DOKUZ EYLÜL UNIVERSITY
GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

ASSESSMENT OF CRITICAL INFRASTRUCTURE PROTECTION: A CASE STUDY FROM URBAN DRINKING WATER SYSTEM

by
Fulden ESKİCİOĞLU TUNGER

October, 2019
İZMİR

ASSESSMENT OF CRITICAL INFRASTRUCTURE PROTECTION: A CASE STUDY FROM URBAN DRINKING WATER SYSTEM

A Thesis Submitted to the
Graduate School of Natural and Applied Sciences of Dokuz Eylül University in Partial Fulfillment of the Requirements for the Degree of Master of Science in Environmental Engineering

by
Fulden ESKİCİOĞLU TUNGER

October, 2019
İZMİR

M.Sc THESIS EXAMINATION RESULT FORM

We have read the thesis entitled "**ASSESSMENT OF CRITICAL INFRASTRUCTURE PROTECTION: A CASE STUDY FROM URBAN DRINKING WATER SYSTEM**" completed by **FULDEN ESKİCİOĞLU TUNGER** under supervision of **ASSOC.PROF.DR. ORHAN GÜNDÜZ** and we certify that in our opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

Assoc. Prof. Dr. Orhan GÜNDÜZ

Supervisor

Doç.Dr. Neval BAYCAN

Jury Member

Dr. Öğr. Üyesi Hasan SARPTAŞ

Jury Member

Prof. Dr. Kadriye ERTEKİN
Director
Graduate School of Natural and Applied Sciences

ACKNOWLEDGEMENTS

First and most of all, I would like to express my sincere gratitude to my supervisor Assoc. Prof. Dr. Orhan Gündüz for providing his guidance, suggestions, comments, encouragement and expertise showed the way of throughout the process of writing this thesis. Besides that, I am conveying my thanks to him, since he is guiding me not only in the academic field, but also in social and business life during both undergraduate and graduate study.

Also I would like to remark that I appreciate Efem Bilgiç for his support during this process.

I would like to give special thanks to my husband Abdullah Tunger for his care and support during my study.

Additionally, I would like to thanks to my family; Venhar Eskicioğlu my father, Jale Eskicioğlu my mother and Fulya Eskicioğlu my sister. They gave their great support during this process as the same all through my life.

Fulden ESKİCİOĞLU TUNGER

ASSESSMENT OF CRITICAL INFRASTRUCTURE PROTECTION: A CASE STUDY FROM URBAN DRINKING WATER SYSTEM

ABSTRACT

Many countries around the world face incidents that threaten their security due to political, economic and social crisis. These threats mostly target critical infrastructure systems that are vital components of modern societies. Communications, energy, water, health, transportation, finance and banking infrastructure are amongst these critical infrastructures. The disruption of their services might influence modern societal life. Today, many countries have started to conduct risk analysis and develop risk management plans for such national and international threats. In this study, a sample risk analysis study was carried out by using the CARVER method and The Vulnerability Self-Assessment Tool (VSAT 6.0) software for analyzing the drinking water infrastructure system of Izmir Province. The aforementioned methods and software was to determine risk levels of various components of the system. Using the CARVER method, surface and ground water resources called the northern and southern water resources of Izmir Province and their critical infrastructure components were examined under various scenarios and risk analyzes were performed. As a result of the analysis, the most important surface water source of the southern region of Tahtalı Dam Lake and the northern water resources of underground water wells were found to be affected from biological, physical, natural disaster and cyber-attack. The Vulnerability Self-Assessment Tool (VSAT 6.0) software was further used to conduct a risk analysis study on the Tahtalı Dam Drinking Water System of Izmir Drinking Water System. . The vulnerability of the system components against different threats was evaluated with VSAT software, and the current situation of the facility was determined by detailed risk analysis works. Accordingly, potential security gaps were determined and the precautionary measures to be taken were determined as a result of the analyzes.

Keywords: CARVER, VSAT, critical infrastructure facilities, drinking water system, Izmir, Tahtalı Dam

KRİTİK ALTYAPI GÜVENLİĞİNİN DEĞERLENDİRİLMESİ: KENTSEL İÇME SUYU SİSTEMİ ÖRNEĞİ

ÖZ

Dünyadaki birçok ülke, ekonomik, politik ve sosyal krizler sonucu güvenliğini tehdit eden olaylar yaşamaktadır. Bu tehditler ile çoğu zaman, modern toplumsal yaşamın vazgeçilmez bileşenlerinden olan kritik altyapı sistemleri hedef alınmaktadır. Bu sistemlerin başında haberleşme, enerji, su, ulaşım, sağlık, ulaşım, finans ve bankacılık alt yapıları gelmektedir. Söz konusu kritik alt yapılardan herhangi birinin durdurulması, tüm gündelik toplumsal yaşamı etkilemektedir. Günümüzde ulusal ve uluslararası tehdit olarak algılanan bu durumlar için ülkeler çeşitli metot veya yazılımlar geliştirerek kritik altyapı tesislerinin risk analizlerini gerçekleştirmektedir ve değerlendirmeler sonucunda, tehdit altındaki kritik altyapı bileşenleri için risk yönetim planları hazırlamaya başlamıştır. Bu çalışmada, dünyada genel olarak kullanılan metot ve yazılımlar incelenerek İzmir İli içme suyu altyapı sistemi için CARVER metodu ve Self-Assessment Tool (VSAT 6.0) yazılımı kullanılarak örnek risk analizi çalışmaları gerçekleştirilmiştir ve sonuçları değerlendirilmiştir. CARVER metodu kullanılarak, İzmir İli kuzey ve güney su kaynakları olarak adlandırılan yüzeysel ve yeraltı su kaynakları ve bunlara ait kritik altyapı bileşenleri çeşitli senaryolar altında incelenmiş ve risk analizleri gerçekleştirilmiştir. Analiz sonucunda güney bölgesinin en önemli yüzeysel su kaynağı olan Tahtalı Baraj Gölü'nün ve kuzey su kaynakları olan yeraltı su kuyularının biyolojik, fiziksel, doğal afet ve siber saldırıdan etkileneceği belirlenmiştir.Vulnerability Self-Assessment Tool (VSAT 6.0) yazılımı kullanılarak ise, Tahtalı Barajı İçme Suyu Sistemi için bir risk analizi gerçekleştirilmiştir. Tahtalı Barajı İçme Suyu Sistemi bileşenlerinin farklı tehditlere karşı kırılganlığı VSAT yazılımı ile değerlendirilmiştir ve tesisin mevcut durumu detaylı risk analizi çalışmaları ile belirlenmiştir. Buna göre, potansiyel güvenlik açıkları belirlenerek yapılan analizler sonucunda alınması gereken önlemler belirlenmiştir.

Anahtar Kelimeler: CARVER, VSAT, kritik alt yapı tesisleri, içme suyu sistemi, İzmir, Tahtalı Barajı

CONTENTS

Page

LIST OF FIGURES

Page

LIST OF TABLES

Page

CHAPTER ONE
INTRODUCTION

1.1 Critical Infrastructures

In recent years, global warming, natural disasters and increasing terrorist attacks in the world have led many countries to reconsider their global and regional security measures. Every attack, event and natural disaster creates serious problems and risks for the security of the countries and the welfare of the nations. Often, these attacks and incidents are aimed at critical infrastructures that are necessary for people to sustain their vital activities such as health, basic security and economic and social wellbeing. In many cases, such attacks bring these vital activities to a halt when they fail to perform their functions partially or completely. Critical infrastructures are systems that are used at every moment of the daily life of the communities, provide indispensable and irreplaceable services, and when they are stopped, they can disrupt the daily lives of people and sometimes expose public health risks. Although there are many critical infrastructure systems that are vital for countries, the most important of these are water, energy, health, finance and banking, transportation and communication infrastructures.

Figure 1.1 Critical infrastructures (DHS, 2017)

In the United States, the National Protection and Programs Directorate (NPPD) has initiated a National Infrastructure Protection Plan (NPPD) by launching a project to protect all critical infrastructure under the same roof Plan (NIPP). This initiative aims to protect the security and welfare of the nation by establishing a dynamic security mechanism through the continuous updating and development of this plan (U.S. Homeland Security, 2010).

In general, United States The Department of Homeland Security (DHS) is obliged to increase security and resistance to attacks. In this context, it is also responsible for mitigating risks of all attacks against critical infrastructure and the effects of natural disasters (DHS, 2017). Security measures include safeguarding some critical information systems against cyber attacks, taking measures to make critical structures, buildings and facilities more resistant to physical attacks, and strict control of the entrances and exits of all critical structures and facilities. In order to increase the resistance to attacks, it is primarily responsible for sensitivity analysis, preparing dynamic plans for changing conditions, providing backup and emergency power for important facilities, and producing and using durable materials for buildings.

To this end, a special assessment plan and associated software for water and wastewater systems have been developed in the United States. With the help of the program called Vulnerability Self-Assessment Tool (VSAT), developed by the U.S. Environmental Protection Agency (EPA), each local drinking water and wastewater enterprise needs to conduct a risk analysis to identify the vulnerabilities to potential threats to its facility and to identify the consequences and perform corrective and preventive actions (EPA, 2016). This software was used in this study for risk analysis of Tahtalı Drinking Water System, which is the most important water source of Izmir. With this assessment made by the help of VSAT software, it is aimed to determine the vulnerability of Tahtalı Drinking Water System against possible threats and hazards.

In this study, the "CARVER" method, which is used as the first assessment tool, is a method developed primarily for the purpose of military target analysis. The

CARVER method allows the assessment of the risks, to which a critical infrastructure element will be exposed to by scoring under the headings of **C**riticality, **A**ccessibility, **R**ecuperability, **V**ulnerability, **E**ffect and **R**ecognizability, the initials of which form the name of the method (Federation of American Scientists, 2010). The "CARVER" method was used to reveal the current situation of critical infrastructures, to identify and prioritize the risks to which the infrastructure elements will be exposed under the scenarios identified.

In this study, a comparative risk analysis of northern and southern water resources of Izmir province was performed by using CARVER method. While the risk situations of these facilities, which meet the drinking water needs of Izmir province under different threats, have been compared comparatively, the measures to be taken to ensure the safety of the related facilities and units have also been evaluated.

In addition to the research conducted from various sources, visits were made to İZSU (Izmir General Directorate of Water and Sewerage Administration) SCADA unit, which is responsible for conducting water and sewerage services of Izmir Municipality. During this visit, the opinions of the authorities were obtained and information exchange was made about the facilities and their risk status. During the interviews, information about surface and underground water resources, drinking water distribution system, treatment plants, water tanks, pumping stations serving to Izmir Province was shared and opinions were exchanged about the threats & attacks that may affect this system and possible consequences. Due to confidentiality and security risks, all information and data are not fully shared. Therefore, the risk analyzes provided in this study should be considered as a general assessment and no definite judgments were made. The possible threats and possible consequences were evaluated and their effects on the drinking water critical infrastructure components were assessed.

The primary purpose of this thesis is to raise awareness about the security of critical infrastructures in Turkey, and evaluating the applied procedures in the world of risk analysis methods and emergency action plans to gain perspective on adaptations to our country. The studies carried out within the scope of this thesis

have been presented in two different congresses and it has been provided to reach the authorized persons responsible for the operation of drinking water facilities. The first congress was held on February 13-17, 2017 in Antalya. “International Water and Health Congress”, in which the results of the assessment of risk analysis of Izmir drinking water system by CARVER method were shared (Eskicioğlu, Bilgiç, & Gündüz, 2017). The other congress was held on November 2-4, 2017 in Izmir, "International Water Congress-Water Management in Smart Cities". In this congress, the risk analysis study and results of VSAT software for Izmir drinking water system were shared (Eskicioğlu & Gündüz, 2017).

1.2 Objective of the Study

Water infrastructure is one of the most important infrastructures for human existence. Providing safe drinking water is an indispensable element in meeting all human activities and providing general public health and is essential for the sustainability of modern life and national economy. Attacks to water infrastructures can be listed as deliberate mixing of chemical/biological agents, contamination, physical attacks of terrorism, cyber attacks that can affect the water infrastructure control and management tools, and partial/complete destruction of the component due to natural disasters. As a result of such threats, the system becomes unusable and consequently, numerous illnesses and even deaths can occur in extreme situations. Water infrastructure also affects other interconnected critical infrastructures such as health facilities, fire department, energy, transportation, food and agriculture. Therefore, any disruption or pause in the operation of the water infrastructure can have serious consequences for modern urban life style.

For all these reasons, a risk analysis was deemed necessary by developed countries to ensure the safety of water infrastructures and led them to initiate action plans. The literature review conducted within the scope of this thesis has shown all risks associated with water infrastructures, their assessment methods and applications from all around the world but did not reveal any previous cases of risk analysis studies for drinking water critical infrastructure system in Turkey although risk analysis of other critical infrastructure systems, such as banking & finance database

system and electricity system has been evaluated previously. An important objective of this study is to raise awareness about the importance of drinking water system, to demonstrate ways on how a general assessment can be made, to present the risk status of Izmir Water System and to present possible threats and to propose preventive-corrective action plans to reduce all potential risks.

1.3 Scope of the Study

In this thesis, a risk analysis of the critical drinking water infrastructure of the City of Izmir in Turkey was conducted. Considering the geographical and geopolitical situation of Izmir, various scenarios was identified by considering all possible threats and risk analyzes were performed by using the CARVER method and VSAT software. The results of this analysis were evaluated and assessed to obtain potential mitigation measures to these risks.

By using the CARVER method, risk analyzes of critical infrastructure components of the northern and southern water resources of Izmir were conducted and a comparative assessment was made. While most of the resources identified as southern water sources are surface waters from Tahtalı Dam, the sources identified as northern water sources are groundwater resources extracted from Sarıkız, Göksu, Menemen-Çavuşköy and Halkapınar wells. In this context, while assessing the risk levels of north and south water resources under possible threats, a comparison of the risks to surface and ground water resources was also made. While the risk situations of these facilities meeting the drinking water needs of Izmir province under different threats, have been compared comparatively, the measures to be taken to ensure the safety of the related facilities and units have been evaluated.

Later, risk analysis of Tahtalı Dam Drinking Water System was performed with VSAT software. The vulnerability of the facilities of Tahtalı Dam Drinking Water System against the possible attacks and threats has been examined, and a detailed risk analysis has been made by revealing the current situation and the security deficits of the facility were identified. Finally, the precautions to be taken for each critical infrastructure component was also revealed as a result of the analysis.

CHAPTER TWO
LITERATURE REVIEW

2.1 General Literature Review

Drinking water and wastewater systems protecting the water infrastructure is very important for public health and welfare. Inability to serve due to malicious actions, natural disasters and systemic problems that countries may encounter, bring along many diseases and damages as well as negative economic consequences. Negative impact of the water sector will also affect other sectors such as energy, transport, industry, food and agriculture. Considering the failure of fire extinguishing systems, disruption of hospital services, stopping of food services and agriculture sector or the impacts of untreated wastewater on the environment and human health, it is possible to say that the impact on the water infrastructure can deeply influence the whole country (Baylis & et al., 2016) (Figure 2.1).

