Indonesian Journal of Electrical Engineering and Computer Science
Vol. 8, No. 1, October 2017, pp. 184 ~ 191
DOI: 10.11591/ijeecs.v8.i2.pp184-191

Assessment of Power System Risk in Cyber-Attacks in View of the Role Protection Systems

Hui Hwang Goh*[1], Sy yi, Sim[2], Omar Abdi Mohamed[3], Ahmed Farah Mohamed[4], Chin Wan[5], Ling, Qing Shi, Chua[6], Kai Chen, Goh[7]
[1,3,4,5,6]Department of Electrical Engineering, Faculty of Electrical and Electronic Engineering, Universiti Tun Hussein Onn Malaysia, 86400 Parit Raja, Batu Pahat, Johor, Malaysia.
[2]Department of Electrical Engineering Technology, Faculty of Engineering Technology, Universiti Tun Hussein Onn Malaysia, 86400 Parit Raja, Batu Pahat, Johor, Malaysia.
[7]Department of Construction Management, Faculty of Technology Management and Business, Universiti Tun Hussein Onn Malaysia, 86400 Parit Raja, Batu Pahat, Johor, Malaysia
*Corresponding author, e-mail: hhgoh@uthm.edu.my

Abstract

This paper presents a risk assessment method for assessing the cyber security of power systems in view of the role of protection systems. This paper examines the collision of transmission and bus line protection systems positioned in substations on the cyber-physical performance of the power systems. The projected method simulates the physical feedback of power systems to hateful attacks on protection system settings and parameters. The relationship between protection device settings, protection logic, and circuit breaker logic is analyzed. The expected load reduction (ELC) indicator is used in this paper to determine potential losses in the system due to cyber attacks. The Monte Carlo simulation is used to calculate ELC's account to assess the capabilities of the attackers and bus arrangements are changed. The influence of the projected risk assessment method is illustrated by the use of the 9-bus system and the IEEE-68 bus system.

Keywords: *Cyber security; Protection system; Expected load reduction*

1. Introduction

The advent of cyber threats puts various components of the energy system at risk by exploiting the increased complexity and interconnectedness of sensitive infrastructures [1]. For example, corrupted data applications in supervisory control and access to data (SCADA) may resent unexpected risks to the operation and control of the power system. In 2004, the US Department of Energy (DO) published a roadmap to address cyber security threats in computer-based systems, which also referred to issues related to the operations of the energy system [2]. Therefore, the large data management systems provided by smart grid applications for power grids can be critical in promoting the efficient and reliable operation of the electricity infrastructure. At the same time, the continued transition to the smart grid offers a significant level of information and communications technologies in the operations of the energy system, which will increase cyber security challenges [3]. Additional efforts have been committed to reducing cyber security weaknesses in energy systems [4]. A survey on cyber security of smart grid infrastructure was presented. The cyber security communications infrastructure and power system have been discussed in [5]. Counterfeit data attacks have been analysed in the proposed optimal solution to minimize power system weaknesses.

It was discussed in an overview of intelligent network security testing that included control, communication, and physical system components to provide a physical environment and various test research applications [6]. In the included anomaly recognition method has been clarified to enhance cyber security of network-based substations. Cyber attackers, who are well-known with syntax and semantics of computer systems, power systems and protection relays, can find weaknesses in control systems and infect the power system with malicious code, and then remote control the power system by sending illegal commands to hide the emergency event [7]. Once access to the rights of the system administrators is illegal, cyber attackers can easily initiate the failure of a sequence or power outage by subverting secondary electrical

Received June 22, 2017; Revised August 21, 2017; Accepted September 8, 2017

components, i.e., protection systems. Therefore, cyber security in energy systems should be enhanced not only deliberate attacks on ICTs but also responses from secondary electrical systems, which rely directly on ICTs [8]. Moreover, the report on the issues covered by the security of electronic communication paths to protection relays. The error has been analysed in the use of context information, such as sub-voltage and current. The unconditional security authentication code for security systems was analysed in. The security of differential bus relays has been systematically identified based on scenario attacks. Most cyber security-related studies have focused on information systems for protection devices that do not take into account coordination between protection systems and do not consider bus arrangements related to cyber security in the protection of energy systems. In our view, the interactions of the relays and primary energy system are components of cyber security studies [9]. In this paper, we are developing a methodology to analyse the impact of transport and bus line protection systems in substations on the cyber security performance of energy systems. We also use the corresponding results to calculate the risk of cyber security taking into account parameter attacks and their correlations with the logic of protection and physical bus links in power systems.

