Complexity of Systems:
Object Oriented Instruments for Critical Infrastructure Protection

Jarutpong VASUTHANASUB
Old Dominion University, United States of America
5115 Hampton Boulevard Norfolk, VA 23529, USA

Paul NICULESCU-MIZIL GHEORGHE
National Institute for Research and Development in Informatics - ICI Bucharest
Mareșal Alexandru Averescu Bvd, Nr. 8-10, Bucharest, Romania
paul.niculescu@ici.ro

Abstract: The research of complex systems is transforming to an important issue in the natural and social global sciences. It is frequently implied the existence of a complex system transversely all the disciplines. For the Critical Infrastructure Protection context, there is need to illustrate a complex system, and study a fundamental set of features that are generally related with complex systems. The notion of complexity is defined to exist as a part of a new unifying framework for science, in a revolutionary way - our comprehension of systems and their behavior. It is quite difficult to forecast and control the economy of the world or the human mind, but the procedure of object-oriented technology offers us solutions that can be implemented in software architectures with easy possibilities of extension, maintenance and testing. This paper studies the complexity of systems in regional areas defined as Critical Infrastructures and the approach of protecting them by using object-oriented instruments, metrics and programming. To validate the efficacy of an object-oriented instrument solution, the methodology is merged with the TopEase® - Decision Support System, developed by Action 4 Value, a Swiss-German company, as a distinct example.
Keywords: Design Metrics, Object Oriented Metrics, Resilience, Decision-Support Systems, Critical Infrastructures Protection, TopEase®

INTRODUCTION: REPRESENTATION OF SYSTEM COMPLEXITY VIA OBJECT ORIENTED INSTRUMENT

Object Oriented Programming – OOP, is a programming paradigm that refers to the usage of „objects" to design applications and computer programs. This body of knowledge was created based on several concepts and techniques, including abstraction, encapsulation, modularity, and inheritance. In OOP, the objects may contain data, in the form of fields (attributes) and code, in the form of procedures (methods). They are capable of interacting with one another by receiving messages, processing data, and sending information to others. Each of them acts as an independent unit with a distinctive role and responsibility *[Ancel, 2011]*. Overall, the paradigm aims to support the development of efficient data structures and to target the behaviors of real-world elements within the digital environment. The OOP is substantially important to Critical Infrastructures due to the fact that it can very well assimilate the complexity of any scenarios that need to be addressed to and

INTRODUCTION: REPRESENTATION OF SYSTEM COMPLEXITY VIA OBJECT ORIENTED INSTRUMENT

Object Oriented Programming – OOP, is a programming paradigm that refers to the usage of „objects" to design applications and computer programs. This body of knowledge was created based on several concepts and techniques, including abstraction, encapsulation, modularity, and inheritance. In OOP, the objects may contain data, in the form of fields (attributes) and code, in the form of procedures (methods).

They are capable of interacting with one another by receiving messages, processing data, and sending information to others. Each of them acts as an independent unit with a distinctive role and responsibility *[Ancel, 2011]*. Overall, the paradigm aims to support the development of efficient data structures and to target the behaviors of real-world elements within the digital environment. The OOP is substantially important to Critical

