurement signals are digitized as Sampled Values (SVs). The format of SV is defined in IEC 61850-9-2 Light Edition with a transmit rate at 80 messages per cycle, i.e., 4000 sample/s at 50 Hz or 4800 sample/s at 60Hz [47]. These digital measurement values are transmitted via optic fibers in the substation secondary Ethernet communication networks, which can be subscribed to by the IEDs for various protection and control applications.

In order to build a resilient substation Ethernet network, fast recovery after communication failure is required. Existing technologies such as rapid spanning tree protocol (RSTP) can only restore the data transfer in tens of milliseconds [48]. Data being transmitted may be lost during this communication dead time, which is not allowed in time-critical protection applications. Two seamless redundant architectures, Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR), based on IEC 62439-3 have been introduced [49]. Both protocols enable duplicated messages to be sent in the network in either distinct paths (i.e. PRP) or clockwise and anticlockwise directions in a ring (i.e. HSR).

Protection and control applications have to be executed in a timely manner. Delayed delivery of SVs to IEDs may slow down the application process which may lead to catastrophic failures. The maximum transfer time for a SV message (classified as raw data for protection functions) in the substation network is 3 ms as defined in IEC 61850-5 [50]. In addition, IEC 61850-90-4 specifies the maximum acceptable network latency as 600 µs (20% of the total transfer time) [51]. Therefore, examining the latency for SVs in different possible data flow paths and under various network conditions becomes critical in the design and commission of IEC 61850 substations.

Many power utilities have begun to implement HSR for process bus and station bus in IEC 61850 substations. For example, Great Britain's Pilot Multi-Vendor Digital Substation project, FITNESS utilizes HSR topology for one protection bay which contains nine IEDs and Redboxes [52]. To practically reflect real operating characteristics, a laboratory testbed representing a small-scale IEC 61850-based substation with a station bus and a protection bay is shown in Fig. 5. It is used for measuring SV transfer latency in a highly redundant substation Ethernet network architecture. A highly redundant substation Ethernet network architecture formed by nine HSR Redundancy Boxes (Redboxes) is shown in the red dashed box. The station bus HSR ring and process bus HSR ring are joined together to increase the overall system reliability. The bandwidth of communication links for both station bus and process bus were 100Mb/s. SV messages, sent from the Merging Unit (MU), were transmitted to the network via HSR Redbox 1, and the destination IED received these SVs from Redbox 9. The size of each SV frame was 126 bytes and the transmission rate was set to 4000 sample/s (at 50Hz system).

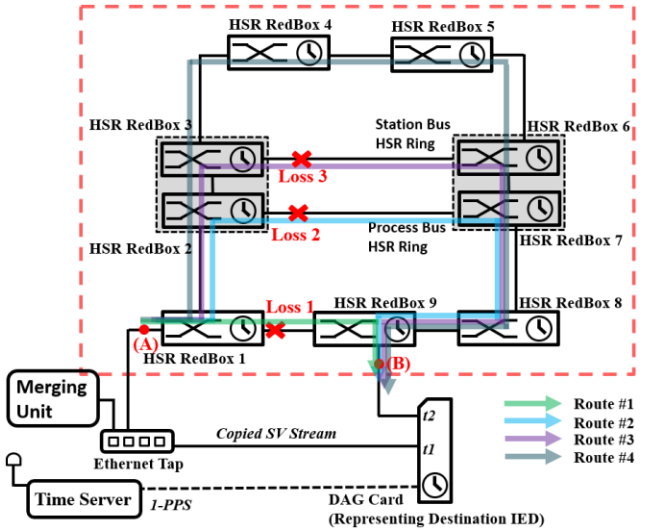


Fig. 5. Data flow path and latency measurement of SV message stream in HSR-HSR topology under various communication loss conditions

Four possible data flow paths, marked as route 1 to 4, are highlighted in different colors. According to the discarding mechanism of HSR, the first arrival of SV message will be used by the IED and the latter will be discarded. Hence, the SV latency should be evaluated based on the shortest path between MU to IED. When the network is in healthy condition, i.e., no link or node failures occur, the SV latency is the time spent on Route 1. If the communication link between Redboxes 1 and 9 are outage (Loss 1), the shortest time for SVs to reach IED should be via Route 2. If both Loss 1 and Loss 2 occur simultaneously, SVs have to use Route 3 as the shortest path. In the worst-case scenario (Loss 1, Loss 2, and Loss 3 occur at the same time), the longest path (Route 4) will be used.

