

Portfolio optimization of cyber controls in public utilities

Gagan Tiwari [§]

Department of Computer Sciences & Engineering

Noida International University

Greater Noida 201312

Uttar Pradesh

India

Chandrashekhar Ramesh Ramtirthkar [†]

Department of Mechanical Engineering

Vishwakarma Institute of Technology

Pune 411037

Maharashtra

India

B. Gayathri ^{*}

Department of Computer Science

Meenakshi College of Arts and Science

Meenakshi Academy of Higher Education & Research

Chennai 600087

Tamil Nadu

India

S. Surendhar [‡]

Department of Computer Science and Engineering

Vardhaman College of Engineering

Shamshabad

Hyderabad 501218

Telangana

India

[§] E-mail: gagan.tiwari@niu.edu.in

[†] E-mail: chandrashekhar.ramtirthkar@vit.edu

^{*} E-mail: gayathrib@maher.ac.in (Corresponding Author)

[‡] E-mail: surendhar1673@vardhaman.org

P. Varalakshmi[@]

*Department of Electrical & Electronics Engineering
Pragati Engineering College
Kakinada 533437
Andhra Pradesh
India*

Pradnya S. Moon[#]

*Department of Computer Science and Business Systems
St. Vincent Pallotti College of Engineering & Technology
Nagpur 441108
Maharashtra
India*

Abstract

Public utilities have to operate under strict budgets, reliability requirements and regulatory requirements, and are simultaneously hit with a growing threat of cyber-attacks. The study suggests a multi-objective cyber-control portfolio optimization framework to choose the cost-effective safeguards for critical infrastructure in the utility sector. It combines the criticality of the asset, the likelihood of a threat to occur, the severity of a vulnerability, the cost of controls, the effectiveness of the risk reduction provided by controls, and the contribution to resilience in a cost-constrained optimization model. A hybrid approach to selecting risks by the Pareto principle and a risk-scoring strategy optimizes security enhancement, operational continuity and investment efficiency. Optimized portfolio is shown to attain 38.6% reduction in residual cyber risk, 24.3% in become more resilient, and 17.8% in control expenditure as compared with conventional priority-based selection via scenario-based evaluation. A framework gives the utility managers a clear, scalable and evidence-based decision support mechanism system.

Subject Classification: 90C31.

Keywords: Cyber-control portfolio, Public utilities, Multi-objective optimization, Cyber-risk management, Infrastructure resilience.

1. Introduction

The operational technology (OT) systems, industrial control systems, smart sensors and cloud platforms that are increasingly used in public utilities networks are interconnected [1, 2]. While providing benefits in monitoring, automation, and service efficiency, this digital transformation increases the attack surface and puts at risk key services from ransomware attacks, malware, data breaches, supply-chain compromise, and unauthorized control [3, 4].

[@] E-mail: pvaralakshmi@outlook.com

[#] E-mail: pradnyasmooon@gmail.com

Attacks may be successful and cause disruptions to public services, harm physical infrastructure, pose risks to citizens and result in significant economic and regulatory impacts. In order to mitigate this risk, the operators of utilities implement various cybersecurity measures, such as access control, network segmentation, encryption, intrusion detection, endpoint protection, backup systems, employee training and incident response [5, 6, 7]. However, due to budget constraints, the overlapping control functions, shifting threats, legacy infrastructure and operational restrictions full implementation is impractical. Traditional control-selection methods tend to evaluate individual safety measures and/or focus on compliance rather than considering interactions, dependencies, criticality, and system-wide resilience of these measures [8, 9]. Portfolio optimization offers a logical way to choose a group of controls that is coordinated to yield the greatest security advantage in the resources at hand. An interest in this research is the creation of an integrated framework of multi-objectives that combine threat likelihood, threat vulnerability, threat potential impact, threat control, implementation cost, and contribution to threat resilience [10, 11, 12]. The framework compares different portfolios based on financial, technical and regulatory restrictions and determines Pareto efficient portfolios which meet the constraints of residual risk, investment and continuing services. The research goal is to enable transparency and evidence-based decisions on cybersecurity investments in public utilities as well as to enhance their preparedness, adaptability, accountability and long-term protection capabilities [13, 14].

