

Assessing the impact of investment levels on power system security enhancements and substation automation upgrades

Dharmesh Dhabliya [†]

Department of Information Technology

Vishwakarma Institute of Technology

Pune 411037

Maharashtra

India

Vimal Bibhu ^{*}

Department of Computer Science & Engineering

Noida International University

Greater Noida 203201

Uttar Pradesh

India

Ponmurugan Panneerselvam [§]

Centre for Doctoral Studies

Meenakshi Academy of Higher Education and Research

Chennai 600078

Tamil Nadu

India

Naveen Jain [‡]

Department of Mechanical Engineering

Shri Shankaracharya Institute of Professional Management & Technology

Raipur 492015

Chhattisgarh

India

[†] E-mail: dharmesh.dhabliya@viit.ac.in

^{*} E-mail: vimal.bhibu@niu.edu.in (Corresponding Author)

[§] E-mail: ponmurugan@maher.ac.in

[‡] E-mail: n.jain@ssipmt.com

Avinash M. Pawar^{*}

Department of Mechanical Engineering
Bharati Vidyapeeth's College of Engineering for Women
Pune 411043
Maharashtra
India

Abstract

This research looks at how different levels of spending affect the safety of the power system and the automation of substations. Power networks are facing more and more cyber and physical dangers, such as SCADA hacks and cascading breakdowns, as they rely more and more on digital control and tracking systems. The study looks at low, medium, and high spending plans using cybersecurity risk score models and dynamic stability tests in MATLAB/PSCAD. The results show that higher spending greatly lower risks, make systems more reliable, and boost the efficiency of automation. The results make it clear how important it is to keep giving focused funds to make sure that energy systems are strong, scalable, and ready for the future so they can handle new security problems.

Subject Classification: 68M25.

Keywords: Power system security, Substation automation, Cybersecurity risk scoring, Dynamic stability modeling, Investment impact.

I. Introduction

Investing strategically in security improvements and base automation changes is becoming more and more important for bringing electric power systems up to date [1, 2]. Cyber and physical dangers to power networks are

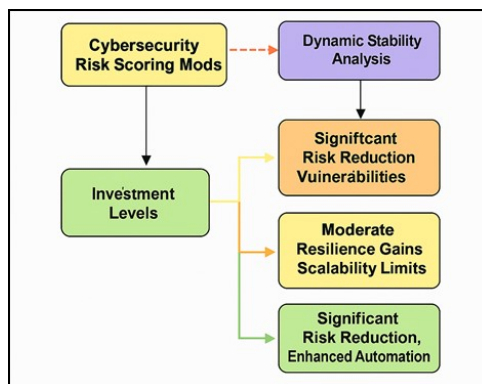


Figure 1
Multicolor Architecture of Investment Impact on Power System Security and Substation Automation

^{*} E-mail: avinash.m.pawar@bharativedyapeeth.edu

growing. These include malware attacks on supervisory control and data acquisition (SCADA) systems and failures that happen one after another because of not enough protection measures [3]. As more utilities switch to digital tracking and control systems, the area that can be attacked grows. This makes hacking an important part of keeping the power system stable [4, 5, 6].

At the same time, adding automation technologies improves speed, problem finding, and real-time reaction, but the benefits depend a lot on how much money is spent on these changes [7, 8]. How strong the technical side of these modernisation attempts is and how long they can last economically depend on how much money is invested (Illustrate in Figure 1). Low levels may only lead to small improvements that don't fix weaknesses. Medium and high levels, on the other hand, can lead to steady changes in resistance and scale [9, 10].

II. Method Work

A. Cybersecurity risk scoring models for automation infrastructure

Cybersecurity risk score models look at holes in automation infrastructure and make security ratings based on how likely it is that an attack will happen, how important the assets are, and how vulnerable they are to threats [11, 12, 13]. These ratings help people decide where to put their money.

