CrossMark

Review and prospect of hidden failure: protection system and security and stability control system

Lili ZHAO[1], Xueming LI[1], Ming NI[1], Tianyu LI[2], Yameng CHENG[3]

MPCE

Abstract With the construction of the "3-level, 3-vertical-line, and 1-circle" power backbone in China, it's stricter and stricter on relay protection system and security and stability control system (SSCS) for reliable power transmission. Lots of blackouts in the world had happened, one main reason for which is the hidden failures of relay protection system or SSCS. Much work had been done about the hidden failure of relay protection, including classification, probability model, analysis methods of effects on power grid, and monitoring measures, which was summarized in the paper. The operation experiences of SSCS indicated that there might be hidden failures in five links of the security and stability control device (SSCD), e.g. measuring, control strategy, setting, communication and voting pattern. In addition, the coordination hidden failure among relay protection system, SSCS, and power plant's parameters related to the power grid was pointed out for more attention. In the future, amounts of work will be expected to be conducted on hidden failure: model building, assessment methods, application of research achievements, operation management of secondary equipment, and coordination problem between the relay protection system and the SSCS.

✉ Lili ZHAO
    zhaolili@sgepri.sgcc.com.cn

1   Nari Technology Development Limited Company, Nanjing
    211106, Jiangsu, China

2   Nanjing University of Posts and Telecommunications,
    Nanjing 210046, Jiangsu, China

3   Jiangsu Electric Power Research Institute, Nanjing 210093,
    Jiangsu, China

1 Introduction

In China, a "3-level, 3-vertical-line, and 1-circle" power backbone will be formed in the future, where the ultra-high-voltage (UHV) AC and DC transmission projects have been built, to help transferring power energy from large-scale energy bases to the major load centers. In order to ensure the security and reliability of power transmission, the protection system and security and stability control system (SSCS) must be highly reliable, being its strong backing. Committed to reducing the failure losses as best as possible by taking different control measures, the antecessors of China's electricity proposed the concept of three-defense lines with relay protection system and SSCS respectively lying in the first and second defense lines (See Fig. 1 [1]). So the reliability of the relay protection system and the SSCS plays an important role in the stability control of power system. However, because of technology limitations, miss-operations, weak management system of maintenance etc., there can be defects, great or minor, in relay protection and security and stability control device (SSCD), leading to hidden failures and security risks if not found in time.

Hidden failures are caused by the device's defects or human factors, bound to weakening the device's reliability. They produce no immediate action on the device and power system in a normal operating environment, and only possibly are triggered in an abnormal pressure state, e.g. grounded short-circuit fault, load-flow reversion and great drop of voltage or a harsh operating environment.

Obviously hidden failures are covert, once triggered, leading the improper operation of relay protection and
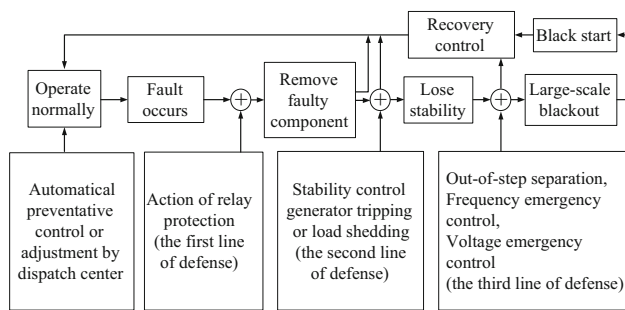
Springer

Fig. 1 The stability control and the three-defense lines power system in China

SSCD, which possibly cause cascading failure of power system with huge losses of load and power supply, even blackouts, and further bring about a great loss of the national economy. Although hidden failures are uncovered by some other events in a quite low probability, they might break through the first and second defense lines of China's power system once triggered, which can't be ignored for the profound impact on power grids and society.

Hidden failures of relay protection caused many blackouts of power systems, i.e. the WSCC blackout in 1994 [2], the "8·14" Blackout in America and Canada in 2003, the large-scale power failure in Brazil in 2011 [3], and the power failure in Indonesia in 2012. Blackout accidents resulted from hidden failures of SSCD have also happened many a time, such as the two WSCC blackouts in 1996 [2] and the large-scale power failure in 2009 [4]. What's more, the "7·1" accident of Central China (Henan) Power Grid in 2006 is evoked by hidden failures of both relay protection devices and security control devices.