The network latency measurement of SVs from sending point A to receiving point B was achieved using an Ethernet Tap (NetOptic 10/100/1000 Tap), a Time Server and a Network Capture Card (Endace DAG). The Capture Card obtains the time-of-day information using Network Timing Protocol (NTP) from the host PC and finely synchronizes its oscillator via Time Server's 1-PPS signals, which gives an overall 7.5 ns timestamp resolution. The Tap creates two identical SV streams; one stream is directly time-stamped by the card at time $t_1$, whilst the other one is captured at $t_2$ after going through the substation Ethernet network. These two timestamps mark the time instances when a SV message enters and leaves the network, and hence the network latency is equal to $t_2$ - $t_1$. More descriptions of the setup can be found in [53]. A traffic generator was used to inject background SV traffic at 50Mb/s (with the same frame size but different multicast addresses) from Redbox 8. Communication link failures were achieved by disabling the ingress/egress port that sets up the communication channel between Redboxes. Table IV gives a summary of SV network latency from point A to point B under various link losses and traffic scenarios. The average latency was evaluated based on 20,000 recorded samples.

TABLE IV. SV SAMPLE NETWORK LATENCY FOR EACH TRAFFIC ROUTE

| | Average Latency (μs) | |
|---|---|---|
| **Route** | **Without Traffic** | **With 50 Mb/s Traffic** |
| **1** | 60.98 | 64.00 |
| **2** | 99.74 | 102.71 |
| **3** | 214.23 | 217.83 |
| **4** | 240.01 | 243.24 |

The results show that the maximum network latency is 243.24μs using route 4 in the presence of 50Mb/s background SV traffic. It is worth noting that this laboratory testbed only represents a small scale of real substation network. In reality, station bus or process bus ring may contain dozens of devices, and therefore the maximum accepted latency (i.e., 600μs) can be violated easily. In this case, it is sensible to set the latency threshold $t_\theta$ to 220 μs for the case study.

On the other hand, the Mean-Time-to-Failure (MTTF) of and Mean-Time-to-Repair (MTTR) of the HSR RedBox are 135 years and 24 years, respectively [54]. Therefore, the Mean-Time-between-Failures (MTBF) can be calculated using (12).

$$MTBF = MTTF + MTTR \tag{12}$$

Hence, the failure rate $\lambda$ of the HSR RedBox is simply the inverse of its MTBF values, as calculated by (13).

$$\lambda = 1/MTBF \tag{13}$$

Assuming the reliability $R$ of the device does not change with time, and therefore, the reliability of the RedBox at time $t$ can be calculated to be 0.994, using the formula (14).

$$R = e^{-\lambda t} \tag{14}$$

### B. Risk Assessment

Consequently, and following the above procedure, by applying the formula (3), the SRI of the Ethernet network is calculated to be 1.6. After that, two IMs, i.e., SRAW criticality and SRDW criticality of each communication component are calculated based on (10) and (11), and results are presented in Fig. 6.