Define asset set: $A = \{a_1, a_2, \dots, a_n\}$

Define threat set: $T = \{t_1, t_2, \dots, t_m\}$

Estimate threat likelihood: $L(t_j) \in [0,1]$

Define vulnerability severity: $V(a_i, t_j) \in [0,1]$

Calculate exposure:

$$E(a_i, t_j) = L(t_j) * V(a_i, t_j) \quad (1)$$

Compute asset risk contribution:

$$R(a_i, t_j) = w(a_i) * E(a_i, t_j) \quad (2)$$

Aggregate over threats:

$$R(a_i) = \sum (R(a_i, t_j)) \text{ for } j = 1 \text{ to } m \quad (3)$$

Normalize asset risk:

$$R_{norm}(a_i) = \frac{R(a_i)}{\max(R(a))} \quad (4)$$

Define system risk index:

$$R_{sys} = \left(\frac{1}{n}\right) * \sum (R_{norm}(a_i)) \text{ for } i = 1 \text{ to } n \quad (5)$$

Introduce mitigation factor:

$$M(a_i, t_j) \in [0,1]$$

Adjusted risk:

$$R'(a_i, t_j) = R(a_i, t_j) * (1 - M(a_i, t_j)) \quad (6)$$

Aggregate mitigated risk:

$$R'(a_i) = \sum (R'(a_i, t_j)) \text{ for } j = 1 \text{ to } m \quad (7)$$

Normalize mitigated system risk:

$$R'sys = \left(\frac{1}{n}\right) * \Sigma \left(R' \frac{ai}{\max(R'(a))}\right) \text{ for } i = 1 \text{ to } n \quad (8)$$

Cybersecurity risk score:

$$CRS = 100 * (1 - R'sys) \quad (9)$$

B. Power system dynamic stability modeling (e.g., MATLAB/PSCAD)

Dynamic stability modelling in MATLAB or PSCAD models shocks, checks how the system responds, and finds stability boundaries. This makes sure that successful automation changes improve operational robustness at different levels of investment.

Define bus set:

$$B = \{b1, b2, \dots, bn\}$$

Define generator set:

$$G = \{g1, g2, \dots, gk\}$$

Represent system with admittance matrix: Ybus

Generator swing equation:

$$Mi * \left(\frac{d^2\delta i}{dt^2}\right) + Di * \left(\frac{d\delta i}{dt}\right) = Pmi - Pei \quad (10)$$

Electrical power output:

$$Pei = |E'i|^2 Gi + \Sigma |E'i||E'j|(Gij \cos \delta ij + Bij \sin \delta ij), j \neq i \quad (11)$$

Rotor angle difference:

$$\delta ij = \delta i - \delta j$$

Linearize dynamics:

$$\Delta x_{dot} = A\Delta x + B\Delta u \quad (12)$$

State vector:

$$x = [\delta, \omega]^T$$

Jacobian matrix:

$$J = \frac{\partial f}{\partial x} \quad (13)$$

Stability condition:

$$Re(\lambda k) < 0 \forall k$$

Damping ratio:

$$\zeta = \frac{-\sigma}{\sqrt{\sigma^2 + \omega^2}} \quad (14)$$

Critical clearing time:

$$tc \approx \frac{(2H(\delta cr - \delta 0))}{Pa} \quad (15)$$

Lyapunov function:

$$V(\delta, \omega) = \left(\frac{1}{2}\right) M \omega^2 + \int (P_m - P_e) d\delta \quad (16)$$

Improved stability index:

$$SI = \frac{SM}{(1 + e^{-\alpha})} \quad (17)$$

III. Impact of Investment Levels on Power System Security

A. Low-level investments: minimal improvements and vulnerabilities

Low-level purchases don't make a big difference because they only improve basic system tasks. Critical flaws still exist, cybersecurity isn't getting enough money, and changes to resiliency aren't enough to stop failures from spreading when things go wrong.