Study of hidden failure holds great significance for ensuring security and stability of power grid, people's lives, and national development, including the mechanism of hidden failure's impact on power systems and the hidden failure monitoring approaches. Large amounts of studies and discussions about protection hidden failure have been done at home and abroad. This paper reviews these work and summarizes issues related with protection hidden failures: classification methods, probability model, research methods and monitoring measures. The possible hidden-failure risks of SSCD are presented based on the knowledge of the devices' characteristics and operating experience. It also briefly analyzes the influence of hidden failures caused by cooperation problem among relay protections, SSCSs, and parameters of power plants in operation related to the power grid. Last but not least, it proposes prospects on hidden-failure research, including modeling, risk evaluation methods, research result application, the coordination problem hiding between the relay protection and the SSCS, and operation management of

secondary equipment, hoping to provide some reference for the future research in this field.

2 Analysis of relay-protection hidden failures

2.1 Classification of protection hidden failures

Since the concept of relay-protection hidden failures [5] was put forward for the first time in 1994, the influence of relay-protection hidden failures with its research has been paid more and more attention. The protection hidden failures are classified in different ways, which are generally based on the causes of the hidden failures [6, 7], protection element functionality defect (PEFD) [8], and the dynamic and static characteristics of relay protection devices [9]. The detail of the three ways is as follows:

1) Classification based on the causes of the hidden failures. It divides hidden failures into five ones: a. hidden failures caused by hardware faults, such as damages or defects of device elements; b. hidden failures caused by system errors of protection software, such as logic errors of protection principle and version errors of software; c. hidden failures caused by protection setting values, such as improper settings and man-made setting errors; d. hidden failures caused by natural environment, like bad climatic conditions or storm disasters; e. hidden failures caused by improper manual operation or ill maintenance.

2) Classification based on PEFD. It consists of hidden failures caused by hardware faults (PEFD-A) and by human errors and protection settings (PEFD-B).

3) Classification based on the dynamic and static characteristics of relay protection devices. It divides hidden failures of protection devices into dynamic hidden failures and static hidden failures. The static characteristic of protection devices is that if the protection device doesn't fulfill the starting conditions, it will only do electric-parameter measurement and calculation or do data collection and start judgment; while the logic comparison and tripping output are not in consideration, mainly with the hardware devices, mutual-inductor measurement circuit, connecting cables, terminals, preprocess circuit of relay protection, sampling and sampling-value calculation. The hidden failures in these links are called static hidden failures. Dynamic characteristic of protection is that when the protection meets with the starting conditions, the fault parameters will be measured and logic comparison will be done, mainly with links of measurement, calculation, and blocking-signal inspection. The hidden failures in these links are called dynamic hidden failures.

Although the three classification methods of hidden failures appear different, all of them think over the classification from hardware and software, and then classified hidden failures by considering detailed factors like human behaviors and design defects of devices.

2.2 Probability models of hidden failures of relay protection system

The probability of relay-protection hidden failure is the first problem to be solved during the research, which can be solved now mainly by probability statistical method and probability model method. The probability value obtained by probability statistical method is a fixed value, which can be used to evaluate the cascading failure risk caused by hidden failures, but can't reflect the change of hidden failure probability value along with the real-time operating-condition such as line power flow, bus voltage, and system frequency. By the probability model method, the hidden failure probability of a particular protection system or a particular protection scheme can be worked out under different operating conditions. So far, 4 probability models of relay protection hidden failure have been proposed: hidden failure probability model of zone III transmission-line distance protection [10, 11], hidden failure probability model of over-current protection [12], hidden failure probability model of line protection considered over-flow [13], and hidden failure probability model of generator protection considered terminal-voltage [14]. The hidden failure probability value of zone III transmission-line distance protection is decided by the impedance seen by protection devices; the hidden failure probability of over-current protection devices is related to the magnitude of line current; the hidden failure probability of line protection considered over-flow is related to the magnitude of active line-load-flow; the hidden failure probability of generator protection considered terminal-voltage is related to the magnitude of generator's terminal voltage. The [15] catalogued protection's failure to operation and second-type mal-operation as hidden failures in consideration of the types of relay protection failures. Taking the probability obtained from the above hidden-failure probability models as the probability of protection's second-type mal-operation, a general hidden failure probability model is built on the basis of Markov, in which the protection system involves protective devices with associated circuit breakers.

