Risk Matrix-Based Method for Critical Infrastructure Safety Assessment Taking into Account Interdependencies

Eugene Brezhnev[1,2,a], Bogdan Chernetskiy[1]

[1]Department of computer systems and networks, National Aerospace University " KhAI", Kharkiv, 61070, Ukraine
[2]RPC Radiy, Kirovograd, 25006, Ukraine

Abstract. This paper is devoted to development of method for critical infrastructure (CI) safety assessment taking into account the different types of interdependencies: logical, physical, geographical, etc. There are many existing approaches for CI safety assessment. But the limited number of them consider the interdependencies focused on safety. Only few of them focus on interdependencies formalization. The suggested approach is based on application of risk matrixes built for each CI systems. Criticality of state is considered as safety value. The risk matrixes are developed for each CI life stage. The initial risk matrix is developed during CI design stage. All operational risk matrixes are built based on fuzzy logic and system field data.

1 INTRODUCTION

1.1 Motivation

Modern society has become widely dependent on the reliability and safety of critical infrastructure (CI). Critical infrastructure refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of people and the effective functioning of government. Critical infrastructure can be stand-alone or interconnected and interdependent within and across provinces, territories and national borders. There are many types of CI. These CIs are: telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, etc.

Disruptions of critical infrastructure, decrease of its safety could result in catastrophic loss of life, adverse economic effects and significant harm to public confidence. These CIs are supported by an array of physical assets, functions, information, people, and systems, forming what has been called the nation's critical infrastructures. These infrastructures have grown complex and interconnected, meaning that a disruption in one may lead to disruptions in others.

The significant increase in disasters of a natural and/or technological origin seen today has serious consequences for CI, the population, the environment, and the economy. These consequences have been exacerbated by the development of sociotechnical systems such as transport networks and industrial plants, their interdependencies, and their sensitivity to major hazardous events.

Many CI accidents are aggravated by systems interdependencies, when risk (safety) of one system is determined by risk (safety) of other system. Interdependence is a major challenge for risk management in CI. This gives rise a phenomenon known as "cascading events" – that is, once one disruption occurs, others are likely to follow within systems and processes that are connected to the infrastructure affected by the initial disruption. There is a strong need to consider the interdependencies in CI for safety and risk assessment.

1.2 Work Related Analysis

There is a significant number of risk assessment methodologies for CIs. In general the approaches that are used rather common and linear, consisting of some main elements: Identification and classification of threats, identification of vulnerabilities and evaluation of impact. These are well known and established

[a] Corresponding author: e.brezhnev@csis.org.ua

approaches for evaluating risks it is the backbone of almost all risk assessment methodologies.

Better Infrastructure Risk and Resilience [1]. The methodology covers the facilities in many critical infrastructure sectors (Energy, critical manufacturing etc.). This methodology has a sectoral approach that goes down to the assets level and gives priority on the protection measures that are applied mainly against terrorist threats. Concluding, this methodology is excellent for being applied to assets of critical infrastructures, it does not consider the interdependencies between safety states of systems.

Protection of Critical Infrastructures - Baseline Protection Concept [2] sets as basis the cooperation between infrastructures operators and state for reassuring the smooth operation of infrastructures with importance to the whole society. It is mentioned that infrastructure operators are the ones that should implement security measures as they have in-depth knowledge of their infrastructure and the way it operates. To this end, it provides recommendations on the identification of threats, vulnerable points and risk management elements, but safety is not considered and interdependencies that can undermine CI safety values aren't considered as well.

Counteract [3] is focused on assets and operators of any size, thus excluding an approach at the systems level. The security risk assessment is divided in two parts, the risk analysis and the vulnerability assessment.

The risk analysis focuses on the probability of an event and the impact it may have, while the vulnerability assessment evaluates the safeguards in place for the corresponding risks for the various assets. It is a rather different approach as to what is risk assessment with respect to what is widely acceptable.

This approach is not focused on interdependencies analysis between CI safety states.

1.3 Goal of the Paper

The aim of this paper is development of method for CI safety assessment considering the interdependencies among systems.

2 METHOD FOR CI SAFETY ASSESSMENT CONSIDERING THE INTERDEPENDENCIES

2.1 Interdependencies type description

There are four primary classes of interdependencies [4, 5, 6]:

– Physical Interdependency – two infrastructures are physically interdependent if the state of each depends upon the material output(s) of the other;

– Cyber Interdependency – an infrastructure has a cyber interdependency if its state depends on information transmitted through the information infrastructure. The computerization and automation of modern infrastructures and widespread use of supervisory control and data acquisition systems have led to pervasive cyber interdependencies [7, 8];

– Geographic Interdependency – infrastructures are geographically interdependent if a local environmental event can create state changes in all of them. This implies close spatial proximity of elements of different infrastructures, such as collocated elements of different infrastructures in a common right-of-way;

– Logical Interdependency – two infrastructures are logically interdependent if the state of each depends upon the state of the other via some mechanism that is not a physical, cyber, or geographic connection.