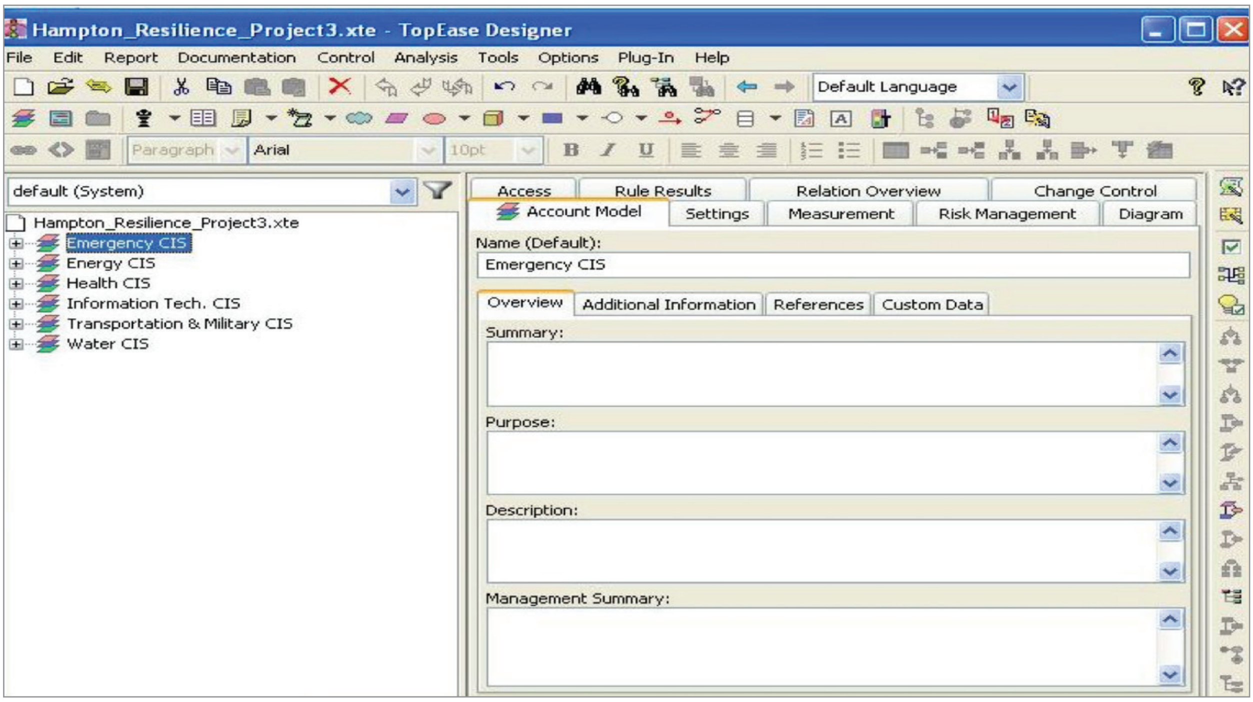

***Fig. 1:** Primary CI Sectors in Focus as Layers*

Infrastructures due to the fact that it can very well assimilate the complexity of any scenarios that need to be addressed to and coordinate a dynamic functioning of different systems at large, by modelling and designing adequate scalable system architectures.

TopEase® Designer is an OOP software that allows the user to manage critical information of focused systems and to visualize those entities in a holistic view of a complex system *[Pulfer & Schmid, 2006]*. The tool was developed by a Swiss company, named Action4Value. It is a commercial software product, which was intentionally designed to handle business processes and originally used in various fields of the business sector, such as financial institutions, healthcare providers, and real estate firms.

The software, which has been used for more than 20 years as a business application tool, comes with the capability to provide methodological procedures to capture a desirable end-state of the organization, company, or enterprise while highlighting the gap between the current „system as is" and desired „system to be" states, see ***Figure 1***.

The idea behind the development of the software was to establish a balance between principles and pragmatism. This fundamental concept is laid on the axioms „**1-Methodology - 3-Layers - 5-Models - 7-Questions**".

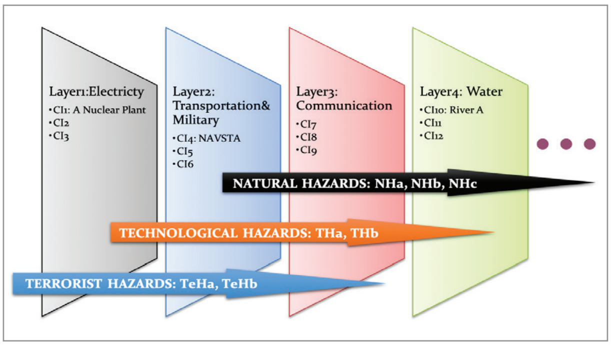

Fig. 2: *Selected Critical Infrastructures and Associated Threats*

The implications of each term can be briefly described as follows:

• **1-Methodology**: The software utilizes only one methodology, which attempts to accomplish its targets or goals based on a pragmatic solution and a balanced manner.

• **3-Layers**: In TopEase®, There are three layers, including definition, support, and implementation. This feature assists the user in obtaining a target audience related business structure.

• **5-Models**: The models allow inputs and data structures to be modeled, documented and elaborated. With a system analysis and design through TopEase®, the output can be validated through value chains and questions, in case all required elements are modeled appropriately. Five models are classified as business, resource, information, delivery, and change.

• **7-Questions**: This function supports the process of interpreting the connections between three layers and five models. It helps the user to determine and verify interrelationships among nodes and objects that are constructed. These questions are about cost, benefit, risk, quality, feasibility, manageability, and impact.

Nowadays, TopEase® offers even more flexible but powerful features at every step of analysis and design processes to assist the user in achieving continuous improvements and meaningful results. In ***Figure 2***, the CI layers representation aims to provide sustainable solutions to the system problems by concentrating on the management of system complexity, transparency of data structure, and control of transformation processes. In Phase IV of this ReIDMP - Resilient informed Decision-Making Process platform development, the goal is to present the benefits of adopting the OOP paradigm as a mean to address and visualize the system complexity. Accordingly, this section will focus on how the OOP based software approach could be useful in handling emergency management operations as enterprise management processes, particularly through the

