Reliability Assessment of Distribution Network Considering Multiple Types of Cyber Disturbances

LI Guiping¹, ZHANG Shuyuan²

¹China Southern Power Grid of Kunming Bureau, 650011 Yunnan, China
²State Grid Zhangzhou Electric Power Supply Company, 363000 Les Fujian, China

* Corresponding author: ncepuhh@126.com

Abstract. The improvement of power grid intelligence depends on the development of communication technology. The wide application of communication technology in power grid has brought new security threats. In order to comprehensively and quantitatively evaluate the impact of external threats and cyber element failures on power supply reliability in the whole process of distribution network operation, reliability state models of different types of cyber disturbances are proposed, the impact of different types of cyber disturbance on the cyber availability is analyzed and a framework of distribution network reliability evaluation considering multiple types of cyber disturbance is constructed. Finally, the simulation test of IEEE33 bus distribution system verifies the feasibility and effectiveness of the proposed model and method.

1. INTRODUCTION

With the construction of intelligent power system, communication technology gradually deepened, thus power system has gradually developed into Cyber Physical System(CPS)[1]. The application of cyber technology has played an important role in the aspect of flexibility and self-healing capabilities, but potential security threats will have extreme effects on the operation of power system[2]. To effectively guarantee the development of Active Distribution Network(AND), it is necessary to comprehensively quantify the impact of various types of cyber disturbances like external threats and internal threats on the reliability of ADN.

The external security threats of cyber systems are mainly cyber attacks. Ref.[3] proposed a attack and defense vulnerability assessment model from the aspects of attack modeling, security assessment and defense monitoring, then discussed the influence of cyber attacks on power system. Ref.[4] constructed risk assessment models considering the success rate and consequences of attacks. The internal threats are mainly cyber element failure. Ref. [5] used correlation characteristic matrix to characterize the connectivity and accuracy of cyber system and analyzed the impact of different cyber failure scenarios on distribution network operation. Ref. [6-7] analyzed the influence that cyber elements failure exert on microgrid based on the coordinated and optimized control of microgrid units relying cyber system.

The two threats above show different characteristics and fault transfer mechanisms, but they all affect the validity of cyber system. From this, a reliability state model of various cyber disturbances and a unified reliability assessment framework taking multiple types of cyber disturbances into account are presented, and distribution network using centralized control of master station is taken as an example to detailly elaborate the assessment process.
2. RELIABILITY MODELE OF DISTRIBUTION CPS CONSIDERING CYBER DISTURBANCES

The impact of cyber disturbance on CPS is mainly reflected in the change of cyber network topology and the destruction of data integrity and availability. The modeling part of this paper starts from two aspects: external threat and internal threat. The external threat is the attack reliability model, and the internal threat is the network topology reliability model.

2.1. Network attack reliability modeling

Network attacks usually use security weaknesses of elements to tamper with original data by injecting bogus data[8]. In distribution network, the potential attack points are the servers in control center and the Intelligent Electronic Devices (IED) connected by switches. The random sampling model[9] is used to represent the state of attack point considering the choice of attacker and the attacking difficulty of cyber elements.

\[ R_0 = \begin{cases} 0 & \delta > P_{z_i, i \in S_{ac}} \\ 1 & \delta < P_{z_i, i \in S_{ac}} \end{cases} \]

(1)

Where \( R_0 \) is attacked state of cyber element, \( R_0 = 1 \) means it is attacked, \( R_0 = 0 \) not attacked. \( P_{z_i, i \in S_{ac}} \) is the probability of attack point \( i \) being used by attackers, \( S_{ac} \) is the set of optional attack points in cyber system. \( \delta \) is random number subject to average distribution \([0,1]\). The probability of an attack point \( i \) being used by attacker is:

\[ P_{z_i} = p_{ac,i}/\rho_{ac,i} \]

(2)

Where \( p_{ac,i} \) is the probability that attack point \( i \) is selected, which is related to the social attention \( \omega_i \) and the difficulty of attack access \( \lambda_i \) of \( i \).