Countries have to take precautions to avoid the negative effects of all these situations. These precautions should be taken with the awareness of eliminating risk at source. Considering the safety of the whole drinking water system, the risks that may arise from water sources and water intake points to the point where water reaches the end user should be considered. Action plans should be developed to prevent protection and threats on a provincial and country basis, starting from local facilities. Of course, in order to create these plans, firstly, the current risk situation should be determined by using a risk assessment method or software appropriate to the system where the assessment will be made.

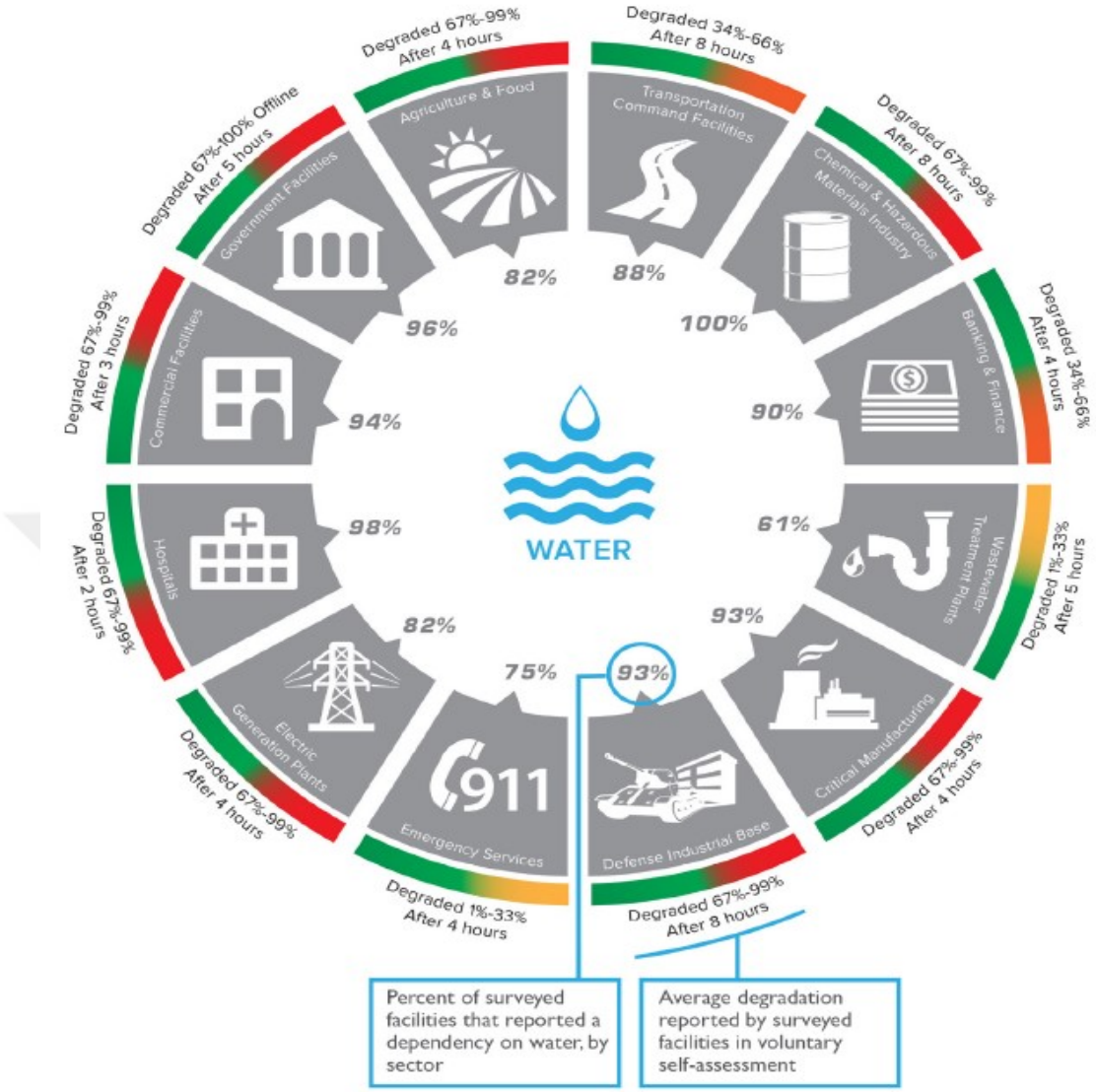

Figure 2.1 Potential function degradation following loss of water services (Baylis & et al., 2016)

Effective and comprehensive risk assessment methodologies form the basis of a successful critical infrastructure protection program. In the analysis, it is very important to use correct and sufficient data that are necessary for the evaluation considering the characteristics of the assets of the facility or the system. It is also very important that the people who will be evaluating during the analysis (municipality officials, engineers, operators, etc.) dominate the plant / system. In general, the approach in risk assessment methodologies; include identification of the threats and their probability of occurrence, identification of security vulnerabilities of

the facility and assessment of the potential impacts as a result of threat realization (Baker, 2005).

The evaluation the results and preparation of the risk management plan is just as important as the analysis stage. Based on the results, it is necessary to prepare a real and applicable corrective-preventive action plan, to make improvements against security gaps, to prepare defense plans using developing and changing technologies, to be ready and active for all kinds of threats and to update the plans and mitigation measures at various periods.

Risk analyzes can be conducted at local, regional, national or international levels. However, the most important point is to perform risk analysis with the correct data from the source of the system. For example, a local entity should incorporate the characteristics of the assets of its facility into the analysis in detail and identify the effects or potential threats to the area it serves to obtain accurate results. However, it may not be able to calculate the interaction of the system with other systems (electricity, fire, hospital, food, industry, etc.) that it interacts with (Figure 2.1 and Figure 2.2).

In order to prevent this situation, the enterprise should cooperate by notifying their plans to a higher governing bodies at district, provincial, regional, and state levels. Accordingly, infrastructure interdependencies can be evaluated accurately. Only when these interdependencies are properly determined, the consequences of any failure in the water infrastructure can be predicted in other systems to which it is connected.

In this way, in case of a crisis, detrimental results can be prevented and their effects can be reduced. An example for system interdependencies are shown in Figure 2.2 and Figure 2.3.

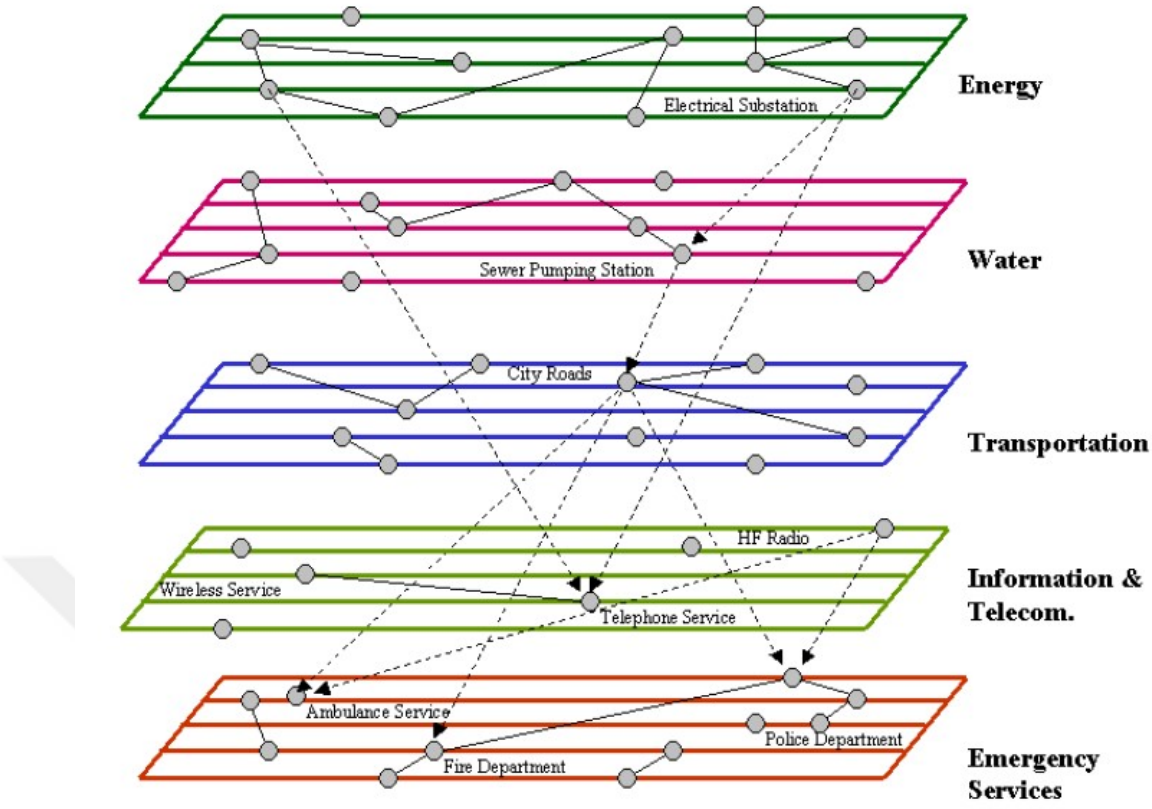

Figure 2.2 Infrastructure interdependencies (Pederson, Dudenhoeffer, Hartley, & Permann, 2006)

In general, critical infrastructures were less interdependent in previous years. Due to technological advances and the need for increased productivity, these infrastructures have become increasingly automated and interconnected. Although these developments had positive effects, they also brought in a number of negative effects. As critical infrastructures become increasingly interdependent, infrastructure systems become more vulnerable to gradual failures in other systems (Pederson, Dudenhoeffer, Hartley, & Permann, 2006). Interconnected critical infrastructures can become even more vulnerable under any threat with a dependency ratio. Risks that may occur as a result of an unintentional breakdown or an intentional attack on the system have greatly increased due to the interrelationship, complexity and dependence of these infrastructures. Increased use of information and telecommunications technologies to support, monitor and control the functions of critical infrastructures has contributed to this. Another example interdependency between critical infrastructures are shown at Figure 2.3.

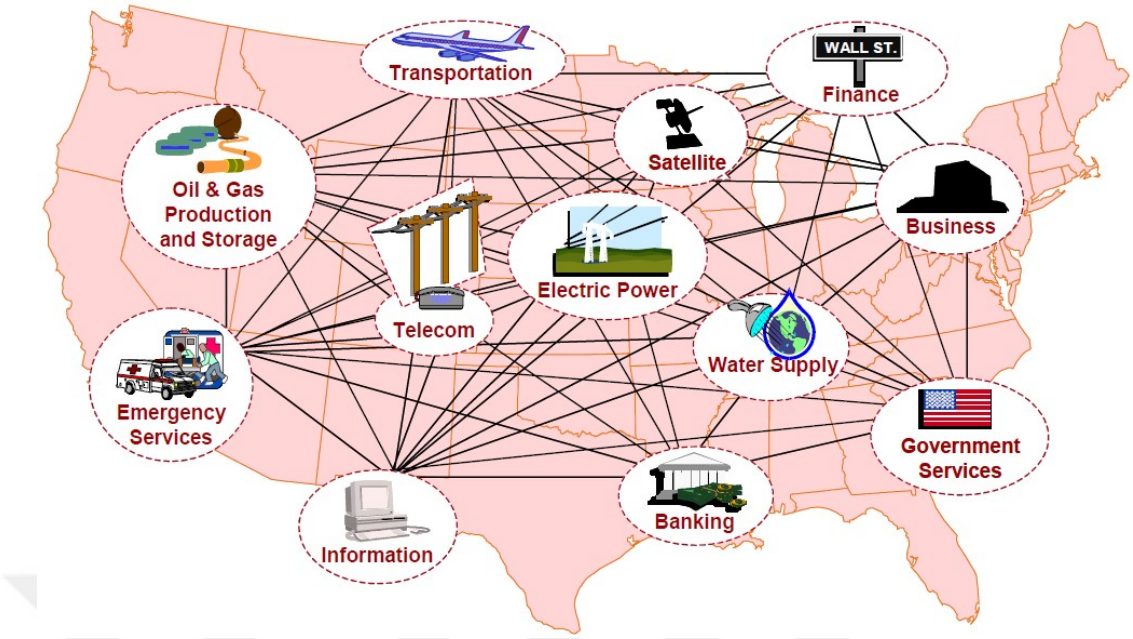

Figure 2.3 Interdependent critical infrastructures (Gilette, Fisher, Peerenboom, & Whitfield, 2002)

Critical infrastructures, such as electric power grids, natural gas pipelines, water distribution networks, transportation networks, and internet communication networks, play a fundamental role in providing essential services. A failure in any of these networks may affect others. Disruption of interconnected networks can have serious negative consequences for the modern society. Therefore, it is necessary to examine the interdependence of critical infrastructures. Electric power and water distribution networks are typical examples of interdependent infrastructure networks (Zhang, Yang, & Lall, 2016).

A simple example to this interdependency can be explained as follows: pump stations, control units (SCADA) and water storage tanks in the water network need a direct power supply to function. When an electric power failure occurs, the water distribution network is directly influenced (Zimmerman, 2009).

There is also the concept of cascading interdependencies. A perfect example to cascading failures in interdependent networks is the power blackout that happened in many parts of eastern USA on 14th August 2003. In addition to direct consequences of power failure on the society, the failure also caused water shortages and affected other critical infrastructures. Another example is the power blackout resulting from

Hurricane Sandy in 2012, which led to a loss of water supply in New York City (Zhang, Yang, & Lall, 2016).

These examples address the importance of the sensitivity of interconnected energy and water networks to cascading failures. Predictive approaches can provide important information to facilitate proactive risk management of specific interdependent infrastructure networks.

In this section, some of the risk analysis methodologies and software used in the world are evaluated and two methods are selected for the water sector's critical infrastructure analysis and risk assessment.

2.2 The Policy Framework In Worldwide

Critical infrastructures are networks, assets, systems and structures that will have serious impacts on the health, safety and economy of the citizens as a result of the negative impacts on the environment, vital activities and maintenance of public services where it cannot function partially or completely (Leuven, 2011).

The concept of critical infrastructure was first introduced in developed countries, especially in the USA. In October 1996, "The Commission for the Protection of Critical Infrastructure" was established by the President of the United States and the definition of critical infrastructure was first defined in this commission. Infrastructures that will be negatively impacted from terror/sabotage, natural/man-made disasters, biological/chemical attacks, technology and cyber-attacks are considered to be critical for the society. Security concepts are developed for these infrastructures to sustain the modern societal life.

The September 11 attacks in the United States and Hurricane Katrina, the terrorist attacks on passenger trains in Spain in 2004 and the terrorist attacks in Britain in 2006, the cyber-attacks in Estonia in 2007 and Georgia in 2008 are all considered to be external impacts on various infrastructures and the community that benefit from them. Human or natural disasters, terrorism / sabotage and other incidents have led to

a serious consensus on the need to identify and protect critical infrastructure for the safety of countries and the welfare of citizens (Copeland, 2010).

In recent years, the increasing threat of terrorism and major disasters have led countries to develop policies, strategies, legislation, plans and programs to protect critical infrastructures. The developed countries, especially the USA, Japan and EU member states, identified critical infrastructures, prepared legislation on the protection of these infrastructures and identified institutions and organizations responsible for the protection of these critical infrastructures.

