Reliability Assessment of Distribution System Considering Cyber-Induced Dependent Failures in Substation

H J Yuan1, 2, G F Li1, Z H Bie1

1The State Key Laboratory of Electrical Insulation and Power Equipment, the Shaanxi Key Laboratory of Smart Grid, Xi’an Jiaotong University, Xi’an 710049, China

Emile: jueshifeixia@163.com

Abstract. With the increasing dependencies on Information and Communication Technologies (ICTs), the smart distribution system has similar characteristics to Cyber-Physical System (CPS) and is seen as the so-called "cyber-physical power system" (CPPS). However, the impact of upstream substation is becoming one of the main factors impacting on distribution reliability. To avoid the too optimistic conclusion, the Cyber-Induced Dependent Failures (CDFs) of upstream substation are important to be considered. Thus the cyber security risk brought by both the malfunction of ICT components and the cyber-attack should be taken into account. This paper provided a methodology to incorporate both the two sides of CDFs in upstream substation into cyber-enabled distribution system reliability assessment. In the sequential Monte Carlo simulation (MCS), the game process between attackers and defenders can be modelled as the semi-Markov Chain (SMP), and indices are calculated by the minimal path method. The effects of CDFs are quantified and converted onto the joint feeders, based on the Breadth-First-Search (BFS), as well. Some conclusions for the distribution and substation automation planning have been made and verified by the cyber-extended Roy Billinton Test System (RBTS).

1. Introduction

The Cyber-Physical System (CPS) is a concept that a new kind of composite system consists of the traditional physical system and cyber system with advanced ICT and Intelligent Electronic Devices (IEDs) [1]. The smart grid has similar characteristics: to ensure the normal operation of the smart grid, the supports from both the primary and the secondary side are indispensable, which can be seen as a kind of cyber-physical integration.

Similarly, the so-called "cyber-physical power system" (CPPS) is becoming more and more achievable with the progress of several cyber functions, such as communication, protection, and self-healing. But increasing dependencies on ICT should be considered because they may bring complex cyber risks as well.

Several methods were proposed for CPPS reliability assessment by recent publications [2]-[6]. The architecture of the IEC61850 was depicted in [2] and the CPIM method was defined to analysis the cyber-induced dependent failures (CDFs) in a sequential MCS. In [3], a typical a breaker-and-a-half configuration with detailed cyber architecture was expanded and the fault tree analysis (FTA) is used to quantified the reliability. [4] discussed the difficulties of the sampling the CDFs in composite power system, and developed the solution by generating the representative state space. The methods of modeling
the Intrusion Tolerance system (ITS) and the game process were provided in [5]. In [6], an analytically reliability assessment was performed for the cyber-enabled feeders, and the placement problems of remote-controlled switches (RCS) and fault detector (FD) are discussed. A real-time optimal power flow framework was developed in a medium-voltage distribution system, and the discrete voltage at slack bus was considered as a curtailment factor [7]. Based on this method, further studies were conducted on dispatching strategy [8].

Recent works mainly focus on the internal CDFs [2]-[3] and composite system [4]-[5], or evaluate the distribution system individually [6]. However, some serious CDFs, such as external cyber-attack, could be more likely to result from upstream substation.

In view of the developments of IEC-61850 and the substation and distribution automation, the impact of upstream substation taken into account as one of the main factors impacting on distribution reliability [2-4], including the CDFs brought by both the malfunction of ICT components and the cyber-attack. Besides, after having broken into the control center or SCADA, and gained higher privilege level, it may not be worthwhile for attackers to only send false trip signal to some switches [5]. Therefore, as a complement to previous researches, in this paper, a comprehensive reliability methodology of distribution system is propose to consider the two-sided CDFs caused by the upstream substation, including internal CDFs and external malicious cyber-attack. The main contributions are summarized as:

- Developing a distribution CPPS and analyzing the features of cyber-physical integration.
- Modeling the internal CDFs and the malicious cyber-attack CDFs caused by upstream substation.
- Performing a comparison on resistance to CDFs between some typical kinds of main wiring.

2. Architecture of the Cyber-enabled distribution system
An extended 33/11kV substation of RBTS BUS2 is depicted in figure 1, according to the IEC 61850-based substation [2]. Instead of analyzing 11kV distribution system only [9], the failures or CDFs in 33kV system and 33/11kV substation, are all considered. This system not only incorporates the physical part and cyber part, but also the distribution feeders and its upstream substation.

