RISKS OF CASCADING FAILURES IN CRITICAL INFORMATION INFRASTRUCTURE

Arzu Babayeva[1], Yadigar Imamverdiyev[1]

•

[1]Azerbaijan Technical University, Baku, Azerbaijan
arzu.babayeva@aztu.edu.az , yadigar.imamverdiyev@aztu.edu.az

Abstract

The article presents an analysis of risk research related to cascading failures in critical information infrastructure. An example of a systems approach implemented in the areas of critical information infrastructure (CII) activity is considered. A model for the spread of cascading failures between interdependent CII objects is proposed, using a weighted graph model. Based on this model, formulas for calculating reliability dependencies and assessing risks between CII objects are presented. Additionally, a risk assessment method accounting for cascading effects for CII objects has been developed and applied.

Keywords: Critical Information Infrastructure (CII); Critical Information Infrastructure Object; Critical Information Infrastructure Subject; Failure; Cascading failure; Risk; Risk assessments; The graph; Probability; Information security.

I. Introduction

Critical Information Infrastructure (CII) refers to a set of information systems, automated control systems, and information-communication networks that support activities in essential areas, the disruption of which can cause significant harm to the interests of citizens, society, and the state [1]. Worldwide, and especially in the Republic of Azerbaijan, in recent years, issues related to ensuring the security and stability of these systems have become particularly relevant, considering their high degree of interconnection.

One of the most important aspects of risk management in CII is the prevention and minimization of the consequences of potential failures. One of the threats that is of significant interest for research is cascading failures.

A cascading failure is a process in a system of interconnected parts in which the failure of one or several parts can trigger the failure of other parts, and so on. Cascading failures in CII can be especially dangerous, as they can lead to widespread consequences, affecting not only one object or component of the system but also causing failures in other parts of critical infrastructure. Cascading failures are extensively studied in power grids. Effective risk assessment of cascading failures includes the probability of failures, potential consequences, and the impact of one object's failure on others [2-11].

The goal of this work is to study the interconnected and interdependent risks of cascading failures between CII objects.

II. Analysis of the Research Area

The main components and assets of Critical Information Infrastructure (CII) are the objects and subjects of CII, as well as the critical processes that take place within them. According to the Law of the Republic of Azerbaijan "On Information, Informatization, and Information Protection," a CII object is an information system, an automated control system, and/or an information-communication network. The subjects of CII are government bodies (institutions), legal entities, and individual entrepreneurs. According to this law, the most important areas of CII activity in the Republic of Azerbaijan include government administration, defense, healthcare, the financial market, energy, transport, information technology, telecommunications, water supply, and ecology [1].

In the work [2], the subject of CII is considered as a system of interacting CII objects, as well as the means of their communication, owned by a specific CII subject. Based on this, it can be assumed that such systems are implemented in 10 areas of CII activity. As a result, interconnected cascading failures in CII can occur in the following directions: between objects within the same system, between different systems within the same activity area, and between systems from different CII activity areas. The third case occurs, for example, when a failure in the energy sector system can disable a system in the water supply sector.

The article [3] provides an example of a risk dependency graph for interdependent CIIs, where the consequences of one risk arising in one CII and affecting other dependent critical infrastructures are assessed. Operational risk assessment methods adopted in financial organizations are used as a method.

The values of interconnection and interdependence are determined by the concept of mutual influence. The authors [3], [4], [5] in their works have examined the types of mutual influences. The main types can be highlighted as follows: physical, geographical, and informational.

- The physical type defines the influence caused by the exchange of energy or matter between systems, which changes their state.
- The informational type refers to the influence arising from the exchange of data, signals, or information between systems, leading to a change in their state.
- The geographical type is determined by the spatial arrangement of systems, which spreads the consequences based on their proximity.

The article [5] discusses a method for assessing the risks of cascading failures (breakdowns) using dynamic criticality matrices. The method is based on the application of linguistic approximation, which allows for heuristic forecasting of accident developments.

The work [6] presents a model for the spread of cascading failures of elements in an electric power network across its cuts based on a dependency graph. Within this model, network reliability indicators were introduced. Methods for exact and approximate reliability calculation of the network were developed based on the Monte Carlo method, as well as a cumulative method for refining reliability boundaries.

III. Model of Cascade Failure Propagation Between Interdependent CII Objects

Probabilistic models are typically used to analyze the reliability of a network and assess risk in the event of cascading failures, which consider the failure dependencies between its elements [6].

To study the model of interdependent CII objects, we will use a weighted graph G=(V, E) (Figure 1).

Let the vertices of the graph V represent the CII objects (O1 …On), and the edges of the graph E represent the failure dependencies between these objects. Assume that the vertices of the graph

occur with probability p_v=1, while the edges occur with probability 0≤p_e≤1 within a specified time interval. Suppose that for each object i in the system, there is a weight w_i that can be used to weight the probability of failure of the object (or the vulnerability degree of the nodes).

