# Substation communication network architecture evaluation Based on the destructive nature of reliability and survivability

**Meng Yin[1], Jing Zeng[2], Gang Cheng[2] and Zhifang Wang[3]**

*1. China Mobile Group Design Institute Co., Ltd Beijing Branch*
*2. State Grid ZiYang Power Supply Company*
*3. China Electrical Power Research Institute*
*Beijing , P.R.China*

***Keywords:*** Communication network architecture；Anti-destroying ability；survivability；effectiveness

**Abstract:** Wide-area power system reliability research contained within the substation and transformer substation network communication between the wide area communication network reliability research. Substation is the basic component of power wan system based on the substation building local area network is a point in the power wan system, is composed of a number of such points through the trunk communication network constitutes the wide-area communication network of electric power system. Substation communication network must meet the requirements of reliability and real-time performance. Anti-destroying ability, survivability and effectiveness is the basic measure of network reliability research. Anti-destroying ability and survivability study mainly from the perspective of network topology, effectiveness in their part on the basis of considering the demand of business performance, from the perspective of network availability, the reliability of the entire network measure are given.

## 1.Introduction

Wide-area power system reliability research contained within the substation and transformer substation network communication between the wide area communication network reliability research. Substation is the basic component of power wan system based on the substation building local area network is a point in the power wan system, is composed of a number of such points through the trunk communication network constitutes the wide-area communication network of electric power system. Therefore, the reliability of substation communication network is an important factor decided to wide-area communication network reliability. Substation communication network must meet the requirements of reliability and real-time performance. Reliability refers to the requirements of the network node sends an important message not due to the competition for resources of multiple nodes collision or lost due to other reasons, and packet loss can be transmitted retransmission methods to ensure reliable. Refers to the real-time demand per unit time should satisfy within the substation communication network transmission of information, especially the event of a failure communication requirements. Therefore, it is necessary to research and evaluation on the performance of the network, and then according to the requirement to select the appropriate network structure, configuration of network parameters, and the appropriate network communication protocol. And network topology is one of the key factors of communication network reliability and real-time performance. Due to the power grid is a complex network system, if some key node is destroyed, could trigger a cascading jump, eventually even may cause the electrical system of large area of paralysis.

## 2 Metric analysis

Anti-destroying ability, survivability and effectiveness is the basic measure communication network reliability research. Anti-destroying ability and survivability study mainly from the perspective of network topology, effectiveness in their part on the basis of considering the demand of business performance, from the perspective of network availability, the reliability of the entire network measure are given. Literature points out that network validity and reliability are two different concepts. Reliability only consider the failure rate of network components, regardless of the repair rate, however, the effectiveness of the network into account both failure rate and repair rate, therefore, with the said network performance is much more comprehensive effectiveness.

### 2.1Anti-destroying ability to measure

First, Uncertainty measure Anti-destroying ability is usually determined by the reliability of the two measures - sticking together and connectivity, it is from the perspective of network connectivity to describe the influence of network topology structure of communication network reliability. Connectivity is directions of connectivity, network is not connected to remove the minimum number of nodes, the minimum node cut set corresponds to the network. For a connected network, define the connectivity to break let all pathways between node $(x, y)$ pair needed to remove the minimum number of nodes, the network connectivity for

$$CN = \min_{i,j} \lfloor CN_{ij} \rfloor \tag{1}$$

Cohesive degree refers to the connectivity and edge is the minimum number of edges to network is not connected to remove, the minimum link cut set corresponds to the network. For a connected network, the definition of cohesion to disconnect between a pair of node $(i, j)$ all the path needed to get rid of the minimum link number, the network of cohesive degrees for:

$$CH = \min_{i,j} \lfloor CH_{ij} \rfloor \tag{2}$$

Second, random measurement

Uncertainty measurement analysis and calculation of only considering the network topology, without considering the influence of links and nodes, its advantage is simple calculation, the disadvantage is that don't consider the reliability of the network elements themselves, so you can't fully reflect the actual situation of the whole system. The random measurement is different, it not only consider the topology of the network, also considers the node and the influence of the random variation of link reliability of structure. Usually, the analysis of random anti-destroying ability is based on the analysis of the connectivity between nodes. But because the network nodes in between a large number of circuitous path, therefore, based on the connectivity of the randomness of the anti-destroying ability analysis and reliability analysis, need to compute complex conditional probability, the precise solution is very difficult. Describe anti-destroying ability evaluation method based on node will not only consider the network structure, at the same time, considering the influence of nodes and links, and compared with other methods, this method not only reduces the computational complexity, simple and effective. The main steps of the method described below:

(1) Anti-destroying ability of the whole network is the average of all nodes anti-destroying

ability.

$$I = \frac{1}{n}\sum_{i=1}^{n} I_i \tag{3}$$

Among them, on behalf of the node $V$ , anti-destroying ability, namely

$$I_i = 1 - \prod_{j=1}^{I_i} (1 - r_{ij} r_n^2) \tag{4}$$

## 2.2 Survivability measure

Often like network topological structure of internal nodes in the network failure or external attack is not easy to damage, even to the damage to the network, also wants the rest of the network should still have certain ability to connect, to realize the restructuring of the network topology. In the research on the vulnerability of network, the above mentioned connectivity is the network connectivity is the most basic measure, it can only reflect the network to the difficulty of the destruction, and to the extent of the damage and destruction of network after the rest of the network connecting ability assessment serious deficiencies. In order to solve such problems, in 1978, Jung first suggested a Number of discrete (Scattering Number) concept, 1987 Barefootli23] proposed the Integrity (Integrity) index, Cozzens, etc in 1995 degrees (Tenacity) toughness index is put forward. A vertex set ", and five edge set, both of a simple network graph $G(7, f)$, *S* network graph *G* point cut, "said from *G* interrupt some rest after cut the number of nodes in the largest connected component of network, from *G* interrupt some rest after cut set network on the number of connected component. $I(G)$, $S(G)$ and $T(G)$ respectively complete degrees, discrete and spread three indicators, their specific expression is:

$$I(G) = \min_{S \subseteq V}\{|S| + M(G-S)\} \tag{5}$$

$$S(G) = \max\{\omega(G-S) - |S|\} \tag{6}$$

$$T(G) = \min\left\{\frac{M(G-S) + |S|}{\omega(G-S)}\right\} \tag{7}$$

The above indicators from different angles describe the network topology of vulnerability. Through the above three defined type, as long as know in the network, $T(G), S(G)$ and $I(G)$ can be obtained at the beginning of the number of discrete, integrity and degrees of three indicators. Point cut set describes a fault let the ability of interconnected networks, which reflects attack network cost. To express the degree of difficulty of restructuring its value, the greater the show from *G* interrupt some rest after cut set in the network needs to reconstruct the more subnet, so it's quite difficult restructuring of the entire network. From $G, \omega(G-S)$ show that interrupt some rest after cut set *S* network in the largest connected component of the number of nodes in the order, it reflects the remaining network communication ability can achieve the extent of its value, the greater the residual network interconnection, the greater the range of the remaining network that the greater the size of normal communication. Is between each other constraints, however, and their calculations have proved to be NP hard problem. Through the study of toughness index, it contains a $S, M(G-S)$ and $\omega(G-S)$ three parts.

The computation of the topological structure of the degree of sex is to adopt exhaustive method, less in the node is relatively simple, along with the increase in the number of nodes, the calculating process of this algorithm's mad, and the amount of time complexity exponentially with the increase of the number of nodes, to solve the long running time and low efficiency. When the number of nodes in the network is *N*, the algorithm's time complexity is very high. And the spread of the algorithm above is only according to the structure itself, does not consider the reliability of node, the node into consideration the reliability analysis of network survivability.

Set network node number is $N$, the number of edges between nodes for the *E*, both formed a large network $G=(V,E)$.Hop count between nodes refers to the shortest link between two nodes connection number; And node $I$ one hop away from all the nodes and its connecting link between the nodes and node $I$, is formed together with the number of node $I$ apart a jump jump. Hypothesis is the biggest jump from node $I$, $M$ or $m$ and all of the nodes are maximum hop count to $I$.Define jump surface nodes to jump $m$ to $m+1$ surface on the number of links between nodes normalized factor to $\eta_m$, it reflects each node and two adjacent to jump in-plane link connection between nodes.

$$\eta_m = \frac{n_{m+1}}{N+1} \frac{l_m}{n_m n_{m+1}} = \frac{l_m}{n_m (N-1)} \tag{8}$$

Type $\eta_m$ (8) reflect the value, the greater the jumped surface nodes in the network's largest jump from $M$ is smaller, so the more circuitous route between nodes, and the higher the importance;Due to the more circuitous route between nodes at the same time, the network nodes in the average maximum jump away from the smaller $M$, therefore, the network topology anti-destroying ability is better.So $\eta_m$ values reflect the network nodes between the connected reliability, and network topology anti-destroying ability.