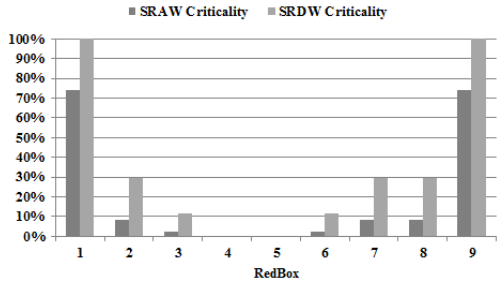


Fig. 6. SRAW Criticality and SRDW Criticality of each communication component at $t_\theta$ =220 μs

The results reported in Fig. 6 highlight the importance of RedBoxes 1 and 9 for their critical topological positions in the network, as they are directly connected to the source node MU and the target node IED, respectively. On the contrary, RedBoxes 4 and 5 are not included in the control loops (with and without traffic) that satisfy the latency requirement specified in IEC 61850-5, and therefore their reliabilities have negligible impact on such type of application. Both SRAW and SRDW criticalities gave consistent rankings for the rest of the RedBoxes, which is $C_2$=$C_7$=$C_8$>$C_3$=$C_6$, in which "C" refers to "criticality". From a system protective perspective, SRDW value makes a larger differentiation of system components' criticalities as it put more emphasis on system's structural vulnerability, whereas, SRAW provides more insight into network's reliability, i.e., redundant communication equipment plays a considerable role in the overall network reliability enhancement strategy.

## VI. CONCLUSIONS

This paper presented an innovative method to efficiently identify the cyber risks for the power system communication networks. Conventional graph-based reliability evaluation approaches are too computationally intensive for large complex networks with repeated probability computations. The

methodology established within this paper addresses this gap and has shown to provide a reliable quantification of cyber network's risks related to specific latency requirements.

The results obtained from the case study on the substation Ethernet network show that SRAW and SRDW criticalities provide different insights into the importance of communication network components – the former emphasizes more the reliability enhancement while the latter highlights components' structural importance. The results also highlight the importance of equipment redundancy as well as the significance of efficient management of data and optimal design of routing strategies in the reliable operation of communication networks. Nevertheless, different types of communication device might have different reliability, and real engineering networks contain uncertainties such as uncertain latencies that are difficult to anticipate.

Therefore, the Part 2 of this paper will introduce a more detailed model of the ICT network, and the proposed two-step framework and the Importance Measures proposed here will be applied to assess the risks associated with an uncertain cyber network under different latency requirements.

## REFERENCES


[1] M. Ni and M. Li, "Reliability Assessment of Cyber Physical Power System Considering Communication Failure in Monitoring Function," in *Proc. 2018 Int. Conf. on Power Syst. Technol. (POWERCON)*, Guangzhou, China, 2018, pp. 3010-3015.

[2] B. Falahati, A. Kargarian and Y. Fu, "Impacts of information and communication failures on optimal power system operation," in *Proc. 2013 IEEE PES Innovative Smart Grid Technologies Conference (ISGT)*, Washington, DC, 2013, pp. 1-6.

[3] M. Tritschler and W. Mackay, "UK Smart Grid Cyber Security," Energy Networks Association, London, UK, UK, Rep. no. 16010846D004, 2011. [Online]. Available: http://www.energynetworks.org/assets/files/electricity/futures/smart_grids/UK_Smart_Grid_Cyber_Security_Report.pdf

[4] R. Billinton and R. N. Allan, *Reliability evaluation of power systems*, 2nd ed. New York, NY, USA: Plenum Press, 1996.

[5] *IEEE Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems*, IEEE Std P493/D4, 2006.

[6] *IEEE Recommended Practice for Analyzing Reliability Data for Equipment Used in Industrial and Commercial Power Systems*, IEEE Std 3006.8-2018, 2018.

[7] C. Singh and Y. Kim, "An Efficient Technique for Reliability-Analysis of Power-Systems Including Time-Dependent Sources," *IEEE Trans. Power Syst.*, vol. 3, no. 3, pp. 1090-1096, Aug. 1988.

[8] H. Lei *et al.*, "Security and Reliability Perspectives in Cyber-Physical Smart Grids," in *Proc. 2018 IEEE Innovative Smart Grid Technologies - Asia (ISGT Asia)*, Singapore, 2018, pp. 42-47.

[9] G. Huang *et al.*, "Cyber-Constrained Optimal Power Flow Model for Smart Grid Resilience Enhancement," in *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 5547-5555, Sept. 2019.