2.2. Network topology reliability modeling

The cyber elements failure will cause network topology change, thus destroying end-to-end connectivity. In distribution CPS, the cyber system usually adopts ring topology, so there are multiple paths from IED to master station, when the connectivity of all paths are interrupted, the information cannot be transmitted to master station. So the connectivity state \( R_1 \) of end-to-end network can be expressed as:

\[ R_1 = \begin{cases} 0 & \bigcup_{l \neq 0} p(l)=0 \\ 1 & \bigcup_{l \neq 1} p(l)=1 \end{cases} \]

(3)

\( R_1 = 1 \) means connective while \( R_1 = 0 \) means interrupted. \( A \) is the number of communication paths. \( p(l) \) is the connectivity state of path \( l \), \( p(l)=1 \) indicates \( l \) is connective, \( p(l)=0 \) indicates interrupted. Assuming that IEDs, switches and servers are the nodes of path, communication channels are links of path. So the connectivity of path \( l \) can be determined by the state of nodes and links:

\[ p(l) = \begin{cases} 0 & \prod_{i=1}^{N} S(C_i) \prod_{j=1}^{L} S(f_j) = 0 \\ 1 & \prod_{i=1}^{N} S(C_i) \prod_{j=1}^{L} S(f_j) = 1 \end{cases} \]

(4)

Where \( N \) and \( L \) are the number of nodes and links of path \( l \). \( S(C_i) \) and \( S(f_j) \) are the state of the node \( Ci \) and link \( f_j \).
3. ANALYSIS OF THE INFLUENCE THAT CYBER DISTURBANCES EXERT ON DISTRIBUTION NETWORK

3.1. Influence analysis when distribution network operate normally
If cyber attackers attack IEDs, the situations are as follows: 1) If IEDs fault, cyber attacks will not affect the power system. 2) If IEDs are attacked during normal operation, the consequence is related to the states of loop switches and the number of attacked IEDs. When loop switches are uncontrollable, only manual processing can be used to restore power supply. When loop switches are controllable, the impact of attacking single IED and many IEDs are shown in Fig.1(a) and (b). Where solid represents closed state, hollow is open state.

If cyber attackers attack master station, the situations are as follows: 1) If cyber system completely fails, the master station of distribution network cannot be attacked, so it will not cause load outage. 2) If part of cyber system fails, the attacker can use master station to control IEDs. 3) If cyber system is normal, attacked master station may cause entire distribution network fail, which is shown in Fig.1(c).

3.2. Influence analysis under distribution network failure process
When power system fails, master station centralized control will be used to realize fault location, isolation and restoration[10].

3.2.1. Analysis during fault location
Based on the received fault current signal, fault location determines the fault point located in the section connected to the last switch that has experienced the fault current from the power supply side to the tip. If cyber disturbances occur during the process, the information uploading will be affected, which may lead to incorrectly judgement of fault point. If the received current signal can constitute complete fault current path, the location of the fault point can be directly determined, as shown in Fig.2(a). Where 1 represents fault signal while 0 non-fault signal. If the received current signal cannot constitute complete fault current path, distribution network will analyze the status of these fault current signals and do global optimization among multiple sets of feasible solutions to obtain the complete current path that is closest to the actual fault state, thus obtaining the location of fault point, as shown in Fig.2(b). If cyber system fails and mater station cannot receive any fault signal, distribution network cannot determine the location of the fault point, as shown in Fig.2(c).
3.2.2. Analysis during fault isolation

Once cyber disturbance occurs during fault isolation process, it will affect the issuing of control instructions, thus generally causing switch lose remote control[11].

If the fault location is correct, the fault isolation range is only related to the controllability of the switch: 1) if the switches on both sides of the fault point are controllable, the fault is isolated successfully; 2) If there are uncontrollable switches on both sides of the fault point, the system will search for other controllable switches on one side of the uncontrollable switch and make them open. At this time, the fault can be isolated successfully, but the scope will be expanded.

If the fault location is wrong, the fault isolation range is related to the controllability of the switch and the location of the original fault point: 1) if the area between the two switches contains the original fault point after the switch acts, the fault isolation range is expanded; 2) If the area between the two switches does not contain the original fault point after the switch is operated, the system will locate and isolate the fault twice based on the interval between the trip breaker and the switch after the action.

If the system can not locate the fault point, the contact switch can be closed at this time. If the system can judge the fault point, the fault area can be determined by referring to the secondary fault location process; If the system is still unable to determine the fault point, it needs to deal with the fault manually.