2. Scheme Analysis

2.1. Bus Protection Scheme Analysis

In this section, real-time relays are analysed to assess the power system's risk of cyber attacks that may result in illegal access and changes in relay system parameters [1].The BP-2C-D bus protection product, which is produced by Nari-Relays in China, is an example of a logical scheme for differential protection. This BP-2C-D bus protection operate by classify current condition and the system decide the programed operation to carryout. Total six conditions is programed for this model of bus protection system.

2.2. Transmission Line Protection Scheme Analysis

Protection schemes for transmission lines need the coordination of settings, operation times, and operation characteristics. In this review paper, RCS- 941 formed by Nari-Relay Company in China is working to illustrate the relationship between input parameters and CB states [10]. The one line diagram of CT/VT, CBs, and line protections for substation two is shown in Figure 1. Four computer-based line protection strategies are included and each measuring line current and bus voltage and controlling the state of CBs.

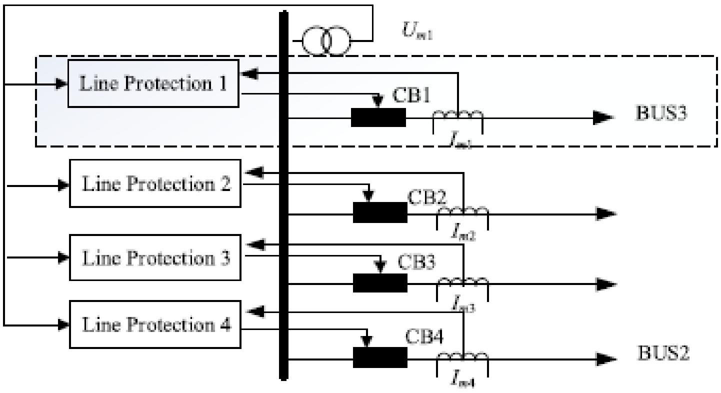


Figure 1. Protection configuration for transmission lines

Three protection pattern including current protection, distance protection, and pilot differential protection is set up to protect transmission lines using RCS- 941. Suppose that the distance protection is adopted for each line in Figure 1.

Then, the control logic which includes trip situation phase selector, operation condition, operation logic, and export logic, i s illustrated in Figure. 5. The line protection input criterion x_1. . . x_p, y_1, . . . , y_r, in Figure 2 are similar as those for bus protection, including the background values and CT/VT ratios [11].

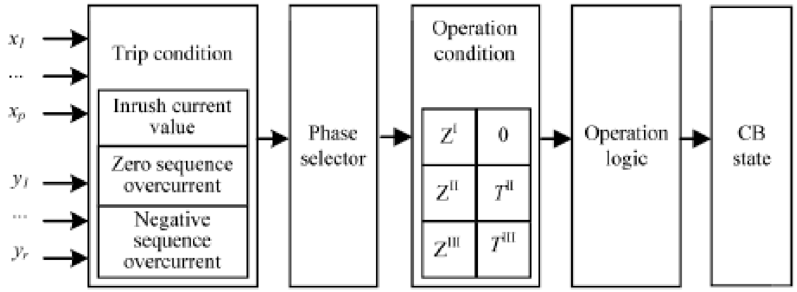


Figure 2. Logic framework between states of circuit breakers and input parameters for transmission line protection [1]

The trip condition consists of three principles including inrush current, zero sequences over current and negative sequence overcurrent. The phase selector components are planned to minimize the burden of computing impedances. In RCS-941, various methods can be selected in the phase selector stage [12, 13].