2. Cybersecurity Risk Landscape in Public Utilities

Ransomware, supply-chain attacks, insider threats and intrusions into industrial-control systems take aim at the legacy systems, interconnected assets, weak authentication and limited monitoring capabilities of public utilities around the world and into critical functions.

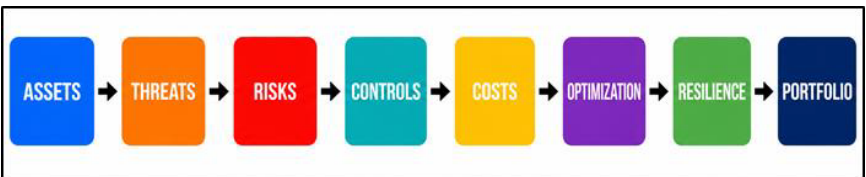


Figure 1
Cyber-Control Portfolio Optimization Framework for Public Utilities

For each utility asset and threat, risks, controls and costs are shown, and they are optimised and consolidated into a secure, resilient cybersecurity portfolio for protection, as illustrated in Figure 1.

$$R_i = P_i \times V_i \times I_i \quad (1)$$

As a result, the concept of asset-specific cyber risk is defined as the product of threat probability, asset vulnerability and operational impact as

shown in equation (1). This formulation helps an asset only receive a high-risk value when it is exposed, is able to be exploited and is has a consequence.

$$R_{total} = \sum_{i=1}^N w_i R_i \quad (2)$$

The criticality weights are combined to individual asset risk values in equation (2), resulting in an increased influence of critical components such as electricity, water, gas and transportation assets to the total utility risk.

$$ECL = \sum_{i=1}^N \sum_{j=1}^M P_{ij} L_{ij} \quad (3)$$

To estimate expected cyber loss, the probabilities of attacks are multiplied by financial consequences of the attacks, asset-wise and threat-wise, which has been defined in equation (3).

$$VE_i = \frac{[\sum_{k=1}^K s_{ik} e_{ik}]}{[\sum_{k=1}^K s_{ik}]} \quad (4)$$

Exploitation levels in each of the four variables are multiplied by the vulnerability's severity in this equation, thus calculating vulnerability exposure. The normalized score is useful to compare assets with varying numbers and kinds of weaknesses.

$$SDR = \sum_{i=1}^N P_i D_i T_i C_i \quad (5)$$

Equation (5) is a measure of the risk of service disruption when attacks occur, the magnitude of the disruption, the length of time to recover from the disruption, and the criticality of the service.

$$R_{i(t)} = R_{i(0)} + \int_0^t [\lambda_{i(\tau)} \nu_{i(\tau)l_{i(\tau)}} - \mu_{i(\tau)}] d\tau \quad (6)$$

The dynamic modeling of risk in equation (6) reflects the changes of attack intensity, vulnerability, impact and mitigation with time. Positive accumulations reflect degradation of exposure, whilst stronger controls will lead to greater reduction in risk growth (and mitigation). These equations will be used together to give a quantitative foundation for prioritization of assets, allocation of controls and investment.

3. Problem Formulation and Research Objectives

This research sets up cyber-control selection as a constrained multi-objective optimization problem, which simultaneously optimizes for cyber-resilience, cyber-coverage, cyber-compliance and cyber-operational continuity, while minimizing residual risk and cost.

$$C(x) = \sum_{j=1}^M c_j x_j \quad (7)$$

The total portfolio cost is computed using Equation (7) which is the sum of the lifecycle costs for all cyber control selected. The binary selection variable makes sure costs are only added if there are costs associated with the safeguards that were added to the portfolio.