Among the factors that result in hidden failures of relay protection equipment, there is no lack of human negligence or errors, production quality of devices, devices management & maintenance, etc. These factors usually have effects on the fitness of software/hardware system and control scheme of the secondary equipment to the grid operation mode at that time. Throughout all processes of protection hidden failure modeling, there are two ideas. One which is often used is to work out hidden failure probability of relay protection devices and how it changes with the electric parameters (voltage, current, and line power flow) by taking the equipment's software/hardware and control scheme into account. The other one is to work out hidden failure probability by considering the relay protection as a whole. These modeling processes only reflect the consequences of human negligence or errors, production quality of devices, equipment management & maintenance, etc., but don't embody how these factors affect protection hidden failure probability. The problem is worth thinking over, and if solved will help reduce human negligence or errors, perfect the devices, and improve the coordination between devices and power grid.

2.3 Effects and research methods of hidden failures

The relay protection's failure actions or malfunctions caused by its hidden failures weaken the reliability of protection system. When the power grid is abnormal, the triggering of relay-protection hidden failures may result in N-2 events [16], even cascading failures, which increases the insecurity and instability, bringing load isolation, power-supply isolation, out-of-step separation and even overall instability.

Lots of risk assessment methods have been proposed for quantifying the influence severity of relay-protection hidden failures on power system. Risk assessment methods which are the most used in assessing reliability are developed and improved on the basis of certainty analysis methods and probabilistic analysis methods [17]. So they synthesize technical economics and quantitative economics. The risk assessment methods analyze relay protection reliability in terms of risk, mainly by Markov, event tree and fault tree. The output risk indicators of device level separately are failure rate and availability of a device, risks of load isolation & power-supply isolation, and the margin of interface transmission. In addition, the risk indicators of primary-system level that is security & stability indicators can also be obtained by event tree analysis method. The risk indicators of primary-system level including grid separation risk and integrated risk can be obtained by fault tree analysis method.

The three analysis methods, i.e. Markov, event tree and fault tree, have different characteristics of application in the effect analysis of relay-protection hidden failures on power grid. Compared with the probability method, Markov is more applicable to the relay protection system that is a repairable system [18, 19]. Currently, the probabilistic statistical method is often used to build hidden failure probability models of relay-protection, in terms of the state

change of power system, like load-flow transfer. But it is not as accurate as Markov method in assessing the hidden failure probability of protection. However, Markov method needs lots of samples to ensure the accuracy of Markov, which must bear a heavy computation burden. In Markov method, the event's current state depends only on the last state, while event tree obeying the time sequence starts from the primary event, reasons out possible outcomes and identify the hazard source. For an example, based on the analysis of the hidden failure triggering conditions of relay-protection by event tree, it starts from a certain initial event and reason out the malfunction probability model of associated relay-protection under different contingences [20]. However, the event tree requires confirming object firstly, which demands thorough knowledge of the system structure, occurrence & probability of relevant accidents and the severity of consequences caused by accidents. Similar to the analysis by event tree, the analysis by fault tree is intuitively, straightforward, clear and logical. E.g., the dynamic process of the cascading resulted from relay-protection hidden failures is analyzed by fault tree so as to find out the line or generator protection "pre-malfunction set" [21] (the "pre-malfunction set" means the set of line or generator protection associated with the removed lines).

Aside by the above methods, certainty method, probability method and risk method, protection reliability is analyzed by other methods such as GO method [22] and the importance analysis on relay-protection hidden failures based on risk assessment [23]. The importance analysis on relay-protection hidden failures is derived from the element importance analysis which is an important approach for system reliability analysis. Its purpose is to identify the key elements that have crucial effect on system's reliability so as to objectively increase the overall reliability of the system at low cost [24].

The influence of protection hidden failures on system can also be analyzed by simulation. Monte Carlo [25] and Importance Sampling [26] are important tools for simulation analysis. Monte Carlo, the simulation method in probability method, take advantage of the comprehensive statistical data of power system state, to calculate the reliability indicators of a certain period of time, and can't be fit to analyzing the frequency and probability of events that do not often occur. Based on whether the simulation periods are a sequence, the Monte Carlo method can be divided into Monte Carlo method with time sequence and Monte Carlo method without time sequence. The importance sampling method does not use the primary probability of hidden failure model; instead, in order to increase the probability of cascading, it does simulation with a probability value greater than the primary probability under the premise that the mean of probability value remains

constant. Submission of a manuscript implies: that the work described has not been published before; that it is not under consideration for publication anywhere else; that its publication has been approved by all co-authors, if any, as well as by the responsible authorities—tacitly or explicitly—at the institute where the work has been carried out.