3. Methodology

3.1. Proposed Approach to Risk Assessment

Some methods are used in this part such as Markov chain, Petri net and Bayesian net, these methods are to assess illegal access prospects. So we are going to emphasize and studying any reaction from the local protection system to the cyber attacks, as well as the causing risks in power system processes [14].

By assuming M is referred in substation (protection schemes), and N_i for parameters (protection locations), while $CT/_{VT}$ ratios in the protection system i. At that time, the number of substation parameters is $N=\sum_{i=1}^{M} N$. Suppose P is the capability of attackers, and it realizes the ratio of the parameters attacker [15]. Then, the real number locate is given $n = N * p$ and the amount of arrangements for parameter reforms is C_N^n. By assuming Q_s max and Q_s min this means by reforming max/min values of parameters, then the reforms parameters values are equal as shown in Equation 1.

$$X_s = Q_{s,\min} + \alpha^* \left(Q_{s,\max} - Q_{s,\min}\right) \tag{1}$$

Where α has represented a random digit between 0 and 1 with constant supply.

Initially, the system topology G will determine on n forms and relate the change has been done for this parameter. The performance of the power grid under cyber attacks might be meaningful compared to that grid which faces natural disasters [16]. On the other hand, both cyber attack and natural disasters could activate, cascading failures and risk the power system security. However, this could not be long-term damage, and it can be finished when system workers take actual measures, for example, concise system separation to avoid an additional deterioration of power systems [17]. In this paper, we use simply load curtailment strategies for the current algorithm provided in power, to evaluate power grid contingencies, without regarding the details of power grid performance. Let assume LS(G) is load curtailment of topology G and P(G) is the prospect of the system topology. Therefore, the risk of the power system measured by the expected load curtailment and is calculated as shown in Equation 2.

$$ELC = \sum\nolimits_{\forall G} P(G) * LS(G) \tag{2}$$

There are several techniques for obtaining a topology G by using a given P(G). In dangerous cases, topology G can be related with work attacks such as, a random attack which accepted to avoid discovery by grid operators [18]. The Monte Carlo simulation has been utilized in this paper and applied in practical form to obtain the power system danger. The reform factors in the power system are chosen casually while the number of modified parameters is fixed and represented as n. from the calculation we get (1) as the value of the modified parameter. From that result, we can obtain the topology by using protection logics, if the entire number of simulation is NJ, we can conceder ELC as shown in Equation 3.

$$ELC = \frac{1}{NJ}\sum\nolimits_{J=1}^{NJ} LS(G_j) \tag{3}$$

The suggested risk assessment framework that reflects the reaction of protection systems to cyber attacks, the outline is separated into three parts [18]. For the first part has been the focus in bus arrangements such as single- bus, double-bus single-breaker, and breaker-and-a- half, also protection systems have been analysed for example bus protection, transmission line protection and others. Protection logics may it joins temporally, and created protection locations and $CT/_{VT}$ ratios, which are protection tools inputs and can simply adjust by cyber attacks are also studied in this part.

The second part, the Monte-Carlo model has achieved a casual modification of parameters such as protection setting and $CT/_{VT}$ ratios for each situation, the influence of cyber attacks on the power grid performance which rely on protection logics and CB_s tasks are studied in third part [19]. The power grid connectivity needed to investigate if the connectivity of the network is preserved, and the power flow is achieved to check damages. If the result of power flow is possible, the risk assessment will be followed, else, the basic load curtailment approach has to reduce by 10% when generations and loads are decreased for every cycle is performed while waiting for the power flow to be functional. Practically, an extra developed of the load curtailment processing it might supposedly reduce any load limitations [19]. The possibility of risks is figured out base on the random event probabilities and prospective system. In practice, the MW load reduction has been used to avoid potential system contingencies because of the cyber attacks, which allow the ability of protection systems. It is necessary to protect power systems so that electrical faults can be detected and isolated quickly. The basic form of protection for transmission systems that contain high-voltage critical lines of the system and some distribution systems is the current differential protection [5]. Current differential protection relays (or intelligent electronic devices)(IEDs) compare the current measurements measured at each end of the line. If the vector total of these phasors is equal to zero, within the configuration tolerance, then the protection system will issue a flight signal to the circuit breakers to isolate the line of altars from the rest of the system.

