Design and Implementation of a Process of Risk-Based Criticality for Network Utilities Asset Management

Diseño e implementación de un proceso de criticidad basada en el riesgo para la gestión de activos de utilidades de red

Markus Dwiyanto Tobi Sogen
Politeknik Katolik Saint Paul - Indonesia
dwiyanto@poltekstpaul.ac.id
Retnawati Siregar
Universitas Medan Area, Medan - Indonesia
Phong Thanh Nguyen[1]
Ho Chi Minh City Open University - Vietnam
phong.nt@ou.edu.vn
E. Laxmi Lydia
Vignan's Institute of Information Technology - India
shankarcrypto@gmail.com
K. Shankar
Alagappa University, Karaikudi - India
shankarcrypto@gmail.com

ABSTRACT

The prioritization of critical assets and foundations of criticality of infrastructures is required for basic framework security. Be that as it may, criticality examination isn't yet institutionalized. This paper studied the connection of criticality and risk. Basic risk assessment management model is proposed and also take a look about criticality analysis. For network utility asset management a process of risk based critically is designed and implemented. The result of performance is shown through the performance curve.

Keywords: critical assets, criticality, network based, risk management.

RESUMEN

La priorización de los activos críticos y los fundamentos de la criticidad de las infraestructuras es necesaria para la seguridad básica del marco. Sea como fuere, el examen de criticidad aún no está institucionalizado. Este artículo estudió la conexión de criticidad y riesgo. Se propone un modelo básico de gestión de evaluación de riesgos y también eche un vistazo al análisis de criticidad. Para la gestión de activos de servicios públicos de red, se diseña e implementa un proceso de riesgo basado críticamente. El resultado del rendimiento se muestra a través de la curva de rendimiento.

Palabras clave: activos críticos, criticidad, basada en redes, gestión de riesgos.

RESUMO

A priorização de ativos críticos e os fundamentos da criticidade das infra-estruturas são necessários para a segurança básica da estrutura. Seja como for, o exame de criticidade ainda não está institucionalizado. Este artigo estudou a conexão entre criticidade e risco. O modelo básico de gerenciamento de avaliação de riscos é proposto e também analisa a análise de criticidade. Para o gerenciamento de ativos de serviços de rede, um processo de risco crítico é projetado e implementado. O resultado do desempenho é mostrado através da curva de desempenho.

Palavras-chave: ativos críticos, criticidade, baseada em rede, gerenciamento de riscos.

1 Corresponding author. Department of Project Management, Ho Chi Minh City Open University, Vietnam.

Recibido: 24/07/2019 Aceptado: 16/09/2019

I. INTRODUCTION

It can define that a critical infrastructure (CI) is a facility, service or a group of facilities or services, on the economic, physical, environmental or social well-being or security of the network the loss of which will have serious antagonistic consequences (Huff et al., 2019). A critical infrastructure consolidates services, material, networks, installations and information assets (Ugulu et al., 2019). On these frameworks all critical infrastructures depend strongly and use communications technology (ICT) systems and information (Ouyang et al., 2019).

II. CRITI NCALITY

To characterize an infrastructure as critical the most widely recognized methodology is to survey the effect level within the sight of security-related dangers (Humphreys, 2019). On the results of an occasion most techniques center around like "result of a circumstance or occasion communicated subjectively or quantitatively just like a misfortune, damage, detriment or addition" (Kattel & Aros-Vera, 2019).

Table 1. Criticality approaches (impact factors).