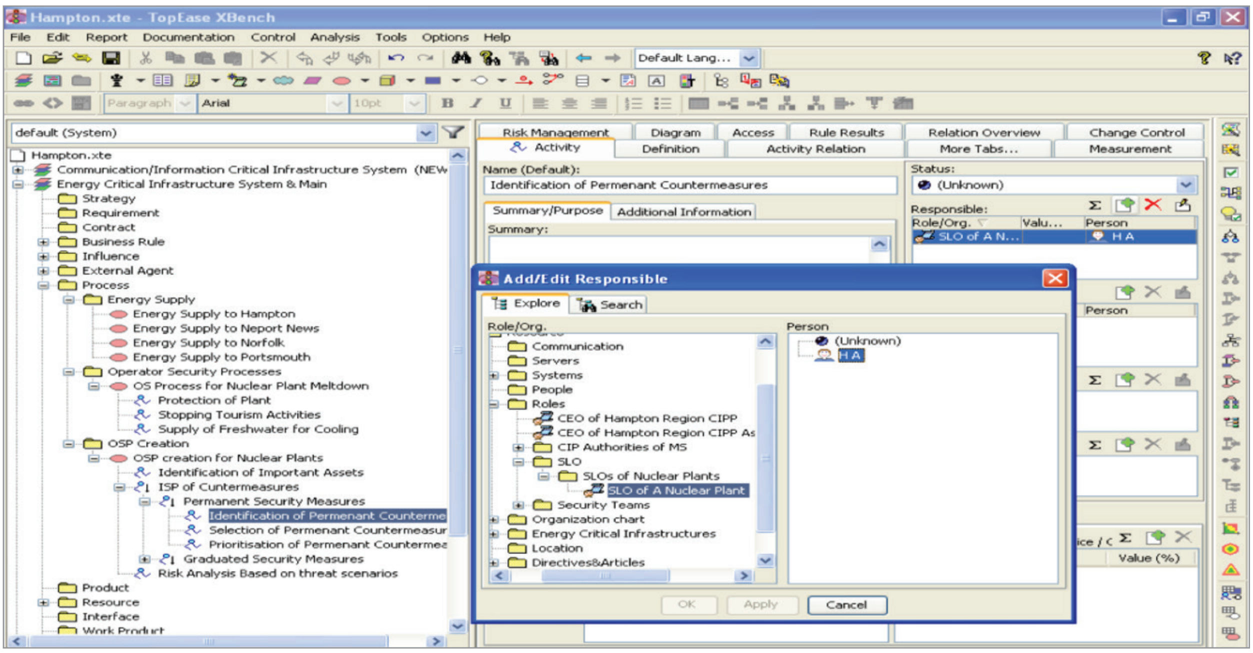

Fig. 3: *RACI Matrix Function Wizard (Responsible)*

study and investigation from a granted project sponsored by the U.S. DHS – Department of Homeland Security.

CRITICAL INFRASTRUCTURE RESILIENCE OF HAMPTON ROADS REGION / TEST REGION

The safety of Critical Infrastructures systems is one of the highest priority tasks for national security. Service interruption on any one or more of them due to either man-made threats or natural disasters, such as terrorist attacks, pandemics, hurricanes, and earthquakes could result in catastrophic failure, not only for the region but also for the entire nation. Thus, after the incidents of the 9/11 Attacks in 2001 and a Hurricane Katrina in 2005, it was obvious that a protection plan itself would not be sufficient and a new perception must be placed on CIs. There is a necessity in establishing more resilient infrastructures to minimize extreme impacts and to withstand damages or disruptions from both expected and unexpected events. However, the main problem in enhancing the resilience capacity of CI systems is that it requires a comprehensive approach and an appropriate tool to incorporate existing protection plans with emergency preparedness actions, like in ***Figure 3***.

Regarding the implementation of this organization chart, the software also provides the feature, called RACI matrix, to support the user in evaluating the characteristics and responsibilities of various positions in the organization chart. In TopEase®, the term „RACI" refers to Responsible, Accountable, Concerned and Informed. This function facilitates the process by mapping all detail and information in the data structure, which allows the user to analyze the entire organization chart and to identify the influence factors and interdependencies among the objects.

Throughout the past two decades, the security and protection of CI systems have received significant attention from and have become a major concern to the U.S. DHS. Numerous research projects in the area of risk and vulnerability of CIs have been funded to address the key issues and pragmatic solutions. Among those developments, one of the projects, namely „Critical Infrastructure Resilience for the Hampton Roads Region (CIRHRR)," involved in analyzing and assessing the factors that could affect functionality, reliability, security, and resiliency of four particular CI

RACI Matrix

Object	R	A	C	I
The Governor declares a state of emergency.	Governor			
Direction of the Director or the Coordinator of EM	Coordinator of Emergency Management/ Manager A A		The City Attorney/ The City Attorney B B	Police Chief/ Police Chief Z Z
A disaster threatens or occurs in the city	City Manager/ Manager A A		The City Attorney/ The City Attorney B B	
Provide initial warning and alerting	Police Chief/ Police Chief Z Z			
Backing-up computers, automated data systems, and data regularly	Information Technology Department			
Ensure adequate communications	Information Technology Department			
Coordinating State	Director of Emergency Management/ Manager A A			
Activation of the EOC	Director of Emergency Management/ Manager A A Emergency Management Coordinator of Police Dept./ Police Cpt-HQ	Police Chief/ Police Chief Z Z		
Order of EOC Activation	Director of Emergency Management/ Manager A A			
Public Information Function	Public Inf. Offcer for Fire Dept./ Public Inf. Offcer for Fire Dept. M M Public Inf. Offcer for Police Dept./	Director of Emergency Management/ Manager A A		

Fig. 4: RACI Matrix Output

sectors in the region, including energy, water and wastewater, transportation, and communications *[Holling, 1996]*.

The study introduced a strategic risk assessment process established by the International Risk Governance Council (IRGC), called Risk Governance Framework, to identify systemic risks of imminent threats or adverse events and then employed an object-oriented instrument to demonstrate a multi-dimensional complexity of interconnection and interdependence between two or more large-scale infrastructure systems. The goal of the project was to develop high-level risk management on economic and social impacts from identified threats and to create a risk assessment model that can be implemented as standard procedural security and countermeasure for other regions, ***Figure 4***.

Hampton Roads is a region in which consist of a body of water and the surrounding metropolitan areas located in the Southeastern United States. The entire area comprises sixteen jurisdictions, including nine cities and seven counties, with a population over 1.7 million. Hampton Roads has a unique characteristic and highly critical to national security as it is home to the world's largest naval complex station and the second-largest port on the Atlantic Coast. Besides its prominence as the economic hub and one of U.S. military stronghold, the location of a region, though, is low-lying in term of geographic condition, so that it is more likely susceptible to the floods and vulnerable to the effects of seasonal hurricanes and occasional tornadoes.