4. Results and Discussion

An adapted 9-bus system and the IEEE 68-bus system are simulated and discussed to illustrate the usefulness of the proposed method [1].

4.1. Modified 9-Bus System

The modified 9-bus system in Figure 3 is handled to illustrate the cyber attack risks with respect to protection system functions. The adapted system has two generators, eight buses, and 12 CBs [1]. Three-phase CTs are installed in all transmission lines and the coupler CB circuit, and three-phase VTs are equipped on I-Bus and II-Bus of Bus 8. Imagine that Bus 3 is located in a substation and has a double-bus-sing-breaker arrangement. Also assume that the distance protection RCS- 941 is installed on lines 1-5, and the bus protection BP-2C-D is set up on Bus 8.

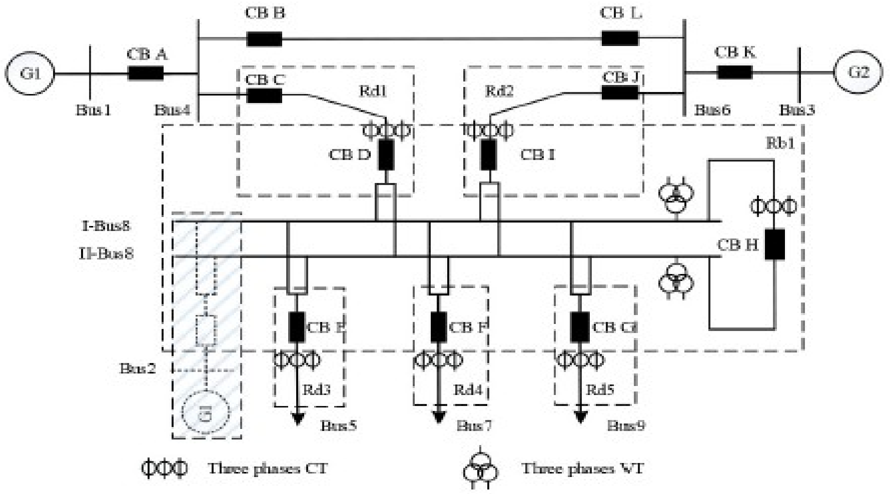


Figure 3. Modified 9-bus test system [1]

Figure 4 shows that there are 60 and 24 changeable parameters related to the transmission line and bus protections, respectively. As some parameters appear multiple times, the total number of changeable parameters is 60. Figure 4(a) includes the background x_{b1}, x_{b2} and CT ratios for each transmission phase, y_{11}-y_{61}, y_{12}-y_{62} and y=-y_{63}. Figure 4(b) consist of the background x_{11}-x_{16}, x_{21}-x_{26}, x_{31}-x_{36}, x_{41}-x_{46}, x_{51}-x_{56}, CT ratios y_{11}-y_{13}, y_{21}-y_{23}, y_{31}-y_{33}, y_{41}-y_{43}, y_{51}-y_{53}, and VT ratios y_{1a}-y_{1c}, y_{2a}-y_{2c}.Two sets of VT ratios contained in Figure 4(b) are I- Bus voltage ratios y_{1a}-y_{1c}, applied by transmission line protection Rd1 and Rd3, and II-Bus voltage ratios y_{2a}-y_{2c}, applied by protection Rd2, Rd4, and Rd5.

