Risk Assessment of Power System considering the CPS of Transformers

Long Zhou\textsuperscript{1}, Zewu Peng\textsuperscript{1}, Xindong Liu\textsuperscript{2}, Canbing Li\textsuperscript{3}, Can Chen\textsuperscript{4}

\textsuperscript{1}Guangdong Power Grid Company, Information Department, Guangzhou Guangdong, China
\textsuperscript{2}Jinan University, College of Electrical and the Information, ZhuHai Guangdong, China
\textsuperscript{3}Hunan University, the College of Electrical and Information, Changsha Hunan, China
\textsuperscript{4}Guangdong Power Grid Company, Zhuhai Power Supply Bureau, ZhuHai Guangdong, China

baiom@126.com

Abstract. This paper constructs a risk assessment framework of power system for device-level information security, analyzes the typical protection configuration of power transformers, and takes transformer gas protection and differential protection as examples to put forward a method that analyzes the cyber security in electric power system, which targets transformer protection parameters. We estimate the risk of power system accounting for the cyber security of transformer through utilizing Monte Carlo method and two indexes, which are the loss of load probability and the expected demand not supplied. The proposed approach is tested with IEEE 9 bus system and IEEE 118 bus system.

1. Introduction

With the development of Information Communication Technology (ICT), the interdependence between physical network and information network will be further improved [1-3]. Cyber-physical system (CPS), which is the integration of information systems and physical systems, plays a significant role in achieving smart grid at present. However, CPS brings unprecedented challenges to the network security of the power system. Risks in information network may be transmitted to the physical network, resulting in power equipment malfunction or even blackout [4-5]. For instance, in 2010 Stuxnet virus attacked in Iran's nuclear facilities and thereby engendered the inappropriate operation of the nuclear facilities [6]. Stuxnet targets specifically at programmable logic controllers (PLCs) and modern SCADA. Although power system in China uses a dedicated information network, there are still security risks such as internal attacks and systematic attacks by specialized hackers.

The information networks reliability is not only affected by natural disasters, component failures, man-made operations, etc., but also by the threat of cyber security. Network attackers usually exploit the vulnerabilities and cyber black hole to attack the hardware, software and data. The power system risk assessment considering the information of devices are discussed in [7]-[8]. Two probabilistic indices Power Loss Probability and Expected Demand Not Supplied (EDNS) which measure the risks considering online state of circuit breakers are studied in [9]. The network attacks in power system are analyzed in [10-13]. A kind of test platform of power cyber security, which contained equipment of...
control, communication and physical system, was introduced in [10]. In [11], a new Petri-net construction method is used to model and analyze the collaborative attacks at a device level. A comprehensive anomaly detection method for substation cyber security was proposed in [12]. Reference [13] summarized the information security of protection relays and associated equipment.

Power transformer is one of main equipment in power system. Many monitoring and protection systems are installed to protect transformers. Reference [14] discussed the reliability of protection systems considering the setting values. The setting values of protection systems play an important role in power systems. This paper proposes a power systems risk assessment framework considering device-level information. The typical protection configuration of power transformer is discussed, and Monte Carlo method is utilized to evaluate the risk of power system considering transformer cyber security.

2. Risk assessment framework considering cyber security of transformers

![Fig.1 Structure of power system and cyber security](image)

Cyber attacks mainly occurred in the network layer and application layer in power system. The structure of power system and cyber security is shown in Fig.1. The protection systems in substation could be operated at control center, substations, space layers et al. The cyber attacks could falsify the protocols among the control center, substations, and devices, leading to unexpected risks in power systems. Power transformer, which with lots of protection devices to keep equipment’s safety range, is of the core equipment in substations. Once the setting values and control logics of these protections are attacked illegal falsified, the transformers will outage and serious consequences are followed.
Risk assessment of power system includes reliability and security. Reliability is the ability of power system to meet all load requirements. This paper uses two indexes, LOLP and EDNS, proposed in [9], as reference to measure the reliability. The reliability of power system can be represented as (1)-(2)

\[ L_{LOLP} = \sum_{i=1}^{n} I_f(x)P(x) \]  
\[ L_{ENDS} = \sum_{i=1}^{n} I_f(x)L_i(x)P(x) \]

where \( x \) is the status of power system operation, \( L_i \) is the probability about loss of load in the state of \( x \), \( L_i \) is the minimum load reduction in the case of pulling power system back to a safe operation state. The set of system operation is a state-combination of each transformer running in various status.