Impact Criteria	Approach
Public Health and Safety	[7, 8, 17, 26]
Economic	[7, 8, 17, 22, 26]
Environment	[7, 8, 17]
Political/Governance/Mission	[7, 8, 17, 26]
Psychological/Social/Public Confidence	[7, 8, 17, 22, 26]
Interdependency	[7, 8, 13, 16, 22]
Complexity	[13]
Vulnerability	[13]
Market Environment	[13]
Concentration of People and Assets	[22]
Scope/Range	[7, 8, 17, 22]
Service Delivery/Recovery Time	[7, 8, 16, 17, 22]
National/Territorial Security	[17, 26]

Table 1: Impact Criteria

To prioritize infrastructures and assets critical asset factors or impact factors are criteria used. With respect to three essential attributes the impact is generally measured (Mitchell et al., 2019). These three characteristics are as follows:

1. Spatial distribution or scope: this is defined as the geographic region that could be influenced by inaccessibility of a basic framework or that could be influenced by the loss.
2. Magnitude or severity or intensity: this can defined as the outcomes of the destruction or disruption of a specific basic foundation
3. Temporal distribution or effects of time: This can defined as the time at which it can give the serious impact with the loss of a component.

III. CRITICALITY ANALYSIS

On the basis of potential risk a process is defined as Criticality analysis through which it can assign the rating of criticality to assets (Herrera & Maennel, 2019). It considers criticality investigation as a feature of bigger disappointment modes, impacts analysis (Fekete, 2019). An approach that distinguishes every single imaginable ways that hardware can fail is defined as FMEA. This approach breaks down the impact that those disappointments can have on the framework in general. With each failure mode by evaluating the risk related FMECA makes it a stride further and afterward organizing remedial move that ought to be made (Gow, 2019).

Criticality analysis performance

For criticality analysis there are two ways to carry out. As a final product both methodologies RPN (risk priority number). The criticality of each asset can rank through this number (Nguyen, 2019). In the first approach a 6×6 grid is used, against the probability of that outcome happening that is Y axis, severity of a given outcome is plotted that is X axis. Due to severe operational problem and great personal injury if segment of equipment will fail, then the segment should be accordingly prioritized and that segment is consider as very critical. For any segment of equipment at the cross section of priority and severity the number is consider as the segment of equipment RPN.

Probability						
	6	12	18	24	30	36
	5	10	15	20	25	30
	4	8	12	16	20	24
	3	6	9	12	15	18
	2	4	6	8	10	12
	1	2	3	4	5	6
	Severity					

Figure 1: Kovacevic grid

RELIGACION. VOL 4 N° 19, Septiembre 2019, pp. 280-285

Equipment	Health & Safety	Environmental	Operational	RPN
Forktruck	5	2	1	**10**
Conveyor system	2	1	4	**8**
Mixing tank	2	5	4	**40**

Table 2: through consequence category critical analysis

Risk Category	RPN
Extreme Risk	107-125
High Risk	88-106
Medium Risk	37-87
Low Risk	19-36
No Risk	0-18

Table 3: by risk category grouping the assets

IV. USE A CRITICALITY VS. RISK APPROACH

In an effective and efficient way the major problem that appears insurmountable to handle in transit is the huge backlog of deferred maintenance (Thompson, 2019). Every asset presents to the organizations Operational Excellence goals for understanding the risk and criticality in a proper manner (Fang & Sansavini, 2019). The table given below shows the matrix of risk vs. critical analysis

		A	B	C	D	E
		Negligible	Minor	Moderate	Significant	Severe
E	Very Likely	Low/Med	Medium	Med/Hi	High	High
D	Likely	Low	Low/Med	Medium	Med/Hi	High
C	Possible	Low	Low/Med	Medium	Med/Hi	Med/Hi
B	Unlikely	Low	Low/Med	Low/Med	Medium	Med/Hi
A	Very Unlikely	Low	Low	Low/Med	Medium	Medium