Taking those characteristics and identities of a region into consideration, the Port of Hampton Roads, also officially known as „Port of Virginia", is a key Critical Infrastructure in the Hampton Roads region *[Gheorghe, Tokgoz, Cakir, & Vamanu, 2008]*. Concerning the Port of Virginia, it is a natural deep-water harbor that has a depth of 50-feet with unobstructed channels and berths. Consequently, an autonomous agency is the only major operating port on the U.S. East Coast that receives congressional authorization for 55-feet depth channels *[Virginia Port Authority, 2017]*. It is located just 2.5 hours to the open sea and operates on a year-round schedule due to an ice-free condition. Most activities and services are facilitated by a total of 22 Suez-class ship-to-shore cranes port-wide and almost 7 miles of on-dock rail track *[Virginia Port Authority, 2018]*.

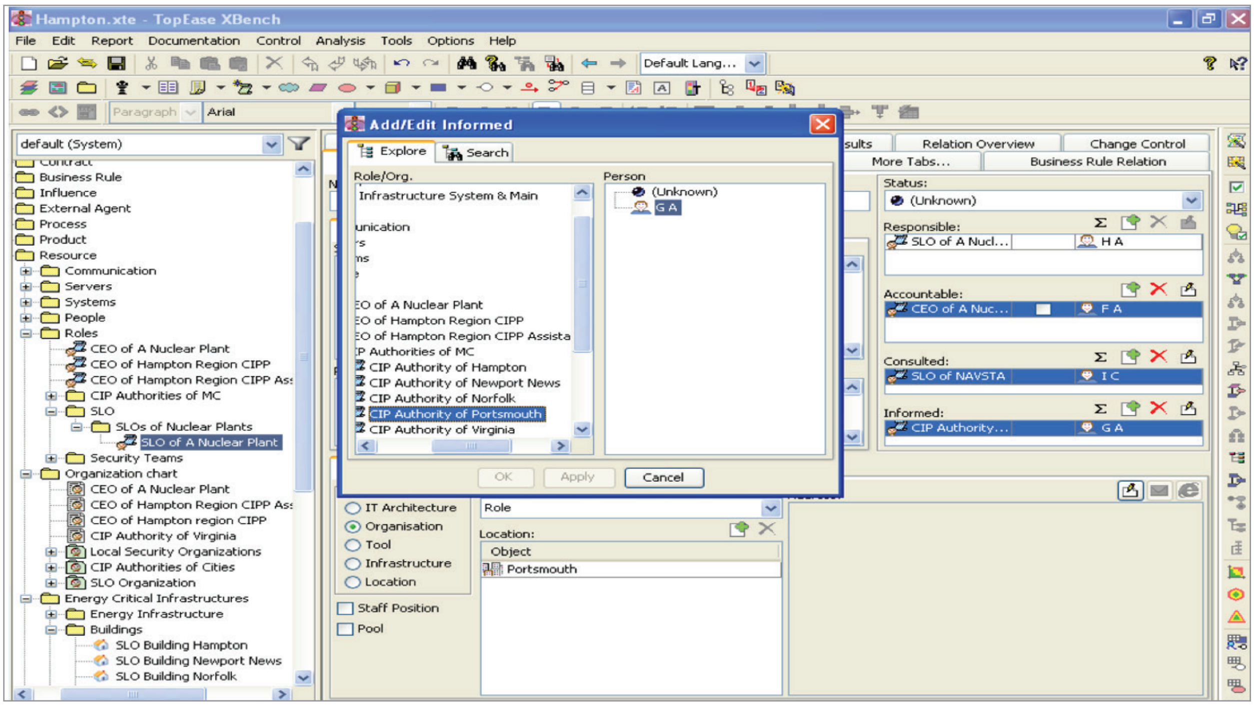

Fig. 5: RACI Matrix Function Wizard (Informed)

Furthermore, in the ***Figure 5***, the four principal facilities, which includes Norfolk International Terminals (NIT), Portsmouth Marine Terminal (PMT), Newport News Marine Terminal (NNMT), Virginia International Gateway (VIG), waterways, and coastal areas are occupied with military assets, nuclear power plants, oil refineries, fuel tanks, pipelines, chemical plants, cargo terminals, and passenger terminals. They, particularly, have inherent security vulnerabilities *[Gheorghe et al., 2008]*. Each facility is relatively spacious and easily accessible by water and land. The terminal is also located in the crowded industrial zone and connected with a transportation network that stretches throughout the nearby metropolitan areas, including Norfolk, Portsmouth, Newport News, Hampton, Virginia Beach, Chesapeake, and Suffolk (DHS, 2005). This transportation system consists of infrastructures and assets, such as roads, railroad, bridges, tunnels, and hundreds of miles of highway. Under these circumstances, the bridges and tunnels are considered vulnerable spots in the area, which pose a significant threat during any event of emergency and crisis situations *[Gheorghe et al., 2008]*.

As a Critical Infrastructure and key national resource, the Port of Virginia is a vital part of the complex systems necessary for the public well-being, national security and global economy. The port and its facilities along with the vessels and barges that sail through the harbor of Hampton Roads are the indispensable components in supporting the free movement of goods and passengers into and out of the United States and the world. Some physical and virtual assets of the port, as well as other associated infrastructures, also even tied to the resistance function and countermeasure ability of the U.S. defense infrastructure systems. A single unexpected attack by terrorist on one or more parts of this Critical Infrastructure may cause temporary disruption, massive casualties, or economic damages, but in the worst-case scenario, the action could even result in the catastrophic failure on the entire system (DHS, 2005). In addition to the man-made threats, the natural disasters are another threat in the Hampton Roads as a region borders with the Atlantic Ocean. So much so that the region is no stranger to risks of storm surges and flash floods. In this area, most flooding could happen from surges, heavy rains, rainstorms, or hurricanes.