2.4 Monitoring method of hidden failures

In recent years, many researches on protection-system hidden failure have been done, i.e. researches on protection system reliability modeling and influence of protection devices on Power System's reliability. Research on the monitoring and control of protection hidden failure is also involved [7], which is aimed at taking precautionary measures against hidden failures to avoid serious cascading of power system. A technology embodiment for the monitoring and control system against relay-protection hidden failures [27] was proposed by AG Phadke and JS Thorp of Virginia Tech in 1995, but it was not applied in industry since the technology was not mature enough. In 2004, a monitoring system was developed against hidden failures by the wide-area protection system, however was of poor reliability and the cost was high [28]. The detection of hidden failures depends on the running state of Power System [29]. The off-line detection which is widely used now can't meet with the requirements, high security, high reliability and real time, and is unable to do an exhaustive detection for hidden failures. Therefore, new methods should be worked out for on-line detection.

That off-line setting value is improper is main contributor to hidden defects of protection settings. The off-line setting values are mostly set and modified manually, thus easily result in security risks. Particularly, off-line settings if have not been modified for a long time, will deteriorated the performance of devices, and may be not adapt to the real-time operation mode of power grid. One of the solutions to get over off-line setting defects is on-line setting [30] for protection devices. An online intelligent early warning system of protective relaying [31] was developed and applied to the power grid of some domestic province. Based on the warning system Scholars at home checked setting hidden defects of protection online, and assessed the risk brought by these defects for the weak links of protection hidden failures. The early warning system sent signals about these weak links and associated measures could be taken timely for the security of power grid.

The hidden failures of protection system are proved to be the key contributors to the wide-area disturbance [32]. Identifying the key lines affected by hidden failures [33] and taking associated measures can inhibit cascading development and reduce blackouts. Thus, some researches built pre-malfunction sets of lines where protection hidden

failures might be triggered. But these pre-malfunction sets are only sets of lines connected with the primary fault line and the researches didn't analyze the cause of line protection malfunctions systematically from the point of the essence of hidden failures, which lead to the obtained pre-malfunction sets incomplete. This problem has got solved in [34] that firstly put the protection hidden failures as a part of contingencies constituted by different accidents, secondly exposed the hidden risks of cascading during selecting N–k contingencies, and last found out vulnerable lines and the key protection. The hidden failure monitoring of other equipment like control circuit in high voltage circuit breaker in protection system is to check hidden failures by reverse point-by-point investigation method [35].

3 Analysis of hidden failures of SSCD

SSCDs widely used in China are the second defensive line [36] which is aimed at ensuring security, stability and reliability of power system. The SSCDs of multiple power plants or substations communicate with each other, constituting a SSCS with a hierarchical classification of control scheme like Electric Power Alarming and Coordinated Control System (EACCS). The EACCS in Jiangsu Province of China has a typical control structure of 4-hierarchy, dispatch center station-control station—control substation—implementation station from top to bottom. Since the SSCS takes charge of a regional power grid, once it goes wrong, enormous losses will take place, which has been proved by the "7·30" Load-Shedding Fault in Zengcheng in Guangdong province of China in 2004 and the "7·1" Accident of Central China Power Grid in 2009. The losses are so huge that it cannot wait to conduct researches on the hidden failures in SSCDs and associated effects on the power grid.

According to the accident experiences in power grids and the structure of the SSCS, the hidden failures of the SSCD are described in five links: measuring, strategy, setting, communication, and voting pattern.

1) Measuring

CT and PT are used for the measuring of electric parameters by the SSCD. The break-line accidents of PT are easy to take place and remain hidden until triggered by other events; the remaining current of CT second winding can influence the judgment of SSCD [37]. In addition, that the chip of measuring circuit goes wrong will influence the accurate of measured values which reflect electric information, easily resulting in incorrect judgment and malfunction of the SSCD.

2) Strategy

A SSCD is the implementation medium of various control measures. The ways of carrying out its control strategies usually include off-line decision and on-line pre-decision. If control strategies cannot fit the real-time operation mode of power grid, malfunction of the SSCS including over-shedding, under-shedding and mal-shedding will take place, further expanding the accidents in power grid [38].

3) Setting

The correctness of setting in device determines the efficiency of device and whether the monitored object can make right judgment about the type of faults as fast as faults occur. Unreasonable or incorrect settings impair the security of the SSCD and the stability of power system [39]. For instance, in the "7·1" Accident of Central China Power Grid, the mismatching between a setting and the real-time operation mode of power grid led to action failure of the security & stability control devices in Songshan substation and finally expended the accident.

