변전소 IED의 보안과 신뢰성에 관한 고찰

관창, 한승수, 이승재
명지대학교 차세대전력기술연구센터

Analysis On Security and Dependability for IED System in SAS

Qiang Guan, Seung-Soo Han, Seung-Jae Lee
Myongji University, Next-generation Power Technology Center

Abstract - As a general rule for evaluating dependability of a system, reliability is commonly considered which barely pays attention to the system behavior, however the estimation is based on the assumption of a fault-frost system, which may be impracticable and inaccurate especially for complicated system. This paper introduces a security and dependability integrated approach to analyze the availability of a fault-active system both from dependability and security points of view. Two fault modes involved are discussed about the impairment to the system reliance. The approach can be well applied to estimate and quantify the attribute of system robustness with the help of Markov chain process, which is good at solving status related problem. The comparison result between dual system and IEC61850-based almighty backup system is shown to support the suggested approach.

1. INTRODUCTION & BACKGROUND

Reliability/dependability analysis, applying to two-status system as shown in some material, has played major roles in substation protection technology. Actually, the estimation is based on the assumption of a fault-frost system, where the component will announce his fault and terminate after a fault. Nowadays the fault-active system, where the fault component will still be active and ready to puzzle other ones, is often involved and considered. It arise the third status, which can hardly be analyzed merely from a reliability/dependability point of view. In section 2, the security integrated reliability model will be discussed, and the secure availability measurement is introduced. System analysis is shown that how we can apply the model to improve the system from two aspects.

As the development of substation system protection, a large number model of security and dependability was investigated. Erland Jonson was one of the famous to put forward the combined model [1] [2] [3]. It inherits from traditional dependability model and some viewpoints of security concepts are appended. In this paper these models is embodied in substation system protection, while some unnecessary detailed is neglected with some helpful assumptions.

2. RELATED WORK

2.1 Security Aspects Considered In A Reliability Mode

Security refers to the system's ability to prevent the system availability from unauthorized information access or mistake operation. Commonly security is decomposed into three aspects: *confidentiality*, *integrity* and *availability*[1]. Here Integrity reflects the influence from the environment factor, e. g. undesired signal or noise.[4] Confidentiality presents the system ability of denial of service to non-user. As well as availability denotes the ability of delivery service to user. Nowadays security settings of firewall and filters can basically secure the integrity and access control, cryptogram and VPN (virtual private network) have already been used to improve the performance of confidentiality. As it is shown in figure 1 the security issue also contribute the final reliability of the system. Therefore, the output of the system to the authorized user should be composed of two aspects, defined Secure Availability, which denotes the system behavior of anti-undesired-operation, as well as Dependent Availability, which denotes the reliability of delivery-of-service. In order to guarantee the system availability /reliability, both two availabilities are need. Fault from either security aspect or dependability aspect can induce system failure.

System availability = Dependent availability · Secure availability

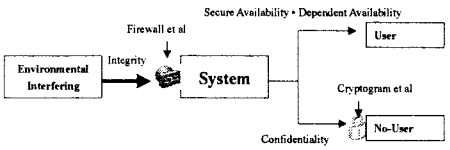

Fig.1 The Security Factors Imbedded Diagram

Usually there are two major failure modes in protection system: no-operation and undesired-operation.[5] If a normal protective device detects a failure, the device will convert to a normal-trip condition, otherwise, it will come to a no-operation condition or undesired-operation condition, and both of them will case cascading outages to the system. This three-status model we name it fault-active model.

Former studies simply assume that the protection system is on an idealized condition that the protection system is free of failure. From reliability point of view these two failure modes are treated compatibly as an unavailable status. This kind of model we call it a fault-frost model. Sometimes that may simplify the analysis of system, since the number of status has been reduced from 3 to 2, even though, for actual application, it is not accurate enough for helping finding the vulnerability of the system.

2.2 Dual System analysis

In substation system, dual IED (Intelligent Electronic Device) model is widely made use of. As it is shown in Fig2, the Bay IED represents the task-carrying component, while the OR gate works as a protective device.