The physical part consists of transformers, circuit breakers (CB) and transmission lines, etc., while the components in cyber part mainly refer to the IEC 61850-based substation [2]. The cyber part consists of current transformers (CTs), potential transformers (PTs), Ethernet switches (ES), merging units (MUs), communication links, and other protection IEDs. Besides, 22 independent protection structures with circuit breakers and some IEDs, can be partitioned according to the terminal units and switches. The protection zones are the smallest unit in assessment, simplifying the minimal path method.

For example, when zone 7 malfunctions, the circuit signals will be measured by CT4/6 and PT4/6, be digitized by MU4/6, and be sent to the PB. Then it will be sent to protection IEDs by the ES, and the measurements can help the dispatchers in upper level (including human machine interface (HMI) and SCADA system) to make the decision and send CB4/6 a trigger signal.
Figure 1. The architecture of the extended RBTS as well as substation based on the IEC61850
It is unlikely for internal CDFs to disturb the upper level of control center. But the cyber-attack can maliciously modify the communication between the control center and station bus by hijacking a host and sending fabricated certificate to control center [5]. The failures of these components will interrupt the communication process and result in different degrees of cyber-dependent failures. While a successful attack will interrupt the entire system.

### 3. Distribution system reliability assessment considering CDFs of upstream substation

The impacts of cyber-physical integrations are classified as the internal CDFs and the external cyber-attack. The former one means the impacts of CDFs, which result from the faulty ICT components. While the latter one represents malicious cyber-attack from external attackers. This section provide a tractable approach to consider the two-sided effects in a sequential MCS.

#### 3.1. The internal CDFs of substation and distribution system

The CPIM and the CEM are shown in equation (1) and (2). Detailed steps on obtaining a CPIM via FMEA (Failure Modes and Effects Analysis) have been provided, and its utility in a sequential MCS has been proven [3-5].

To extend application of this method in distribution, the Breadth-First-Search (BFS) method is used to obtain the CPIM, and CDFs’ impacts on distribution reliability are calculated by zone partitioning and minimal path method. The CPIM and CEM represent the possible CDFs mode of each zone. The elements of CPIM are the probabilities of CDFs, while the ones in CEM represent the consequent effects of CDF. It can be formed as binary numbers to save memory, and the “1” in strings represents that the adjacent zone is affected [3]. A random probability $P$ uniformly distributed over interval $[0, 1]$ is generated when zone $m$ fault. The event $n$ will occur if $P$ satisfies the condition that $P_{\text{event } n-1} < P < P_{\text{event } n}$.

$$\begin{align*}
\begin{bmatrix}
\text{event.1} & \text{event.2} & \cdots & \text{event.n} \\
\text{zone.1} & 0.96 & 0.02 & \cdots & \text{event probability} \\
\text{zone.2} & p_{2,1} & p_{2,2} & \cdots & p_{2,n} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
\text{zone.m} & p_{m,1} & p_{m,2} & \cdots & p_{m,n}
\end{bmatrix}
\end{align*} \tag{1}$$

$$\begin{align*}
\begin{bmatrix}
\text{event.1} & \text{event.2} & \cdots & \text{event.n} \\
\text{zone.1} & 100\ldots00 & 110\ldots00 & \cdots & \text{binary number} \\
\text{zone.2} & B_{2,1} & B_{2,2} & \cdots & B_{2,n} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
\text{zone.m} & B_{m,1} & B_{m,2} & \cdots & B_{m,n}
\end{bmatrix}
\end{align*} \tag{2}$$

Where $m$ and $n$ are the number of zones and subsequent events respectively; $P_{m,n}$ is the corresponding probability and $B_{m,n}$ is the fault scope; the string in $B_{m,n}$ shows the affected zones in the $n$-th CDF event induced by failures in zone $m$.

#### 3.2. Malicious Cyber-Attack

Some researches of IEC 61850-based substation were based on an assumption that the HMI and SCADA system works reliable [4]. Intrusion Tolerance system (ITS) is an approach of computer security and also installed in the SCADA system [6]. This model mainly quantified the ITSs of substation SCADA system.
The game process between attackers and defenders can be modeled as the semi-Markov Chain (SMP), see figure 2. Three steps are required for a successful attack, including attacking communication host, gaining trust for the substations and gaining trust of the control center, respectively. The SMP can model a stochastic process with non-exponential distributions for the state transition probabilities [6]. Thus the uniform distribution is applied to describe the attacks.