Thus, one approach would be to use a calculation that takes into account the contribution of each object to the system's failure. Formula (1) allows for the calculation of the probability that at least one object i will be responsible for the system's failure, considering its weight.

$$P(A) = 1 - \prod_{i=1}^{N}(1 - w_i * p_i) \tag{1}$$

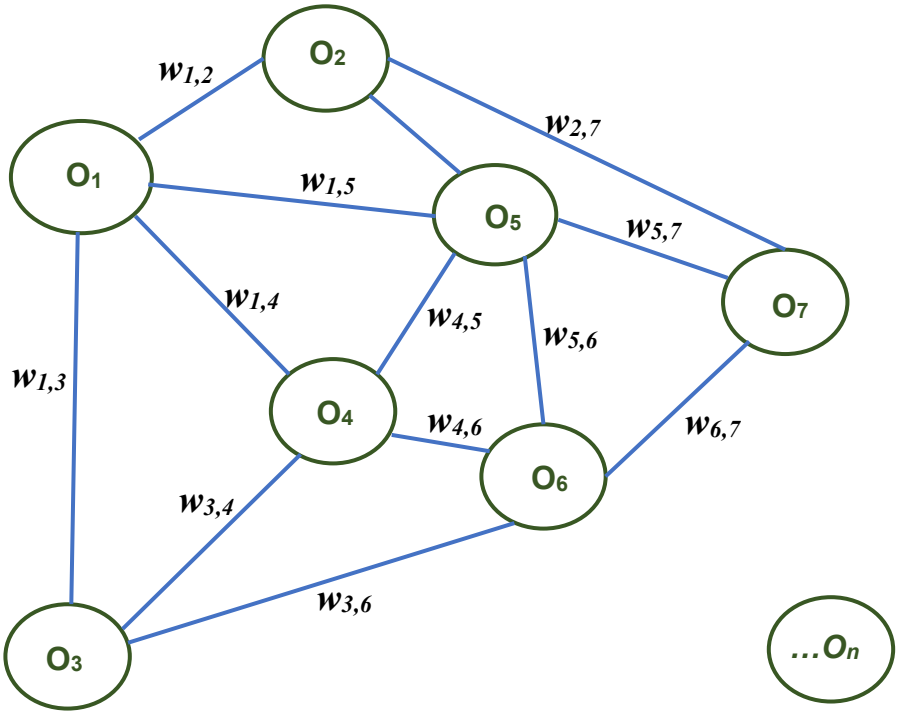

Figure 1: *Example of a weighted graph model of CII objects*

Now, if we want to take the weights into account when calculating the probability that a specific object i will be responsible for the system's failure, we can use the following formula (2):

$$P(B_i) = \frac{w_i * q_i}{\sum_1^N w_j * q_j} \tag{2}$$

And finally, to calculate the probability that the failure of a specific object i will lead to the failure of the entire system, considering its weight, the formula will be as follows: Formula (3):

$$Q_i = P(A) * P(B_i) = \frac{(1-\prod_1^N p_i)*w_i*q_i}{\sum_1^N w_j*q_j} \tag{3}$$

If the failure of one or more objects in the system can lead to a complete system breakdown, then this probability becomes an important element for assessing risk factors. The connection

between probabilistic failure models and risks is that these models not only allow for the estimation of failure probabilities but also enable the analysis of how the failure of each object may affect the overall risk of the system.

Formula (1) takes into account how the risks of individual objects (their failure probability and importance to the system) influence the overall risk of the system as a whole.

Formula (2) allows the calculation of the probability that the failure of a specific object i will be responsible for the total system failure. This helps to identify key risks within the system — objects with high values of w_i (object weight) and q_i (failure probability), which can significantly impact the system.

Formula (3) helps link the probability of failure of a specific object i to the overall system failure probability. By considering Q_i, we can assess how the failure of a specific object affects the risk to the entire system.

IV. Risk Assessment of Cascade Failures

Risk assessment in information security (IS) plays a crucial role in ensuring the protection of information infrastructure. Risk assessment can be performed using two main methods:

- Qualitative risk assessment;
- Quantitative risk assessment.

Qualitative risk assessment methods include: expert judgment method, rating assessment method, analogy method, and others. Quantitative methods include techniques such as scenario analysis, simulation modeling (Monte Carlo simulation method, historical simulation method), situation modeling based on game theory, tree-building methods, methods based on artificial intelligence systems, and so on [7].

According to the work [8], the qualitative and quantitative risk assessment of the information security (IS) of a CII object is determined as the product of C — the potential damage (consequences) caused to the i -th information resource of the designated security zone, and the probability P_j of the occurrence of the j-th threat and the probability P_k of exploiting the k -th vulnerability. The formula (4) is as follows:

$$R_i = P_j * P_k * C_i \tag{4}$$

A threat can arise from both natural and artificial phenomena and includes the probability that it exists or may occur. Vulnerability is a weak point or limitation that a threat can exploit. Consequences refer to the cost and loss coefficient for risk assessment [9].