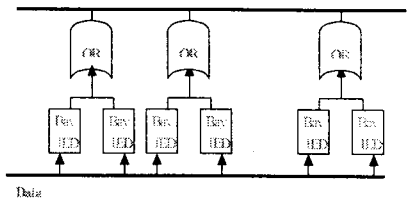

Fig 2 Dual System Model

2.2.1 Fault-active dual system

Two IEDs transact the same task in parallel. Each performs a backup to the other. In the end, an OR gate is implemented for managing the trip signals from each IED. Totally, N pairs compose the system. As we see, considering that it is a real application in substation. Three statuses of IED, normal operation, no-operation, undesired-operation, have to be considered. Therefore, the security issue, named SA (Secure Availability), represents the probability of anti-impairment caused by undesired-operation, is appended into the model. The dependability issue, named DA (Dependent Availability), represents the probability of anti-impairment of no-operation.

The state space diagram of fault-active dual system is shown in Figure 3:

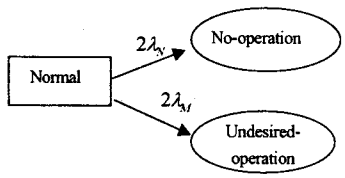

Fig 3 State Space Diagram of Fault-active Dual System

Either IED, encountering either fault operation status, will trigger a paralysis of power supply.

The following equations using Markov method is associated with Fig 3:

$$\frac{dP_{nomal}(t)}{dt} + (2\lambda_M + 2\lambda_N)P_{nomal}(t) = 0$$

$$\frac{dP_{no}(t)}{dt} - 2\lambda_N P_{nomal}(t) = 0$$

$$\frac{dP_{uo}(t)}{dt} - 2\lambda_M P_{nomal}(t) = 0$$

$$t = 0, P_{nomal}(t) = 1, P_{no}(t) = 0, P_{uo}(t) = 0$$

Where:

λ_N Is the failure rate of no-operation

λ_M Is the failure rate of undesired-operation

Thus, the system Secure Availability and Dependent Availability is given by:

$$DA(t) = 1 - P_{no}(t)$$

$$SA(t) = 1 - P_{uo}(t)$$

$$System\ Availability = [DA(t) \times SA(t)]^N$$

2.3 ARET (Agent-based Reliability Enhancement Technology) System Analysis

Considering that the efficiency and the reliability of dual system are very low (2N IEDs work for N functions), an error detecting process is designed for evaluating the reliability with almighty backup IEDs, which can perform any IED in the system. We call it ARET system.

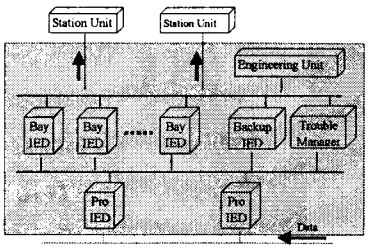

Fig 4 ARET System

The system provided----Integrated *M*: *N* protection switching (*M* switchable almighty spare IEDs for *N* working IED) is a three-layers protective system shown in Fig 4. Data from line will be put in and some protective policies are executed on the lower two layers. The output is display on top layer in manner of reports and alarms.

2.3.1 Error detecting process of ARET system

In ARET system a Trouble Manger is implemented. Fig 5 shows the process of error detecting. Within the process, tested IED is replaced by the almighty IED temporally and goes into a diagnostic state. First a test request pattern with error data will be sent to testing IED from Trouble Manager, if there comes a silence, we can simply consider the testing IED having a no-operation failure, because the IED has already slept from a fault, and then the IED will be isolated by the backup IED, otherwise, returning a correct trip signal denotes that it is normally working. Secondly, Trouble Manger sends a request with normal data, if a trip signal is generated by the IED, we can conform that it is working under a undesired-operation status, it will be isolated at once avoiding further impairment. The fault of undesired-operation response may impair the security of the system, since other IEDs cannot differentiate the cheating trip response from a normal trip response. The system is going to de exposed to the risk of cascading outages.

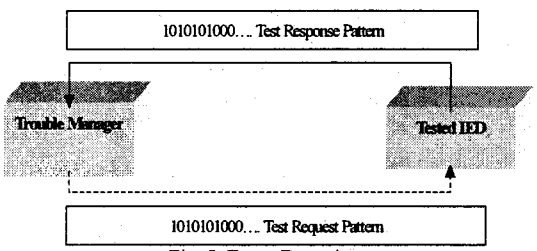

Fig 5 Error Detecting

2.3.2 Availability/Reliability Analysis

The ARET system model is expanded to include the possible states of protection system shown in Fig 8, for simplification, only one backup IED is implemented. So we have the following states:

State 1: N IEDs normally work and Backup IED is off

State 2: TM detects a no-operation working IED and backup IED take the place of it. From then on the backup IED performs equally to the Bay IED.

State 3: TM detects an undesired-operation working IED, then backup IED take the place of it.