To sample the cyber-attack sequentially, the impact of attack is processed as a multistate element. The duration of each state will be compared with the time to failure (TTF) and time to repair (TTR) of power components. Thus the transition condition of state $i$ can be formulated as:

$$
TTF_i = -\frac{1}{\lambda_i} \ln \beta_i \\
TTR = r_j \ln \beta_i \\
T_i = \min \{\cdots TTF_j / TTR_j, \cdots\}
$$

The distribution function is formed as:

$$
F(t) = P(\min(A, D) \leq t) = 1 - (1 - F_t(A)) (1 - F_t(D))
$$

The mean durations of each stages are formed as:

$$
mean(T_i) = \int_0^D [1 - F(t)] dt = \frac{A}{3} + \frac{D}{3} - \frac{A^2}{6D}
$$

And the density function of the attack time required in $i$-th attack phase is generated by:

$$
TTT(u) = \frac{1 + \sqrt{4D_j (D_j - A_j) u + 1 + 4D_j A_j}}{2}
$$

Where and are attackers’ needed time and defenders’ needed time at $i$-th phase respectively, and $u$ is a random-number following a uniform distribution $U(0,1)$.

3.3. Detailed steps

The detailed steps on of the assessment is shown as follows:

1) Obtain the partitioning zone and the minimal path sets.
2) Obtain the CPIM and CEM (Cyber Effort Matrix) [2] based on the depth-first-search method.
3) Sample the cyber-attacks or primary failures by state duration sampling approach [6].
   i. If the external cyber-attack is sampled, the upper layers above PB are all damaged.
   ii. If the primary failures happens, determine the internal CDFs mode according to CPIM.
a) If the failures (or CDFs) happen in feeders, find the minimal path affected.

b) As for the external cyber-attack, use DFS method to calculate the indices, and add them to subordinate feeder.

4) Locate the faulty zones and find the minimal path affected.
5) Calculate the impact on reliability indices of each load point.
6) Return to the step 2) until the convergence criterion is achieved.
7) Calculate and record the system indices.

For convenience of analysis, several assumptions are made:

1) All CDFs (expect for the system-wide breakdown) will be isolated in the next adjacent protection zones. Namely, the repeated CDFs are neglected for low probabilities.
2) Every device is analyzed independently, and the symmetrical devices and structures are the same.
3) CDFs will occur simultaneously with the primary failures, and will not change the sample time.
4) The outage time of affected zones is the manual handling time [4], instead of primary duration.

4. Case study

4.1. Introduction of test system

The RBTS BUS2 is used as test system, with four feeders and 22 load points. Components’ reliability data are from references [4] and [9], and the cyber-extended RBTS is shown in figure 1. Voltage levels at feeders may change little in CDFs but bring many uncertainties. Thus they are supposed to be constant. Similarly, renewable energy generation is ignored to simplify the algorithm [7-8].

Three cases are investigated: firstly, the cyber-extended distribution system will be sampled together with upstream substation (see figure 1); then, the cyber-attack is considered based on this system; finally, the simulation has been performed using different main wiring forms of upstream substation.

4.2. RBTS BUS2

The simulation time is about 5 hundred years, and the affected reliability indices under CDFs and cyber-attacks are calculated and tabulated in figure 3-6.

Figure 3. The result of test system only considering internal CDFs
Some conclusions are able to be made:

- The CDFs mainly impact on SAIFI, SAIDI, with the rises of SAIDI and the declines of SAIFI. This is because the outage time of CDFs is the manual switch time for a redundant ICT system [2], bringing more short-time failures.
- The comparison of case B/D and F shows that the RCS and alternative supply even make the failure duration longer, because the alternative supply and RCSs bring more CDFs risk.
- The development of distribution automation improves the reliability dramatically, and it will be more obvious in a system lacking switch elements.
- The impacts of cyber-attacks is far more significant than internal CDFs, and the fault degrees are associated with the systems’ dependency on its cyber part, which correspond to the features of cyber-physical integration in distribution system.
- AS it is shown in table 2, the comparison between the effects of cyber-attack in distribution system [5] and upstream substation are significant, which means the cyber security of distribution deserves more attention.

4.3. Main wiring of substation

In order to demonstrate further, three typical kinds of main wiring of substation configuration is discussed, including sectionalized single-bus configuration, double-bus with auxiliary bus configuration, and 3/2 circuit breakers configuration, see figure 5-6.