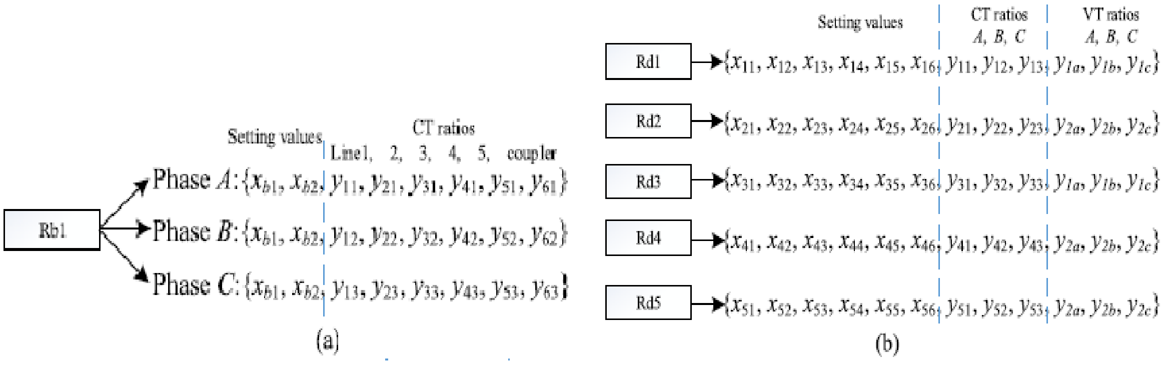

Setting values
CT ratios
Line1, 2, 3, 4, 5, coupler
Rb1
Phase A: {x_b1, x_b2, y11, y21, y31, y41, y51, y61}
Phase B: {x_b1, x_b2, y12, y22, y32, y42, y52, y62}
Phase C: {x_b1, x_b2, y13, y23, y33, y43, y53, y63}
(a)
Setting values
CT ratios A, B, C
VT ratios A, B, C
Rd1 {x11, x12, x13, x14, x15, x16, y11, y12, y13, y1a, y1b, y1c}
Rd2 {x21, x22, x23, x24, x25, x26, y21, y22, y23, y2a, y2b, y2c}
Rd3 {x31, x32, x33, x34, x35, x36, y31, y32, y33, y1a, y1b, y1c}
Rd4 {x41, x42, x43, x44, x45, x46, y41, y42, y43, y2a, y2b, y2c}
Rd5 {x51, x52, x53, x54, x55, x56, y51, y52, y53, y2a, y2b, y2c}
(b)

Figure 4. Modifiable parameters for bus and transmission line protections, (a) Setting values and CT Ratios for Bus Protection. (b) Setting values, CT Ratios and VT Ratios for Transmission Line Protection

Assume that all CBs in Figure 3 are closed and the initial settings for bus protection $\Delta Idset$ and *Idset*are x_{b1}=15 and x_{b2}=15, respectively [1]. The primary settings for the transmission line protection are recorded in Tables III and IV. The ELCs, which measure the cyber attack risks, are 43MW for 10% attacks risk 195MW for 50% attacks risk and 302MW for 90% attack risks of all parameters.

Figure 5 shows the ELC as a work of the number of Monte Carlo simulations when 10% of the parameters are attacked. The ELC reaches about 43MW, although with small differences, after 2000 simulations, related to which the simulation is measured to be concentrated.

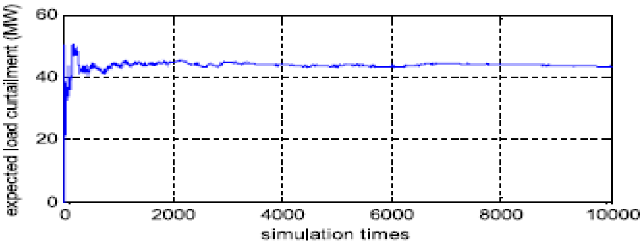


Figure 5. ELC for the modified 9-bus system when 10% of parameters are attacked [1]

4.2. IEEE 68-Bus System

The IEEE 68-bus system is used to additional test the proposed risk assessment method. This system has 16 machines, 86 transmission lines, and five areas, which perform the minimized News England test system (NETS), linked with the New York power system (NYPS). Six line protections and one bus protection are installed in the substation [9]. Lines 53-54A, 53-27A, 53-30, and Load 1 are connected to the II-Bus of Bus 53. Lines 53-54B, 53-27B, 53-31, and 53-47 are linked to the I-Bus of Bus 53. CBs A-F, H and I are close. The Monte Carlo simulation results for the two modes are outlined in Table 1. Here, the resulting ELC when the coupler CB is open is less than that when the coupler CB is closed [20, 21]. This consideration implemented to all cases with a variety of attacking efficiency. The result expressed that, when facing cyber attacks, the risk for the two-bus- single-breaker arrangement is smaller if the coupler CB is open. However, when the attacking ability to perform becomes stronger, the difference in ELCs, thus the power system risks, between the two bus activity approaches gets to be smaller.