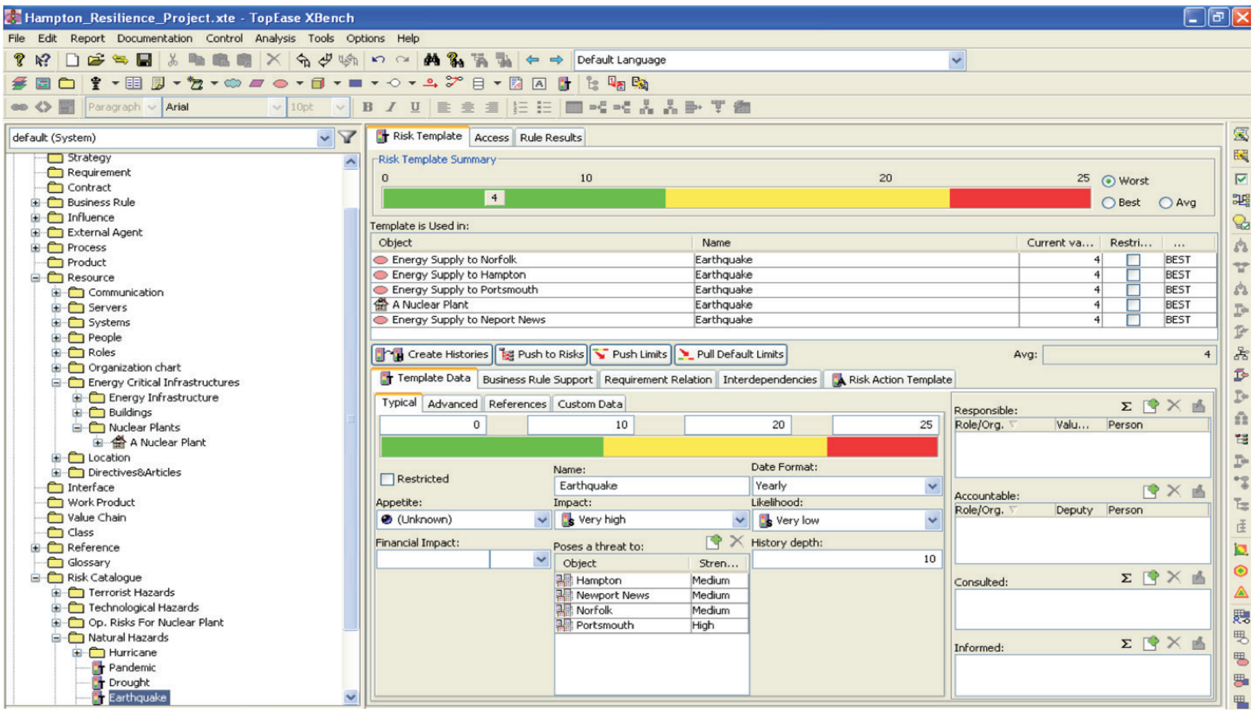

Fig. 6: *Risk Template: Selection of a Disaster Risk*

These events have been known for bringing traffic to a grinding halt and affecting underpasses, tunnels, and bridges, which can be the causes of activity discontinuation and services interruptions between the main facilities and branch locations. As a result, the availability of the Port of Virginia must be constantly assured for national security operations. Addressing the risks and mitigating their potential impacts should remain top priorities, not only to the general public but also to Hampton Roads policy and decision makers.

CIRHRR - CRITICAL INFRASTRUCTURES RESILIENCE FOR THE HAMPTON ROADS REGION PROJECT AND THE IMPLEMENTATION OF TOPEASE® DESIGNER

CIRHRR - Critical Infrastructures Resilience for the Hampton Roads Region project deals with the fact that resilient infrastructures are components, facilities, assets, or systems, whether physical or virtual, that must be able to withstand disruption and damage, but if affected, can be readily recovered or cost-effectively restored *[Gheorghe et al., 2008]*. In order to establish regional disaster mitigation, response, and recovery plan as well as enhance regional security and resiliency of Hampton Roads, a complex set of management and policy issues are required to be addressed. A complete list of critical assets and essential resources, both public and private, need to be integrated as a regional model. All involved facilities, relationships among them, and their dependences over one another must also be analyzed to determine the capabilities of response and recovery in each of jurisdictions during emergencies *[Gheorghe et al., 2008]*.

However, in the ***Figure 6***, with the complication of diversity on local authorities, federal agencies, and private organizations in multiple jurisdictions, consequently, the City of Hampton was selected as a model city to develop its Emergency Operation Plan (EOP). So much so that the idea of using TopEase® in CIRHRR project is to convert the EOP of the City of Hampton into a form of a digital model for illustrating the interdependencies among CIs.