4) Communication

Generally, how to configure a SSCD in the power grid should take control range and functions to be achieved of the device and power system planning into consideration. In order to achieve large-scale stability control, SSCDs of multiple plants are usually configured as a SSCS via communication channel and communication interface equipment, and work cooperatively, to achieve the regional security and stability control. However, in the communication progress between SSCDs, the reception and execution of commands in the SSCS are affected by error codes, unstable transmission in communication channel, not-in-time information transfer. It brings about that the strategy cannot be executed at right time or security & control devices cannot act properly, resulting in more serious accidents. On July 30, 2004, the security and stability control subsystem of Zengcheng, Guangdong mal-operated with 714 MW load shedding for the reason that communication codes were error and there were loopholes in the communication module and the verification links.

5) Voting pattern

Redundancy design is introduced into enhance the security and reliability of the SSCS. The voting pattern determines the characteristics of the malfunction prevention of a SSCS, so in the process of redundancy design it needs to consider the type of voting pattern of control outlet logic in a SSCS. There are mainly three types of voting patterns, e.g. "2 out of 3" pattern, "2 out of 2" pattern, and "1 out of 2" pattern.

In the "2 out of 3" pattern, only when at least two of three sets of SSCDs act can the outlet action be permitted. This will prevent malfunctions of the SSCS that are caused by hidden failures in any one of the three sets of SSCDs. But this pattern is the least adopted because of high cost, wiring complexity, operation and maintenance difficulty, etc.

In the "2 out of 2" pattern, the outlets of the two sets of SCCDs are connected serially, so the outlet tripping can be achieved only when both of the two sets of devices act. This will effectively prevent malfunctions of the system caused by hidden failures in either one of the two sets and ensure the reliability of the system. However, if neither of the 2 sets acts for their hidden failures, tripping pulse will not be transferred to the ultimate executive and then action failures of the SSCS will come into being.

The "1 out of 2" pattern is the most adopted at present. In this pattern, if either set of SSCDs acts, the outlet will be permitted [40]. This can prevent action failures that are caused by failures of either set of SSCDs, but it cannot prevent the mal-operation of the SSCS for hidden failures in the SSCDs. Various measures of preventing mal-operation have to be taken to ensure the reliability of a SSCS.

4 Analysis of coordination hidden failures of relay protection system and SSCS

Among reasons of blackouts, there are also coordination hidden failures, which may lie between relay protections, between SSCSs, between the relay protection system and the SSCS, or among power plants' parameters related to the grid, relay protection system and SSCS, affecting the security of power grids, sometimes even deadly.

4.1 Coordination hidden failures between relay protections

What a relay protection cares about is the element in power grid and relay protections make decisions all alone [41], which make the coordination between relay protections poor.

The poor coordination between relay protections mainly results from the unreasonable setting matching between one protection and its lower protection [20], i.e., that zone II or zone III setting of distance protection doesn't satisfy the selectivity results in the disharmony cooperation between a main protection and its associated backup protection or its lower protection. The hidden defects of cooperation between relay protections may be caused by other factors like design schemes. i.e., there exists a coordination hidden defect in the design scheme that the bus couple auto-switch protection (BCASP) and bus

differential protection (BDP) block each other. The hidden defect remains undetected by the occurrence of a single simple fault, but when complicated failures occur and cannot be identified by the judgment circuit of the relay protection for the coordination hidden defect between BCASP and BDP [42], serious failures may follow.

4.2 Coordination hidden failures between SSCSs

The conventional SSCS takes charge of the stability of a regional power grid, usually restricting the control range in a provincial grid. Distributed in a regional power grid, the early SSCS made decisions independently and took appropriate measures against failures listed in the control strategy. With the development of EHV AC/DC transmission network, strong electrical connection will be established between regional power grids. It may occur that the operation of some SSCS in region A becomes a disturbance to the SCCS in region B, though the operation is correct for the stability problems caused by faults in region A [35]. For example, the rapid and large-scale transfer of load flow caused by generator tripping or separation in region A can lead to action failures, malfunctions or unexpected actions of the SSCS in region B. Therefore, in order to prevent such hidden failures, the coordination between SSCSs in different regions must be considered and attached importance to.