Table 1. ELC for different bus operation modes and attacking capabilities

% of Parameters Attacked	10%	50%	90%
Coupler CB G is closed	1000MW	1700MW	2000MW
Coupler CB G is open	340MW	1350MW	1800MW

Figure 6 shows the progress of ELCs if 10% of the parameters are attacked. Alike to the 9-bus system case study, the Monte Carlo simulation assembles within the 2000 scenarios. Similar trends would be noticed when a higher number of parameters are attacked.

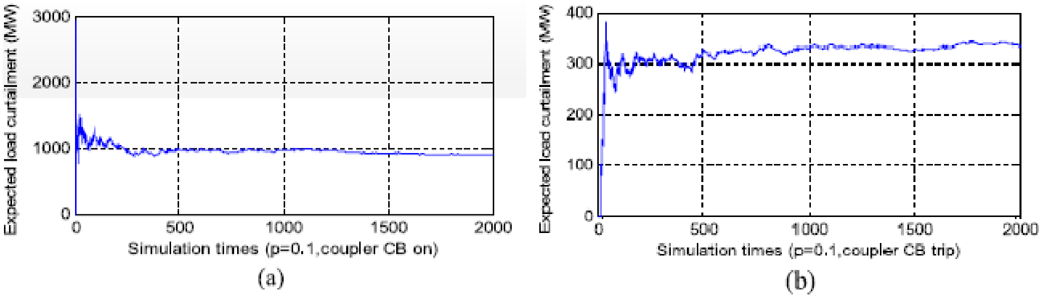


Figure 6. ELC based on Monte Carlo simulation for the IEEE 68-bus system when 10% of parameters are attacked. (a) Monte Carlo Simulation Results When Coupler CB G is on. (b) Monte Carlo Simulation Results When Coupler CB G is off [1]

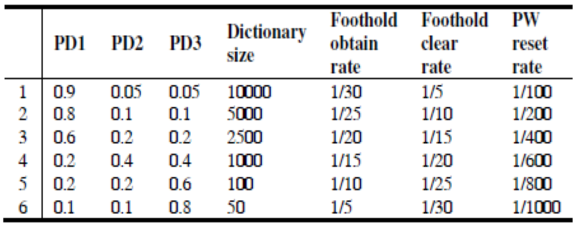
4.2.3 Three-Layer Cyber-Physical Risk Assessment

The main objective of this paper is to learn a risk assessment and how to determine the effective of a cyber attack on the production of the system protection scheme. This section provides a Deterministic and Stochastic Petri-Net base on the three-layer cyber-physical risk assessment method which proceeds to the reflection both cyber intrusion and the way how system protection scheme will reply. Cyber-class model represents infiltration of cyber operations through various contact points and the first point there is no action at all. Physical layer modelling has own target and needs to build SPS DSPN model, and the modelling plan is SPS data movement leaning. The process of an action plan for most SPSs contains gathering data, centralized calculation, and control [10]. Any connection from one party to the concerned party can be act toward as flow of data in a series that passes a particular way containing some devices. Petri-Net model act as a place for each device. A particular protection which consists of some independent series running in parallel.

4.2.4 Three-layer DSPN Model

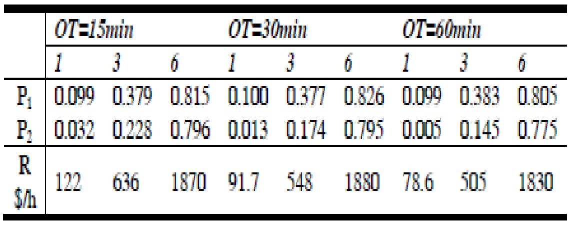
Tables below shows that we have six different set parameters of DSPN model. V. PD1-PD3 are the prospects for the attacker to select low level, middle level or high-level DoS attack.[10]. The different result in the table appears for the probable result needed to delay exponential transformation. The possibility of a stable state is only one line (P1), both lines (P2) and parallel risk values (R) with factor been set 1, 3 and 6 are given in Table 2 and the results tabulated in Table 3. Figure 7 and Figure 8 are covered the result in all parameters sets. In Figure 8, will much focus on when striker select a high-level DOS and at that moment it has a great exceptional. The possibility being stumbled is almost the same because the order will reject the generation in practical by selecting different parameters with a risk it shows us the result which more frequent pw resetting and attacking the foothold attack will minimize the risk of the system [10].