All of these types of interdependencies shall be considered for possible influence on system safety state. System safety state is considered as state when all risks are controlled or eliminated. These interdependencies influence the system safety in different way during different system life stage. Criticality of system state is considered as a safety value for systems in CI. The more system criticality is the less its safety. The typical risk (criticality) matrixes (FMECA like) usually allow to allocate system in particular boxes giving a clear understanding of the current safety state.

2.2 Description of the method stages

At each stage of CI life cycle the criticality assessment and adjustment of risk matrixes, taking into consideration probable changes, are carried out. A set of CI criticality matrixes failures is divided into two subsets:

- the subset of subsystem failures that criticality is located above the diagonal of the criticality matrix M^S_{crt} (the set of critical failures), and

- the subset, where criticality – under the diagonal of M^S_{crt} (the set of noncritical failures).

The hierarchy of risk matrixes is based on system hierarchy considering the real risks of each system (subsystems, components).

The sequence of carrying out CI safety assessment taking into account interdependencies between systems is shown in Fig. 1. The approach is bottom – up. The safety assessment is carried out from bottom up to the system top level. It allows considering the negative effects of components' failures on system as a whole.

Existing approaches for CI safety assessment do not consider any relation between subsystem failures of one hierarchy level. In this regard, the interdependencies when subsystem failures of i-level (on subsystem failure criticality of the same level) and its influence on subsystems of (i-1)-level (higher) is important.

The uncertainty takes into consideration information incompleteness and uncertainty related to the conditions that cause CI accidents, insufficient knowledge about CI, nature of new risks, etc.

The results of CI safety assessment are represented as risk matrixes' hierarchy.

CI initial safety assessment is done during CI development (or design) stage. Existing methods of criticality analysis for systems use standard algorithms of reliability analysis, one of which is FMECA.

Constructing the hierarchy of design criticality matrixes, CI project safety assessment, obtaining the safety value are tasks done during CI development stage.

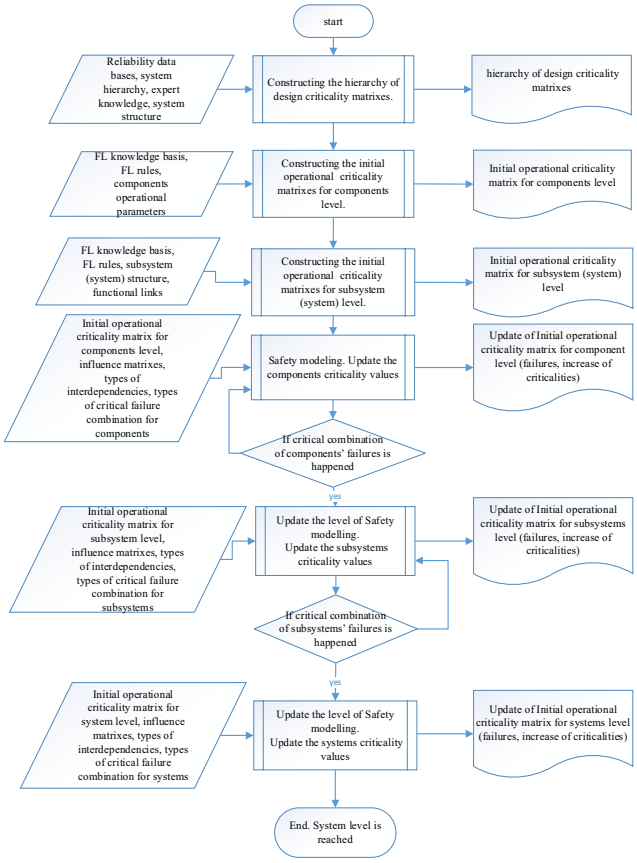

Fig 1. Algorithm of method.

As far as the stage of design analysis is characterized by high level of uncertainty, criticality design assessment can differ from CI safety operating values. This fact can be explained by inefficiency of reliability design measures at design stage when conditions of system operation are not expected or different (change of environment parameters).