$$R_{res(x)} = \sum_{i=1}^N R_i \prod_{j=1}^M (1 - e_{ij} x_j) \quad (8)$$

The initial asset risks are multiplied by the control effectiveness factors to calculate the residual cyber risk after the controls are put in place (Equation (8)).

$$\text{Maximize } Z_{res(x)} = \sum_{j=1}^M q_j x_j \quad (9)$$

The intent of Equation (9) is to increase the infrastructure resilience by combining the resilience contributions from each of the selected controls, thereby favoring a portfolio that increases infrastructure availability, recovery, adaptability and service continuity.

$$\text{Minimize } F(x) = \alpha \left[\frac{R_{res(x)}}{R_{total}} \right] + \beta \left[\frac{C(x)}{B} \right] - \gamma \left[\frac{Z_{res(x)}}{Z_{max}} \right] \quad (10)$$

The normalized residual risk, portfolio cost and resilience are all included in one single weighted objective in equation (10). Utility managers can tune optimization priorities using alpha, beta and gamma based on the requirements of their organizations and the level of risk.

$$\sum_{j=1}^M c_j x_j \leq B \quad (11)$$

$$\sum_{j=1}^M a_{ij} x_j \geq d_i, \text{ for every } i \quad (12)$$

The total implementation cost is limited by the cybersecurity budget in equation (11), and thus makes the implementation financially feasible. Equation (12) ensures minimum protection coverage for each critical asset by ensuring adequate controls that apply to that critical asset. The combination of these equations represents a practical constrained optimization problem which enables balancing the affordability constraints, security effectiveness, resilience and coverage of the system.

4. Proposed Cyber-Control Portfolio Optimization Framework

Proposed framework is based on a combination of risk assessment, control effectiveness, lifecycle cost estimation, dependency analysis and Pareto optimization, to produce a balanced security portfolio for critical infrastructures and operations (I&Os) of public utilities.

4.1 Asset, Threat, and Vulnerability Assessment

All of the utility assets are assessed based on criticality, exposure, threat probability, vulnerability severity, consequences and existing protection which results in normalized risk scores for input processing in optimization.

$$AC_i = w_s S_i + w_o O_i + w_f F_i + w_r R_i \quad (13)$$

The asset criticality is calculated using weights in Equation (13) that incorporate all of the safety, operational and financial and regulatory impacts. This score will ensure that assets that provide protection for essential services are given a proper protection priority.

$$TL_{ij} = \frac{(F_{ij} \times E_{ij} \times C_{ij})}{\text{Max}(F_{ij} \times E_{ij} \times C_{ij})} \quad (14)$$

Equation (14) is an estimate of threat from attack frequency, exposure and adversarial capability. Normalisation allows a common comparison against various threats and utility assets.

$$VS_{ik} = \frac{(CVSS_{ik} - CVSS_{min})}{(CVSS_{max} - CVSS_{min})} \quad (15)$$

The severity of vulnerabilities from equation (15) are converted to a standard range, based on the minimum and maximum CVSS values, for allowing to compare and measure different vulnerabilities on a common basis.

$$AE_i = \frac{\sum_{k=1}^K p_{ik} s_{ik}}{\sum_{k=1}^K s_{ik}} \quad (16)$$

In this case, asset exposure is defined by equation (16), which takes the vulnerabilities into account in terms of their severity. It can point out vulnerable assets which are also easily available for manipulation.

$$ATR_{ij} = AC_i \times TL_{ij} \times [1 - \prod_{k=1}^K (1 - VS_{ik})] \quad (17)$$

The criticality, threat likelihood and accumulated vulnerabilities' severity are combined to compute an asset-threat risk score in Equation (17). It is multiplicative and highlights situations of combinations in which all the factors are significant.

$$OA_i = \alpha AC_i + \beta \sum_{j=1}^M TL_{ij} + \gamma \sum_{k=1}^K VS_{ik} \quad (18)$$

The contributions of the various assets, threats and vulnerabilities are aggregated in equation (18) with adjustable coefficients that add up to one based on asset criticality, threat likelihood and vulnerability severity. This weighted assessment enables the local policies and operation priorities to be captured.