The introduction of jump surface nodes can reflect circuitous routes between nodes, thus further puts forward the concept of accumulation point group. Accumulation point group refers to a certain node within adjacent jump surface all nodes as well as a collection of interconnected link together. Accumulation point at the center of the node is called poly nuclear, and poly nuclear the same hop away from all the nodes to a surface, surface within all link called gathering, nuclear power is gathering point of degree, accumulation point mass of the structure of the star shape. Based on the definition of cluster point group, accumulation point group survival degree is refers to the surface of nuclear and gathering all the nodes between the connected probability, thus, its survival degree expression is:

$$S_i = p_i \sum_{m=1}^{i} P_{im} \frac{l_{im}}{n_{im}(N-1)} \tag{9}$$

Entire network degree *S* expression for survival:

$$S = \frac{1}{N} \sum_{i=1}^{N} \alpha_i S_i \tag{10}$$

## 3 Analysis of examples

### 3.1 Anti-destroying ability analysis

Against destroyed by numerical analysis, anti-destroying ability measurement uncertainty in the measurement using connectivity analysis, random measure anti-destroying ability based on the node analysis method.

(1) star, ring and star - ring topology connectivity.

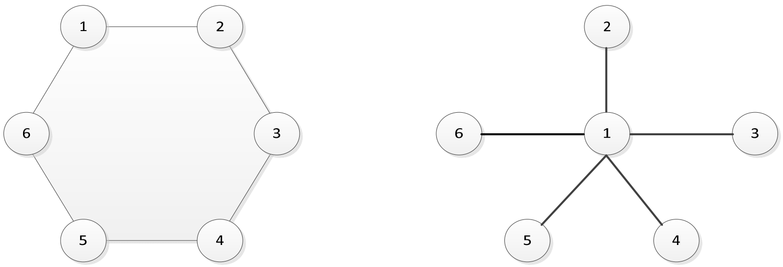

Figure 1 different topology connectivity

Using the calculation method of connectivity, easy to get four kinds of structure connectivity respectively 1, 2, 2, 3, and their structure diagram as shown in figure 8.They are in the same way by six structure connectivity, respectively, 1, 1, 2, 2, 1 and 2.The reliability of the results and the analysis results are consistent. Therefore, the connectivity of the calculation is simple and effective, from the perspective of connectivity can roughly judge the reliability of the topology, this saves a lot of reliability calculation, especially for high voltage level, equipment more substation meaning is greater. However, the results also show that often have different structure with the same connected situation.

Therefore, in the same connectivity topology, how to further determine the reliability of their more practical significance.

(2) star, ring and star - to measure the randomness of the ring topology

First, star and ring topology analysis of the contrast

Based on existing equipment to improve the substation communication network anti-destroying ability, thus the optimized network topology structure makes it have high anti-destroying ability as much as possible. Assume that all nodes in the network and link reliability for *r,* comparing the two most common topologies, anti-destroying ability of star and ring structure.

Listed in table 1 when the reliability of node and link from 0.1 to 0.9, anti-destroying ability numerical star and ring network structures, the graph as shown in figure 2.

Table 1 star and ring topologies anti-destroying ability

| Reliability | Anti-destroying ability | |
|---|---|---|
| | ring | star |
| 0.1 | 0.001999 | 0.001665 |
| 0.2 | 0.015936 | 0.013228 |
| 0.3 | 0.013228 | 0.043817 |
| 0.4 | 0.123904 | 0.100263 |
| 0.5 | 0.234375 | 0.185349 |
| 0.6 | 0.385344 | 0.297301 |
| 0.7 | 0.568351 | 0.432098 |
| 0.8 | 0.761856 | 0.588721 |
| 0.9 | 0.926559 | 0.773923 |