3.2.3. Analysis during recovery process

After fault isolation, the distribution network can be divided into fault and non-fault areas. Ignoring the automatic fault location and isolation time. Let $t_1$, $t_2$, $t_3$ represent manual fault search time, manual fault isolation time and fault repair time, according to the failure time during fault process, the load points can be divided into five types in Tab.1.

| Load type | Outage time | Load type | Outage time |
|-----------|-------------|-----------|-------------|
| A         | $t_2$       | D         | $t_2+t_3$   |
| B         | $t_1$       | E         | $t_1+t_2+t_3$ |
| C         | $t_1+t_2$   | -         | -           |

4. RELIABILITY ASSESSMENT OF DISTRIBUTION CPS

4.1. Reliability indices

In this paper, the System Average I Duration Index (SAIDI) and Expected Energy Not Supplied (EENS) are taken as reliability indices, which are expressed by $T_{SAIDI}$ and $E_{EENS}$ respectively.
\[ T_{SAIDI} = \sum_{i \in R} p_i N_i \]  
\[ E_{EENS} = \sum_{i \in R} p_i c_i \]  

Where \( p_i \) is the probability of system state \( i \), \( N_i \), \( t_i \), \( c_i \) are the number of outage users, outage time and load loss under state \( i \). \( R \) is the set of all system states.

4.2 Steps of reliability assessment

The evaluation steps based on Sequential Monte Carlo Simulation method[12] is as Fig.3.

Fig. 3. Reliability assessment flowchart

5. CASE STUDY

The improved IEEE33 bus distribution system is used for example analysis. The number in Fig.4 (a) represents the location of each component of the cyber system, and the number in Fig.4 (b) represents the load node of the physical system. The reliability parameters of each element are shown in Tab. 2.
Fig. 4. Reliability assessment flowchart

Tab.2. Reliability parameter of cyber elements.

| element         | Failure rate | Repair time/h |
|-----------------|--------------|---------------|
| feeder          | 0.065        | 5             |
| communication line | 0.004      | 24            |
| switch          | 0.05         | 12            |
| IED             | 0.06         | 12            |
| server          | 0.0013       | 8             |

5.1. Simulation results
The simulation period is set as 100 years, and the reliability indexes without considering information disturbance and considering information disturbance are calculated as shown in Tab.3.

Tab.3. Calculation result of indices.

| Indices                        | $T_{SAIDI}$ | $E_{EENS}$ |
|--------------------------------|-------------|------------|
| No cyber disturbances          | 1.98        | 7.35       |
| Considering cyber disturbances | 4.65        | 17.27      |

It can be seen that when the influence of cyber disturbances are taken into account, the system reliability is greatly reduced, and $T_{SAIDI}$ is increased from 1.98 to 4.65, an increase of 134.85%. It can be seen that the influence of cyber system on physical system cannot be ignored.

5.2. Influence of different cyber disturbances on system reliability
(1) impact of cyber attacks on system reliability

In order to analyze the impact of different cyber attack objects on the system reliability, the calculation is divided into three cases below, and the results are shown in Tab.4.
Tab.4. Reliability indices with different cyber attack objects.

| objects     | $T_{SAIDI}$ | $E_{EENS}$ |
|-------------|-------------|------------|
| Master station | 0.23        | 0.85       |
| One IED     | 2.34        | 8.69       |
| Two IEDs    | 1.11        | 4.14       |

It can be seen from Tab.4 that the impact of the cyber attack object on the system reliability is from one IED to two IEDs and the distribution master station in order from large to small, indicating that for the information layer with more points of action, in this information layer, choosing the method with higher success rate to carry out cyber attack will cause greater economic losses to the system.

In order to study the impact of specific IED attacks on system reliability, based on the two situations of normal operation and failure of the physical system, various scenarios of information attacks on one IED and two IEDs are calculated separately. The types of scenes are shown in Tab.5, the results are shown in Fig. 5.