The European Union put the issue of protection of critical infrastructures in 2004 for the first time. The Commission issued a communiqué entitled 'Protecting the Critical Infrastructure in Combating Terrorism' in response to a request from the Council. In this communiqué, the definition of the critical infrastructure has been made and the activities to be done for the protection of the infrastructure elements in the fight against terrorism are summarized. In the light of this document, the European Program for the Protection of Critical Infrastructures (EPPCI), which was prepared in 2006, defines the critical infrastructure as physical and technological systems that will have serious impacts on the health, safety and economy of the member states and their citizens if they become dysfunctional. In this context, a detailed list of the critical infrastructures, facilities and assets within the EU has been prepared (AFAD, 2014).

With the Communiqué of the European Program for the Protection of Critical Infrastructure published on 12 December 2006, the critical infrastructure sectors have been identified, and the member states have determined what they should do to protect their critical infrastructures against all kinds of attacks, terrorism, sabotage. The final regulation outlining the final framework is Directive 114 of 8 December 2008 "Identifying European Critical Infrastructures and Increasing Protective Measures" (AFAD, 2014).

Unfortunately, there is no legal regulation in Turkey to protect critical infrastructures against threats. Considering the geopolitical importance of Turkey,

the country's critical infrastructures are not only likely to influence the local societal life, but also all the countries whose infrastructure are interdependent to that of Turkey's. For example, the energy pipelines that pass through Turkey and reach to Europe is a potential target for such attacks and any potential impact on these pipelines is likely to equally influence the importer countries of Europe. Therefore, any natural or intentional impacts on these international infrastructures are likely to create cross-border impacts and influence the socioeconomic welfare of European countries.

In Turkey, The Disaster and Emergency Management Presidency (AFAD) is responsible for the development and implementation of policies, taking necessary measures to ensure the effective implementation of disaster and emergency situations and civil defense services at the country level. It is also in charge of preparing and mitigating the occurrence of such events, intervening during the event, coordinating the improvement activities to be carried out after the event and ensuring coordination among these matters. Regarding the protection of critical infrastructures, the EU and US policies are examined and a road map has been determined and the general framework for the tasks and responsibilities is under preparation by AFAD authorities (AFAD, 2014).

2.3 Generally Used Risk Analysis Methodologies, Approaches and Software Programs In The World

2.3.1 RAMCAP-Plus

The RAMCAP-Plus methodology has been developed as a risk and flexibility assessment methodology for all hazards. This methodology developed by American Association of Mechanical Engineers (ASME). The scope of the methodology has been prepared to cover all critical infrastructures in order to protect them from threats, avoid negative consequences, and providing flexibility in returning the facility back to normal functioning after a damage occurs (Giannopoulos, Filippini, & Schimmer, 2012).

Unnecessary details are avoided in the RAMCAP-Plus methodology, it has a simplified approach to risk assessment that can be implemented realistically. The methodology application involves seven steps; characterization of plant or system assets, identification of potential threats, outcome analysis, vulnerability analysis, threat assessment, risk and flexibility assessment, risk and flexibility management (Giannopoulos, Filippini, & Schimmer, 2012).

2.3.2 Risk And Vulnerability Analysis (RVA)

The RVA methodology was developed by the Danish Emergency Management Agency (DEMA). The scope of the RVA methodology has been developed in order to identify the threats, including risks of major accidents, natural disasters, sabotage or terrorism, and to assess the risks and vulnerabilities of critical infrastructures of all sectors (Giannopoulos, Filippini, & Schimmer, 2012).

The methodology consists of four different steps. These steps are; purpose and scope of analysis, scenario development, assessment of risks and fragilities, graphical representation of risk and fragility profile. All assessments "probability, consequences and vulnerabilities" levels are scaled between 1 and 5. 1 is considered the best and 5 is the worst (Giannopoulos, Filippini, & Schimmer, 2012).

Risk and vulnerability assessment analyzes are not at the level of detail, they are carried out to reveal the general situation. In general, the goal is to sustain critical social needs in the event of major accidents or natural disasters. It aims to eliminate the possibility of stopping the entire system by setting minimum requirements to achieve this goal (Giannopoulos, Filippini, & Schimmer, 2012).

2.3.3 Better Infrastructure Risk And Resilience (BIRR)

The Better Infrastructure Risk and Resilience (BIRR) methodology was developed by the Argonne National Laboratory. This laboratory is U.S. Department of Energy’s oldest and largest national laboratory and one of the main domains is national security and protection of critical infrastructures. Research conducted in this

direction is mainly oriented towards policy needs of the Department of Homeland Security (DHS). The Argonne National Laboratory, which supports this activity, is developing various methods for the security of infrastructures of various sectors including water treatment plants, financial system, banking system, electric energy, and transportation (Giannopoulos, Filippini, & Schimmer, 2012).

This methodology prioritizes protection measures against the assets of facilities generally implemented against terrorist threats and has a sector-based assessment approach. In this methodology, “Resilience Index”, “Vulnerability Index”, “Protective Measures Index” and are emphasized. An important parameter of this methodology is that the operator can evaluate the security of the system's assets according to specific scenarios and compare the security level with that of similar sectors or sub-sectors and have knowledge of their dependencies (Giannopoulos, Filippini, & Schimmer, 2012).

2.3.4 Protection of Critical Infrastructures - Baseline Protection Concept (BMI)

The Federal Ministry of Interior, the Federal Criminal Police Office, the Federal Office for Civil Protection and the Disaster Response and the Federal Criminal Police Office have prepared a baseline protection plan, in Germany. This protection plan is not only a government risk assessment methodology, but also a protection plan that encompasses and emphasizes the importance of private companies. A problem that may occur in any infrastructure, regardless of private or state, can affect everyone in the city like the domino effect. Therefore, the state and the private sector play an important role in ensuring cooperation with all infrastructure operators and ensuring that infrastructure is functioning properly for the whole community. It is explicitly 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 (Giannopoulos, Filippini, & Schimmer, 2012).

2.3.5 Sandia Risk Assessment Methodology

Sandia National Laboratories prepared a risk assessment methodology for the protection of physical critical infrastructures. The methodology aims to enable critical infrastructure to function properly even in the event of an attack.

The methodology consists of seven separate steps; characterize facility, identify undesired events, identify threats, determine the consequences of undesired events, define threats to the facility, analyze protection system effectiveness, estimate risks, suggest ad evaluate upgrades to the system.

Using the error tree analysis approach, vulnerabilities are identified. By applying error tree analysis, threat scenarios and critical elements that disrupt the functioning of the system's assets can be identified. In this risk assessment methodology, a different path is taken than a traditional methodology. The risk methodology proceeds as follows; it is based on the undesirable consequences of the threat occurring and is intended to reduce the number of possible threats. Potential threats are prioritized, risk analysis is put forward by assessing the effectiveness of protection systems that will prevent successful threats. The final step of the methodology is to evaluate whether the risk is acceptable or not. In cases where the risk is unacceptable, all assumptions are reassessed and counter measures are improved (Giannopoulos, Filippini, & Schimmer, 2012).

2.3.6 Network Security Risk Assessment Modeling (NSRAM)

The “Network Security Risk Assessment Modeling” methodology has been developed by the Institute for Infrastructure and Information Assurance at James Madison University. The NSRAM covers all interdependent critical infrastructures and has been developed to determine how systems will respond in case of attacks such as major accidents, disasters, sabotage, terrorism, and how infrastructures can have effects on each other (Giannopoulos, Filippini, & Schimmer, 2012).

2.3.7 Multilayer Infrastructure Network (MIN)

The “MIN” is a methodology that has been developed by the Purdue School of Civil Engineering. The objective of the “Multilayer Infrastructure Network” methodology is to generalize the paradigm of transportation network infrastructures, and apply optimization. It can be adapted as a risk assessment tool not only for the transportation network but also for infrastructures of all sectors (Giannopoulos, Filippini, & Schimmer, 2012).

2.3.8 Fast Analysis Infrastructure Tool (FAIT)

The Fast Analysis Infrastructure Tool (FAIT) has been developed by the National Infrastructure Simulation and Analysis Centre for the support DHS by determining the significance and the interdependencies of US critical infrastructures. Obviously, this tool is aimed at policy-making decision-makers (Giannopoulos, Filippini, & Schimmer, 2012).

FAIT software requires extensive infrastructure data and requires expert knowledge to evaluate the data. This software consists of four main elements: detailed information of critical infrastructures, evaluation of dependencies with other infrastructures, information gathering and economic impact. The procedure is specifically designed to assess economic impact that is likely to occur after an event (Giannopoulos, Filippini, & Schimmer, 2012).

2.3.9 Critical Infrastructure Protection Modeling And Analysis (CIPMA)

The Critical Infrastructure Protection Modeling and Analysis project is a major security initiative launched and developed by the Australian Government to protect the country's critical infrastructure. In this context, simulation models, databases, GIS and software that combines economic models are used. With this methodology you can analysis GIS visualization of results within economic and population information, failure time, dynamics of critical infrastructure systems. It involves identifying particularly vulnerability points and includes the creation and elaboration

of risk maps. Also it can be helps reveals investment and mitigation strategies (Giannopoulos, Filippini, & Schimmer, 2012).

2.3.10 The DECRIS Approach

The DECRIS approach is based on sectoral risk assessment methodologies currently in Norway. The objective of this methodology, which is common at global level, is exactly the sectoral approach and the assessment of each sector independently. The DECRIS methodology can be helps, establishment of event taxonomies and risk dimension, simplified risk and vulnerability Analysis for the identified events, selection of events to be further analyzed and detailed analysis of selected events.

A typical risk assessment, a purification mechanism has been added to narrow down the list of events that need to be evaluated for the most important difference. This purification mechanism (selection process) is the most important feature of this methodology. The selection process includes the importance of risk, the affected part of the critical infrastructure and the proportion of people affected by the occurrence of the hazard.

This methodology was applied to the city of Oslo. Various scenarios have been identified for each of the critical infrastructure categories of water, communication, transportation and electric energy. For each of these events, the above mentioned criteria are applied and a short list of scenarios to be further assessed is established. In principle this methodology fosters the collaboration between the various stakeholders in the different sectors in order to widen their understanding on the interdependencies across sectors (Utne et al., 2008).

2.3.11 Athena

Athena is an analysis and modeling tool that is designed to analyze a network of nodes (actors, concepts and physical) as a “system of systems” by merging various political, military, economic, social, information, and infrastructure models and their

associated cross dependencies. Athena incorporates several reasoning algorithms that allow sophisticated inter- and intra-dependency analysis between and through nodes (Pederson, Dudenhoeffer, Hartley, & Permann, 2006).

2.3.12 CARVER – 2

CARVER-2 is a simple software program that provides a quick and easy way to prioritize potential terrorist targets. It compares and rates the critical infrastructure and key assets in jurisdictions by producing a mathematical score for each potential target. It is the first step for conducting more in-depth vulnerability assessments. CARVER-2 helps users to make comparisons such as a water system vs. an energy grid vs. a bridge (Pederson, Dudenhoeffer, Hartley, & Permann, 2006).

2.3.13 Critical Infrastructure Protection Decision Support System (CIP/DSS)

The Critical Infrastructure Protection Decision Support System (CIP / DSS) helps to simulate the dynamics of individual infrastructures and interconnects separate infrastructures based on their interconnectedness. For example, repairing damage to the electric power grid in a city requires transportation to failure sites and delivery of parts, fuel for repair vehicles telecommunications for problem diagnosis and coordination of repairs, and the availability of labor crews. The CIP / DSS helps, functionally representing all critical infrastructures sectors with their interdependencies, calculation of human health and safety, economic, public and national security and environmental impacts and also synthesis of a technically fact-based defensible and extensible methodology (Pederson, Dudenhoeffer, Hartley, & Permann, 2006).

2.3.14 Net-Centric Effects-Based Operations Model (NEMO)

The Net-Centric Effects-Based Operations Model (NEMO) is a software tool, which is the analysis of cascading impacts on other critical infrastructures with which critical infrastructures are interfered as a result of any emergency situation for example natural disaster, terrorist attack, sabotage. NEMO software tool helps to

monitor the interactions of any system with the other different sector systems (water, gas, electrical energy, road) it is dependent on in the event that the operation is impaired. The tool performs vulnerability analysis in order to facilitate decision making under the different emergency situation examples. It also facilitates the process of planning an infrastructure system, so it can be used with geographical information systems software (Yusta, Correa, & Lacal-Arantegui, 2011).

2.3.15 The Urban Infrastructure Suite (UIS)

The Urban Infrastructure Suite (UIS) is a set of interoperable modules that employ advanced modeling and simulation methodologies to represent urban infrastructures and populations. These simulation-based modules are linked to a common interface for the flow of information to model water distribution infrastructures, transport, telecommunications, community public health, energy, banking and financial infrastructures and their interdependencies between UIS sector simulations (Pederson, Dudenhoeffer, Hartley, & Permann, 2006).

2.3.16 The Water Infrastructure Simulation Environment (WISE)

The Water Infrastructure Simulation Environment (WISE) is an analytic framework supporting the evaluation of water infrastructure in terms of both infrastructure specific and interdependency issues (Pederson, Dudenhoeffer, Hartley, & Permann, 2006).

CHAPTER THREE
METHODOLOGY

3.1 Data Collection and Expert Opinion System

In this study, expert opinion system was used. In the Expert system, the evaluation is made by using the opinions of the relevant experts and the estimated approaches. In this study, opinions of experts in Izmir Water and Sewerage Administration were taken. At the same time, estimated data were entered by using the opinions of the lecturers working on the subject at the university and possible effects were predicted under various scenarios and their results were evaluated.

Within the scope of the thesis, visits were made to the mentioned facilities (Tahtalı Dam, Halkapınar deep water wells, Arsenic Treatment Plants) and field observations were made. The facilities which could not be visited were searched on the internet and information and visuals were obtained. In this way, threats that could affect the facility and its assets were identified and scenarios were created. Due to confidentiality, all data could not be reached, so the estimated data was used. Therefore, the results of the methods applied will be subjective and relative and vary.

3.2 CARVER Methodology

The CARVER method consists of 6 criteria: **C**riticality, **A**ccessibility, **R**ecuperability, **V**ulnerability, **E**ffect, and **R**ecognizability. All criteria are scored on a scale ranging from 1 to 10 according to their importance, and the total relativity score is calculated among the elements considered. In general, the evaluation criteria for the analysis and prioritization of potential military attack targets are aimed at selecting the best target and target components for attack. By scoring each target on a criterion basis, the numerical score is determined to show how suitable the target is to attack. All the numerical values given for the criteria are arranged in a matrix and total scores are obtained for each target. The total score in question is a score of the target and the target with the highest score is considered the best target. The CARVER method is also used to identify and prioritize the sensitivity of components

to target threats to critical urban infrastructures (Federation of American Scientists, 2010). The criteria used in CARVER method can be explained as follows:

Criticality: This criterion expresses the public health (illness, injury, fatality number etc.) and economic impact of the threat to the system component. If there is any threat / attack on the component, it is classified in terms of the number of people that may be effected or the number of possible fatalities (Table 3.1).