As shown in Fig.2, this paper puts forward a risk assessment framework considering cyber security of transformer. The assessment is divided into three parts. In the first part, the relay protection system of transformer is modeled, including the analysis of protection structures of transformer, setting protection parameters and the realization of protection logic. In addition, transformer protection logic control system are build through establishing mathematical models of operating characteristics of various components in the relay protection configuration. In the second part, we simulate network attacks by Monte Carlo method and set the network attack range. The protection parameters within the attack range are selected randomly. Then the changed protection parameters are selected in the logic control system. In the third part, we analyze the updated topology network, and the program will exit if the topology is incomplete. Otherwise the Optimal Power Flow (OPF) is employed to solve the power flow.

3. Protection systems of Transformer
The transformer protection mainly aims at the transformer fault and the abnormal operation state. Transformer faults include internal tank failure and external tank failure. Internal tank failure includes phase faults, earth faults, inter-turn short-circuit and core burning. The external fault of the oil tank
contains the phase to phase short circuit and the earth-connect fault. Abnormal operation state of transformer contains the phase to phase short circuit, earth fault or overload outside the transformer.

Transformer protection configurations contains main protection, backup protection and other types of protections. The main protection includes gas protection and differential protection. Gas protection is a kind of non-electric parameter protection, and consists of light gas protection and heavy gas protection. Early-warning signal is sent out when light gas protection triggered, and heavy gas protection acts on circuit breakers at the both sides of transformer. The differential protection is usually used for internal fault in the transformer. The transformer protection configuration are varied according to specific situation. This paper focuses on normally configuration protection, shown as in Fig. 3. Fig.3 shows five kinds protection configurations of two winding transformer. All protections could disconnect the circuit breakers which located outside of the transformer. Relay 1 is differential protection which detects the magnitude and phase of the current on both sides of the transformer. Relay 2 and Relay 3 are overcurrent protections. Relay 4 and Relay 5 are earth fault protections.

This paper takes the differential protections of RCS-978 protection devices as an example to introduce the protection logic of transformers. RCS-978 protections include differential quick-break protection, steady-state ratio differential protection and power frequency variation differential protection. The working logics are showed in Fig.4. Operate conditions are list in the left side of Fig.4, the logic judgments list in the middle section, and the trip signals are list in right part in Fig.4.

**Fig.3 Relay configuration of power transformer**

**Fig.4 Logic framework of differential relay systems**
In Fig.4, Starting condition (A) of differential quick-break protection is the differential current starting condition, the starting criterion is shown in (3).

\[
\max |I_{d,\phi}| > I_{op,\text{min}} \tag{3}
\]

where \(I_{d,\phi}\) represents three phase differential current. \(I_{op,\text{min}}\) is the starting setting value of differential current according to the setting value of maximum unbalanced current.

The differential quick-break protection criterion device (B) is shown in (4).

\[
I_d \geq I_{s,\text{set}} \tag{4}
\]

where \(I_d = |I_a + I_b|\) and are current of high voltage side and low voltage side. \(I_{s,\text{set}}\) is the value of tripping current setting for instantaneous trip protection.