Define risk exposure factor:

$$RE \in [0,1]$$

Residual vulnerability:

$$V_{res} = V_0 * (1 - I_{low})$$

Define resilience function:

$$R_{low} = \alpha_1 * I_{low}$$

Cybersecurity improvement:

$$C_{imp} = \beta_1 * I_{low} \quad (18)$$

Failure probability:

$$P_f = V_{res} * (1 - R_{low}) \quad (19)$$

Reliability index:

$$RI = 1 - P_f \quad (20)$$

Automation effectiveness:

$$AE = \gamma_1 * I_{low} \quad (21)$$

Security index:

$$SI = \frac{(R_{low} + C_{imp})}{2} \quad (22)$$

Net performance gain:

$$PG = \frac{RI + AE + DR}{3} \quad (23)$$

Sustainability score:

$$SS = PG - C_f \quad (24)$$

Overall low-level impact:

$$I_{Low} = \theta_1 * (SI + PG + SS) \quad (25)$$

B. Medium-level investments: moderate resilience gains with scalability limits

Medium-sized investments make systems more resilient by adding better automation and some safety measures. But scale is still limited, long-term

flexibility is also limited, and new threats may be bigger than the defences that are currently in place.

Define investment level:

$$IL_{med} \in (0.3, 0.7]$$

Cybersecurity enhancement:

$$Cenh = \beta_2 * \log(1 + IL_{med}) \quad (26)$$

System recovery factor:

$$SR = \gamma_2 * \sqrt{IL_{med}} \quad (27)$$

Failure probability:

$$Pf = V_{med} * (1 - R_{med}) \quad (28)$$

Security effectiveness:

$$SE = \frac{R_{med} + Cenh + SR}{3} \quad (29)$$

Net resilience index:

$$NRI = \frac{RI + AImpr + DR}{3} \quad (30)$$

Long-term adaptability:

$$LA = SC - CI$$

Performance gain:

$$PG = \frac{SE + NRI + LA}{3} \quad (31)$$

Normalized performance:

$$PN = \frac{PG}{(1 + e^{-IL_{med}})} \quad (32)$$

Overall medium-level impact:

$$IMed = \theta_2 * PN$$

IV. Result and Discussion

Table 1 shows that low spending only lowers hacking risk by 18.5%, with 74.2% reliability and 62.7% automation efficiency, which means that there aren't many changes.

Table 1
Security and Operational Performance Across Investment Levels

Investment Level	Cybersecurity Risk Reduction (%)	System Reliability Index (%)	Automation Efficiency (%)
Low	18.5	74.2	62.7
Medium	46.8	85.6	79.3
High	72.4	94.1	91.5

Medium spending leads to better results, lowering risk by 46.8%, increasing reliability to 85.6%, and increasing efficiency to 79.3%, but it's still

hard to make the system bigger. When you spend a lot of money, you get the best results: 72.4% less danger, 94.1% more stability, and 91.5% more efficiency (in Figure 2). This makes the system much more resilient.

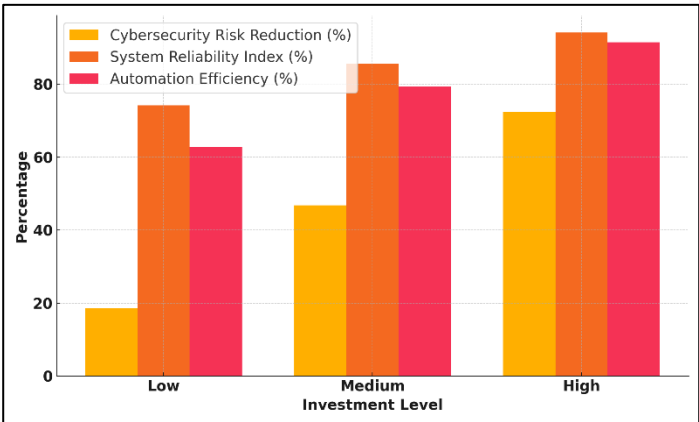


Figure 2
Impact of Investment Level on Cybersecurity, Reliability, and Automation

V. Conclusion

This study shows how important funding levels are for making the power system safer and automating substations. Low investments only make things a little better, leaving weaknesses that can't be fixed. Medium investments make things somewhat more resilient, but they can't be expanded. To protect against changing physical and online dangers, you need focused, long-term funds along with advanced modelling and automation strategies. Prioritising optimised investment improves system stability, reliability, and flexibility, protecting important assets and helping to build secure energy networks that are ready for the future.