The Hampton Roads Region has unique characteristics and is strategically critical to national security, especially economy and military. For this reason, the existence of multiple jurisdictions, military assets, and private utility facilities require an analytical solution through the

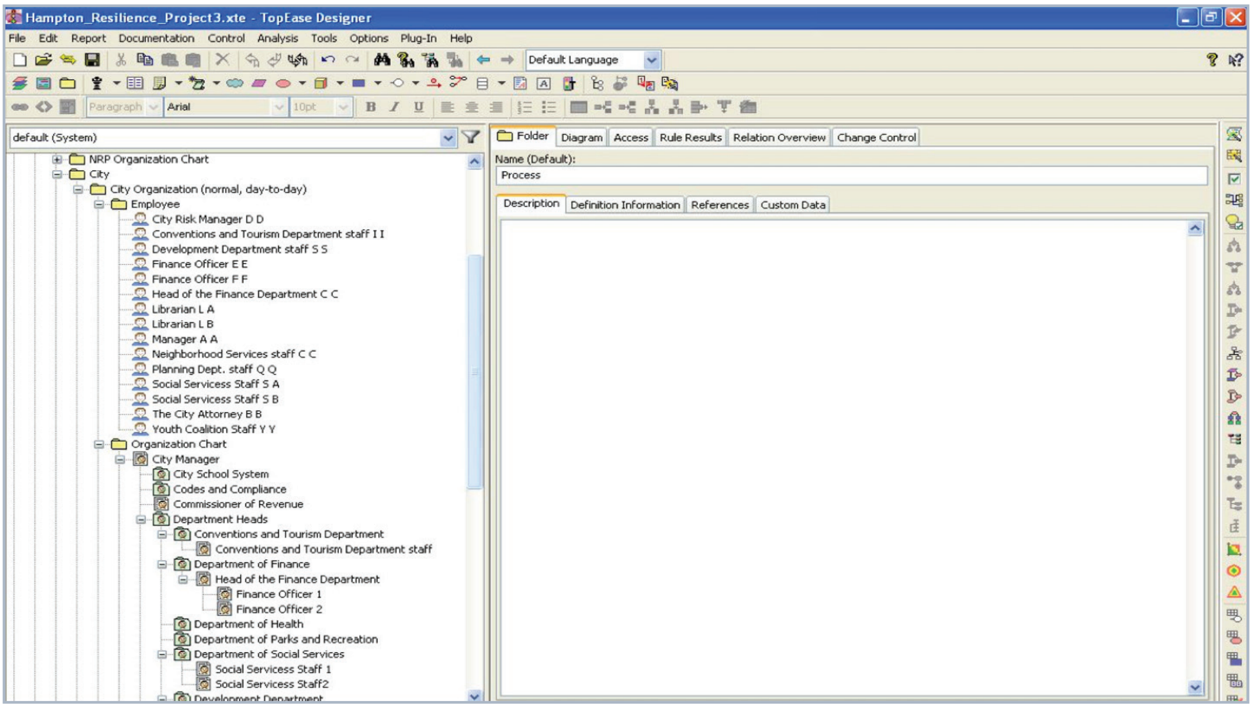

Fig. 7: *Process Support Interface of Emergency Management Complexity*

Table 1. *Decision Matrix - Model of Decision Theory*

application of the system of system technology. To analyze the current state of an emergency plan, the process was initiated within TopEase® by outlining four primary CIs in focus as layers. Each of them represents a specific sector of Critical Infrastructures and selected infrastructures, which includes electric power, water and wastewater, transportation and military, and communication. The functionalities of these integrated CI layers and EOP against different threats are cross-cut as predefined issues.

As an example of implementation is the modeling of the organizational chart and the visualization of complexity among entities. At this point, it should be noted that when using TopEase® to develop models, every output result needs the input data. In other words, the user must enter all detail and information in which as same as constructing the data structure to generate the models. So that by defining stakeholder, personnel, roles, and responsibilities, the software would produce the graphical output model that shows the relationship between objects and the complexity of emergency management in the format of process input interface, as displayed in ***Figure 7***.

Managing emergency operations is a very challenging task. The delay responses to the incidents in minutes or just seconds due to overlapping authority and unclear instructions could lead to an undesirable outcome. To avoid such unnecessary confusions and errors, all possible external factors must be identified and included in the plan. In the CIRHRR