Table 2. DSPN parameter sets



	PD1	PD2	PD3	Dictionary size	Foothold obtain rate	Foothold clear rate	PW reset rate
1	0.9	0.05	0.05	10000	1/30	1/5	1/100
2	0.8	0.1	0.1	5000	1/25	1/10	1/200
3	0.6	0.2	0.2	2500	1/20	1/15	1/400
4	0.2	0.4	0.4	1000	1/15	1/20	1/600
5	0.2	0.2	0.6	100	1/10	1/25	1/800
6	0.1	0.1	0.8	50	1/5	1/30	1/1000

Table 3. Simulation results



	OT=15min			*OT=30min*			*OT=60min*		
	1	*3*	*6*	*1*	*3*	*6*	*1*	*3*	*6*
P_1	0.099	0.379	0.815	0.100	0.377	0.826	0.099	0.383	0.805
P_2	0.032	0.228	0.796	0.013	0.174	0.795	0.005	0.145	0.775
R $/h	122	636	1870	91.7	548	1880	78.6	505	1830

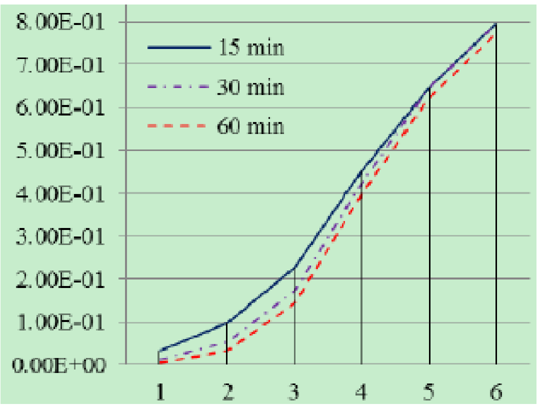


Figure 7. Probability that both lines are tripped with different attack levels and overload tolerance levels

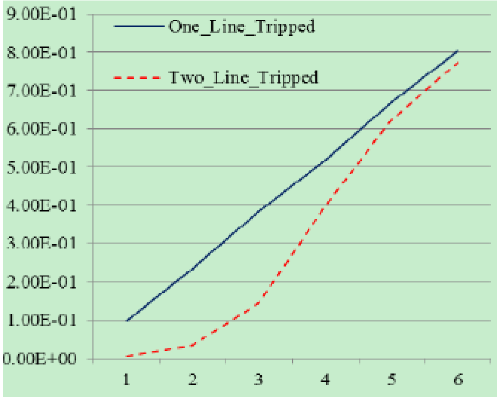


Figure 8. Probability of line loss under different attack level when overheat tolerance level is 60min

4. Conclusion

The typical feature of protection system products, the bus arrangements, and the bus operation modes play a critical role when evaluated the cyber security of power systems. This review studies the bus protection product BP-2C-D and transmission line product RCS-941 for power system risk assessment in cyber attacks considering the role of protection systems. By applying different protection product, a diverse set of results is believed to exist. However, the risk assessment method for the cyber security evaluates in power systems given the role of protection systems still applies. The protections systems could also be more complicated in practical power systems as transformer protection, ground protection, and CB malfunction protection is often included. However, the planned physical behaviour risk assessment method still be quite appropriate for recognizing the trend in this well-timed subject. System protection system is commonly used in the smart grid to address new challenges such as increasingly stressed transmission.