4.3 Coordination hidden failures among relay protection, SSCS and parameters of power plants related to power grid

It also should be paid attention to that whether it's coordinate among relay protections, the SSCS and parameters of power plants related to power grid. The incoordination among the three was also looked on as one of contribute factors to some blackouts by some experts. The consequences resulted from the coordination problem had been proved by the WSCC 2 blackouts of United States in 1996 [2], the "8·14" Blackout in America and Canada in 2003 [43], and the Italian blackout in 2003 [44]. The series of accidents alarm that close attention should be paid to the coordination hidden failures between the relay protections and the SSCS, or among parameters of power plants related to power grid, the relay protection and the SSCS. With the large scale new energy connected to power grid in China, the grid-connected control and protection of wind energy generation and photovoltaic power generation brings a new challenge to the relay protection system and the SSCS. The operating experience about new energy indicates that the tripping accident of large-scale wind turbine generators in Northwest China Power Grid in 2011 was caused by hidden coordination problem among the feeder protection, SVC/

SVG and the grid-connected protection of wind turbines. Moreover, that large-scale new energy is connected to the power grid in centralization brings new challenges to the adaptability of various criterions of the SSCS. Among these challenges the criterion for fault trip and control measures may become invalid. Therefore, there is necessity to study hidden failures caused by generator-power grid coordination problem; otherwise a tiny accident could lead to instability and large scale blackouts of power grid.

5 Conclusions

By summarizing and analyzing the research on hidden failures of the relay protection and the SSCS, the author thinks that the further research on hidden failures of the relay protection and the SSCS in the future should be conducted as follows:

1) Hidden failure modeling. So far, most are hidden failure probability model of over-current protection and distance protection, current differential protection which is often used as main protection seldom included. Research on hidden failure in SSCS is just in its infancy. It will be a key to build a proper probability model of hidden failure in the SSCS. The control scheme of the SSCS is a distributed control scheme and more complicated than that of the relay protection. During the model building of hidden failure in the SSCS, it has to consider the effect of action failures or malfunctions of devices caused by hidden failures not only on protected elements and the neighboring elements, but also on the area charged by the SSCS. So inevitably it is more complicated to build hidden failure model of the SSCS. The probability and severity of consequences caused by different hidden failures might be different and should be taken into account to assess the effects of hidden failures. The outcome of the assessment should be taken as one of considerations in building probability model of hidden failures in secondary equipment. Work in the field is underway and the details will be introduced in follow-up articles.

2) Risk assessment of hidden failure. As members of secondary equipment, relay protections and SSCDs are a part of operational risk sources of power grid. Until now, the severity assessment of the effect of hidden failures in the relay protection on power grid is generally carried out based on the point of risk. According to the ideas of risk assessment proposed in the research with achievements, such as research on power grid faults caused by lighting [45], hidden failures of secondary equipment will be treated as a new input to assess risk online and analyze the security of power grid, which will be a new trend to study hidden failures. The modeling and analysis of hidden failures in the relay protection and SSCS need the support of large amounts of operating data, but the categorization of operating data is not complete, and the expert knowledge is of ambiguity and uncertainty. To acquire adequate data it needs to reinforce the unified management of the monitoring and accident record of secondary system. However that's not enough. New methods should also be explored simultaneously to evaluate the risk of hidden failure under the condition of data deficiency.

3) Coordination hidden failure of the relay protection and the SSCS. Although the coordination problem between relay protections has been concentrated on, research on the coordination problem is still relatively deficient and requires further studies. Furthermore, after the separation of power grid and power plants, the coordination problem among the relay protection, the SSCS and parameters of power plants related to power grid has been gradually becoming outstanding, which has to be paid attention to since it is a big threat hiding in the operation of power grid.

4) Application of hidden failure research. The achievements of hidden failure research should be helpful to enrich the collection of contingencies and pre-decision system, and strengthen the prevention and emergency control system. Simultaneously, it should also be helpful to identify the coordination hidden failures between different controls on security and stability of power system, and find out the weak links of power system. Then associated measures can be taken timely to enhance the security and reliability of power system.

5) Operation management of secondary equipment. Human factors are also contributors to hidden failures of the relay protection and the SSCS. The limitation of testing-personnel quality and testing technology could bring about hidden failures for ignorance of some defects in devices. So it should be done to obey relevant electric regulations strictly, to update these regulations with the development of power grid, and to reinforce the management of the links like debugging, operation & maintenance, and setting. Then some hidden dangers can be avoided and series accidents evoked by tiny problems can be reduced as much as possible. Though action criterions for relay protections and SSCDs have been established based on the operating characteristics of the power grid, these criterions can't be adapt to the operating characteristics of power grids forever and need to be updated timely. A device itself has to be faced with many operation problems such as harsh operating environment and

aging of components resulted from device's long time operation, possibly becoming contribute factors to hidden failures too. So in order to reduce accidents caused by devices' hidden failures as much as possible strict supervision and early warning should be done with the condition-based maintenance date of secondary equipment.