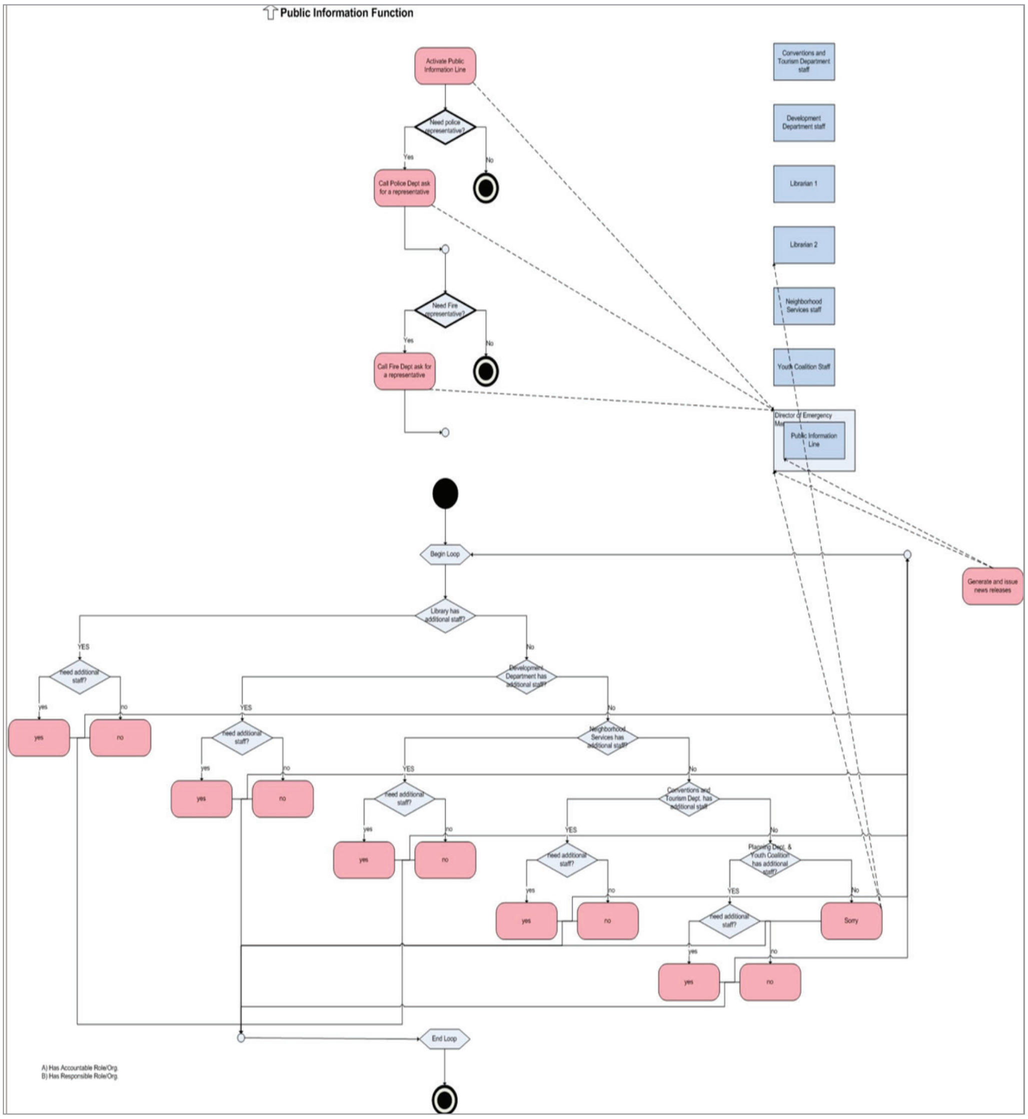

Fig. 8: *Visualization Diagram of Activities, Processes, Roles, and Responsibilities*

project, this step has incorporated additional information, such as the explanatory glossary, detail activities, process lifecycle, influence agents, and reference database, which were directly adapted from the EOP – Emergency Operation Plan of the City of Hampton into the TopEase®. With the data structures of those sets of input, as a result, they would allow the software to produce an inclusive visualization of a model which includes activities, processes, roles, responsibilities, and people in the same diagram. An example of a partial output representation is exhibited in ***Figure 8***.

In addition to the capability of creating the models and graphic representations, TopEase® also comes with the risk catalog function. This feature can handle any kinds of risk to the system that is being analyzed and modeled. In TopEase®, the risk is defined by two parameters, which are likelihood and impact. The scales and descriptions of each category are exemplified in ***Table 1.***

Likelihood Ranking			Impact Severity		
Description	**Frequency of Occurring Event**	**Probability of 1-off Event**	**Description**	**Safety**	**Security**
Improbable	Once Every 10,000 Years	1 in 1,000	Minor	Minor Injuries	Minor Breach
Remote	Once Every 1,000 Years	1 in 100	Moderate	Major Injuries	Major Breach
Occasional	Once Every 100 Years	1 in 10	Significant	Single Fatality	
Probable	Once Every 10 Years	Likely	Substantial	Multiple Fatalities (10+)	
Frequent	Once Every Year	Certain	Mega	Multiple Fatalities (100+)	

Table 1: *Categories of Likelihood and Impact in TopEase® [Gheorghe, et al., 2008]*

According to the CIRHRR project, it suggested that Hampton Roads is vulnerable to both man-made disasters and natural catastrophes. Some are considered significant threats to the Hampton Roads *[Gheorghe et al., 2008]*. Thus, the study approached this aspect by assigning the risk of having a disaster on any operation or CI to calculate the total risk of that event. ***Figure 9*** and ***Figure 10*** show a risk template dialog windows, where an earthquake was entered as a selected disaster and then assigned to a specific Critical Infrastructure, especially nuclear power plants. In TopEase®, the assigned