[10] G. Celli *et al.*, "Reliability assessment in smart distribution networks," in *Electric Power Systems Research*, vol. 104, pp. 164-175, Nov. 2013.

[11] M. Pruckner, A. Awad and R. German, "A study on the impact of packet loss and latency on real-time demand response in smart grid," in *Proc. 2012 IEEE Globecom Workshops*, Anaheim, CA, USA, 2012, pp. 1486-1490.

[12] K. Marashi, S. S. Sarvestani and A. R. Hurson, "Consideration of Cyber-Physical Interdependencies in Reliability Modeling of Smart Grids," in *IEEE Trans. Sustain. Comput.*, vol. 3, no. 2, pp. 73-83, 1 April-June 2018.

[13] R. R. Zhang *et al.*, "Design and Implementation of a RBD-Based Algorithm for Reliability Analysis of Electric Power Communication Network," in *Proc. T& D Asia: 2009 Transmission & Distribution Conf. & Expo.: Asia and Pacific*, 2009, pp. 710.

[14] C. M. Lin *et al.*, "A mesh network reliability analysis using reliability block diagram," in *Proc. 2010 8th IEEE Int. Conf. on Ind. Inform.*, 2010, pp. 975-979.

[15] M. Walker, L. Bottaci, and Y. Papadopoulos, "Compositional temporal fault tree analysis," in *Proc. Computer Safety, Reliability, and Security*, vol. 4680, pp. 106, 2007.

[16] S. Lin, Y. H. Wang, and L. M. Jia, "System Reliability Assessment Based on Failure Propagation Processes," *Complexity*, 2018.

[17] B. Falahati, Y. Fu, and L. Wu, "Reliability Assessment of Smart Grid Considering Direct Cyber-Power Interdependencies," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1515-1524, Sep. 2012.

[18] Y. Zhang *et al.*, "Simulation Approach to Reliability Analysis of WAMPAC System," in *Proc. 2015 IEEE Power & Energy Soc. Innovative Smart Grid Technologies Conf. (ISGT)*, 2015.

[19] K. Jiang and C. Singh, "New Models and Concepts for Power System Reliability Evaluation Including Protection System Failures," *IEEE Trans. Power Syst.*, vol. 26, no. 4, pp. 1845-1855, Nov. 2011.

[20] T. Elperin, I. Gertsbakh, and M. Lomonsov, "Estimation of Network Reliability Using Graph Evolution Models," *IEEE Trans. Rel.*, vol. 40, no. 5, pp. 572-581, Dec. 1991.

[21] R. Gulati and J. B. Dugan, "A modular approach for analyzing static and dynamic fault trees," in *Annu. Rel. and Maintainability Symp. - 1997 Proc.*, 1997, pp. 57-63.

[22] R. A. Sahner, K. S. Trivedi, and A. Pulia, *Performance and Reliability Analysis of Computer System*, New York, NY, USA: Springer-Verlag, 1996.

[23] X. Zang, H. Sun, and K. S. Trivedi. *A BDD-Based Algorithm for Reliability Graph Analysis*. Tech. Rep., 2000. [Online]. Available: http://citeseer.ist.psu.edu/213187.html

[24] M. C. Kim and P. H. Seong, "Reliability graph with general gates: an intuitive and practical method for system reliability analysis," *Reliab. Eng. Syst. Safe.*, vol. 78, no. 3, pp. 239-246, Dec. 2002.

[25] M. C. Kim, "Reliability block diagram with general gates and its application to system reliability analysis," *Ann. Nucl. Energy*, vol. 38, no. 11, pp. 2456-2461, Nov. 2011.

[26] F. T. Boesch, X. Li, and C. Suffel, "On the Existence of Uniformly Optimally Reliable Networks," *Networks*, vol. 21, no. 2, pp. 181-194, Mar. 1991.

[27] O. Goldschmidt, P. Jaillet, and R. Lasota, "On Reliability of Graphs with Node Failures," *Networks*, vol. 24, no. 4, pp. 251-259, Jul. 1994.