The operating criterion of steady-state ratio differential protection (C) of two-winding transformers is shown in (5).

\[
I_d > \begin{cases} 
0.2I_{res} + I_{op,\text{min}} & I_{res} \leq 0.5I_e \\
0.75[I_{res} - 0.5I_e] + 0.1I_e + I_{op,\text{min}} & 0.5I_e \leq I_{res} \leq 6I_e \\
5I_{res} - 0.25I_e & I_{res} \geq 6I_e 
\end{cases} \tag{5}
\]

where, \(I_{res} = 0.5(|I_a| + |I_b|)\) is restrained current. \(I_{op,\text{min}}\) is the setting value of minimum operating current. \(0.5I_e\) is the setting value \(I_{\phi \geq 0}\) of restrained current match the first inflexion point, and \(6I_e\) is the setting value \(I_{\phi \leq 1}\) of restrained current match the second inflexion point. \(K_\phi\) is the setting value of braking ratio.

In the discriminant (D) of inrush current, the criteria identifying inrush current by using the double-frequency and triple-frequency of three phase differential current are shown in (6).

\[
\begin{cases} 
I_{d,2} \geq K_{\phi \leq 0}I_{op1} \\
I_{d,3} \geq K_{\phi \leq 1}I_{op1} 
\end{cases} \tag{6}
\]

where \(I_{d,2}\) and \(I_{d,3}\) are double-frequency and triple-frequency of three phase differential current. \(I_{op1}\) is the setting value of differential current of three-phase fundamental. \(K_{\phi \leq 0}\) and \(K_{\phi \leq 1}\) are the restraint coefficient of double-frequency and triple-frequency, respectively.

TA saturation discriminant (E) judges whether TA is saturated by the second and third harmonic content of TA secondary current.

\[
\begin{cases} 
I_{\phi 2} > k_{\phi \leq 0} * I_{\phi 1} \\
I_{\phi 3} > k_{\phi \leq 1} * I_{\phi 1} 
\end{cases} \tag{7}
\]

where, \(I_{\phi 2}\) is the second harmonic and \(I_{\phi 3}\) is the third harmonic. \(K_{\phi \leq 0}\) and \(K_{\phi \leq 1}\) are proportionality constants.

Overexcitation discriminant (F) uses the fifth harmonic of differential current to judge.

\[
I_{d,5} > k_{\phi \leq 0} I_{d,1} \tag{8}
\]

where, \(I_{d,1}\) and \(I_{d,3}\) are fundamental current and the fifth harmonic of per-phase differential current successively.

Protection devices are commonly used to send out alerting signals and tripping signals according to sample values. As shown in Fig.5, \(\{y_1, y_2, \ldots, y_n\}\) is consisted of sampling value, which are uploaded from secondary circuit of current transformer. According to the operating criterion of each element, \(\{y_1, y_2, \ldots, y_n\}\) multiply ratio and actual current \(\{xop1, xop2, \ldots, xopn\}\) are obtained. Setting parameters, which are operational criteria of each element in local control system of transformer relay protection, store in the system in the form of a fixed value \(\{x_{set1}, x_{set2}, \ldots, x_{setn}\}\). Users can set or modify these settings according to the actual situations and applications. Meanwhile, the control center of substation can read and modify these settings through network.
Settings value of transformer protection system are high-value-targets for the network attack. Hackers can falsify these settings xseti through attacking protection system. The protection will tripped as soon as the parameters are falsified, and fault range would expand in this case. Suppose the parameters of differential protection become a target x, shown as in (9).

$$\{x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}\}$$

When transformers operate normally, the circuit breaker status set S for each side of the transformer depends on attack object x.

$$S = f(x_1, x_2, x_3, \ldots, x_{12})$$

When network attackers attack these protection parameters, and the subsets of status set are satisfied, the circuit breakers will be tripped. The criterion of successful cyber attack are shown in (11)-(16).