Figure 2: Criticality vs. Risk Matrix

V. CLEAR VIEW OF ASSET CRITICALITY AND RISK RANKINGS

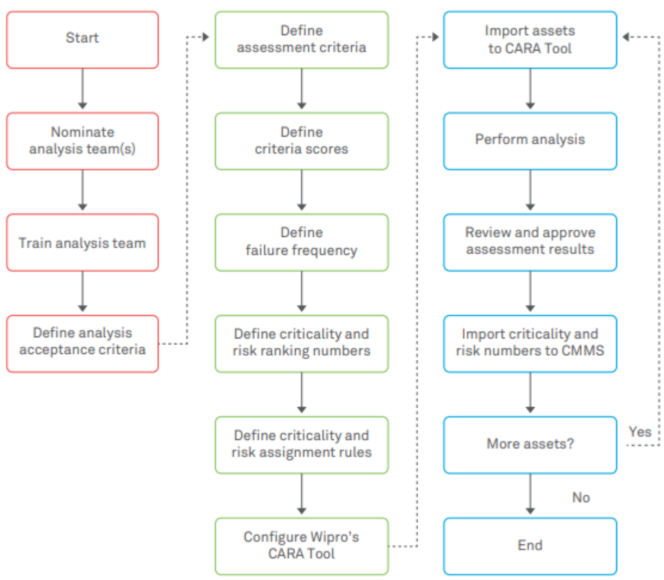


Figure 3: Wipro's CAR Process

VI. BENEFITS

Some benefits of criticality analysis are given below:

- Provides contribution to chance administration (Monstadt & Schmidt, 2019).
- Increases trust in a guide to condition-based support
- Enhances deceivability and comprehension of benefits' criticality and positioning
- For risk management provide input
- Assists in setting up hardware saves methodology
- Optimizes sending of assets

VII. APPROACH TO ASSET RISK

As shown in the figure 4, it represents an approach of asset risk this is fully with ISO31000 risk management system; this is known as Risk managed performance (RMP). In order to strike the suitable balance between asset risk control and asset performance an effective mechanism of decision-making is provided by this approach. The risk management performance approach is shown in figure 5.

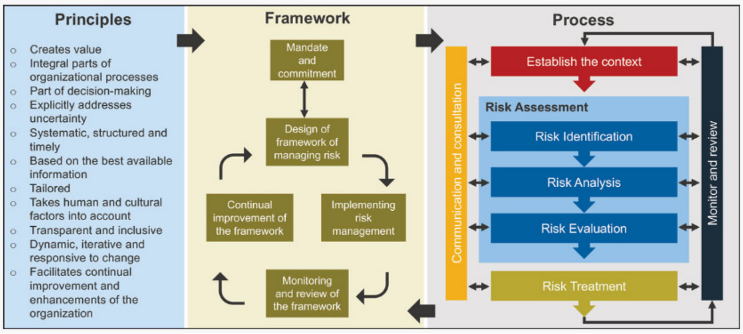


Figure 4: ISO31000 risk management system

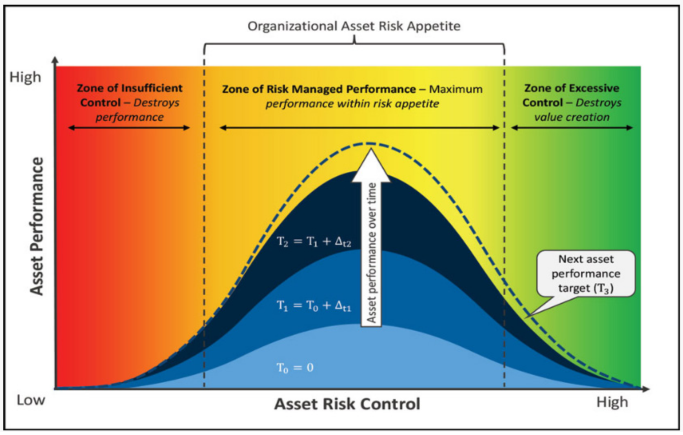


Figure 5: The risk managed performance approach

VIII. NETWORK ASSET RISK ATTITUDE AND LEVEL OF RISK ASSET

With respect to their asset risk for organizations the proper reaction is relies upon the asset risk attitude of organization and on level of asset risk (Weir et al., 2019). For level of asset risk the mathematical expression is shown in figure 6.

Because the condition of risk does not mathematically alter the equation this articulation doesn't disregard the ISO31000 meaning of risk. During the process of asset risk analysis it is a discretionary info parameter and it can give extra basic leadership understanding (Rehak et al., 2019).