References

[1] Xiao SJ (ed) (2011) Control technology of security and stability in power system. China Electric Power Press, Beijing (in Chinese)
[2] He DY (1998) The successive ponderation (layers-built analysis) over U.S. WSCC two outages in 1996. Electr Power 31:37–40 (in Chinese)
[3] Lin WF, Sun HD, Tang Y et al (2010) Analysis and lessons of the blackout in Brazil power grid on November 10, 2009. Autom Electr Power Syst 34(7):1–5 (in Chinese)
[4] Lin WF, Tang Y, Sun HD et al (2011) Blackout in Brazil power grid on February 4, 2011 and inspirations for stable operation of power grid. Autom Electr Power Syst 35(9):1–5 (in Chinese)
[5] Tamronglak S (1994) Analysis of power system disturbances due to relay hidden failures. Dissertation, Virginia Polytechnic State University
[6] Zhang XS, Wang HF, Huang XM et al (2011) Discussion on hidden failures in relay protection system. Electr Power Constr 32(2):47–51 (in Chinese)
[7] Zhang JJ (2012) Research on hidden failures related issues of relay protection system. Dissertation, HeFei University of Technology (in Chinese)
[8] Xu J (2011) Analysis and research on complex power system cascading failures considering hidden failure of protection. Dissertation, China Electric Power Research Institute (in Chinese)
[9] Wang ST (2010) Research on the monitoring methods of hidden failures in relay protection. Dissertation, Chongqing University (in Chinese)
[10] Yang MY, Tian H, Yao W (2010) Analysis of power system cascading failure based on hidden failures of protective relaying. Power Syst Prot Control 38(9):1–5 (in Chinese)
[11] Bae K, Thorp JS (1998) An importance sampling application: 179 bus WSCC system under voltage based hidden failures and relay operation. Decis Support Syst 24:259–268
[12] Yu XB, Singh C (2004) A practical approach for integrated power system vulnerability analysis with protection failures. IEEE Trans Power Syst 19(4):1811–1820
[13] Sun YZ, Cheng L, He J (2012) Power system operational reliability theory. Tsinghua University, Beijing
[14] Cheng YM, Chen X, Ren JF, Li XM (2013) Study on hidden failure of relay protection in power system. In: Paper presented at 2013 IEEE 3rd annual international conference on cyber technology in automation, control and intelligent systems (CYBER), Grand Metropark Hotel Nanjing and Nanjing University of Science and technology (NJUST), 26–29 May 2013
[15] Wu X, Zhang JH, Wu LW et al (2012) Method of operational risk assessment on transmission system cascading failure. Proc CSEE 32(34):74–82 (in Chinese)
[16] De La Ree J, Elizondo DC (2004) A methodology to assess the impact of hidden failures in protection schemes. IEEE PES Power Syst Conf Expo 3:1782–1783. doi:10.1109/PSCE.2004.1397501
[17] Guo CX, Lu HB, Yu B et al (2013) A survey of research on security risk assessment of secondary system. Power Syst Technol 37(1):112–118 (in Chinese)
[18] Wang SC (2005) Markov model for reliability analysis of dual-redundant relays. Relay 33(18):6–10 (in Chinese)
[19] Chen SH, Ma BY, Lei Y et al (2007) Integrative and quantitative calculation of reliability for relay protection system. Autom Electr Power Syst 31(15):111–115 (in Chinese)
[20] Wu WC, Lv Y, Zhang BM (2009) On-line operating risk assessment of hidden failures in protection system. Proc CSEE 29(7):78–83 (in Chinese)
[21] Chen WH, Jiang QY, Cao YJ (2006) Risk assessment of power system cascading failures considering hidden failures of protective relayings. Power Syst Technol 30(13):14–19 (in Chinese)
[22] Wang C, Gao P, Xu Z et al (2007) Application of GO methodology in reliability assessment protective relays. Autom Electr Power Syst 31(24):52–56 (in Chinese)
[23] Huo C, Zhang PC, Liao XH (2008) Analytic method for relay protection importance with consideration of hidden failures. East China Electr Power 36(3):63–65 (in Chinese)
[24] Kececioglu D (1991) Reliability engineering handbook, vol 2. PTR Prentice Hall, Englewood Cliffs
[25] Chen J et al (2005) Cascading dynamics and mitigation assessment in power system disturbances via a hidden failure model. Electr Power Energy Syst 27:318–326
[26] Bae K, Thorp JS (1999) A stochastic study of hidden failures in power system protection. Decis Support Syst 24:259–268
[27] Phadke AG, Horowitz SH, Thorp JS (1995) Anatomy of power system blackouts and preventive strategies by rational supervision and control of protection systems. ORNL/Sub-89-SD630C/1. Oak Ridge National Laboratory, Oak Ridge
[28] Huang J (2004) Adaptive wide area protection of power system. Dissertation, Iowa State University
[29] Sun X (2009) Research on the detection of hidden failure in relay protection and risk analysis. Dissertation, Chongqing University (in Chinese)
[30] Duan XZ, Yang ZL, Cheng Xiao (2005) Performance analysis of relay settings determined according to off-line calculation and on-line calculation. Autom Electr Power Syst 29(19):58–61 (in Chinese)
[31] Lv Y, Sun HB, Zhang BM et al (2005) Research and development of an online intelligent early warning system of protective relaying. Autom Electr Power Syst 30(4):1–5 (in Chinese)
[32] Bae K, Thorp JS (1999) Hidden failures in protection systems and their impact on wide-area disturbances. Decis Support Syst 24:259–268
[33] Wang H, Thorp JS (2001) Optimal locations for protection system enhancement: a simulation of cascading outages. IEEE Trans Power Deliv 16(4):528–533