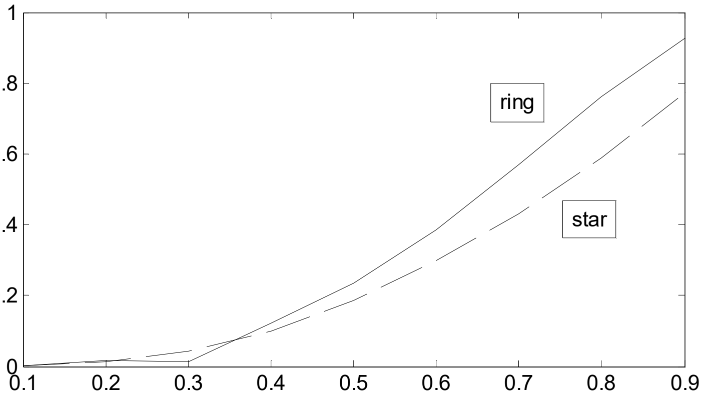

Figure 2. star and ring topologies of invulnerability

Real network node and link reliability is far higher than 0.9, according to the below as shown in table 2 node and link reliability value from 0.99 to 0.999, the calculation of actual power system communication network anti-destroying ability, the graph as shown in figure 3.

Table 2 star and ring topologies anti-destroying ability in actual power system

| Reliability | Anti-destroying ability | |
|---|---|---|
| | ring | star |
| 0.99 | 0.999118 | 0.975249 |
| 0.991 | 0.999284 | 0.977702 |
| 0.992 | 0.999433 | 0.980160 |
| 0.993 | 0.999565 | 0.982622 |
| 0.994 | 0.999680 | 0.985090 |
| 0.995 | 0.999777 | 0.987562 |
| 0.996 | 0.999857 | 0.990040 |
| 0.997 | 0.999919 | 0.992522 |
| 0.998 | 0.999964 | 0.995010 |
| 0.999 | 0.999991 | 0.997502 |

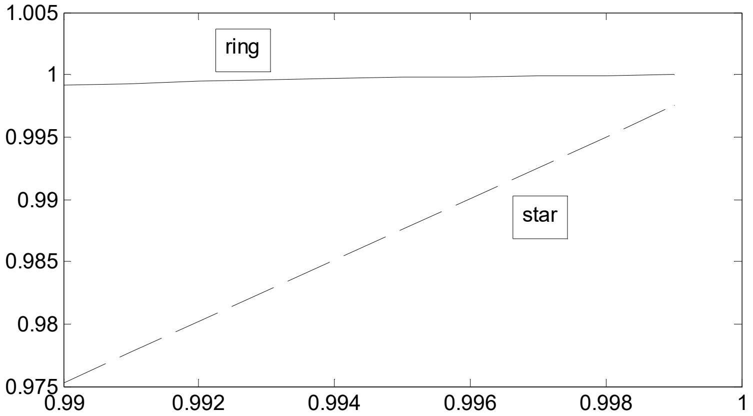

Figure 3 star and ring topologies anti-destroying ability in real power system

Second, ring, and star - ring topology analysis of the contrast.

The above example has been clear about the ring structure anti-destroying ability better than the star structure.Below the ring and star - ring topology anti-destroying ability calculation comparison.

As shown in figure 6 to 8, the structure has two core nodes, and each node has six link connected with them.Therefore, anti-destroying ability as the core node

$$I_1 = I_2 = 1-(1-r^3)^6 \tag{11}$$

The rest of the four nodes is only 2 link is connected with the, then

$$I_3 = I_4 = I_5 = I_6 = 1-\left(1-r^3\right)^2 \tag{12}$$

### 3.2 Survivability analysis

Survivability system is an important feature in the face of the invasion, fault and emergencies when still can provide basic services.Is the core of the concept of survivability in the operational system determine the critical nature of basic services and support services.In order to ensure to provide core services, system can survive must have four key attributes.As shown in table 6 and 3, respectively called: Resistance (hold), identification.

Table 3 can survive system properties

| The key properties | Describe | Example |
|---|---|---|
| Against attacks | Resist attack strategy | Safety certification<br>Access control<br>Encryption<br>Information filtering<br>System diversification<br>Function of independent |
| To identify intrusion behavior | To identify intrusion behavior strategies and to evaluate the degree of danger | Intrusion detection<br>Integrity testing |
| After the invasion of service recovery | Limit damage, save the hazard information.During the system operation maintenance or save the basic service strategy | Redundant part<br>data backup<br>System backup and restore<br>The emergency plan |
| To improve and upgrade the system, in order to reduce the influence of future attacks | According to the invasion of the knowledge of system survivability improvement strategies | To join the new intrusion recognition model |

Table defines some against common attacks survivability strategies, some of which improve survivability technology borrowed from other areas, such as safety, fault tolerance, etc.