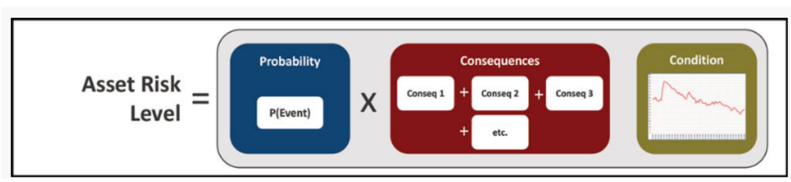


Figure 6: For asset risk mathematical expression

Risk Option	Description
Avoid the risk	Discontinue the activity that provides the origin of the risk
Take on more risk	Use a calculated understanding of risk to exploit risk opportunities
Address risk source	Remove or modify the risk initiator to operate at a lower risk level
Change the probability	Through the combination of understanding the primary functions and failure modes, apply the appropriate range of reliability engineering tools and processes
Alter the consequences	Change the outcome of the event should a risk occur
Share the risk	Distribute risk or insure against risk outcome with another party or parties
Retain the risk	Accept the fact that in the real world, some risks will remain, but understand fully the retained risk that is in place

Table 4: Risk Treatment Options of ISO31000

IX. RISK-BASED ASSET MANAGEMENT MODEL

For the survival of an organization a strategy that based on risk asset management and that provide Straightforwardness to risk is very necessary and along with reputation of the companies, health and safety it can provide the large effect on the environment (Chou & Ongkowijoyo, 2019). Without a formalized resource the board framework set up this is not possible (Maseleno et al., 2017; Maseleno et al., 2019). It is defined by LCE's risk-based asset management model that has four phases it is shown in figure 7. This model is required for making operational security and risk management.

Figure 7: Risk-based Asset Management Model of LCE

By assigning the document to the types of asset we can assets the catalog when it has a documented diagram to refer (Maseleno et al., 2016). Logical grouping like control strategies, assets and failure of similar functional allow by types of asset (Huang & Zhu, 2019). To delineate connection between the assets it should choose a model at this point. For linear assets like railways and pipelines it used the network model.

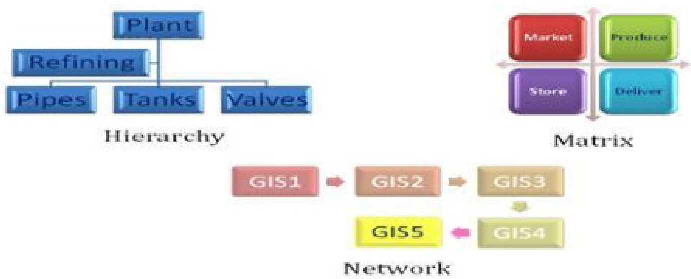
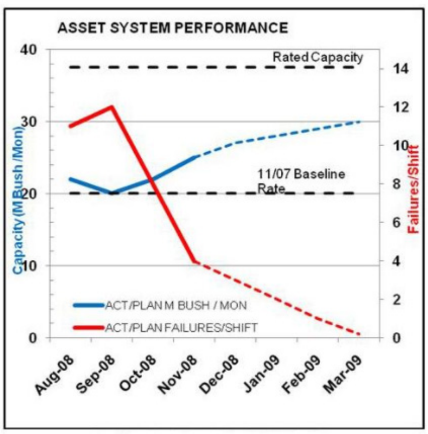


Figure 8: Asset Relationship Models



X. CONCLUSION

The prioritization of critical assets and foundations of criticality of infrastructures is required for basic framework security. For network utility asset management a process of risk based critically is designed and implemented. To characterize an infrastructure as critical the most widely recognized methodology is to survey the effect level within the sight of security-related risk. It considers criticality investigation as a feature of bigger disappointment modes, impacts analysis.

BIBLIOGRAPHIC REFERENCES

Chou, J. S., & Ongkowijoyo, C. S. (2019). Hybrid decision-making method for assessing interdependency and priority of critical infrastructure. International Journal of Disaster Risk Reduction, 101134.