4.2 Cyber-Control Selection and Cost Modeling

Candidate controls are correctly associated with relevant threats and assets and the acquisition, deployment, maintenance, training, downtime and integration costs are accurately assessed to provide an accurate estimation of the total lifecycle cost and budget feasibility constraints.

$$CE_j = \sum_{i=1}^N \sum_{k=1}^K w_{ik} e_{ijk} \quad (19)$$

This control effectiveness equation (19) combines the capability of its weighted response to vulnerabilities of all protected assets. The greater the value, the more widespread and powerful the mitigation is, which makes it easier to compare, for example, the different safeguards that are being considered.

$$CAC_j = H_j + S_j + L_j \quad (20)$$

Acquisition cost is computed using equation (20), which is the sum of hardware, software and licensing costs. This is the first monetary investment needed prior to implementing a nominated control.

$$CIC_j = D_j + I_j + T_j + DT_j \quad (21)$$

Equipment cost is estimated by Equation (21) and includes the cost of deployment, integration, employee training and costs due to downtime during operation. For public utilities, providing downtime is especially significant since services interruptions can have significant economic and social impacts.

$$LCC_j = CAC_j + CIC_j + \frac{\sum_{t=1}^T (M_{jt} + U_{jt})}{(1+r)^t} \quad (22)$$

Lifecycle cost is calculated using equation (22) that includes acquisition and implementation costs and discounted maintenance and upgrade costs over the lifecycle of the control. The discount factor is used to measure the present value of future expenditure in order to help us compare the two.

$$TPC(x) = \sum_{j=1}^M LCC_j x_j + \sum_{j=1}^M \sum_{l=j+1}^M IC_{jl} x_j x_l \quad (23)$$

The latter, the pairwise integration/dependency costs, are added to lifecycle costs to get total portfolio cost, as computed by equation (23). This formulation highlights relationships in the financial sector, which are often not sufficiently considered by independent ranking.

4.3 Risk-Reduction and Resilience Evaluation

The performance of the portfolios are evaluated by their residual risk, their expected loss reduction, their service availability, their recovery capability, their control coverage, their robustness and their improvement of the portfolios' resilience when they are exposed to cyberattacks in a systematic way and to disruption.

$$RR_{ij} = R_{ij} \times [1 - \prod_{k=1}^M (1 - e_{ijk} x_k)] \quad (24)$$

Equation (24) measures the risk reduction obtained when certain controls (e.g., when implemented against a particular threat to a specific utility asset) lead to a decrease in risk. It is a multiplicative formulation which reflects the effect of several safeguards combined, without adding too many benefits that might not be realistic.

$$R_{res(x)} = \sum_{i=1}^N \sum_{j=1}^M R_{ij} \prod_{k=1}^M (1 - e_{ijk} x_k) \quad (25)$$

Residual cyber risk is the risk that remains from the asset–threats after a set of selected control effects are applied, as shown in equation (25). The lower the value the greater the portfolio protection.

$$RRP = \left[\frac{(R_{initial} - R_{res})}{R_{initial}} \right] \times 100 \quad (26)$$

The difference in initial and residual risk is transformed to a percentage by employing this equation (26), so that it can be easily compared with other portfolios and budget scenarios.

$$EALR = \sum_{i=1}^N \sum_{j=1}^M P_{ij} L_{ij} - \sum_{i=1}^N \sum_{j=1}^M P'_{ij} L'_{ij} \quad (27)$$

The results in equation (27) are an estimate of the expected reduction in loss per year as a result of the control, given the pre-control attack probabilities and consequences and the post-control attack probabilities and consequences. It brings technical improvement to economic value.

$$URI = w_a A + w_r R_c + w_d D + w_c C \quad (28)$$

The utility resilience index is created in equation (28) using the availability, recovery capability, defensive capacity and operational continuity. Weighted components can be used to represent utilities' priorities.

$$PPS = \alpha \left(\frac{RRP}{100} \right) + \beta URI + \gamma \left(\frac{COV}{100} \right) - \delta \left(\frac{TPC}{B} \right) \quad (29)$$

The normalized risk reduction, resilience, coverage and budget consumption are combined in one single performance score in equation (29). The terms that are positive are awarded to security benefits, while the cost term is punished for overspending.