In the field of resisting attacks, could use some technology.Using user authentication mechanism, only approved users can access the system, it involves simple passwords and password combination, specific method such as bioassay.Access control can be applied to the system access, a single program or data resources.Access control is a trusted operating system, enforce automatically reject or accept a user access strategy.Encryption can be within a system or the system communication between protect data from monitoring or capture.Now confidential technical enough to resist all kinds of feasible way of violent attacks, so it is a kind of effective means of defense.Encryption technology can also be applied to the authentication and integrity checking, etc.Information filtering is a typical application in transmission system boundary to restrict access to the system.The message filter can be designed to prevent news associated with known attacks.System diversity combining redundant execution unit, increased the difficulty of the attack.Defensive coding can make the program to avoid wrong information input processing.Functional independence as much as possible to avoid the dependence between service, thereby reducing the likelihood of being attacked.Sharing a processor service between depend on each other because of the CPU and memory resources.Maybe they also share a disk or network adapter, and other resources.Likely a processor through exclusive DOS attack by these resources for other machines, which can lead to paralysis of the whole system.Quota mechanism of sharing resources independence requirements, it can be extended to the physical separation of the system function.

In the field of the invasion of recognition, intrusion detection systems are usually looking for evidence of the known attack model, or normal system behavior benchmark model is used to distinguish between potential attacks.System audit and application logs is check the invasion of sources of information.At present, the system will appear the omission phenomenon, especially for those novel attacks, as well as high rate of false positives.Integrity check can detect those who are protected to modify system files and data.This check using the checksum or password first signature generate a protected files benchmark model, and then periodically compare to the file.Using these techniques, the system's ability to fight against will strengthen greatly, in practice, can be combined with a variety of means against the invaders and sudden accidents.

## 4. Conclusion

For recovery, when a devastating attack or fault is found, it is necessary to immediately take measures to restore basic services, eventually restore all of the service.Redundancy technique is the key to face failure maintenance of all services, when a component after paralysis, redundant components can ensure the normal operation of the task.In some cases, the key data backup is the main way to get back.When basic services is to use the database and so on, can be in other server running on the backup database at the same time, the core data real-time backup.Real-time backup all your data resources, as well as in the original or other platforms to recover the data mechanism constitutes the key part of the recovery strategy.To modify files after closing, it is necessary to file backup, as well as backup operation process.Other cases, the daily or weekly backup should be enough.When the system is under attack or after failure may be dynamic configuration system, the core service from the attack of components transferred to other can run a, to avoid as far as possible to reduce the core in the process of service.Survivability improvement is the hardest part of a system, make its robust enough, can resist various attacks and invasion ever seen.Because the attacker is always looking for new easy to attack the weaknesses, the defender must be based on the analysis of the original attack, create new measures to prevent, anticipate new attack possible direction.

## References

[1]CAO Na,LI Gang，WANG Dong-qing.Key technologies and construction methods of smart substation[J].Power System Protection and Control,2011,(05):63-68.

[2]ZHAO Jian-li.Research on real time and reliability of communication system in Intelligent Substation[D].Hebei University of Technology,2012.

[3]Wei Bin. Research on network security architecture of new generation intelligent substation [J]Electrotechnical Application,2015,(S2):693-697.

[4]Yang Bing-lu.Research on substation communication network architecture and its key technologies [D].Chongqing University,2015.

[5]Zhang Jia-zhu,Zhang Zhen-liang.Research on reliability of network architecture in smart grid communication system [J].Electric power information, 2010, (07): 229.

[6] Zhu Ma, Li Yong, Zhang Jian-min, et al. based on OPNET digital substation DoS attack modeling and Simulation[J]. Electrical and mechanical engineering, 2017, 34 (3).

[7] Yang Li, Lin Mao-sheng, Zhang Hong-wei, Deng Xiao-lei,Deng Guo-min. Medium voltage distribution network invulnerability evaluation of typical network structures [J].Automation of electric power systems. 2012 (01).

[8]Wang Xiang-qun, Huang Zhi. The security of communication technology in Intelligent Substation[J].Power system communication. 2012 (08).

[9]R. Bulbul, P. Sapkota, C. W. Ten, L. Wang and A. Ginter.Intrusion Evaluation of Communication Network Architectures for Power Substations[J]. in IEEE Transactions on Power Delivery, 2015:1372-1382.

[10]I. Ali and M. S. Thomas.Substation Communication Networks Architecture[J]. 2008 Joint International Conference on Power System Technology and IEEE Power India Conference, New Delhi, 2008: 1-8.