The tripping criterion of differential-instantaneous-trip protection (11)-(12) can be derived from (3)-(4).

$$\max |I_{d,1}| > x_1$$

$$I_d > x_2$$

Steady-state ratio differential protection (13) can be derived from (5).

$$I_d > 0.2I_{rs} + x_1 \quad I_{rs} \leq x_3$$

$$I_d > x_1[I_{rs} - x_1] + 0.1I + x_1 \quad x_1 \leq I_{rs} \leq x_4$$

$$I_d > 0.75[I_{rs} - x_1] + x_1[x_1 - x_1] + 0.1I + x_1 \quad I_{rs} \geq x_4$$

Criterion (C) which distinguishes internal faults from inrush currents and criterion (D) of TA saturation can be derived from (6)-(8).

$$I_{d,1} \leq x_6 \times x_8$$

$$I_{d,2} \leq x_7 \times x_8$$

$$I_{d,3} < x_9 \times I_{pl}$$

$$I_{d,4} < x_{10} \times I_{pl}$$

Overexcitation criterion (F) can be derived as (16).

$$I_{d,5} < x_1 \times I_{d,3}$$

$$I_{d,6} > x_1 \times I_{d,3}$$

According to the logic of differential protection, status set S of circuit breaker can be represented as (9)-(16) when protection system facing cyber attack. Differential protection devices operate on both sides of the circuit breaker and the two circuit breakers are combined into two states, $S = \{(0,0),(1,1)\}$, where 0 represents tripping of circuit breakers and 1 represents no tripping as shown in Table 1.
According to the protection logic shown in Fig.4, it can be conclude that if the protection parameters are falsified and the formula (11) and (12) are satisfied, the circuit breakers in both side will trip by differential protection.

Tab 1. Breaker sets states after attacked parameters

| Criterion combination | Action device type | Breaker state set |
|-----------------------|--------------------|------------------|
| (14) ∪ (15)          | Differential quick break protection | (1,1) |
| (14) ∪ (16) ∪ (17) ∪ (18) ∪ (19) | Steady-state ratio differential protection | (1,1) |
| Other combination     |                     | (0,0)            |

4. Case study

4.1. Parameters and setting values of differential relays
IEEE 9 bus and IEEE 118 bus system are employed to test the proposed method. The setting value of the transformer protection system mainly includes: device parameter setting, system parameter setting and protection setting value. In this paper, network attack is aiming at the protection system setting values, which include the value of main protection and backup protection. The fixed values and its setting range in main protection, including differential quick-break protection, steady-state ratio differential protection and power frequency variation rate ratio differential protection, are shown in Table 2.

Tab.2 Parameters and setting values of differential relays

| A phase | B phase | C phase | Setting range |
|---------|---------|---------|---------------|
| \( I_{p,m} \) | \( I_{p,m} \) | \( I_{p,m} \) | 0.1Ie~1.5Ie |
| \( I_{e} \) | \( I_{e} \) | \( I_{e} \) | 2Ie~14Ie |
| \( k_{e} \) | \( k_{e} \) | \( k_{e} \) | 0.2~0.75 |
| \((k_{e}, k_{e})\) | \((k_{e}, k_{e})\) | \((k_{e}, k_{e})\) | 0.05~0.35 |
| \((k_{e}, k_{e})\) | \((k_{e}, k_{e})\) | \((k_{e}, k_{e})\) | 0.1~0.5 |
| \( I_{c} \) | \( I_{c} \) | \( I_{c} \) | 0.1~0.5 |
| \( I_{c} \) | \( I_{c} \) | \( I_{c} \) | 1.0~1.7 |
| \( I_{c} \) | \( I_{c} \) | \( I_{c} \) | 0.2Ie |