For convenience, all of the substation configurations have 2 incoming lines, 4 outgoing lines, and 2 transformers. Other things being equal, and the cyber extension are similar with figure 1. This paper regard this substation as the upper station of RBTS BUS2, thus the reliability indices can be added to the subordinate 11kV feeders. In reliability indices form, the impacts from substation will be converted onto the joint feeders between distribution system and upstream substation. Besides, in this test system, the substation is operated in closed loop, and the circuit breakers are analyzed separately from the protection structures because it is considered as physical components with a four state model [6].

The effects converted onto feeders are quantified by the results shown in table 1.

- The 3/2 circuit breakers configuration is an ideal choice for cyber protection, because of containing more isolation levels.
- Sectionalized single-bus configuration has not a well performance because of its simple topology and less minimal paths, but the bus coupling circuit breakers help a lot.
- The double-bus with transfer bus configuration is mainly effected by the condition that the key nodes lack of CBs, which makes the CDFs occurring in some paths impact others easily.
Table 1. Comparison of substation main wiring forms

| Main wiring configurations/Indices | SAIFI (int./syst.cust./yr) | SAIDI (hr/syst.cust./yr) | CAIDI (hr/affected cust./yr) | ASAI | ENS (MWh) |
|-----------------------------------|---------------------------|-------------------------|-----------------------------|------|-----------|
| Case A                            | 0.248                     | 3.61                    | 14.55                       | 0.999588 | 37.746    |
| considering cyber part            |                           |                         |                             |      |           |
| difference                         | 0.295                     | 3.69                    | 12.52                       | 0.999578 | 38.738    |
| difference                         | 18.95%                    | 2.22%                   | -13.95%                     | -0.001% | 2.63%     |
| double-bus with auxiliary bus config | 0.300                     | 3.742                   | 12.463                      | 0.999573 | 39.926    |
| difference                         | 20.97%                    | 3.66%                   | -14.34%                     | -0.0015% | 5.78%     |
| 3/2 circuit breakers config        | 0.279                     | 3.676                   | 13.174                      | 0.999580 | 38.507    |
| difference                         | 12.5%                     | 1.83%                   | -9.46%                      | -0.0008% | 2.02%     |

5. Conclusions
In this paper, a comprehensive method was proposed to analyze the impact of CDFs in upstream substation on the reliability of distribution system. CPIM method and the semi-Markov Chain are applied to the assessment incorporating both the internal CDFs and external cyber-attack. The typical main wiring forms are compared to improve the distribution system reliability under CDFs. The results clearly indicate the communication vulnerabilities in upstream substation, as well as its impact of CDFs and cyber-attack on distribution reliability. It is expected that it will make some contribution to the distribution reliability assessment.

Acknowledgments
This work is supported by the National Key R&D Program of China (2016YFB0901900), and the National Natural Science Foundation of China (51607136).

References
[1] National Science Foundation of the United State 2010 *Cyber-Physical System (CPS) Program Solicitation*, US.
[2] Lei H, Singh C, and Sprintson 2014 A Reliability modeling and analysis of IEC 61850 based substation protection systems *IEEE Trans. Smart Grid* 5 2194–202.
[3] Lei H, Singh C 2015 Power system reliability evaluation considering cyber-malfunctions in substations *Electric Power Systems Research* 129 160-9.
[4] Hayati H, Ahadim A, and Aval SMM 2015 New concept and procedure for reliability assessment of an IEC 61850 based substation and distribution automation considering secondary device faults *Frontiers in Energy* 9 387-98.
[5] Zhang Y, Wang L, and Xiang Y 2016 Power system reliability analysis with intrusion tolerance in SCADA systems *IEEE Trans. Smart Grid* 17 669 – 83.
[6] Kaporuchali M H, Sepehry M, Aravinthan V 2018 Fault Detector and Switch Placement in Cyber-Enabled Power Distribution Network *IEEE Trans. Smart Grid* 9 980-92.
[7] Mohagheghi E, Gabash A, Li P 2017 A framework for real-time optimal power flow under wind energy penetration *Energies* 10 535.
[8] Mohagheghi E, Gabash A, Alramlawi M, Li P 2018 Real-time optimal power flow with reactive power dispatch of wind stations using a reconciliation algorithm *Renew. Energy* 126 509-23.
[9] Allan R N, Billinton R, Sjarief I, Goel L, and So K S 1991 A reliability test system for educational purposes-basic distribution system data and results *IEEE Trans. Power Syst.* 6 813-20.