[28] W. T. Zhu, M. Panteli, and J. V. Milanovic, "Reliability and Vulnerability Assessment of Interconnected ICT and Power Networks Using Complex Network Theory," *2018 IEEE Power & Energy Soc. General Meeting (PESGM)*, 2018.

[29] A. Bobbio *et al.*, "A tool for network reliability analysis," in *Proc. Computer Safety, Reliability, and Security SAFECOMP 2007*, vol. 4680, F. Saglietti, and N. Oster Eds. Berlin, Germany: Springer-Verlag, 2007, pp. 417-422.

[30] M. Roosta, "Routing through a Network with Maximum Reliability," *J. Math. Anal. Appl.*, vol. 88, no. 2, pp. 341-347, 1982.

[31] E. Zio, "From complexity science to reliability efficiency: a new way of looking at complex network systems and critical infrastructures," *Int. J. Crit. Infrastruct.*, vol. 3, no. 3-4, pp. 488-508, Jan. 1 2007.

[32] Z. W. Birnbaum, "On the Importance of Different Components in a Multicomponent System," in *Multivariate Analysis II*, P. R. Krishnaiah, Ed. New York, USA: Academic Press, 1969, pp. 591-592.

[33] J. B. Fussell, "How to Hand-Calculate System Reliability and Safety Characteristics," *IEEE Trans. Rel.*, vol. 24, no. 3, pp. 169-174, 1975.

[34] F. K. Hwang, "A new index of component importance," *Oper. Res. Lett.*, vol. 28, no. 2, pp. 75-79, Mar. 2001.

[35] F. K. Hwang, "A hierarchy of importance indices," *IEEE Trans. Rel.*, vol. 54, no. 1, pp. 169-172, Mar. 2005.

[36] W. Kuo and X. Y. Zhu, "Some Recent Advances on Importance Measures in Reliability," *IEEE Trans. Rel.*, vol. 61, no. 2, pp. 344-360, Jun. 2012.

[37] S. Si *et al.*, "System Reliability Allocation and Optimization Based on Generalized Birnbaum Importance Measure," *IEEE Trans. Rel.*, pp. 1-13, 2019.