Fang, Y. P., & Sansavini, G. (2019). Optimum post-disruption restoration under uncertainty for enhancing critical infrastructure resilience. Reliability Engineering & System Safety, 185, 1-11.

Fekete, A. (2019). Critical infrastructure and flood resilience: Cascading effects beyond water. Wiley Interdisciplinary Reviews: Water, 6(5), e1370.

Gow, G. A. (2019). Policymaking for critical infrastructure: a case study on strategic interventions in public safety telecommunications. Routledge.

Herrera, L. C., & Maennel, O. (2019). A comprehensive instrument for identifying critical information infrastructure services. International Journal of Critical Infrastructure Protection.

Huang, L., & Zhu, Q. (2019). Adaptive strategic cyber defense for advanced persistent threats in critical infrastructure networks. ACM SIGMETRICS Performance Evaluation Review, 46(2), 52-56.

Huff, J., Medal, H., & Griendling, K. (2019). A model‐ based systems engineering approach to critical infrastructure vulnerability assessment and decision analysis. Systems Engineering, 22(2), 114-133.

Humphreys, B. E. (2019). Critical Infrastructure: Emerging Trends and Policy Considerations for Congress (No. R45809).

Kattel, P. J., & Aros-Vera, F. (2019). Critical infrastructure location under supporting station dependencies considerations. Socio-Economic Planning Sciences, 100726.

Maseleno, A., Huda, M., Jasmi, K. A., Basiron, B., Mustari, I., Don, A. G., & bin Ahmad, R. (2019). Hau-Kashyap approach for student's level of expertise. Egyptian Informatics Journal, 20(1), 27-32.

Maseleno, A., Hardaker, G., Sabani, N., & Suhaili, N. (2016). Data on multicultural education and diagnostic information profiling: Culture, learning styles and creativity. Data in brief, 9, 1048.

Maseleno, A., Huda, M., Siregar, M., Ahmad, R., Hehsan, A., Haron, Z., ... & Jasmi, K. A. (2017). Combining the previous measure of evidence to educational entrance examination. Journal of Artificial Intelligence, 10(3), 85-90.

Mitchell, E., Bell, P., Hall, A., Kelley, T., Kavaney, M., Butler, R., ... & Nussbaum, B. (2019). Jack Voltaic Critical Infrastructure and Public-Private Partnerships.

Monstadt, J., & Schmidt, M. (2019). Urban resilience in the making? The governance of critical infrastructures in German cities. Urban Studies, 0042098018808483.

Nguyen, L. (2019). Hybrid Conductive Concrete Structures for EMP Protection of Critical Infrastructure Facilities. IEEE Letters on Electromagnetic Compatibility Practice and Applications.

Ouyang, M., Tian, H., Wang, Z., Hong, L., & Mao, Z. (2019). Critical infrastructure vulnerability to spatially localized failures with applications to Chinese railway system. Risk Analysis, 39(1), 180-194.

Rehak, D., Senovsky, P., Hromada, M., & Lovecek, T. (2019). Complex approach to assessing resilience of critical infrastructure elements. International Journal of Critical Infrastructure Protection, 25, 125-138.

Thompson, J. R., Frezza, D., Necioglu, B., Cohen, M. L., Hoffman, K., & Rosfjord, K. (2019). Interdependent Critical Infrastructure Model (ICIM): An agent-based model of power and water infrastructure. International Journal of Critical Infrastructure Protection, 24, 144-165.

Ugulu, R. A., Allen, S., & Arewa, A. (2019). Measuring Infrastructure Skills Productivity: Management of Critical Infrastructure. In Management of Critical Infrastructure: Measuring Infrastructure Skills Productivity (pp. In-press). IntechOpen Limited.

Weir, A., Wilson, T., Bebbington, M., & Deligne, N. (2019). Quantitying the Systemic Vulnerability of Critical Infrastructure Networks to Volcanic Multi-Hazards at Mt Taranaki, New Zealand.