For a more detailed assessment of the risks of cascading failures in a system of critical information infrastructure (CII) objects, we need to consider not only the direct failure risks for each object but also their interconnection. When one object fails, it can affect other objects, causing additional failures, leading to a cascading effect. This effect can be modeled using a risk matrix to systematize and quantitatively assess the impact of failures of different system objects on the operation of the entire CII.

So, to account for cascading effects, we need to adjust the overall risk for each object, taking into account the failure probability of not only the object itself but also the probabilities of failure of other objects that may be triggered by cascading failures. Formula (5):

$$R_i = P_i * w_i * C_i + \sum_{j \neq 1} P_j * w_j * C_j * E(i \to j) \tag{5}$$

Where:

- P_i- is the probability of failure of object i,
- w_i- is the weight of the object,
- C_i is the consequences of the failure of object i,
- $E(i \to j)$ is the cascade effect $(i \to j)$ coefficient, which shows the impact of the failure of object i on other objects j.

Based on formula (5), an example of risk assessment for cascade failures of CII objects can be presented.

Example:

Suppose we have three objects in one CII system with the following data (Table 1, 2):

Table 1: *Cascade Effect Matrix for All Pairs of CII Objects* $(i \to j)$

Object i/ Object j	O_1	O_2	O_3
O_1	*0*	*0.4*	*0.3*
O_2	*0.3*	*0*	*0*
O_3	*0.2*	*0*	*0*

Table 2: *Risk Assessment Matrix for Cascade Failures of CII Objects*

Objects	P_i	w_i	C_i
O_1	*0.1*	*2*	*8*
O_2	*0.05*	*1*	*7*
O_3	*0.2*	*1*	*6*

$$R_1 = 0.1*2*8+0.05*1*7*0.4+0.2*1*6*0.3 = 1.6+0.14+0.36 = 2.1$$

Output:

The risk of failure of object 1 (O_1), considering the cascade effects for the system, is *2.1*. This means that the failure of object 1 not only has its own risk (*1.6*) but can also impact the failure of other objects (*0.14* for Object 2 and *0.36* for Object 3), thereby increasing the overall risk for the entire system.

V. Conclusion

Cascade failure (breakdown) is considered the most complex scenario in terms of design, security assessment, and response to these failures. During the analysis of the topic under study, a systems approach was considered, which is implemented in various areas of CII activities.

A model of cascade failure propagation between interdependent CII objects is proposed, using a weighted graph model as an example. Based on this model, formulas for calculating the reliability of dependencies and risk assessment between critical information infrastructure objects were presented. Additionally, based on both qualitative and quantitative risk assessment methods for information security, a risk assessment method taking into account cascade effects for CII objects was developed and applied.

References

[1] The Law of the Republic of Azerbaijan "On Information, informatization, and information Protection". Official website e-qanun.az - unified electronic database of legal acts. 2022.

[2] Maksimova Elena A., and Sadovnikova Natalya P. "Intersubjective interaction as a source of destructive Influences on the subject of critical information infrastructure". Caspian journal: Control and High Technologies 2 (54), pp. 71-80. 2021.

[3] Imamverdiev Y. N. "Method of Protecting Distributed Networks Through the Formation About Information Exchange". Information Systems and Technologies 111.1, 2019.

[4] Panteleev V. A., Kirillov I. A., Berberova M. A., Klimenko S. V. " Method Cascade and intersystem accidents scenarios description." SCVRT2017, pp. 239-244. 2017.

[5] Brezhnev E.V. "Method of Cascading Failure (Accident) Risk Assessment Based on Application of Dinamic Criticality Matrix". Science and technology of the Air Forces of the Armed Forces of Ukraine No. 1 (18). pp.187-190. 2015.

[6] Migov D. A., Korotkov A. N. "Cuts Using for Modeling the Propagation of Cascading Failures in Electrical Power Grids." Problems of informatics (3). 2021.

[7] Petrova A.V. «Methods of Assessing the Level of Risk in the Enterprise». Economics and Efficiency of Production Organization, (21). pp. 97-104, 2014.

[8] Vulfin Aleksey Mikhaylovich. " Models and methods for comprehensive assessment of security risks of critical information infrastructure objects based on intelligent data analysis." System engineering and information technology 5.4 (13). pp.50-76.2023.

[9] Abdulova E. A., Kalashnikov A.O." On The Issue of Risk Management of Critical Information Infrastructure." Papers. pp.1275-1282. 2021.

[10] Komendantova Nadejda P. " Risk Governance and Vulnerability Factors of Critical Infrastructure." Russian Digital Libraries Journal V. 20. No 1. pp.88-108. 2017.

[11] Kotenko Igor, Saenko Igor, Doynikova Elena. "Risk Assessment in Computer Networks of Critical Infrastructures". Innovations in science 16-1. pp. 84-88. 2013.