In CI systems, there is a possibility for diagnostics of technical state of subsystem and components in accordance with results of physical measurement defining object operation. So, decrease of uncertainty of system safety state leads to changes of values of initial subsystem criticality assessment presented within the criticality matrix hierarchy.

It should be noted that CI failure effects severity can be both external and internal. The external severity is a result of dependent infrastructure damage made by the power system. Failure effect severity will be called internal if the power system compensates it using resources. Internal damage that cannot be compensated by CI is considered internal.

Initial data for revising of CI safety values are its operation parameters and conditions. It is done by application of fuzzy logic approach.

2.3 Description of the Fuzzy logic approach for components (subsystems) criticality assessment

It is proposed to use fuzzy logic definitions to evaluate failure criticality on different CI levels. They will allow to evaluate criticality indexes and arrange a failure set by a potential risk value. The safety assessment is done from the lowest possible level when all (or important operational parameters) are known for operator.

By means of operations $\bigcup$ and $\bigcap$ the FL rule set can be written as follows:

$$\bigcup_{p=1}^{k_j}\left[\bigcap_{i=1}^{n}(x_i = a_i^{jp})\right] \rightarrow y = d_j,\ j = \overline{1,m}. \qquad (1)$$

where $d_j (j = \overline{1,m})$ - linguistic evaluation of Y output (safety) variable determined out of D term-set;

a_i^{jp} - linguistic evaluation of xi input (operational parameters) in p-th line of the disjunction selected out of corresponding Ai term-set,

$$a_i^{jp} \in A_i, i = \overline{1,n}, j = \overline{1,m}, p = \overline{1,k_j}; \qquad (2)$$

kj – quantity of rules that define a value of y=di output variable.

This fuzzy approach is used in the two ways.

At first, as the suggested method is bottom up, the fuzzy logic is used to assess a criticality value of each component (lowest CI level). Fuzzy logic approach takes the real parameters of each components and returns its criticality values. It allows to locate each component into risk matrix on the lowest level of criticality matrix hierarchy. It is done for each systems' components. The lowest level criticality matrix is built.

At the second, this fuzzy approach is used to locate the all higher-level systems into criticality matrixes. This idea is straightforward. When we know the risks associated with each system components we can elaborate the risks associated with all system as a whole. FL approach takes the criticalities of each components and returns the criticality of whole system.

2.4 Approach to revising of systems criticality values due to interdependencies

The linguistic approach based on fuzzy sets has given very good results for qualitative risk-analysis of critical information control system based on FMECA. It is an approximate technique in its essence, which represents qualitative aspects as linguistic values by means of linguistic variables, that is variables whose values are not numbers but words or sentences in a natural or artificial language.

A linguistic aggregation operator based on the extension principle acts according to

$$S^n \xrightarrow{\tilde{F}} F(R) \xrightarrow{app_1(\cdot)} S, \quad (3)$$

where S^n symbolizes the n Cartesian product of S, $\tilde{F}$ is an aggregation operator based on extension principle, F(R) the set of fuzzy sets over the set of real number R, app_1: $F(R) \rightarrow S$ is a linguistic approximation function that returns a label from the linguistic term S whose meaning is the closest to the obtained unlabeled fuzzy number and S is the initial term set. Fuzzy sets C_j (the new values of criticality) are obtained by the means of fuzzy arithmetic for triangular fuzzy numbers. The fuzzy numbers characterize the semantic of linguistic values. Multiplication of two fuzzy numbers P (fuzzy probability) and L (fuzzy severity) may be obtained as $L \odot P \overset{def}{=} C$, where membership function equals

$$\mu_C = \sup_{\substack{x_1, x_2 \\ y = x_1 \cdot x_2}} \min\{\mu_L(x_1), \mu_P(x_2)\} \quad (4)$$

This fuzzy approach allows to update all systems criticalities values when any systems fail. This approach uses linguistic values to formalize the interdependencies and initial criticality values. All interdependencies are formalized as linguistic values (high, medium, low) located in the matrix of influence.

2.5 Assessment of the occurrence of system failures critical combination

It is important to check if there is a critical failure combination after each update of systems criticality. Any systems might have a certain level of resilience, capacity to withstand the occurrence of its systems (components) failures. But each system has its own set of critical failures combination when a whole system fails. In term of the suggested in this thesis approach it asks for updating of level of CI safety analysis. The set of critical failures combination is determined by expert knowledge.

Thus, for instance if all critical components of subsystem fail then it is considered that subsystem fails. In this case we update the level of safety modelling. After this all of stages mentioned above are repeated for next level of CI.