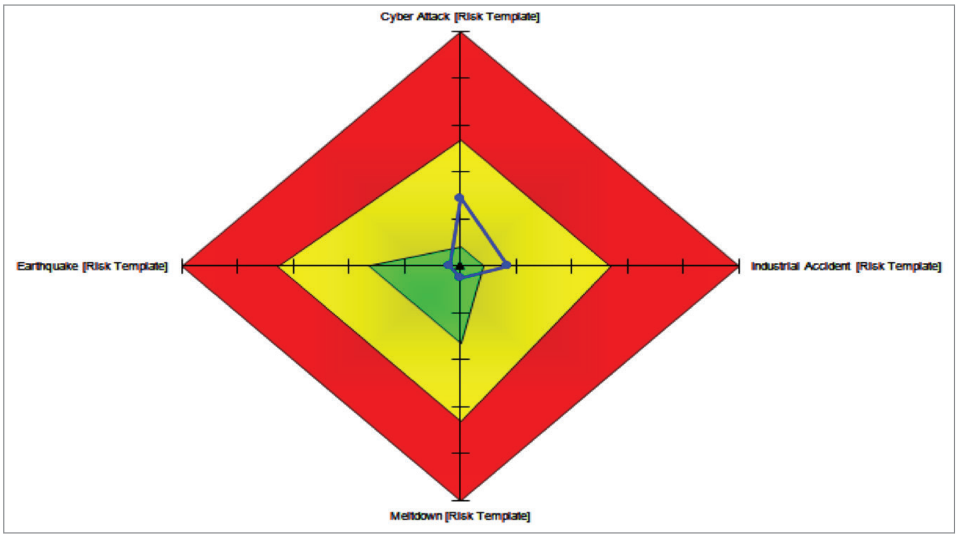

Fig. 9: *Risk Scorecard of Nuclear Power Plan*

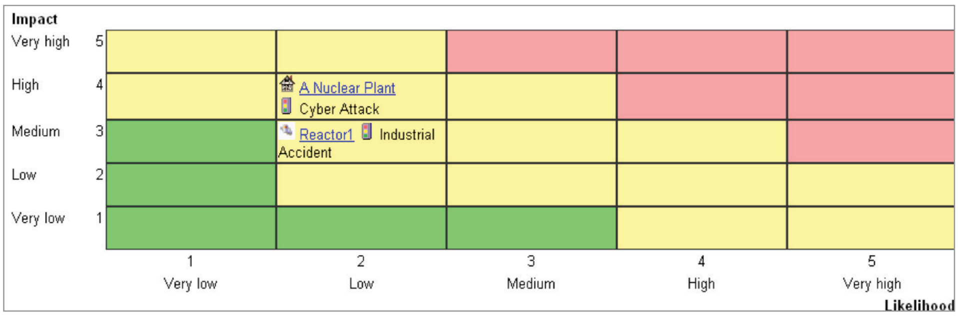

Fig. 10: *Risk Map of Nuclear Power Plan*

risk can be graphically represented with different options, such as risk scorecard matrix or risk interdependency diagram. The examples of the likelihood of having different types of disaster versus impacts of those disasters on a nuclear power plant.

CONCLUSION

Throughout the last aera there were various metrics that were castoff to measure the complexity. These metrics were not efficient, consistent and able to measure the complexity of software by that time. Nowadays, with speedy growth in IT, various metrics were anticipated from diverse researchers in unalike fields of study.

The main goal of the systematic approach of Object-Oriented Instruments for Critical Infrastructure Protection is to further examine the role of metrics in the life cycle of software development which enables companies to enhance quality and improve their productivity. A useful tool proposed by Action4Value, called TopEase® is used to evaluate the metrics of different real-life scenarios to access the vastness of elements that need to be taken into consideration in order to achieve a high level of decision-making programming language. The correct degree of complexity has to be computable and not be maximal for randomness.

The time has come to raise an imperative philosophical question for the science of complexity or any other scientific theories, namely the issue of instrumentalism versus realism in case scenarios based on real environments. What are the prospects for adopting a realist position toward the patterns represented by TopEase® - Decision Support Systems machines as contrasting to the aspect that patterns are valuable tools for forecasting the system's comportment but not real topographies of the world?

With the development of value creating tools for designing and understanding superior architectures for the future of our society, there are to be considered to implementation of next generation solutions like Blockchain technology, Artificial Intelligence, different approaches to IoT - Internet of Things and 5G patterns into consistent Decision Support Systems, in order to truly understand the phenomena of Complexity of Systems.

REFERENCE LIST

Ancel, E. (2011). A systemic approach to next generation infrastructure data elicitation and planning using serious gaming methods. (Doctoral Dissertation), Old Dominion University, Norfolk, VA

Holling, C. S., (1996) Engineering resilience versus ecological resilience. Engineering Within Ecological Constraints. National Academy Press, Washington, DC. pp. 31–44

Gheorghe, A. V., Tokgoz, B. E., Cakir, V., & Vamanu, D. V. (2008). Critical infrastructure resilience for the Hampton Roads region: Policy analysis for regional resilience. Internal Report. Department of Engineering Management and Systems Engineering, Old Dominion University, Norfolk, VA

Pulfer, R., & Schmid, U. (2006). Control Your Business: The Balance between Principles and Pragmatism. Zollikofen: Pulinco

U.S. Department of Homeland Security. (2005). The National Strategy for Maritime Security. Washington, DC: White House Office. Retrieved from https://www.hsdl.org/?view&did=456414

U.S. Department of Homeland Security. (2009). National Infrastructure Protection Plan (Partnering for Critical Infrastructure Security and Resilience). Washington DC: DHS. Retrieved from https://www.dhs.gov/publication/nipp-2009-partnering-enhance-protection-resiliency?topics=all

U.S. Department of Homeland Security. (2013). National Infrastructure Protection Plan (Partnering for Critical Infrastructure Security and Resilience). Washington DC: DHS. Retrieved from https://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience?topics=all

Virginia Port Authority. (2017). Big-Ship Ready (Fiscal Year 2017 Annual Report). Retrieved from http://www.portofvirginia.com/wp-content/uploads/2017/11/The-Port-of-Virginia-FY17-Annual-Report.pdf

Virginia Port Authority. (2018). The Port of Virginia. Retrieved January 13, 2020, from http://www.portofvirginia.com/about/fast-facts/