[38] J. E. Ramirez-Marquez and D. W. Coit, "Composite importance measures for multi-state systems with multi-state components," *IEEE Trans. Rel.*, vol. 54, no. 3, pp. 517-529, Sep. 2005.
[39] E. Borgonovo and E. Plischke, "Sensitivity analysis: A review of recent advances," *Eur. J. Oper. Res.*, vol. 248, no. 3, pp. 869-887, Feb. 1 2016.
[40] E. A. Elsayed, *Reliability engineering*, 2nd ed. Hoboken, USA: Wiley, 2012, [Online]. Available: http://site.ebrary.com/lib/yale/Doc?id=10580167
[41] H. A and R. M, *System reliability theory: models and statistical methods*. New York, USA: Wiley, 1994.
[42] F. C. Meng, "Comparing the importance of system elements by some structural characteristics," *IEEE Trans. Rel.*, vol. 45, no. 1, pp. 59-65, 1996.
[43] F. C. Meng, "Some further results on ranking the importance of system components," *Reliab. Eng. Syst. Safe.*, vol. 47, no. 2, pp. 97-101, Jan. 1 1995.
[44] V. Latora and M. Marchiori, "Efficient behavior of small-world networks," *Phys. Rev. Lett.*, vol. 87, no. 19, Nov. 5 2001.
[45] W. E. Vesely *et al.*, *Measures of risk importance and their applications*. U.S. Nuclear Regulatory Commission, Washington, DC, USA, Rep. no. NUREG/CR-3385 (BMI-2103), 1983. [Online]. Available: https://www.nrc.gov/docs/ML0716/ML071690031.pdf
[46] NUMARC Maintenance Working Group, "Industry guideline for monitoring the effectiveness of maintenance at nuclear power plants," Nuclear Energy Institute, Washington, DC, USA, Rep. no. NUMARC 93-01 (Revision 4A), Apr. 2011. [Online]. Available: https://www.nrc.gov/docs/ML1111/ML11116A198.pdf.
[47] UCA International Users Group, "Implementation Guideline for Digital Interface to Instrument Transformers using IEC 61850-9-2," Raleigh, NC, USA, 2004. [Online]. Available: http://iec61850.ucaiug.org/Implementation%20Guidelines/DigIF_spec_9-2LE_R2-1_040707-CB.pdf.
[48] N. Kerö *et al.*, "Performance and Reliability Aspects of Clock Synchronization Techniques for Industrial Automation," *Proc. IEEE*, vol. 107, no. 6, pp. 1011-1026, 2019.
[49] *Industrial communication networks – High availability automation networks – Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR)*, IEC 62439-3, 2016.
[50] *Communication networks and systems for power utility automation – Part 5: Communication requirements for functions and device models*, IEC 61850-5, 2013.
[51] *Communication networks and systems for power utility automation - Part 90-4: Network engineering guidelines*, IEC 61850-90-4, 2013.
[52] C. Patterson *et al.*, "FITNESS – GB's Pilot Multi-Vendor Digital Substation - Architecture and Design Philosophy," [Online]. Available: https://www.ee.co.za/wp-content/uploads/2017/11/5.3-Graeme-Lloyd-FITNESS-GBs-Pilot-Multi-Vendor-Digital-Substation.pdf
[53] M. Han, H. Guo, and P. Crossley, "IEEE 1588 time synchronisation performance for IEC 61850 transmission substations," *Int. J. Elec. Power*, vol. 107, pp. 264-272, 2019.
[54] J. Tournier and T. Werner, "A quantitative evaluation of IEC61850 process bus architectures," in *Proc. IEEE Power and Eerngy Soc. General Meeting*, 2010, pp. 1-8.

**Wentao Zhu** (S'16-M'20) received the B.Eng. degree and the Ph.D. degree from the University of Manchester, Manchester, U.K., in 2015 and 2019, respectively, both in electrical and electronic engineering. Currently he is a Research Associate at the University of Manchester, working on the technically and economically feasible solutions to the sustainable development of interconnected critical infrastructures.

**Mingyu Han** (S'16) received the B.Eng degree in electrical and electronic engineering in 2016 from the University of Manchester, Manchester, U.K., where he is currently pursuing the Ph.D. degree.

**Jovica V. Milanović** (M'95, SM'98, F'10) received the Dipl.Ing. and M.Sc. degrees from the University of Belgrade, Belgrade, Yugoslavia, the Ph.D. degree from the University of Newcastle, Newcastle, Australia, and the Higher Doctorate (D.Sc. degree) from The University of Manchester, U.K., all in electrical engineering. Currently, he is a Professor of Electrical Power Engineering and Deputy Head of the Department of Electrical and Electronic Engineering at the University of Manchester, U.K., Visiting Professor at the University of Novi Sad, Serbia and University of Belgrade, Serbia. Professor Milanovic is a Chartered Engineer in the UK, Foreign member of the Serbian Academy of Engineering Sciences, Fellow of the IET, Fellow of the IEEE, Distinguished IEEE PES Lecturer and currently serves on IEEE PES Governing Board as Regional Representative for Europe, Middle East and Africa and was a vice chair of the IEEE PES Fellows Evaluation Committee.

**Peter Crossley** (M'95) received the B.Sc. degree in electrical and electronic engineering from The University of Manchester Institute of Science and Technology, Manchester, U.K., in 1977, and the Ph.D. degree in power system engineering from the University of Cambridge, Cambridge, U.K., in 1983. He is a Professor of electrical power systems engineering at The University of Manchester, and the Director of the Doctoral Training Centre, Manchester, U.K. He has published more than 250 technical papers on protection. Prof. Crossley is an active member of various CIGRE, IEEE and IET committees.