State 4: TM detects another no-operation working IED; system fails by a dependability issue

State 5: TM detects another undesired-operation working IED system fails by a security issue.

State 6: A dependability issue caused failure state similar to state 4.

State 7: A security issue caused failure state similar to state 5.

State 8: Backup can't start at all. Before the backup IED is started, it only has no-operation failure rate.

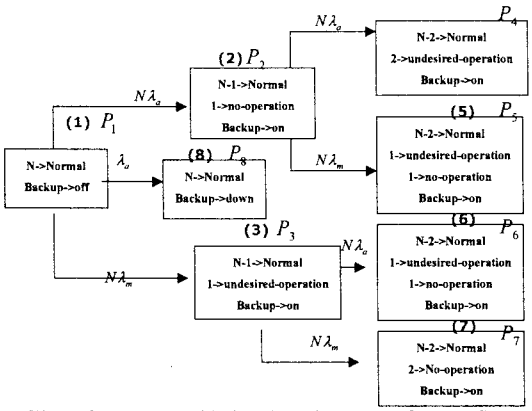

Fig 7 System Considering Security Issues System State Space Diagram

In state 4,state 6,and state 8, system failure comes from a no-operation failure, which is a dependability issue; In state 5 and state 7, system fails because of a undesired-operation failure, which is a security issue. The system Secure Availability and Dependent Availability are given by:

$$DA(t) = 1 - P_4(t) - P_6(t) - P_8(t)$$

$$SA(t) = 1 - P_5(t) - P_7(t)$$

Thus system availability is given by:

$$System\ Availability = DA(t) \times SA(t)$$

Some assumptions are associated:

- Both IEDs are identical and active.
- All the states are independent.
- No fault IED is repaired.
- Failure rate is a constant
- The switch process between bay IED and backup IED is instantaneous
- Both undesired-operation failure mode and no-operation failure mode are always perceptible to the Trouble Manger.
- The diagnosis result is always believable to the user.

With input parameters of $\lambda_m = 2.5752 \times 10^{-4}$[6] $\lambda_a = 3.3602 \times 10^{-4}$[6] the results are shown below:

From the comparison result in Fig 8, the behavior of ARET system is better then traditional dual system with the security integrated dependability model proposed in this paper.

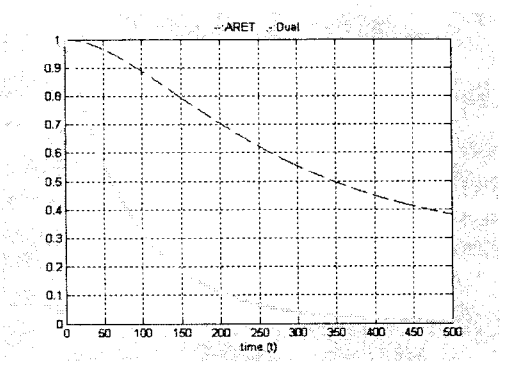

Fig 8 System Availability Comparative Result.

3. CONCLUSIONS

With the development of reliability technology, focuses have already been fixed on the combination of dependability and security, in this paper, the integrated model is attempted to apply to the reliability of substation protection analysis. Any improvement scheme can be divided into two aspects according to corresponding impairments. This analysis method describes a system as a two-inputs and two-outputs black box, which is very conformed to any layers-based system. The two outputs reflect two domains for reliability, the association of the two outputs denotes the final However, in this paper the environment influence and other factors aren't taken in account. It is a little difficult to make all things considered.

Acknowledge

This paper was supported by ERC program of MOST/ KOSEF (Next-Generation Power Technology Center).

[REFERENCE]

[1] Erland Jonsson, "Towards an Integrated Conceptual Model of Security and Dependability", Proceeding of First International Conference on Availability, Reliability and Security (ARES'06).

[2] Erland Jonsson, "On the Functional Relation Between Security and Dependability Impairments".

[3] Erland Jonsson, "An analysis of a secure system based on trusted components". Computer Assurance, 1996, COMPASS '96, "Systems Integrity. Software Safety. Process Security.

[4]National standard of Republic of China, "Performance and testing of teleprotection equipment of power systems command

[5] Xingbin Yu, "A Practical Approach for Integrity Power System Vulnerability Analysis With Protection Failures". IEEE TRANSACTIONS ON POWER SYSTEMS, VOL.19, NO.4, NOVERBER 2004

[6] Weizhong fan, "A New Fault Tolerant Mobile Agent Scheme in IED System" .