Table 3.1 Criticality criteria and scaling (Federation of American Scientists, 2010)

Criticality	**Scale**
Effects 1,000,000 or more people	9-10
Effects between 500,000 and 1,000,000 people	7-8
Effects between 100,000 and 500,000 people	5-6
Effects between 10,000 and 100,000 people	3-4
Effects less than 10,000 people	1–2

Accessibility (A): It is an indication of the physical reach of the target and the ease of exiting the facility after the action is carried out. If any infrastructure system component can be easily accessed and exited by an attacker before an attack is detected, it means that the target is easily accessible and the target is vulnerable to threats (Table 3.2).

Table 3.2 Accessibility criteria and scaling (Federation of American Scientists, 2010)

Accessibility	**Scale**
Easily accessible: The destination is almost easily accessible, open area, not fenced, restricted barriers, not under observation. The attack can be carried out by undetected transport of big volumes of pollutants.	9-10
Accessible: The target is located inside a perimeter fence but outdoors, under observation. The attacker can reach the target in less than 1 hour. The attack can be carried out by undetected transport of large volumes of pollutants, need for concealment.	7-8

Table 3.2 continues

Accessibility	Scale
Partially accessible: Target is in inside a building, probably on ground floor and under regular employee observation. In addition, there may be some physical barriers. There is a time limit and needs to concealment of the pollutant for the attacker to reach the target. Only non-specific and general information about the target can be obtained.	5-6
Hardly accessible: Access is only possible through responsible security personnel of employee. There is a serious time limit for the attacker to reach the target. It has effective security supervision or barriers. Inside a building but on second floor or in basement; climbing or lowering required. Target is in a protected or secured part of the facility.	3-4
Unattainable: Not accessible or extreme difficulty to reach. Physical barriers/fences, alarms present and under security observation. The attacker must carry all the necessary equipment to reach the target in less than 5 minutes. There isn't any public information about the target.	1–2

Recuperability: It is defined as the capability of the system to be reactivated at full capacity after an attack and measured as the re-arming time. This criterion includes the use of another unit instead of the system or the elimination of damage caused by repair (Table 3.3).

Table 3.3 Recuperability criteria and scaling (Federation of American Scientists, 2010)

Recuperability	Scale
Replacement, repair, or substitution requires more than 1 year	9-10
Replacement, repair, or substitution requires less than 6 month	7-8
Replacement, repair, or substitution requires less than 1 month	5-6
Replacement, repair, or substitution requires less than 1 week	3-4
Same day replacement, repair, or substitution	1–2

Vulnerability (V): The target can be defined as an indicator of how effective the threat/attack will be in achieving its purpose and the assessment of how much the

system will be effected as a result of the damage to the target. In Vulnerability criterion, an assessment of both the target itself and its environment is made with the assumption that the target is fully achievable (Table 3.4).

Table 3.4 Vulnerability criteria and scaling (Federation of American Scientists, 2010)

Vulnerability	**Scale**
The target is extremely vulnerable (90-100%) in achieving the goal of the attack.	9-10
The target is highly vulnerable (60-90%) in achieving the goal of the attack.	7-8
The target is partially vulnerable (30-60%) in achieving the goal of the attack.	5-6
The target is less vulnerable (10-30%) in achieving the goal of the attack.	3-4
The target is hardly vulnerable at all or little vulnerable (<10%) in achieving the goal.	1–2

Effect (E): It is the amount of loss of the production potential of the system after the attack. Within the scope of this criterion, the classification was made considering the percentage of loss and the extent of the impact that could occur on the system was determined in this way (Table 3.5).

Table 3.5 Effect criteria and scaling (Federation of American Scientists, 2010)

Effect	**Scale**
Effects the production of the system more than 50%	9-10
Effects the production of the system in the range of 25-50%	7-8
Effects the production of the system in the range of 10-25%	5-6
Effects the production of the system in the range of 1-10%	3-4
Effects less than 1% of system production	1–2

Recognizability (R): It is defined as the degree to which a target is recognized clearly by an attacker without being confused with other targets. Recognizability is

also a measure of the attacker's expertise or technical knowledge required to recognize the system component or target (Table 3.6).

In the CARVER method, first, each target, system or component is scored according to the classes determined on the basis of each criterion. After the evaluation phase is completed, a single value is obtained by summing the scores of each target per criterion and the system components are ranked among themselves. The magnitude of this value is an indication that the system is open to attack and has priority over the measures to be taken.

Table 3.6 Recognizability criteria and scaling (Federation of American Scientists, 2010)

Recognizability	**Scale**
The target is easily recognizable, recognition does not require training.	9-10
The target is easily recognizable, requiring little training to be recognized.	7-8
The target is difficult to recognize. It can be confused with other target. Requiring an average level of training to recognize.	5-6
The target is very difficult to recognize. It can be easily mixed with other target and target components. Recognition requires extensive training.	3-4
The target is not recognized under any circumstances except for experts.	1–2

Within the scope of this study, the resistance of the northern and southern water resources of Izmir City to different threats was examined comparatively and a risk assessment of the drinking water infrastructure of the city was made. In this analysis, the behavior of the components of the critical drinking water infrastructure system under various scenarios involving critical threats was examined and the risk level and urgency of the measures to be taken were determined according to the results obtained.

3.3 VSAT Software Methodology

VSAT Version 6.0 software was created by the U.S. Environmental Protection Agency (EPA) as an information tool to support water and wastewater service

providers to define safety and natural disaster risks. Risk is a measure of potential public health and economic harm involving three items: threat, vulnerability and consequences. Risk assessments include all these 3 factors; as a result of a comprehensive, systematic and defensible assessment of the risk exposure of assets which is carrying out integrated risk mitigation activities (VSAT, 2017).

Performing risk assessment is an important evaluation that utilities need to undertake to understand the actions to eliminate potential threats. These threats include human mistakes as accidental - intentional and natural disaster threats, otherwise known as "all hazards". Important elements in risk assessment with VSAT are stated in the following parts (VSAT, 2017).

VSAT software enables every local business in the US to perform a risk analysis by taking into account the characteristics and location of its drinking water and treatment plant. In this way, all enterprises are able to identify the security gaps of their facilities against possible threats and see how much they are at risk with their current situation. The operating principle of the VSAT version 6.0 software is shown in Figure 3.1. With VSAT software, risk analysis can be carried out separately for the drinking water and wastewater plant, or can be performed in combination at the same time (VSAT, 2017).

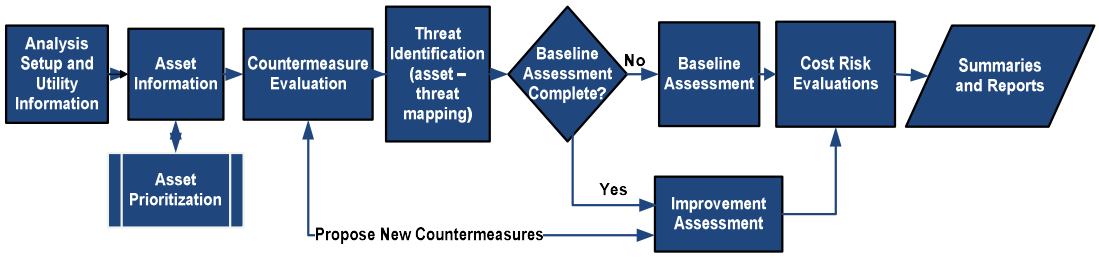

Figure 3.1 VSAT version 6.0 operating principle (VSAT, 2017)

3.3.1 Identifying Facility Information and Assets

In the first step, the location, name, capacity of the facility to be analyzed and information such as the region it serves are entered into the program in detail (VSAT,

2017). At this step, all infrastructure components in the plant are identified as assets of the plant. When determining assets, VSAT software can present all infrastructure components that may be in the facility as options and assign them to specific categories, or new assets that are not among the options can be identified. The critical infrastructure components to be evaluated are then selected and the analysis continues. According to various criteria, the asset range changes from 0 to 10. The most important gets a score of 10. Any asset with a score greater than 7 is automatically included for the next analysis unless selected (Figure 3.2).

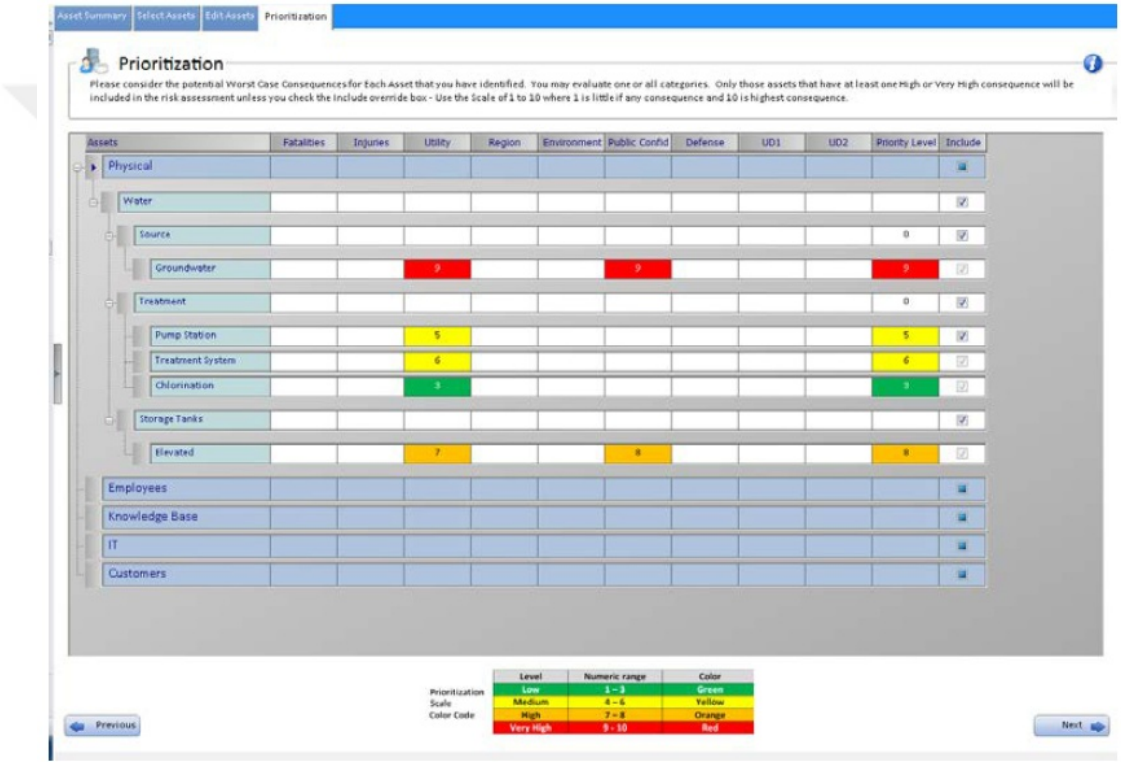

Figure 3.2 Asset prioritization screen from VSAT version 6.0 (VSAT, 2017)

3.3.2 Countermeasure Evaluation

After the assets are identified, the existing countermeasures for each asset are defined for example a pump station. In order to prevent any power failure, generators, inputs and outputs are controlled in order to make the card pass system, camera security monitoring system and SCADA system work properly. When assigning these measures, the task for which the measure is placed is determined

according to the ability of the measure category. These are categorized into 3 categories: 1) to detect the attack, 2) to delay the attack, and finally 3) to respond in the event of an attack. For example, the security camera is used to detect the attack, while the barbed fence around the facility is used to delay the attack and security guards are used to respond to the attack. It is important that these definitions are made correctly to determine where the vulnerability exists (VSAT, 2017).

3.3.3 Identifying Threats

The next step identifies potential threats for each asset. The program presents all possible threats in detail as options, or allows a new threat to be identified that is not among the options. When considering a physical attack for terrorist purposes, many options are presented in the program to select the type of vehicle to be used from land, air or sea. For example, if the facility is at the seaside, attacks from the sea can be defined, and if the facility is in land, different types of attacks can be identified from the land, such as an attack on the facility with a bomb-laden vehicle or direct intruder infiltration and damage to the facility. All these threats are assigned separately for each asset and risk analysis is performed for their effects. The type of asset analyzed at this stage may bear different risks under different types of attacks. For example, in a chemical or biological attack, the wastewater treatment plant may be affected, while the water intake structure, which is reinforced concrete, is not structurally affected.

For water sector risk assessments, VSAT provides a list of reference threats to be considered that include both human-made and natural threats. Additionally, authorities can analyze risks by adding threats of their own study. After finalizing each set of data entered, a basic comparison process is worked to create relevant pairs for analysis. To improve the actions, all actions should be included in capabilities in order to decrease the likelihood of consequences from included threats. These capabilities are detection, delay, response, preparation, active response, recovery and consequence reduction (Figure 3.3).

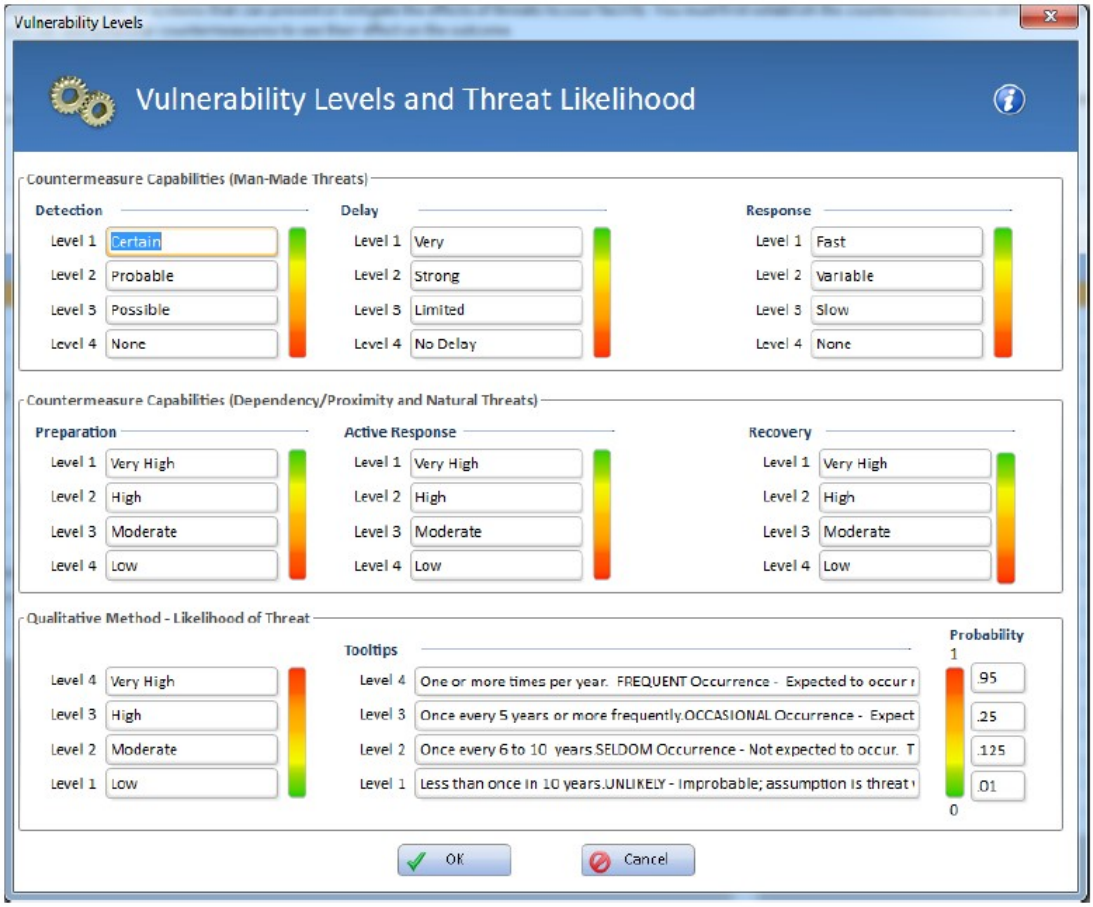

Figure 3.3 Vulnerability levels in VSAT version 6.0 (VSAT, 2017)

For man-made threats, countermeasures fall into three "threat relevant capability" categories such as *detection, delay* and *response* (Table 3.7).