\( I_{e} \) is the rated current of secondary side of transformer

4.2. IEEE 9 Bus System
IEEE 9 bus system contains 9 busses, 3 transformers, 3 generators and 9 branches. We assume that each transformer is equivalent to two parallel transformers. The transformer T3 between Bus 6 and Gen3 is analyzed as shown in Fig.6. According to the status of circuit breakers on both sides of the two power transformers, system state set \( X \) includes four states that is \{x1, x2, x3, x4\}, represented respectively as: #1main transformer off #2main transformer on; #1main transformer on #2main transformer off; #1main transformer off #2main transformer off; #1main transformer on #2main transformer on.
Assume that the protection parameters of the two transformers are randomly chosen by the attacker, and are falsified successively with 10%, 20% and 30% proportions. 2000 Monte Carlo stochastic simulation are performed on the condition of load fluctuation between 0.7 and 1.2 p.u.. Then the system risk assessment are calculated. Shown as in Fig.7, when the parameters are falsified with 20% proportion in the normal operation state of the transformer, the false tripping probability of the transformer is 0.3175, the change rate of the network topology is 0.548, and the system loss-of-load probability LOLP is 0.1301, and EDNS is 147MW. The final statistical results and systematic risk are shown in Tab. 3.

| Cyber attack Trip probabilities | Probabilities of operation state | LOLP | ENDS (MW) |
|-------------------------------|---------------------------------|------|-----------|
|                              | x1     | x2  | x2  | x3     |      |      |
| 10%                           | 0.2025 | 0.146   | 0.164 | 0.043  | 0.648 | 0.0630 | 121 |
| 20%                           | 0.3175 | 0.238   | 0.220 | 0.091  | 0.452 | 0.1301 | 147 |
| 30%                           | 0.7240 | 0.202   | 0.189 | 0.525  | 0.084 | 0.5595 | 172 |

According to the simulation results, system topology changes in the states of x1, x2 and x3. When load fluctuations, the minimum load shedding in the states of x1 and x2 is less than that in the state of x3. In most cases the power system operation state can not restore to normal operation state when the system is in state x3. With the increase of the attack range, as shown by Tab. 2, the false tripping probability of the transformer in the normal working condition increases as well as the corresponding system risk level.
4.3. *IEEE 118 Bus System*

IEEE 118 bus system contains 118 buses, 9 transformers, 116 generators and 186 branches. The two equivalent parallel transformer between nodes 25-26 are selected, and IEEE118 system also includes four states. Falsify the protection parameters of the two parallel transformers, and Monte Carlo simulation results are shown in Table 4. The LOLP and ENDS index at 20% attack range is shown in Fig.8.

| Attack range | Probability of false trip | Probability of System State | LOLP (MW) | ENDS (MW) |
|--------------|---------------------------|-----------------------------|-----------|-----------|
|              | x1                        | x2                          | x2        | x3        |          |          |
| 10%          | 0.2025                    | 0.142                       | 0.182     | 0.042     | 0.635    | 0.023    | 306      |
| 20%          | 0.3175                    | 0.215                       | 0.213     | 0.099     | 0.473    | 0.379    | 357      |
| 30%          | 0.7240                    | 0.220                       | 0.189     | 0.505     | 0.086    | 0.588    | 382      |

![LOLP](image1.png)

![ENDS(WM)](image2.png)

**Fig.8** Risk value when 20% parameters are changed

According to the simulation results with which the 10% parameters are falsified, the probability that the breakers of two parallel transformers between the nodes trip simultaneously is minimal. When the breakers of single transformer trip and the system is in the state of x1, x2, OPF re-convergent after load reduction and generator output power. With the probability of false tripping increases, LOLP and ENDS increase with load fluctuation.

Compared with the results of the IEEE 9 bus system, when the attack range increases, the LOLP and EDNS grow slower in the IEEE118 node system, indicating that when the system is in the x3 state with a large probability, the system can reduce load to restore the system to a safe operating state. With the increase of the simulation times, the LOLP and EDNS tend to be constant, and the value is related to the influence range of the transformer.

5. **Conclusion**

The cyber security structure of electric power system based on power system are proposed, and an evaluation framework of power system considering equipment level cyber security is presented. A typical transformer gas protection and differential protection are taken as examples to simulate the cyber attack, and the LOLP and EDNS are employed to measure the risks.
Acknowledgements
This work was supported by National key R & D projects intergovernmental special projects (S2016G9107).