Acknowledgement

The authors would like to thank the Ministry of Higher Education, Malaysia (MOHE), and the Office for Research, Innovation, Commercialization, Consultancy Management (ORICC), Universiti Tun Hussein Onn Malaysia (UTHM) for financially supporting this research under the FRGS grant No. 1529 and IGSP U667.

References

[1] L. Wei, A. I. Sarwat, and W. Saad. *Risk assessment of coordinated cyber-physical attacks against power grids: A stochastic game approach*. IEEE Ind. Appl. Soc. Annu. Meet, 2016; 1–7.

[2] Y. Soupionis, R. Piccinelli, and T. Benoist. *Cyber Security Impact on Power Grid Including Nuclear Plant*. 2016; 8: 767– 773.

[3] C. Tong. *Research and application of active lightning protection technology*. 2010; 2008.

[4] K. Charitoudi and A. Blyth. *An agent-based socio-technical approach to impact a. ssessment for cyber defense*. 4th Int. Conf. Emerg. Intell. Data Web Technol. 2013; 558–563.

[5] SM Blair, CD Booth. *Application of MPLS-TP for Transporting Power System Protection Data*. 2016.

[6] C. I. Ciontea, C. L. Bak, and F. Blaabjerg. *Decentralized Adaptive Overcurrent Protection for Medium Voltage Maritime Power Systems*. 2016; 2569–2573.

[7] I. P. De Siqueira. *Estimating the Impact of Wide-Area Protection Systems on Power System Performance and Reliability*. 2016; 1– 6.

[8] M. V Andreev, A. O. Sulaymanov, and A. S. Gusev. *Simulation of differential protections of transformers in power systems*. 2016; 1–6.

[9] L. Langer, P. Smith, M. Hutle, and A. Schaeffer-Filho*. Analysing cyber-physical attacks to a Smart Grid: A voltage control use case*. Power Syst. Comput. Conference. 2016; 1–7.

[10] X. Liu, M. Shahidehpour, Z. Li, and S. Member. *Power System Risk Assessment in Cyber Attacks Considering the Role of Protection Systems*. 2016; 3053: 1– 8.

[11] P. Wang, A. Ashok, and M. Govindarasu. *Cyber-physical risk assessment for smart grid System Protection Scheme*. IEEE Power Energy Soc. Gen. Meet. 2015; 0-4.

[12] Y. Peng, T. Lu, J. Liu, Y. Gao, X. Guo, and F. Xie. *Cyber-physical system risk assessment*. 9th Int. Conf. Intell. Inf. Hiding Multimed. Signal Process. 2013; 442–447.

[13] G. Dondossola, F. Garrone, and J. Szanto. *Cyber risk assessment of power control systems - A metrics weighed by attack experiments*. IEEE Power Energy Soc. Gen. Meeting. 2011;1–9.

[14] M. Nasir, A. Dysko, P. Niewczas, and G. Fusiek. *All-optical busbar differential protection scheme for electric power systems*. 1–6.

[15] P. Allenbach and C. A. Platero. *Coordination of a Turbo-Generator protections through Power-System Simulation Software SIMSEN*. 2016; 2206– 2211.

[16] J. R. Pesente, J. G. Rolim, and M. Moreto. *MultiAgent Systems in Power System Protection : Review, Classification and Perspectives*.2016; 14(7): 3285–3290.

[17] NVP Babu, PS Babu, DVSS SivaSarma. *A wide-area prospective on power system protection: A state-of-art*. 2015 Int. Conf. Energy, Power Environ. Towar. Sustain. Growth, ICEPE. 2016.

[18] A. Halinka, P. Rzepka, and M. Szablicki. *Agent model of multi-agent system for area power system protection*. Mod. Electr. Power Syst. 2015; 1–4.

[19] G. Wu et al. *Modelling of Special Protection Systems for power system dynamic simulations*. International Conference on Renewable Power Generation.15:1–5.

[20] M. Farhadi, S. Member, and O. A. Mohammed. *A New Protection Scheme for Multi-Bus DC Power Systems Using an Event Classification Approach*. 2015; 9994: 1–7.

[21] F Shahnia, M Moghbel, HH Yengejeh. *Motivating Power System Protection Course Students by Practic.*