Table 3.7 Capability of countermeasures – man-made threats (VSAT, 2017)

Countermeasure Capability	**Countermeasure Capabilities – Man-made Threats**		
	Detection	**Delay**	**Response**
Low (0 – 2)	None (0)	None (1)	None (0)
Moderate (4 – 6)	Possible (1)	Limited (2)	Slow (1)
High (8 – 16)	Probable (2)	Strong (4)	Variable (2)
Very High (> 16)	Certain (4)	Very Strong (6)	Fast (4)

Detection is the determination that an unauthorized action has occurred or is occurring, including sensing the action, assessing the alarm, and communicating the alarm to a responder (VSAT, 2017).

Delay is the ability to impede adversary penetration into or exit from the vulnerable (protected) area, or otherwise serves to lengthen adversary task time. Delay includes not only access in and out of an area but locks on hatches and other asset-specific hardening (VSAT, 2017).

Response provides the ability to counteract adversary activity and interrupt the threat or attack. For example; guards and external agencies that respond, time between the verification of an event or alarm and the interruption of an attack (VSAT, 2017).

For natural disaster threats, the three threat relevant capability categories of countermeasures are *preparation, active response* and *recovery (Table 3.8)*.

Table 3.8 Capability of countermeasures – dependency/proximity & natural disaster threats (VSAT, 2017)

Countermeasure Capability	**Countermeasure Capabilities Natural Disaster Threats**		
	Preparation	**Active Response**	**Recovery**
Low (< 6)	Low (0)	Low (0)	Low (0)
Moderate (6 – 10)	Moderate (2)	Moderate (2)	Moderate (2)
High (12 – 16)	High (4)	High (4)	High (4)
Very High (> 16)	Very High (8)	Very High (8)	Very High (8)

Preparation: Utilities should prepare and practice plans of action in anticipation of natural disasters occurring. When evaluating capabilities, utilities should consider the extent and frequency of planning efforts, the adequacy of the emergency plans,

and how thoroughly the planning efforts have been communicated and trained (VSAT, 2017).

Active Response: Includes activities conducted while the natural disaster is occurring, including the mobilization of emergency services and first responders in the disaster area. Utility response to any significant disaster—natural or terrorist-borne—should be based on existing emergency management organizational systems and processes, such as the Incident Command System (ICS) and make use of the principles of unified command and mutual aid (VSAT, 2017).

Recovery: Includes all efforts to restore the utility and the affected area to its previous state following a natural disaster. Recovery efforts are primarily concerned with actions that involve rebuilding destroyed property, the repair of essential assets, and restoration of access and safe working environments for all personnel (VSAT, 2017).

3.3.4 Risk Analysis and Risk Reduction

For all assets, risk analysis is performed for prioritization after the existing security measures and potential threats are assigned. Assets with high scores are included in the evaluation and vulnerability analysis is started separately. In VSAT software, two analyzes can be performed under the name of Baseline Analysis and Improvement Analysis. In Baseline Analysis, the effects of the existing measures in the facility are revealed on each asset in case of possible threats. In the improvement analysis, improvements are made against the vulnerabilities determined according to the results of the current situation analysis and the comparison is made by revealing the results obtained.

During the Risk Analysis, a risk value (R) is calculated by taking into account the consequences of threats that affect each asset identified under existing countermeasures, vulnerabilities and the likelihood of a threat (VSAT, 2017).

$$R=C*V*T \quad (3.1)$$

C= Consequence

V= Vulnerability

T= Threat Likelihood

When determining the consequences (C), the user is asked to enter some data to help measure the fatalities, injuries, property damage and economic impacts on the community the serves as a result of the threats identified (Table 3.9 and Table 3.10). These are data such as the expected number of fatalities and injuries, what percentage of the system affects how many days. In addition to these data, financial impact to utilities and economic impact to regional area should be considered.

In determining the vulnerability (V), the result records the likelihood of existing measures and threats for each asset/threat pair analyzed during the analysis. The probability of a threat (T) can be evaluated as a qualitative and quantitative approach to the probability of a threat (Table 3.11).

Table 3.9 Likelihood of consequences or damage classification (VSAT, 2017)

Risk Level (Numeric)	Risk Level (Qualitative)	Risk Description
1	**Low**	Unlikely that damages would occur
2	Moderate	Some damage expected to occur
3	High	Damages very likely to occur
4	**Very High**	Damages certain to occur

Table 3.10 Qualitative estimate likelihood of threat occurrence (VSAT, 2017)

Risk Level (Numeric)	Risk Level (Qualitative)	Risk Description
1	Low	Unlikely. Less than once in 10 years
2	Moderate	Seldom. Once every 6 – 10 years
3	High	Occasional. Once every 5 years
4	Very High	Frequent. Once or more per year

Table 3.11 Qualitative threat levels available in VSAT for 'qualitative method of threat probability of occurrence' (VSAT, 2017)

Threat Level (Qualitative)	Risk Description	Probability Used for Quantitative Risk Calculation
Very High	One or more times per year. FREQUENT Occurrence - Expected to occur relatively often. Threat may have several times in the recent past and can be expected to recur several times in the foreseeable future. Recurrence likely to be intermittent (regular intervals, generally often)	0.95
High	Once every 5 years or more Frequently. OCCASIONAL Occurrence - Expected to occur sporadically. Threat may or may not have occurred locally in the recent past, although it or similar threats may have occurred in neighboring areas or elsewhere within this or a similar industry. Recurrence likely to be irregular.	0.25
Moderate	Once every 6 to 10 years. SELDOM Occurrence - Not expected to occur. Threat is believed to be remotely possible at some time, but occurrence will be rare. May occurs as an isolated incident.	0.125
Low	Less than once in 10 years. UNLIKELY - Improbable; assumption is threat will not occur. Threat occurrence is not impossible, but not expected to occur other than very rarely.	0.01

3.3.5 Baseline Assessment

In this section, users determine potential public health and economic consequences as well as the likelihood of those consequences and the likelihood of threat occurrence. Also estimate asset and economic metrics of resilience using elements of the estimated consequences (VSAT, 2017).

3.3.6 Improvement Assessment (Propose New Countermeasures)

In Improvement Assessment, the risk of the identified threats to their current asset is evaluated. They propose a series of potential countermeasures that could possibly help reduce the consequences or the likelihood of consequences facing defined asset/threat pairs. After that, the economic consequences, expected public health

fatalities and injuries, the likelihood of those consequences and likelihood of the threat occurrence are reassessed (VSAT, 2017).

3.3.7 Cost / Risk Evaluations

In this step, if users have necessary verification, packages of countermeasures are developed and evaluated, with specific focus to cost and effectiveness (VSAT, 2017).

In general, threats are classified into two categories: human impacts or natural disasters. While performing risk analysis for both; the impact on public health is calculated by entering data for the expected number of deaths and injuries when the threat occurs. When this data is entered, the system automatically calculates a predicted cost value when injury and fatality occurs (Figure 3.4).

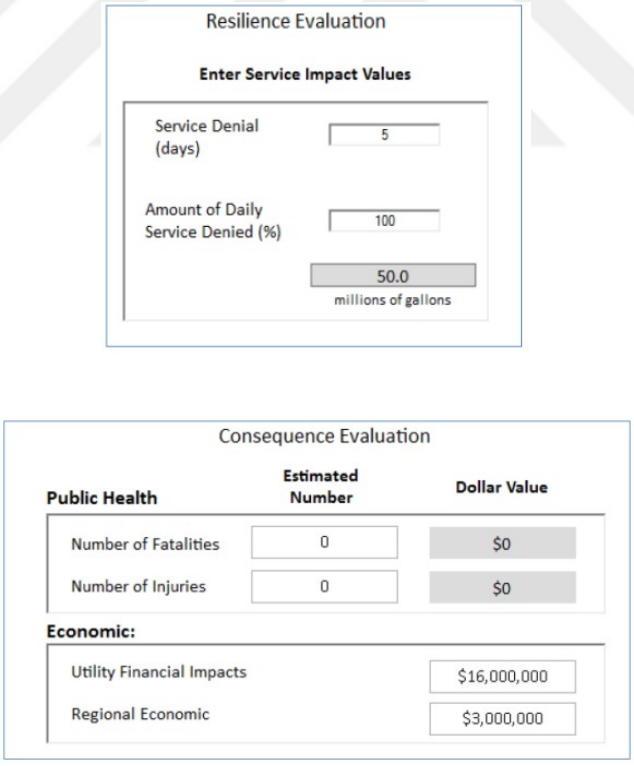

Figure 3.4 Consequences and resilience evaluation (VSAT, 2017)

The economic impact is considered as both the damage to the facility and the impact on the region, and when this calculation is performed, the percentage of the

system and the number of days that the system will affect when the threat occurs is entered into the system. The adequacy of the existing countermeasures in each attack is also assessed. For example, a chemical attack can be easily detected in the drinking water treatment plant, if there are available equipment, whether there are delaying measures and if there is sufficient level and whether the counter-intervention can be done immediately. In case of a natural disaster, for example an earthquake, these are evaluated that whether emergency response procedures exist in case of an earthquake, whether emergency drills are sufficient, whether they are prepared for an emergency and whether they can be intervened or not, and how quickly the system is restored. Existing Situation Analysis is completed by evaluating the probability of being the last of both types of threats.

The next step is to evaluate the measures to be taken by looking at the Existing situation and to carry out Improvement Analysis. Within the scope of this analysis, new security measures are assigned and the risks are mitigated. Accordingly the decreasing risks are evaluated. As a result of the program, various analysis reports can be obtained.

Assessment of consequences of any worse case coming from asset is done by evaluating the severity of negative result on chosen consequences in VSAT; no of fatalities and injuries, financial impact to assets and economic impact to region.

VSAT software also interacts with different software programs. The population that can determine the impact of the threat on public health, the nearest hospitals and health institutions and so on if data are available, more concise results can be put forward to measure the regional / national economic impact of the threat. Once the results and their effects are revealed, it is possible to calculate the necessary investment costs by preparing a package of measures against threats in the Cost / Risk section. Thus, the economic impact that will occur after the threat is realized can be compared with the costs of the measures necessary to eliminate the threat. This comparison can be made not only in terms of cost but also in terms of the extent of the impact on public health.

CHAPTER FOUR
IZMIR DRINKING WATER RESOURCES AND INFRASTRUCTURE

Izmir is Turkey's third largest city with a population of about 4 million people. According to the data of 2015, 52.3% of the sources providing drinking water to Izmir's old metropolitan area are ground water and 47.7% are surface water resources (Figure 4.1). The drinking water resources of the central and northern parts of the city are groundwater obtained from wells in Manisa-Sarıkız, Manisa-Göksu, Izmir-Menemen / Çavuşköy and Izmir-Halkapınar. The groundwater wells in Izmir-Pınarbaşı and Izmir-Buca, which are still in operation but have a very small share in the whole system, are the smallest parts of the system that supplies water from groundwater (İZSU, 2016). These groundwater resources were named as "Northern Water Resources" within the scope of this study.

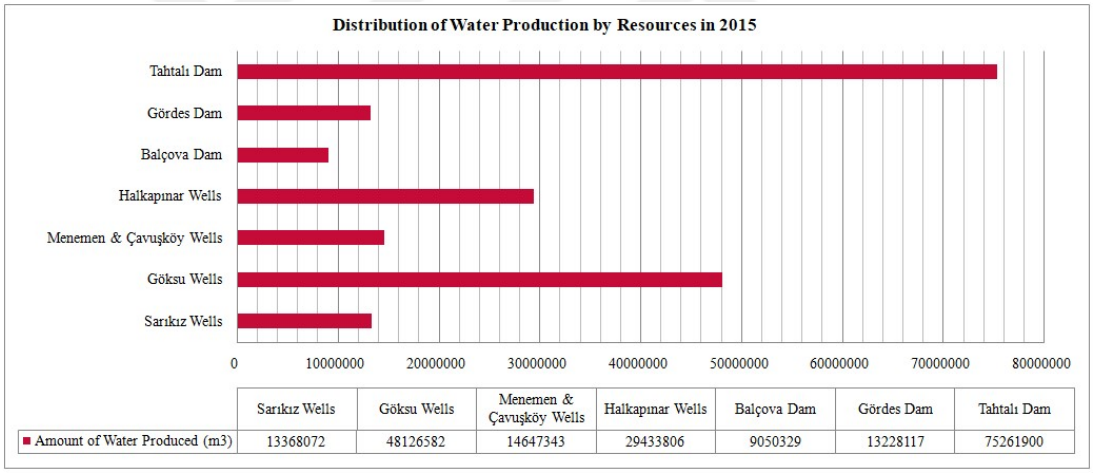

Figure 4.1 Distribution of water production by resources in 2015 (İZSU, 2016)

Tahtalı Dam, which serves the southern parts of the city and is located within the borders of Menderes district to the south of the city, is the most important surface water source of Izmir. Tahtalı Dam and partly Balçova Dam are named as "Southern Water Resources within the scope of this study. Gördes Dam, which is located in the north-eastern part of the city and within the boundaries of Gördes district of Manisa province, has not been used as of 2016 due to the renovation and maintenance works. Furthermore, Güzelhisar Dam, which is sometimes used for water supply of the city

and located within the borders of Aliağa district in the north of the city, was also excluded from the analysis conducted within the scope of this study. All components that supply water to the city are shown in Figure 4.2.