References
[1] K. L. Gao, Y. Z. Xin, Z. Li, "Development and Process of Cyber security Protection Architecture for Smart Grid Dispatching and Control Systems," Automation of Electric Power Systems, vol. 39, no. 1, pp. 48-52, Jan. 2015.
[2] Y. J. Cao, Y. D. Zhang, Z. J. Bao, "Analysis of cascading failures under interactions between power grid and communication network," Electric Power Automation Equipment, vol. 33, no. 1, pp. 7-11, Jan. 2013.
[3] J. H. Zhao, F. S. Wen, Y. S. Xue, "Caber Physical Power Systems: Architecture Implementation Techniques and Challenges," Automation of Electric Power Systems, vol. 34, no. 16, pp. 1-7, Aug. 2010.
[4] S. Su, C. J. Wu, J. Ma, "Attacker's Perspective Based Analysis on Cyber Attack Mode to Cyber-Physical System," Power System Technology, vol. 38, no. 11, pp. 3115-3120, Nov. 2014.
[5] X. M. Ye, F. S. Wen, J. C. Shang, "Propagation Mechanism of Cyber Physical Security Risks in Power Systems," vol. 39, no. 11, pp. 3072-3079, Nov. 2015.
[6] Langner R. Stuxnet: dissecting a cyberwar fare weapon. IEEE Security and Privacy Magazine, 2011,9(3):49-51.
[7] W. C. Wu, L. Y. Ning, B. M. Zhang, "Coherency-based Dynamic Equivalence Algorithm with Community Structure of Complex Network Theory," Automation of Electric Power Systems, vol. 32, no. 7, pp. 1-5, Apr. 2008.
[8] L. Jiang, J. Y. Liu, Z. B. Wei, "Overload Control Method of Transmission Lines Considering Wind Power Characteristics," Automation of Electric Power Systems, vol. 39, no. 13, pp. 51-57, Jul. 2015.
[9] L. Guo, C. X. Guo, Y. J. Cao, "Generator Maintenance Scheduling of Large-scale Wind Power Integration Considering Peak Shaving," Automation of Electric Power Systems, vol. 36, no. 16, pp. 20-24, Aug. 2012.
[10] Hahn, A.; Ashok, A.; Sridhar, S.; Govindarasu, M., "Cyber-Physical Security Testbeds: Architecture, Application, and Evaluation for Smart Grid," Smart Grid, IEEE Transactions on, vol.4, no.2, pp.847,855, June 2013.
[11] Chen, T.M.; Sanchez-Aarnoutse, J.C.; Buford, J., "Petri Net Modeling of Cyber-Physical Attacks on Smart Grid," Smart Grid, IEEE Transactions on, vol.2, no.4, pp.741, 749, Dec. 2011.
[12] Junho Hong; Chen-Ching Liu; Govindarasu, M., "Integrated Anomaly Detection for Cyber Security of the Substations," Smart Grid, IEEE Transactions on, vol.5, no.4, pp.1643, 1653, July 2014.
[13] Ward, S.; O'Brien, J.; Beresh, B.; Benmouyal, G.; Holstein, D.; Tengdin, J.T.; Fodero, K.; Simon, M.; Carden, M.; Yalla, M.V.V.S.; Tibbals, T.; Skendzic, V.; Mix, S.; Young, R.; Sidhu, T.; Klein, S.; Weiss, J.; Apostolov, A.; Bui, D.-P.; Sciacca, S.; Preuss, C.; Hodder, S.; Seifert, G., "Cyber Security Issues for Protective Relays; C1 Working Group Members of Power System Relaying Committee," Power Engineering Society General Meeting, 2007. IEEE, vol., no., pp.1, 8, 24-28 June 2007.
[14] C. G. Yan, Z. G. Hao, B. H. Zhang, "Analysis of transformer protection principle based on voltage and current information," Electric Power Automation Equipment, vol. 30, no. 10, pp. 37-41, Oct. 2010.