2.6 Description of the case study

As a result of these researches a desktop software has been developed that allows to perform a safety assessment of CI considering new risk parameter – interdependencies. The program was developed in C # in Visual Studio design environment in 2012.

The program has the following features:

- set the number of objects;
- set object parameters (probability of failure and the severity of the consequences);
- drawing objects on the panel;
- the ability to create relations between objects (material and information);
- change parameters of objects;
- simulated failure of the object;
- step-change comparison objects;
- system reset.

To prove the approach to the CI safety assessment considering the interdependencies, Russian Sayano–Shushenskaya HPP accident was reviewed. The software was used as a tool to perform a case study taking into account the interdependencies between its hydro units (HUs).

As the approach is bottom up then we use a Fuzzy logic for distributing all HU components inside the risk matrix. The physical interdependencies are considered. It allows to revise the criticality states of all HUs. The system failures occurrence is modeled after obtaining the criticality matrixes for HUs. During this modelling the focus was made on HU 2 (which cause the real accident).

When any failures are happened then this failures are analyzed by software.

Simulation stator stanchion (S_{121}) failure leads to the fact that the criticalities of states of bearing (S_{124}) and other components (S_{128}) are increased.

Simulation upper and lower stator belt (S_{122}) and bearing (S_{124}) failure leads to the fact that the criticality of states of cover fastener systems (S_{127}) and the turbine cover (S_{125}) increases.

The results of HU-2 components' safety modelling is shown on Figure 2.

Fig.2. Modeling HU-2. Simulation upper and lower stator belt (S_{122}) and bearing (S_{124}) failure.

After checking for occurrence the critical combination failures the safety modelling level was updated (upper level, station level, HU as systems), from the level of hydro unit component to the next level, the level of hydraulic units. The critical failures combination is occurred and HU-2 fails (see Fig.3 below).

Fig 3. Modeling Sayano-Shushenskaya HPP. Out of order HU- 2 failure.

When HU-2 failure occurred the level of safety modelling was updated. Next, the safety modelling was done considering functional interdependency between HU-2 and other HUs.

HU-2 (S_2) failure leads to the fact that the criticalities of states of all HUs are increased.

The change of systems criticality values:

$S_2^* \rightarrow S_1\uparrow\ S_3\uparrow\ S_4\uparrow\ S_5\uparrow\ S_6\uparrow\ S_7\uparrow$.

The results obtained from this modelling tell us that even if HU was not thrown away and technical room was not flooded then its failure would have led to all HPP unavailability (but without such losses).

3 Conclusion and Future Work

As a result of method application – uncertainties of CI risk assessment is decreased by consideration on new parameter – type of interdependencies. All types of interdependencies are considered in method.

As this method allows for risk visualization then it becomes a good safety assessment tool for CI operators. The results of case study performed have shown that if these HUs were equipped with devices for measuring all (or most important) operational parameters then the application of this software would allow to on-line risk assessment and taking the preventive measure to decrese the high consequences of this accident.

Next step of method enhancement will be related to consideration of system multiple failures for criticality analysis and development of decision making tool-based system.

Further development of the software is to add it with the feature that suggest a set of preventive measures to decrease risks and its propagation on other CI levels.

References

[1] J. Sagoff, *Better infrastructure risk and resilience*, http://www.anl.gov/articles/better-infrastructure-risk-and-resilience, (2010)

[2] Federal Ministry of the Interior, *Protection of Critical Infrastructures – Baseline Protection Concept*, http://www.preventionweb.net/files/9266_2967ProtectionofCriticalInfrastruct.pdf, (2013)

[3] ForeScout, *ForeScout CounterAct*, https://www.forescout.com/products/counteract/, (2012)

[4] D. Dudenhoeffer, M. Permann, M. Manic, *CISMS*: *A Framework for Infrastructure Interdependency Modeling and Analysis*, (2006)

[5] R. Bloomfield, N. Chozos, P. Nobles, *Infrastructure interdependency analysis: introductory research review,* (2009)

[6] R. Zimmerman, *Decision-Making and The Vulnerability Of Interdependent Critical Infrastructure*, (2004)

[7] Nikolaos G. Bardis, Nikolaos Doukas and Olexander. P. Markovskyi, "*Effective method to restore data in distributed data storage systems", IEEE / MILCOM (2015)*

[8] Nikolaos G. Bardis, Nikolaos Doukas and Olexander. P. Markovskyi, *"Efficient burst error correction method for application in low frequency channels and data storage units", 17th International Conference on Digital Signal Processing (DSP) IEEE, DOI: 10.1109/ICDSP.2011.6004970, Corfu 2011*