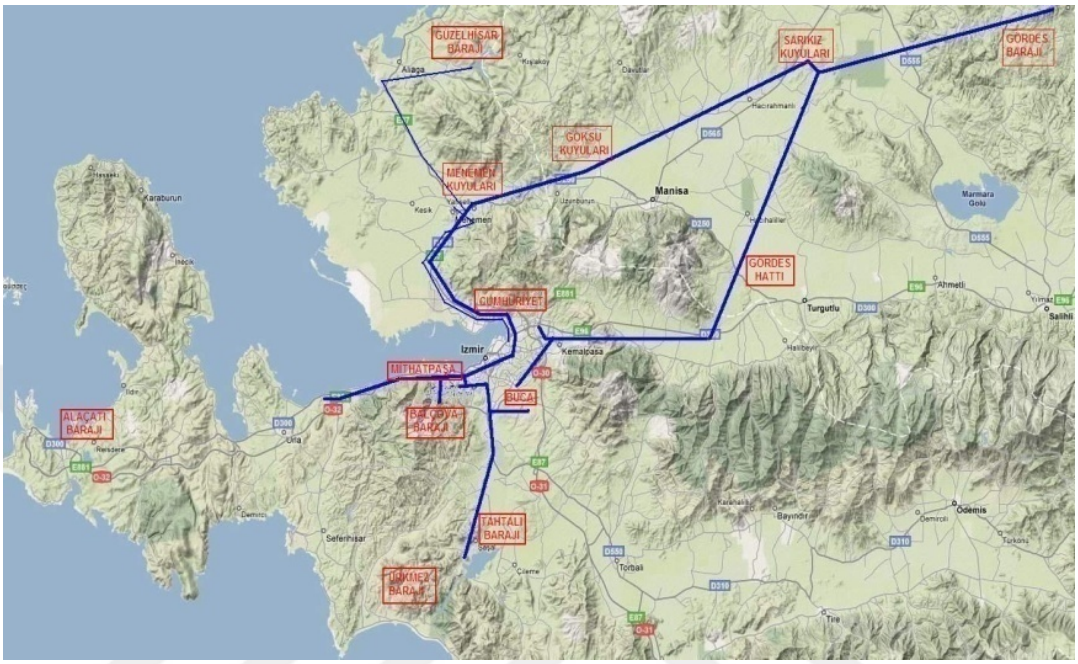

Figure 4.2 Izmir water resources and main distribution infrastructure (İZSU, 2016)

In general, in a water distribution infrastructure, after being treated in water treatment plant drawn from subsurface or surface sources, it is pumped to a tank at higher elevations by the pumps and feeds the network to the end user with gravity flow from this tank. Water distribution infrastructure gets complicated when various sources are included, different storage tanks are used and intermediate pump stations are included in the system. In Izmir city center, water distribution infrastructure has a complex structure. Water obtained from different sources are fed into the water distribution system from different points. In this context, it can be said that Izmir drinking water infrastructure is an integrated system (İZSU, 2016).

The entire control of the system is done by the İZSU SCADA unit in Halkapınar via computers. Within the scope of this monitoring and control made with the central control and management system called SCADA; water sources, dams, storage tanks, transmission lines, pumping stations and some valve points are monitored. Thanks to

this continuous monitoring system that is available for 7 days 24 hours, the water supplied to the city is controlled and instant interventions can be made.

The water distribution system of the city of Izmir includes numerous critical infrastructure facilities such as water resources, transmission and distribution lines, treatment plants, pumping stations and warehouses and distribution network lines.

When the morphology of the City of Izmir is considered, it can be seen that the water system of the city can roughly be considered as two parts that are fed by two different sources, i.e., surface and subsurface water resources. The critical infrastructure system is thus structurally considered as a theoretically separated system with two major portions. The components of these portions are explained and evaluated in the following sections. In this study; Sarıkız, Göksu, Menemen-Çavuşköy, Halkapınar wells are considered to be the groundwater-fed northern system components and Tahtalı Dam and treatment plant are considered to be the surface water-fed southern system components. The southern system typically serves the southern parts of the city while the northern system generally serves the northern parts of the city. For the risk assessment of the system units, the risks that may occur in both systems were evaluated under different scenarios using CARVER method and VSAT software.

4.1 Izmir City Northern Drinking Water Resources and Infrastructure – Groundwater Resources

Sarıkız, Göksu, Menemen & Çavuşköy and Halkapınar groundwater resources are the most important sources providing drinking water to the northern parts of Izmir City. In the resources that make up this system, water is extracted from the underground with wells and given to the network after the necessary treatment processes. The critical infrastructure components of this system, called the northern sources, are the groundwater aquifer and deep wells from which groundwater is extracted, water supply lines, drinking water treatment plants, pumping stations, distribution network and water tanks.

4.1.1 Groundwater Resources and Wells

Groundwater resources providing water to Izmir have a total capacity of 178 million m^3 (İZSU, 2016). The amount of water used from these sources varies according to years. The amount of water supplied to the city from these sources in 2015 is shown in Table 4.1.

Table 4.1 Groundwater resources potential and production quantities (İZSU, 2016)

Underground Water Wells	**Annual Potential (m^3/year)**	**Total Production in 2015 (m^3/year)**
Sarıkız Wells	45,000,000	13,368,072
Göksu Wells	63,000,000	48,126,582
Menemen&Çavuşköy Wells	25,000,000	14.647.343
Halkapınar Wells	45,000,000	29,433,806

Sarıkız Wells are located in Sarıkız Spring region in Lütfiye and Nuriye Neighborhoods of Saruhanlı District of Manisa Province and water is being supplied to the City of Izmir since 1977.A total of 38 deep water wells were drilled in Sarıkız Springs region and there are currently 30 wells active. The depths of these wells range from 77 to 250 meters. The water obtained from these deep wells in 3 different groups in Sarıkız Spring region is collected in the storage tanks of each group and later transferred to Çullu raw water storage tank. Here, it is treated in Çullu Arsenic Treatment Plant after combining with the water produced from Göksu Wells. The treated water is later conveyed to Yahşelli pump station via Çullu clean water tank and then transferred to Izmir city (İZSU, 2016).

Göksu Wells were drilled between 1970 and 1974 in Göksu Spring, 4 km northeast of Muradiye District of Manisa. In 1995, additional wells were drilled and the total number of wells reached 22. These 22 wells are still active today. The depths of Göksu wells vary between 150 and 259.5 meters (İZSU, 2016).

The water obtained from the deep wells of Göksu Springs is collected in a pool and conveyed to Çullu raw water storage tank. Here, it is treated in Çullu Arsenic

Treatment Plant by combining with the water produced by the deep wells of Sarıkız. The treated water is later conveyed to Yahşelli pump station via Çullu clean water tank and then transferred to Izmir city (İZSU, 2016).

Menemen and Çavuşköy Wells are located in Menemen district centre and in Çavuşköy. They were connected to Izmir in 1976. A total of 40 wells were drilled until 2009 and the depths of these wells range from 57 to 179.5 meters. As a result of cancellations and collapses, a total of 30 deep wells are currently active in the region. Menemen deep wells are scattered in agricultural fields (İZSU, 2016).

The water obtained from the deep wells of Menemen and Çavuşköy is conveyed to the Menemen Emergency raw water reservoir and treated in the Menemen Arsenic Treatment Plant. The treated water is then transferred to Menemen Emergency fresh water tank and conveyed to Izmir city with the help of Menemen Emergency pump station with 5 pumps (İZSU, 2016).

Halkapınar Wells are situated within Izmir City center at Halkapınar springs area. They provide water to the city from the wells drilled around the lake located in the Izmir city center. These wells are an important water source for Izmir. Halkapınar springs have been used since 1897 and there are 25 wells in total. 19 of these are actively used today (İZSU, 2016).

The water produced from the deep wells is collected in the storage tank in Halkapınar and treated in the Halkapınar Arsenic Treatment Plant. The treated water is then conveyed to all parts of the city via pumping stations (İZSU, 2016).

4.1.2 Water Transmission Line

Sarıkız – Çullu Water Transmission Line: This line, which is laid between Sarıkız deep wells area and Çullu reservoir (raw water and clean water reservoirs), consists of concrete pipes with Ø 1850 mm diameter. The line carries the water produced by the deep wells of Sarıkız when water is not taken from Gördes Dam; when water is

taken from Gördes Dam, Sarıkız Potable Water carries the water taken from treatment plant (İZSU, 2016).

Göksu – Çullu Water Transmission Line: This line, located between Göksu spring and Çullu pumping station, which carries water produced from deep wells in Göksu region and Çullu raw water tank, consists of concrete pipes of Ø 1850 mm diameter with a total length of 3 kilometers (İZSU, 2016).

Menemen Wells Water Collection Lines: It is a series of lines consisting of steel pipes of Ø 1000 mm diameter which carries the water produced by Menemen deep wells to raw water tank in Menemen Emergency pump station (İZSU, 2016).

Çavuşköy Well Collection Lines: It is a series of lines consisting of steel pipes of Ø 600 mm diameter. It carries the water produced by Çavuşköy deep wells to raw water tank in Menemen Emergency pumping station (İZSU, 2016).

Halkapınar Region Transmission and Distribution Lines: It is the line that sends the water produced from the deep wells in Halkapınar region to the arsenic treatment plant in Halkapınar and then to the distribution system. This line consists of pipes with Ø 1000 mm diameter (İZSU, 2016).

4.1.3 Drinking Water Treatment Plants

The water produced from Sarıkız and Göksu deep wells is treated at Çullu Arsenic Treatment Plant. The water produced from Menemen and Çavuşköy deep wells is treated at the Menemen Emergency Arsenic Treatment Facility. The water produced from Halkapınar deep wells is treated at the Halkapınar Arsenic Treatment Plant. These plants have a similar process that are designed to treat arsenic and other soluble metals/metalloids ground in the ground waters of the region. These plants are designed to reduce arsenic levels to below the 10 µg/L limit set by World Health Organization (WHO) and the national drinking water standards (İZSU, 2016). The capacities of these three arsenic treatment plants are given in Table 4.2.

Table 4.2 Capacities of drinking water treatment plants (İZSU, 2016)

Drinking Water Treatment Plant	**Capacity (m^3/day)**
Çullu Arsenic Treatment Plant	259,200
Menemen Arsenic Treatment Plant	51,840
Halkapınar Arsenic Treatment Plant	86,400

Arsenic Drinking Water Treatment Plants consist pump station, coagulation system, chlorination unit, multimedia filtration unit, storage tanks, chemical sedimentation tank, sludge collection tank, sludge dewatering unit, drainage water reservoir and treated water tank (İZSU, 2016).

The water sent from the deep wells to the water treatment lines reaches the raw water storage tank first and pre-chlorination is made in the pipeline when entering the plant. Later a coagulant (iron III chloride) is dosed into the chlorinated water pipeline. The coagulant dosage is calculated according to the tank volume in the plant and delivered to the line before filtration to allow it to reacts with arsenic so that arsenic can be removed in the filters. The system is subjected to backwashing at certain times depending on the raw water arsenic content. Before backwashing, the remaining water and air in the filter system is discharged. During the backwash, the air blower is activated in the tank and the sludge is transported to the upper layers. The backwash and rinse water of the facility is discharged to the sewerage network (İZSU, 2016). The amount of water treated in Çullu, Menemen and Halkapınar arsenic treatment plants by years is given in Table 4.3.

Table 4.3 Amount of water treated in arsenic treatment plants (İZSU, 2016)

Drinking Water Treatment Plant	**2011**	**2012**	**2013**	**2014**	**2015**
Çullu Arsenic	56,240,977	53,627,990	39,436,312	43,895,311	61,494,654
Menemen Arsenic	16,121,175	17,103,272	15,052,270	15,282,176	14,647,343
Halkapınar Arsenic	31,798,323	31,128,709	33,299,449	29,201,576	29,433,806

4.1.4 Pumping Stations

On the water distribution infrastructure, there are production pumps that pump water from the source and raise water to a higher level. In general, there are also pumps that provide suction and discharge from the line as well as pumps that elevate water from the tank. There are a total of 65 pumping stations in different capacities in 11 districts of Izmir city center (İZSU, 2016).

4.1.5 Water Distribution Network

The distribution network of the city consists of pipelines with diameters ranging from 80 mm to 2200 mm (İZSU, 2016).

4.1.6 Water Storage Tanks

On the water distribution infrastructure, there are water tanks for storage which provides balance in the system during distribution. The largest capacity water storage tanks are Halkapınar water storage tank (55,000 m^3) and Cumhuriyet water storage tank (51,000 m^3). There are a total of 47 water storage tanks in 11 districts of Izmir city centre (İZSU, 2016).

4.2 Izmir City South Drinking Water Resources and Infrastructure - Surface Water Resources

The southern parts of the city of Izmir are mostly fed from surface water resources and the most important sources are Tahtalı and Balçova dams. Of these, Tahtalı Dam was built on Tahtalı Creek within the borders of Menderes district. The water accumulated in Tahtalı Dam Lake is pumped to a balancing tank through the intake pumping station. From here, the raw water is delivered to the Görece Drinking Water Treatment Plant via the transmission line. After being treated here, it is first pumped to Karabağlar water reservoir and later delivered to the city with the distribution network. The critical infrastructure components of the Tahtalı Dam, which is the most important component of this system, called the southern resources, are the dam

structure, the reservoir, the water intake structure and the pumping station, the transmission line, the drinking water treatment plant, the pumping stations, the distribution network and the water storage tanks (İZSU, 2016).

4.2.1 Tahtalı Dam Body and Reservoir

Tahtalı Dam, which is the most important surface water source for Izmir, has been supplying water to Izmir since 1997. It has a 546 km^2 basin area and an average annual water intake potential of 128 million m^3. The height of the dam body, which consists of clay core and rock trench with cutter trench, is 57.5 m from the foundation and the water elevation in the reservoir varies between 31 m and 60.5 m. The active volume of the dam is 287,050,000 m^3 (İZSU, 2016).

4.2.2 Tahtalı Dam Water Intake Structure and Pump Station

The water intake structure is located in Dereboğazı location on the dam lake. It is in the form of a 35 m high concrete tower intake structure with 17 m diameter and a total of intake capacity of 6.134m^3/sec. totally, there are six pumps in the structure. The water intake structure is designed to receive water from 29 m, 36 m, 43 m and 50 m levels of the reservoir. The intake line consists of 2 steel pipes with a diameter of 1600 mm and a length of 580 m. The balancing tank is 6 m in diameter and 15 m in height and has a volume of 400 m^3 (İZSU, 2016).

4.2.3 Water Transmission Line

The water taken from the water balancing tank in Sakartepe is conveyed to the drinking water treatment plant in Görece by a 17505 m long transmission pipeline. The treated water from the treatment plant is transferred to the main water reservoir in Karabağlar via a 14730m long transmission pipeline and delivered to the urban distribution network. The 32235 meters of transmission line between Tahtalı Dam and Karabağlar water reservoir has a inner diameter of 2200 mm and a transmission capacity of 5.94 m^3/sec. It is composed of steel coated pre-stressed reinforced concrete pipes (İZSU, 2016).

4.2.4 Drinking Water Treatment Plant

Tahtalı Drinking Water Treatment Plant located just south of Görece Town of Menderes District. The plant has a capacity of 520,000 m³/day and consists of cascade aeration structure, rapid mixers, chemical building, filters chlorine building, clarifiers, filter press units and clean water tank. The Treatment Plant consists of 2 parallel lines, each with a capacity of 260,000 m³/day (İZSU, 2016).

4.2.5 Pump Station, Water Distribution Network and Water Storage Tanks

Pump station, water distribution network and water storage tanks are other units of the southern system. These are common facilities for the northern (underground) and southern (surface) resources of the city as described in the previous sections. Since the drinking water distribution system of Izmir city is an integrated system, the water produced from surface and ground water sources in the northern and southern parts of the city are combined in the same distribution system. Therefore, the risks involved for these three critical infrastructure elements in the implementation section are considered common for the northern (underground) and southern (surface) systems (İZSU, 2016).