[34] Xu J, Bai XM (2012) Power systems *N-k* contingency analysis in consideration of protection hidden failure. Proc CSEE 32(1):108–114 (in Chinese)

[35] Cui Y, Wang C, Yang JH et al (2011) Inspection and repair method for hidden faults of control circuit in high voltage circuit breaker. High Volt Appar 47(12):96–99 (in Chinese)

[36] Song JH, Li XM, Ji CA et al (2005) Current situation development prospect of security and stability control equipment. Autom Electr Power Syst 29(23):91–96 (in Chinese)

[37] Zhang Y, Li JS, Huang H et al (2009) Improvement of line trip criterion of power system security and stability control equipment. South Power Syst Technol 3(3):74–76 (in Chinese)

[38] Wang W, Chen J, Yu R et al (2012) Analysis of non-fault tripping criterion operation for area-based stability control device. Power Syst Prot Control 40(2):120–124 (in Chinese)

[39] Cai M, Sun GH, Wu XC et al (2007) Analysis and application of AC fault criterion in power system stability control. Autom Electr Power Syst 31(8):46–51 (in Chinese)

[40] Zhu JJ, Huang ZY, Hong J et al (2011) Analysis on Shanghai grid security and stability control device. Power Energy 32(3):190–193 (in Chinese)

[41] You JX, Wu R, Ye K et al (2011) Analysis of a blackout escalation caused by hidden failure lying in blocking logic between auto-switching protection and bus differential protection. Autom Electr Power Syst 35(7):102–107 (in Chinese)

[42] Begovic M, Novosel D, Karlsson D et al (2005) Wide-area protection and emergency control. Proc IEEE 93(5):876–891

[43] Yin YH, Guo JB, Zhao JJ et al (2003) Preliminary analysis of large scale blackout in interconnected North America power grid on August 14 and lessons to be drawn. Power Syst Technol 27(10):8–11 (in Chinese)

[44] Fu ST (2005) Summary on power system security problems on 2004 IEEE PES Meeting and recommendation for developing defence measures. Autom Electr Power Syst 29(8):1–4 (in Chinese)

[45] Xie YY, Xue YS, Wang HH (2013) Space–time early-warning of power grid fault probability by lightning. Autom Electr Power Syst 37(17):44–51 (in Chinese)

Lili ZHAO was born in Jiangsu, P.R. China, in 1988. She is an engineer of Nari Technology Development Limited Company. Her research interests include control technology about security and stability of power system.

Xueming LI was born in Jiangsu, P.R. China, in 1965. He is a tutor in State Grid Electric Power Research Institute and a senior engineering of Nari Technology Development Limited Company. His research interests include control technology about security and stability of power system.

Ming NI was born in Jiangsu, P.R. China, in 1969. He is a tutor in Hohai University and a chief expert of China. His research interests include control technology about security and stability of power system, power system planning, and automation of power system.

Tianyu LI was born in Jiangsu, P.R. China, in 1992. He is a student of Nanjing University of Posts and Telecommunications. His research interests include stability analysis and control of power system.

Yameng CHENG was born in Jiangsu, P.R. China, in 1989. Her work is in Jiangsu Electric Power Research Institute. Her research interests include automation of power system. ….