Tab.5. Scenarios division of cyber attacks IED.

| attack type | Scenario |
|-------------|----------|
| One IED     | 1  IED1 | 2  IED2 | 3  IED3 | 4  IED4 | 5  IED5 | 6  IED6 |
| Two IEDs    | 1  IED2 | 2  IED3 | 3  IED4 | 4  IED5 | 5  IED6 | 6  IED7 |

(a)attack one IED

(b)attack two IEDs

Fig. 5. SAIDI in different IED scenarios with attacks
As can be seen from Fig. 5, for an IED cyber attack, under normal operating conditions of the physical system, the farther away the IED location is from the bus of the substation, the smaller its impact on system reliability. In the case of a physical domain failure, the farther away the IED position is from the bus of the substation, the greater its impact on system reliability. For cyber attacks two IEDs, whether the physical system is normal or failure, the longer the distance between the two IEDs in the attacked IED combination, the greater its impact on reliability. Therefore, it can provide a reference for different IED's vulnerability defense resource investments.

(2) Impact of cyber element failure on system reliability

In order to analyze different types of cyber element failure on reliability indices, the increase percentage of outage time caused by each type of cyber element failure is used to express the effect, as shown in Fig.6.

![Fig. 6. Impact of different failure types of cyber elements on reliability indices](image)

As can be seen from Fig.6, different cyber element types have different degrees of impact on system reliability. Among them, IED and switches have a greater impact on system reliability, and system investment needs to focus on the availability of such elements to improve construction. Communication lines have less impact on system reliability, indicating that the existence of backup paths reduces the impact of communication line failures on system reliability, and because the server has adequate protection measures, its failure probability is the smallest, so the impact on system reliability is minimal.

### 6. CONCLUSION

Based on the structure of the cyber distribution power network system and the centralized control scheme of the master station, this paper analyzes the impact of the disturbance factors of the cyber system on the normal operation and fault handling of the physical system, and establishes a reliability evaluation model for the distribution network CPS. Simulating by an example, the results reached the following conclusions.

1) There are many factors that cause the failure of cyber systems, and they usually affect each other. Therefore, it is necessary to analyze the impact of the failure on the reliability of the distribution network CPS from the perspective of the overall cyber system.

2) The impact of different cyber element failures on system reliability. In addition, Power grid construction can focus on the investment in the impact of high reliability of the system of equipment, such as IED and switches.

### References

[1] Xue W, Wu T. Active Learning-Based XGBoost for Cyber Physical System Against Generic AC False Data Injection Attacks[J]. IEEE Access, 2020.
[2] Huang T, Pi R, Bompard E, et al. Analysis and Visualization of Natural Threats Against the Security of Electricity Transmission System[J]. The Scientific Bulletin of Electrical Engineering Faculty, 2017.

[3] Shi L, Jian Z. Vulnerability Assessment of Cyber Physical Power System Based on Dynamic Attack-defense Game Model[J]. Automation of Electric Power Systems, 2016.

[4] Ansari O A, Chung C Y. A Hybrid Framework for Short-Term Risk Assessment of Wind-Integrated Composite Power Systems[J]. IEEE Transactions on Power Systems, 2019.

[5] Chen L, Yue D, Dou C, et al. Evaluation of cyber-physical power systems in cascading failure: node vulnerability and systems connectivity[J]. IET Generation, Transmission & Distribution, 2020.

[6] Guo J, Zhao T, Liu W, et al. Reliability Modeling and Assessment of Isolated Microgrid Considering Influences of Frequency Control[J]. IEEE Access, 2019.

[7] Barani M, VV Vadlamudi, Heegaard P E. Reliability analysis of cyber-physical microgrids: Study of grid connected microgrids with communication-based control systems[J]. IET Generation, Transmission and Distribution, 2020.

[8] Shobhana S. Refining Bogus Data in Wireless Sensor Network Using Non Repudiation and Enrouting Filter Mechanism[J]. Ijetae Com, 2014.

[9] Liu H, Sadygov R G, Yates J R. A Model for Random Sampling and Estimation of Relative Protein Abundance in Shotgun Proteomics[J]. Analytical Chemistry, 2004.

[10] Wang R, Zhang C, Huang H, et al. An algorithm approach to optical true time delay pool enabled centralized control beamforming for wireless base station[C]// 17th International Conference on Optical Communications and Networks (ICOCN2018). 2019.

[11] Amjadian A, Fereidunian A. Remote Control Switch Deployment to Improve Power Distribution Systems Resiliency: An MILP Formulation[C]// 2019 Smart Grid Conference (SGC). 2019.

[12] Sankarakrishnan A, Billinton R. Sequential Monte Carlo simulation for composite power system reliability analysis with time varying loads[J]. IEEE Transactions on Power Systems, 2002.