CHAPTER FIVE
RISK ANALYSIS WITH CARVER METHOD

In this study, Tahtalı Dam, which is the most important component of the water resources in the southern part of Izmir and Sarıkız, Göksu, Menemen-Çavuşköy and Halkapınar deep water wells which constitute the northern part of the water are investigated. In this context, it is possible to consider this entire risk assessment study as a comparison of surface water and ground water resources of Izmir. Critical infrastructure elements examined in the scope of the study were; aquifer zone, groundwater wells and arsenic treatment plants for groundwater resources; and, the reservoir and the body of the dam, water intake structure and treatment plant for surface water resources. Transmission lines, pumping stations, distribution network and water storage tanks which are in common use for both sources were also included in the study. Four different scenarios were created for both water sources and the risks of potential threats were evaluated by CARVER method. The scenarios examined are: (1) intentional biological / chemical attack by mixing contaminants into the water infrastructure system, (2) physical (terrorist) attacks to interrupt or stop the operation of system components, (3) system components being affected by a natural disaster (earthquake); (4) cyber-attacks of system components. The risks that these critical infrastructure components will be exposed under these scenarios are examined and evaluated comparatively.

5.1 Scenario 1 - Biological/Chemical Attack

In scenario 1, the threat of a biological or chemical pollutant being deliberately mixed into the system and reaching the end user with the components of the system is examined. The results obtained are shown in Table 5.1. Within this scenario, the component with the highest score and therefore the highest risk in terms of being a target is aquifers and dam reservoirs for groundwater and surface water resources, respectively. Due to the fact that the reservoir is easily accessible and easily recognizable, it is considered to be an easy target for an attack. When pollutants are mixed in the lake, it can easily be dispersed throughout the lake. Although groundwater resources are also likely to be affected by this type of impact, it has

been found that there is a lower risk compared to surface waters due to the fact that this source is underground and its accessibility is only possible through wells. Both surface (reservoir) and groundwater resources (groundwater wells) are considered to be the most risky infrastructure components due to difficulties in the treatment of pollutants and the long-term need for recuperability. Other infrastructural components have relatively lower risks, resulting in lower scores as a result of the CARVER method. However, the drinking water treatment plant and the water intake structure & the pumping station and are among the other components that need to be taken against this threat (Table 5.1).

Table 5.1 Scenario 1 results

Critical Infrastructure Components		**C**	**A**	**R**	**V**	**E**	**R**	**Score**
Groundwater Resources	Underground Water Resources (Aquifer)	9	7	9	9	10	3	**47**
	Groundwater Wells (Deep Wells)	10	9	3	9	1	9	41
	Transmission Lines	10	1	2	2	10	1	26
	Arsenic Drinking Water Treatment Plant	10	6	3	7	10	8	**44**
Surface Drinking Water Resources	Dam Body	1	1	1	1	1	10	15
	Dam Reservoir	8	9	10	10	9	10	**56**
	Water Intake Structure&Pumping Station	10	4	1	3	10	6	34
	Transmission Lines	10	1	2	2	10	1	26
	Drinking Water Treatment Plant	10	4	3	1	10	5	33
Common Units for Ground / Surface Drinking Water Resources	Pump Stations	8	6	1	2	5	5	27
	Distribution Network	8	2	4	2	2	1	19
	Water Storage Tanks	6	7	1	2	3	8	27

5.2 Scenario 2 - Physical Attack

In scenario 2, a physical (terrorism, sabotage etc.) attack was considered to interrupt or stop the operation of critical infrastructure facilities (Table 5.2). In this scenario, the probability of damage to physical structures is evaluated. In this context, water intake structure, water wells, dam body and drinking water treatment plants are at risk. It is not possible to re-commission the underground water wells after a physical attack and new wells should be drilled. In addition, these wells are

often risky because they are located in unprotected areas and are vulnerable to attack. The dam body is naturally more resistant to such attacks. However, in the event of a very violent attack, there may be a collapse of the dam, which should be perceived as a catastrophic threat to the downstream regions of the dam. The treatment plants established for both surface and groundwater resources are among the mostly affected structures by physical attacks. In contrast, infrastructure components such as dam reservoirs, groundwater aquifers and distribution networks are predicted to be at lower risk of physical attack than other components.

Table 5.2 Scenario 2 results

Critical Infrastructure Components		**C**	**A**	**R**	**V**	**E**	**R**	**Score**
Groundwater Resources	Underground Water Resources (Aquifer)	1	1	1	1	7	3	14
	Groundwater Wells (Deep Wells)	10	10	9	9	10	9	**57**
	Transmission Lines	10	3	6	5	9	1	34
	Arsenic Drinking Water Treatment Plant	10	6	8	8	9	9	**50**
Surface Drinking Water Resources	Dam Body	10	1	10	5	10	10	**46**
	Dam Reservoir	1	9	1	1	1	10	23
	Water Intake Structure&Pumping Station	10	6	8	7	10	6	**47**
	Transmission Lines	10	3	6	5	9	1	34
	Drinking Water Treatment Plant	10	6	10	6	7	5	**44**
Common Units for Ground / Surface Drinking Water Resources	Pump Stations	8	6	5	7	5	5	36
	Distribution Network	6	2	4	3	4	1	20
	Water Storage Tanks	6	8	4	5	4	8	35

5.3 Scenario 3 - Natural Disaster (Earthquake)

In the third scenario, the risks that critical infrastructure facilities will face in the case of a natural disaster are investigated. Since the assessment according to all natural disasters is very difficult in terms of possible effects, only “earthquake” is considered in this scenario. All buildings are designed considering the earthquake risk during construction. In this scenario, the risks were calculated assuming that a possible earthquake would occur at the highest intensity according to the same geographical conditions (taking into account the possibility of being on the fault line

or being away from the earthquake zone). In this scenario, all facilities except the reservoir are at significant risk. Deep water wells have been identified as the most risky structure because of the high risk of earthquake and groundwater's changing direction and total collapse of water wells. In addition, the dam body, the water intake structure and the pumping station and drinking water treatment plants have emerged as the most critical infrastructure components (Table 5.3).

Table 5.3 Scenario 3 results

Critical Infrastructure Components		**C**	**A**	**R**	**V**	**E**	**R**	**Score**
Groundwater Resources	Underground Water Resources (Aquifer)	10	10	10	10	10	1	**51**
	Groundwater Wells (Deep Wells)	10	10	10	8	10	1	**49**
	Transmission Lines	10	8	5	6	9	1	39
	Arsenic Drinking Water Treatment Plant	10	10	10	8	10	1	**49**
Surface Drinking Water Resources	Dam Body	10	10	10	8	10	1	**49**
	Dam Reservoir	1	4	1	1	1	1	9
	Water Intake Structure&Pumping Station	10	10	8	8	10	1	**47**
	Transmission Lines	10	8	5	6	9	1	39
	Drinking Water Treatment Plant	10	10	10	8	10	1	**49**
Common Units for Ground / Surface Drinking Water Resources	Pump Stations	8	10	4	8	7	1	38
	Distribution Network	6	8	5	5	6	1	31
	Water Storage Tanks	6	10	3	8	5	1	33

5.4 Scenario 4 - Cyber Attack

In scenario 4, possible cyber threats are taken into consideration. In the cyber attack, remote access to the system is considered and the control of the system is taken into the hands of malicious persons. All critical infrastructure facilities are managed by the SCADA system. Accordingly, all infrastructure systems that provide remote access are under threat. In addition, deep wells, water intake structure and pumping stations, drinking water treatment plants, pumping stations and water depots were identified as important target points (Table 5.4).

Table 5.4 Scenario 4 results

Critical Infrastructure Components		**C**	**A**	**R**	**V**	**E**	**R**	**Score**
Groundwater Resources	Underground Water Resources (Aquifer)	1	1	1	1	1	1	**6**
	Groundwater Wells (Deep Wells)	10	6	2	8	10	4	**40**
	Transmission Lines	1	1	1	1	1	1	6
	Arsenic Drinking Water Treatment Plant	10	6	2	8	10	4	**40**
Surface Drinking Water Resources	Dam Body	1	1	1	1	1	1	6
	Dam Reservoir	1	1	1	1	1	1	6
	Water Intake Structure&Pumping Station	10	6	1	7	10	6	**40**
	Transmission Lines	1	1	1	1	1	1	6
	Drinking Water Treatment Plant	10	6	2	8	10	4	**40**
Common Units for Ground / Surface Drinking Water Resources	Pump Stations	8	6	2	6	10	5	37
	Distribution Network	6	6	1	5	10	1	29
	Water Storage Tanks	6	6	1	5	10	7	35

5.5 CARVER Method Results and Recommendations

The most threatened components of the surface and groundwater drinking water system under the mentioned scenarios are summarized in Table 5.5.

As a result of the risk assessment, arsenic drinking water treatment plant will be the most likely to be affected by the threat of “biological or chemical attack", since it will be directly the water source itself, and in addition to being a relatively less complex and small enterprise, the pollutant can easily be released into the system. In this context, it is recommended to create comprehensive protection areas around the structures and to increase the security measures of the area in order to reduce the threats of a possible biological and chemical attack. Arsenic drinking water treatment plants must be strictly controlled for the personnel access in and out of the facility, and it is necessary to raise the awareness of the employees.

Table 5.5 Risk assessment results with CARVER method

Critical Infrastructure Components		**Biological/ Chemical Attack**	**Physical Attack**	**Natural Disaster**	**Cyber Attack**
Groundwater Resources	Underground Water Resources (Aquifer)	**47**	14	**51**	6
	Groundwater Wells (Deep Wells)	32	**57**	**49**	**40**
	Transmission Lines	26	34	**39**	6
	Arsenic Drinking Water Treatment Plant	**44**	**50**	**49**	**40**
Surface Drinking Water Resources	Dam Body	15	**46**	**49**	6
	Dam Reservoir	**56**	23	9	6
	Water Intake Structure&Pumping Station	34	**47**	**47**	**40**
	Transmission Lines	26	34	**39**	6
	Drinking Water Treatment Plant	33	**44**	**49**	**40**
Common Units for Ground / Surface Drinking Water Resources	Pump Stations	27	**36**	**38**	**37**
	Distribution Network	19	20	**31**	29
	Water Storage Tanks	27	**35**	33	**35**

"Physical / Terrorist attack" is one of the easiest threats to deep water wells, as there is generally no protection around groundwater wells. Considering that the borehole will be damaged after a possible attack and its commissioning will take a long time, it is foreseen that this component will be the most critical infrastructure at risk. For this reason, it is recommended that physical protection areas are to be established around the well groups in the northern sources supplying water to Izmir and that the security units should be kept under constant observation. Drinking water treatment plants are relatively less exposed to physical threats as they are often under the continuous supervision of security units. However, more compact facilities such as arsenic treatment plants are subject to greater damage under attack than conventional drinking water treatment plants. In particular, indoor filter units are likely to suffer greater damage in physical attacks. The dam body, the water intake structure and the pumping station are other critical infrastructure elements at risk.

When the earthquake threat is considered as a “natural disaster", it is clear that groundwater resources will be one of the most affected components. Even under small vibrations, the direction of ground water and the well flow rates chance. This was previously observed in wells drilled in Dikili district of Izmir after a nearby earthquake that shake the region. In more severe earthquakes, the groundwater flow in the aquifers may be affected more and the water supply will be cut off due to the collapse of deep water wells. For this reason, it is recommended to take into account the proximity to the fault lines in the selection of the location of the wells planned to be opened and to evaluate the sensitivity of soil. It is clear that all other reinforced concrete structures on the surface will also be affected by the earthquake risk. Under this condition, drinking water treatment plants, dam body and dewatering structures are among the components that will be most affected due to factors such as the length of the re-commissioning after impact. However, considering the earthquake risk in the initial design of these units, it also makes these plants earthquake resistant.

There is a risk occurred that water cannot be drawn from deep wells as a result of cyber attack. Similarly, the effect of a cyber-attack on water intake structure and pumping station in dams can cause a failure of all facilities and units. As drinking water treatment facilities become dysfunctional, the introduction of water to the city without treatment will pose different public health risks. In addition, the “Radio Frequency Storage Tank System - Pump Automation System" provides communication between the water storage tank, pump and promotion units of the settlements, the operation of the pump when the water level of the tank falls below a certain point, and the system components that operate on the principle of stopping the pump when it exceeds a point; floods or outages. Studies should be made on how much resistance the SCADA infrastructure of the city of Izmir will have under a cyber-attack. However, since the SCADA system was commissioned, the fact that the personnel controlling the water in the local enterprises has been assigned to different units and the fact that the personnel are directed from the headquarters to the facilities in case of any problems in the local enterprises increases the time to respond to the possible threats. The fact that there are no experts in the facilities to intervene in an emergency and those who do not know the facility very well will

bring different risks. For this reason, it is thought that it is necessary to have full time technical personnel who can intervene in local enterprises.

CHAPTER SIX
RISK ANALYSIS WITH VSAT SOFTWARE

In this study, the risk analysis of Tahtalı System, which is the most important surface water source of Izmir, was also performed with VSAT software. Critical infrastructure elements examined in the scope of the study include dam reservoir and body, water intake structure, drinking water treatment plant, pumping station, water storage tanks, transmission lines and water distribution network. Four different scenarios were created for the analysis and the risks of potential threats were evaluated with VSAT software. The scenarios examined are: (1) intentional biological / chemical attack by mixing contaminants into the system, (2) physical (terrorist) attacks to interrupt or stop the operation of system components, (3) system components being affected by a natural disaster (earthquake); (4) cyber-attacks of system components. The risks that these critical infrastructure components will be exposed under these scenarios are examined. The critical infrastructure components given in Table 6.1 for the Tahtalı Drinking Water System are defined as the assets of the system. The existing security measures and potential threats are identified for each asset.

Table 6.1 Possible threats to critical infrastructure components

Critical Infrastructure Components	**Threats**			
	Biological /Chemical Attack	**Physical Attack (Terrorist)**	**Natural Disaster (Earthquake)**	**Cyber Attack**
Dam Reservoir	X			
Dam Body		X	X	
Water Intake Structure		X	X	
Drinking Water Treatment Plant	X	X	X	X
Pumping Station		X	X	X
Water Storage Tanks	X	X	X	X
Transmission Lines	X	X	X	X
Water Distribution Network	X		X	X

The current security measures that are known to exist in the Tahtalı Drinking Water System and the functions of these measures are given in Table 6.2.

Table 6.2 Generally available countermeasures for critical infrastructure components

Countermeasures	**Detection**	**Delay**	**Response**	**Planning**	**Active Response**	**Recovery**
Back-up power supply			X			
Generator			X			
Firewall		X				
Perimeter fencing		X				
Security checkpoint		X				
Employee records kept in secure location	X					
Biological measurement systems	X					
Fire detection	X					
Carbon monoxide detectors	X					
Chemical sensors	X					
Continuous process monitoring	X					
Security surveillance system	X					
Camera and Alarm Monitoring System	X					
Antivirus software	X					
Network-based intrusion prevention	X					
Site lighting	X					
Pressure sensors in distribution network	X					
Emergency operating procedural plan			X	X	X	
Search and rescue team					X	
Personal Protective Equipment			X		X	
Training of fire brigade at plant			X		X	

In the use of the program, these measures are assigned to each entity separately. After identifying the assets in the drinking water system, the risk analysis of the existing security measures and threats against them were performed.

6.1 Scenario 1 – Biological/Chemical Attack

In scenario 1, the threat of a biological or chemical pollutant being deliberately mixed into the system and reaching the end user with the components of the system is examined. As a result of the analysis in the threat of chemical / biological attack; drinking water treatment plant, water reservoirs, water distribution network, distribution line and dam reservoir were found to be the most critical infrastructure components to be affected.