References

- [1] M. Bahrami, M. Fotuhi-Firuzabad, and H. Farzin, "Reliability evaluation of power grids considering integrity attacks against substation protective IEDs," *IEEE Trans. Ind. Inform.*, vol. 16, pp. 1035–1044 (2020).
- [2] S. Zhang, G. Pan, B. Li, W. Gu, J. Fu, and Y. Sun, "Multi-timescale security evaluation and regulation of integrated electricity and heating system," *IEEE Trans. Smart Grid* (2024).

- [3] Y. Xiang, T. Wang, and Z. Wang, "A framework for preventive control of power systems to defend against extreme events," *CSEE J. Power Energy Syst.*, vol. 10, pp. 856–870 (2023).
- [4] F. Faramarzi, T. Niknam, J. Aghaei, and M. Rashidi, "Resiliency enhancement of power system against intentional attacks," *IET Renew. Power Gen.*, vol. 16, pp. 3544–3558 (2022).
- [5] L. Che, X. Liu, and Z. Li, "Screening hidden N-k line contingencies in smart grids using a multi-stage model," *IEEE Trans. Smart Grid*, vol. 10, pp. 1280–1289 (2019).
- [6] D. Shete and P. Khobragade, "An empirical analysis of different data visualization techniques from statistical perspective," *AIP Conf. Proc.*, vol. 2839, no. 1, (2023).
- [7] Y. Zhao, Y. Cao, Y. Li, B. Zeng, M. Shahidehpour, and Y. Cai, "Risk-based contingency screening method considering cyber-attacks on substations," *IEEE Trans. Smart Grid*, vol. 13, pp. 4973–4976 (2022).
- [8] N. Romero, N. Xu, L. K. Nozick, I. Dobson, and D. Jones, "Investment planning for electric power systems under terrorist threat," *IEEE Trans. Power Syst.*, vol. 27, pp. 108–116 (2012).
- [9] V. Alok and J. S. Sodhi, "Statistical method for prediction of a targeted spear phishing attack," *J. Inf. Optim. Sci.*, vol. 45, no. 7, pp. 1843–1856 (2024), doi: 10.47974/JIOS-1734.
- [10] T. H. Fritts, "Economic costs of electrical system instability and power outages caused by snakes on the island of Guam," *Int. Biodeterior. Biodegrad.*, vol. 49, pp. 93–100 (2002).
- [11] M. A. A. Sheela, M. Tejaswi, N. B. Prakash, M. D. S. Tulasi, and K. Anitha, "IntegriScan: A Graph-Aided Model for Detecting Corrupted and Anomalous Data Patterns", *IJRAET*, vol. 14, no. 1, pp. 71–78 (Apr. 2025).
- [12] M. G. Dhote, B. M. Nanche, P. N. Mahalle, S. S. Ali, M. Gulhane, and V. S. Karwande, "Deep learning for optimized path planning in autonomous vehicles by integrating reinforcement learning with convolutional neural networks," *Journal of Information and Optimization Sciences*, vol. 46, no. 4-B, pp. 1129–1139 (2025).
- [13] I. Mohan, M. Venkataraman, and K. Thilagavathi, "Investigating utilizations of harmonic univalent functions employing the Prabhakar fractional operator within specific categories," *J. Interdiscip. Math.*, vol. 27, no. 5, pp. 1099–1108 (2024).

Received April, 2025