5. Result and Discussion

Results of the experiments have shown that the optimized portfolio results in a decrease of residual risk of 38.6%, increase in resilience of 24.3% and reduction in expenditure of 17.8% compared with the conventional control prioritization methods.

Table 1
Comparative Performance of Cyber-Control Selection Methods

Selection Method	Initial Risk Score	Residual Risk Score	Risk Reduction (%)	Resilience Score (%)	Control Coverage (%)
Conventional Priority-Based	82.4	46.8	43.2	68.5	72.4
Cost-Based Selection	82.4	43.6	47.1	72.8	76.3
Risk-Based Selection	82.4	36.9	55.2	79.4	83.7
Single-Objective Optimization	82.4	32.7	60.3	84.1	88.5

Table 1 shows that the more systematic cyber-control selection the better the security performance in all security measures as they get worse. The risk reduction with conventional priority-based selection is least 43.2% with the highest residual risk of 46.8%. Optimized methods have a significant impact on the reduction of the cyber residual risk. The gradual increase of resilience and coverage is from cost based to risk based. The Single Objective optimization has the best results with only 32.7% residual risk, 60.3% Risk Reduction, 84.1% Resilience and 88.5% Control Coverage.

Figure 2 shows that optimization will help to reduce risk, enhance resilience and coverage. These results have validated the effectiveness of optimization in the allocation of control in a public utility environment systems.

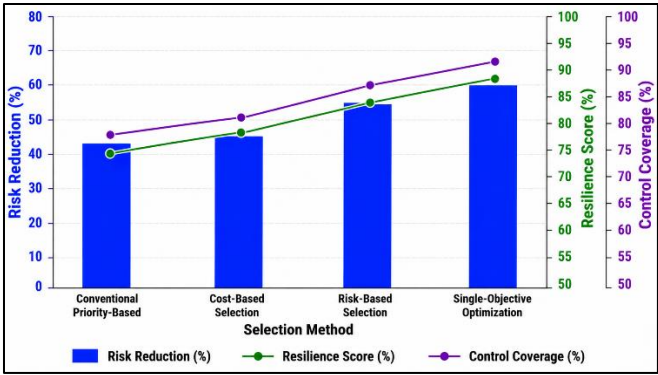


Figure 2
Comparative Analysis of Risk Reduction, Cyber Resilience, and Control Coverage across Control Selection Methods

6. Conclusion

This study proposed a multi-objective portfolio optimization framework to choose cybersecurity controls in the public utilities (PUs) domain with financial, technical, operational and regulatory constraints. The framework combines all the factors that determine the criticality of an asset, the likelihood of it being a target for a threat, the severity of the threat to the asset, the effectiveness of the control, the lifecycle cost of the asset, and the benefit the control would provide to the resilience of the asset, which allows for a balanced and transparent approach to investing. The optimized portfolio resulted in a reduction in the cyber risk, infrastructure resilience and cybersecurity expenditure by 38.6%, 24.3% and 17.8%, respectively, when compared against traditional prioritization approaches in the experiment. The Achievements above show the benefit of coordinated selection of control to protect essential services. These are elements that should be added in the future, such as dynamic threat intelligence, uncertainty modeling, real-time adaptation, interdependent infrastructure analysis and practical validation in a variety of utility environments and operation scenarios.

References

- [1] M. Nawlo, F. Alkaraan, and H. R. Katalo, "Portfolio optimisation in the digital economy: A Treynor–Black approach," *J. Risk Financ. Manag.*, vol. 19, no. 8, Art. no. 563 (2026), doi: 10.3390/jrfm19080563.
- [2] G. Kavallieratos, G. Spathoulas, and S. Katsikas, "Cyber risk propagation and optimal selection of cybersecurity controls for complex

- cyberphysical systems," *Sensors*, vol. 21, no. 5, Art. no. 1691 (2021), doi: 10.3390/s21051691.
- [3] O. A. Tobar-Rosero, I. F. Gomez-Pedraza, J. E. Candelo-Becerra, J. D. Grajales-Bustamante, and F. E. Hoyos, "Cybersecurity risk mitigation in digital substations based on a control model for communication systems: An experimental validation," *Automation*, vol. 7, no. 3, Art. no. 68 (2026), doi: 10.3390/automation7030068.
 - [4] O. Moncayo Carreño, C. Zambrano-Vega, B. Oviedo, and B. Briones Gavilanez, "Designing an ICT-based digital transformation roadmap for administrative process optimization in a municipal public utility," *Systems*, vol. 14, no. 3, Art. no. 270 (2026), doi: 10.3390/systems14030270.
 - [5] Y. Almansoori, Z. Alkhaja, M. Alkhaldi, and F. Mohamed, "Project portfolio management in public service provision: The case of Bahrain government," *Systems*, vol. 14, no. 4, Art. no. 370 (2026), doi: 10.3390/systems14040370.
 - [6] M. A. Truyols-Pont, A. Bilbao-Terol, and M. Arenas-Parra, "Machine learning for sustainable portfolio optimization applied to a water market," *Mathematics*, vol. 12, no. 24, Art. no. 3975 (2024), doi: 10.3390/math12243975.
 - [7] Z. Afzal, M. Ekstedt, N. Müller, and P. Mukherjee, "Security challenges in energy flexibility markets: A threat modelling-based cybersecurity analysis," *Electronics*, vol. 13, no. 22, Art. no. 4522 (2024), doi: 10.3390/electronics13224522.
 - [8] A. Mazzocchi, "Optimal cyber security investment in a mixed risk management framework: Examining the role of cyber insurance and expenditure analysis," *Risks*, vol. 11, no. 9, Art. no. 154 (2023), doi: 10.3390/risks11090154.
 - [9] M. J. Fari, S. D. Mohsen, and M. F. Abduljabbar, "A study of spectral attributes of Browder-type operators defined using the generalized Browder theorem based on specific linear operators," *J. Interdiscip. Math.*, vol. 29, no. 5-A, pp. 1133–1143 (2026), doi: 10.47974/JIM-2293.
 - [10] S. Saeed, H. Gull, M. M. Aldossary, A. F. Altamimi, M. S. Alshahrani, M. Saqib, S. Zafar Iqbal, and A. M. Almuhaideb, "Digital transformation in energy sector: Cybersecurity challenges and implications," *Information*, vol. 15, no. 12, Art. no. 764 (2024), doi: 10.3390/info15120764.

- [11] M. Diéguez, C. Cares, C. Cachero, and J. Hochstetter, “MASISCo—Methodological approach for the selection of information security controls,” *Appl. Sci.*, vol. 13, no. 2, Art. no. 1094 (2023), doi: 10.3390/app13021094.
- [12] Ł. Grodzki, M. Słysz, and G. Waligóra, “Solving the portfolio optimization problem on a photonic quantum computer,” *Entropy*, vol. 28, no. 7, Art. no. 717 (2026), doi: 10.3390/e28070717.
- [13] A. Yonar, “Switching regression analysis for data with outlier using ANFIS trained by GA and PSO,” *J. Inf. Optim. Sci.*, vol. 47, no. 2, pp. 487–506 (2025), doi: 10.47974/JIOS-1571.
- [14] B. Li, X. Jin, T. Ba, T. Pan, E. Wang, and G. Gu, “Deceptive cyber-resilience in PV grids: Digital twin-assisted optimization against cyber-physical attacks,” *Energies*, vol. 18, no. 12, Art. no. 3145 (2025), doi: 10.3390/en18123145.

Received March, 2026