6.2 Scenario 2 - Physical Attack

In this scenario, a physical attack was conducted to interrupt or stop the operation of critical infrastructure facilities. In the threat of a terrorist attack, especially the water intake structure and dam body was found to be quite unprotected.

6.3 Scenario 3 - Natural Disaster (Earthquake)

In the third scenario, the risks that critical infrastructure facilities will face in the face of a natural disaster are investigated. In this scenario, the risks were calculated assuming that the possible earthquake would occur at the highest intensity according to the same geographical conditions (taking into account the possibility of being on the fault line or being away from the earthquake zone). In the event of a natural disaster, such as an earthquake, all reinforced concrete structures, as well as the transmission line and water distribution network are predicted to be the most damaged.

6.4 Scenario 4 - Cyber Attack

In scenario 4, possible cyber threats are taken into consideration. In the cyber attack, remote access to the system has been provided and the control of the system has been taken into the hands of malicious persons. Like all critical infrastructure facilities, drinking water infrastructures are managed by the SCADA system. Accordingly, it was revealed that the pumping station, drinking water treatment plant, water reservoirs, water distribution network, and transmission line where remote access is provided will be intensively affected.

6.5 VSAT Software Results and Recommendations

As a result of VSAT analysis, it is foreseen that the security measures taken in Tahtalı Drinking Water System are generally aimed at detecting the attack and that the intervention will be insufficient in a real attack. The results of the "Baseline Analysis" are shown in Table 6.3.

Before baseline analysis, all assets of the facility were identified and prioritized (Figure 3.2). Possible threat scenarios were identified for each asset as shown in Table 6.1.

The countermeasures (sensor, security guard, fence etc.) that existed in the facility have been identified (Table 6.2). Countermeasures were divided into six categories: Detection, Delay, Response, Preparation, Active Response and Recovery. The purpose of the assumed countermeasures each asset possesses is assessed under potential threats (Figure 3.3). Thus, it is possible to predict the likelihood of threats that may affect each asset, and the damage that may occur to the facility if it occurs (Table 6.3).

Table 6.3 shows the probabilities of occurrence of threats for critical infrastructure components of Tahtalı Dam and probable damages to the system if realized. While performing these calculations, all data processed in VSAT software are taken into account and "Baseline Analysis" result is calculated by the system.

In this study, some assumptions were made because of the lack of precise and detailed information for the facility. In general, the data necessary during the assessment can be listed as follows:

- Existing countermeasures for the assets
- Duty of countermeasures (detection, delay, response, preparation, active response and recovery)
- Threats that may affect the asset
- Probability of threats (historical data)
- Estimated number of days the system may lose its function
- Estimated number of injury/fatalities
- Economic impact

The baseline analysis summary report presented in Table 6.3 shows the likelihood of damage to the facility and the probability of threat occurrence. The score of lake, one of the critical infrastructure components of Tahtali Dam, has been evaluated in detail. The threat, which is expected to have the greatest impact on the reservoir, has been evaluated for the possibility of deliberate mixing of pollutants into the system, i.e. the “chemical / biological threat”.

The chemical / biological threat is a man-made threat. Therefore, in order to examine the probability of the occurrence of the threat, it is necessary to identify the measures that the reservoir has against the chemical / biological threat. The purpose of these measures is evaluated in terms of detection, delay and response. A chemical/biological threat is a threat that is hard to detect when an attack occurs. When any contaminants mixed into the water, it may not be understood that there is an attack if it does not create any color or smell. When mixed into water, it can spread very quickly and at the same time dissolve in water and easily contaminates soil, water and air. In view of these possibilities, it was thought that a precaution that could perform the ”detection” task would be the biological / chemical sensor around the dam and at the water intake points. It is unlikely that the entire dam circumference is continuously controlled by sensors. The pollutant can only be detected if there is a sensor in the water intake zone, if there is no sensor in the water

intake structure it is foreseen to be noticed when it enters the treatment plant. This result is very risky to the public health, and depending on the type of pollutant, it can instantly damage all equipment and bring the system to a standstill for a while. For the stated reasons, there is a low likelihood of the pollutant being noticed. Accordingly, “detection” risk value “Level 3" or "Level 4" can be selected, in this study “Level 3”was selected (Figure 3.3).

When the category of "delay" countermeasures is examined, it is accepted that there isn’t enough measure that can delay the realization of the chemical / biological threat. It is assumed that the field has fence or wall that prevents access from the land around the dam and the entrance and exit of the facility is under control in case of sabotage. These measures can be helping for delay of the attack, but at the same time a large amount of pollutions might also be released from the air or sea in a short time. Therefore, the “delay" category value can also be selected as high, “Level 3” or “Level 4” (Figure 3.3). In this study, “Level 4” was chosen.

When the category of “response" countermeasures is examined, it is unlikely that there will be any "response countermeasures" that can act quickly when a threat/attack occurs around dam reservoir. It is very difficult to correct a contaminant that enters the water, and it is particularly important that the facility has “detection” and “delay” measures against this threat. "Level 2-Variable" was chosen because it is not known whether there is a “response" measure in the facility against the threat of chemical or biological attack from the dam reservoir boundaries (Figure 3.3).

A chemical / biological attack to the reservoir is quite risky, because of human health (viruses, bacteria, etc.) and the possibility of damaging system assets (eg, a material that can clog pipes and solidify after a period of time, or it may be a chemical melting material). Since such a threat has not occurred before in our country, “Level 2 - Seldom Occurrence” selected (Table 3.11) (Figure 3.3). The function of the existing countermeasures and “Probability of threat Occurrence: 0.25“ was determined as a result of “detection, delay and response” evaluation (Table 6.3).

In the event of biological / chemical attack on the reservoir, which serves the starting point of the system, the whole drinking water system is likely to stop for a short or long period. This may vary depending on the type of the pollutant introduced. The system may completely lose its function, all equipment may need to be disinfected or replaced, which means that the system cannot supply water for more than 1 day. Another possibility is that a pollutant entering the system is unnoticed at the plant, reaching the public and bringing about effects such as illness or death. When the probability of failure to supply water to the drinking water system for more than 1 day and the estimated injury / fatality number ranges are entered into the software, the VSAT program reveals the result of ”Baseline Analysis" considering all other data (plant characteristics, countermeasures, etc.). Accordingly, the value of likelihood of damage to the facility was calculated as 62% by VSAT software (Table 6.3). Table 6.3 shows the evaluation results for Tahtalı Dam critical infrastructure components.

Table 6.3 Baseline analysis summary report

Critical Infrastructure Components	**Dam Reservoir**
Threats	Biological / Chemical Attack
Risk Value	**Baseline Analysis**
Likelihood of damage to the facility	**62%**
Probability of threat occurrence	**0.25**

Critical Infrastructure Components	**Dam Body**	
Threats	Physical Attack (Terrorist)	Natural Disaster (Earthquake)
Risk Value	**Baseline Analysis**	
Likelihood of damage to the facility	**34%**	**72%**
Probability of threat occurrence	**0.01**	**1**

Table 6.3 continues

Critical Infrastructure Components	Water Intake Structure	
Threats	Physical Attack (Terrorist)	Natural Disaster (Earthquake)
Risk Value	**Baseline Analysis**	
Likelihood of damage to the facility	**34%**	**72%**
Probability of threat occurrence	**0.01**	**1**

Critical Infrastructure Components	Transmission Lines		
Threats	Physical Attack (Terrorist)	Natural Disaster (Earthquake)	Cyber Attack
Risk Value	**Baseline Analysis**		
Likelihood of damage to the facility	**43%**	**72%**	**34%**
Probability of threat occurrence	**0.125**	**1**	**0.25**

Critical Infrastructure Components	Water Distribution Network		
Threats	Biological / Chemical Attack	Natural Disaster (Earthquake)	Cyber Attack
Risk Value	**Baseline Analysis**		
Likelihood of damage to the facility	**72%**	**72%**	**34%**
Probability of threat occurrence	**0.25**	**1**	**0.25**

Critical Infrastructure Components	Pumping Station		
Threats	Physical Attack (Terrorist)	Natural Disaster (Earthquake)	Cyber Attack
Risk Value	**Baseline Analysis**		
Likelihood of damage to the facility	**53%**	**72%**	**34%**
Probability of threat occurrence	**0.125**	**1**	**0.25**

Critical Infrastructure Components	Drinking Water Treatment Plant			
Threats	Physical Attack (Terrorist)	Biological / Chemical Attack	Natural Disaster (Earthquake)	Cyber Attack
Risk Value	**Baseline Analysis**			
Likelihood of damage to the facility	**34%**	**75%**	**72%**	**34%**
Probability of threat occurrence	**0.125**	**0.125**	**1**	**0.25**

Table 6.3 continues

Critical Infrastructure Components	Water Storage Tanks			
Threats	Physical Attack (Terrorist)	Biological / Chemical Attack	Natural Disaster (Earthquake)	Cyber Attack
Risk Value	**Baseline Analysis**			
Likelihood of damage to the facility	**34%**	**81%**	**72%**	**34%**
Probability of threat occurrence	**0.125**	**0.25**	**1**	**0.25**

As a result of the risk assessment conducted in this study, the threat of biological or chemical attack is among the most important risks. Although the entrance and exit of the drinking water treatment plant is partially controlled, it is determined that adequate security cannot be ensured in any leakage attempt outside the door of the plant. Transmission lines and water distribution network have been identified as less affected units in this threat as they work under pressure and are mostly underground structures. However, water tanks are the most obvious system components of this type of threat. The limited control in most storage tanks draws attention as a risk increasing factor. In addition, early warning sensors that can be placed at different points of the system components are difficult to provide adequate precautions because they are chemical specific and there are thousands of different types of chemical pollutants that may pose a threat. In this context, a contamination with the aim of biological / chemical attack can only be revealed by health problems coming from the public. This situation is very dangerous and the most vulnerable threat is noteworthy. In this context, it is necessary to take preventive measures in the warehouses and treatment plant where such an attack can be done easily. It should be kept in mind that after a possible attack, only measures that reduce health risk can be taken and these can cause serious psychological and sociological adversities on the public.

In the threat of a terrorist physical attack, which is considered as the second scenario, it has been revealed that the water intake structure of the system components and the dam body are quite unprotected. The reason for this is thought to be related to the low probability of such attack and the fact that the system

components are durable reinforced concrete structures. However, it should be remembered that these units are the starting points of the whole system and it should be taken into consideration that a problem that may occur in this system may interrupt the operation of the whole system for a long time. In this context, it should be stated that preventive security measures should be taken considering that the attack can be carried out by air, land or sea.

Natural disaster (earthquake), which is considered as the third scenario, is one of the most vulnerable threats to the system. Despite the relatively improved level of awareness and preparedness in recent years, it is clear that we are not very prepared for natural disasters. It is envisaged that many emergency procedures and exercises will remain on paper and will be inadequate in terms of response and restoration due to lack of planning in case of a real disaster. Considering that the transmission lines and the water distribution network are damaged even by small impact, it is clearly seen that there will be water shortages in an unexpected earthquake. Depending on the length of this process, public health will be adversely affected. In addition, according to the geographical conditions of our country, we may be exposed to all natural disasters and risk analysis should be made separately and different measures should be taken in different system components. In this context, it is important to carry out pipe laying operations carefully and to carry out bearing activities cautiously in order to minimize the risks of transmission lines and distribution network, which are the most vulnerable component to the earthquake threat.

Finally, a possible cyber-attack is also expected to affect system components that are mostly controlled by SCADA. In this context, the water intake structure and the impact of the pumping station may result in the failure of all other connected plants and units. In this case, both the drinking water treatment plant and the distribution network will become dysfunctional. It is considered that an intervention to the treatment plant internal information infrastructure can be detected and corrected relatively easily. It is also possible that the communication system, which operates in coordination between the tank, the pump and the promotion units by a cyber intervention, will disable the system components that operate when the tank water level falls below a certain point and when the pump rises above a certain point, the

system components operate. Such a situation will cause floods or outages in the city. Studies should be made on how much resistance the SCADA infrastructure of the city of Izmir will under a cyber-attack. However, since the SCADA system was commissioned, the fact that the personnel controlling the water in the local enterprises has been assigned to different units and the fact that the personnel are directed from the headquarters to the facilities in case of any problems in the local enterprises increases the time to respond to the possible threats. The fact that there are no experts in the facilities to intervene in an emergency and those who do not know the facility very well will bring different risks. For this reason, it is thought that it is necessary to have full time technical personnel who can intervene in local enterprises.

With the help of VSAT or similar software, all the facilities and critical infrastructure components in Izmir Water and Sewerage Administration (İZSU) should start their own internal audit processes and start the security measures to reduce the sensitivity of risky units and units as soon as possible. As a result of a detailed risk analysis to be conducted with its own staff with all the information, it is recommended to make the necessary risk prioritization and to start work without losing time. In this context, it should be borne in mind that prevention will be easier and less costly than replacing the lost.

CHAPTER SEVEN
CONCLUSIONS

In this thesis, examining the water sector of critical infrastructure risk analysis of the drinking water system is made to Turkey's Izmir province. Two different studies were carried out using CARVER methodology and VSAT software to perform risk analysis. The assumptions accepted to perform the analyzes and the results of the analyzes were evaluated under various scenarios.

With the CARVER methodology, the risk analysis of the whole drinking water system of Izmir including ground and surface water resources was performed. As a result of the analysis, it was found that the ground and surface water source drinking water system could pose different risks under the same scenario. By using VSAT software, risk analysis was carried out by considering Tahtalı drinking water dam, which is the most important and largest surface water source of Izmir.

The following scenarios were discussed in both studies. The impacts that may arise as a result of these scenarios are discussed and discussed in detail in chapters 5 and 6.

1. Scenario: Investigation of the impact on public health by mixing a biological or chemical pollutant into the system
2. Scenario: Physically disrupt the functioning of the system, disrupt, damage to the facility to stop, sabotage, terrorist attacks
3. Scenario: Natural disasters - Impact of very severe earthquake
4. Scenario: Capture of whole SCADA system by cyber-attack, disable network connections, crash system or misuse

Since the risk analysis is performed according to different criteria and assumptions in the CARVER method and VSAT software, it is usual for the risky infrastructure components to emerge to have a different priority. Critical infrastructure components that are generally vulnerable are listed below.

Critical infrastructure components of the drinking water system, which are most at risk from biological or chemical attack; dam reservoir, underground water resources

(aquifers), treatment plants, water tanks, transmission lines and deep water wells. In general, it is expected that reinforced concrete structures will not be affected too much as there is a threat of mixing contaminants into the water. The values obtained as a result of the methods used confirm this.

The critical infrastructure components of the drinking water system, which are most at risk as a result of physical attack; deep water wells, treatment plants, pumping stations, water intake structure, dam body, water tanks and transmission lines. In general, it is foreseen that reinforced concrete structures will be affected and that inefficient pump stations will directly affect the whole system.

The critical infrastructure components of the drinking water system, which are most at risk from severe earthquake are; underground water resources (aquifer), deep water wells, dam body, treatment plants, water intake structure, transmission line and distribution network and pumping stations. It is predicted that the reason of the change of direction of aquifers as a result of earthquakes and the collapse of deep wells drilled in severe earthquakes will directly affect the whole system by discharging the underground water resources. The most critical components of the analyzes are also shown in Table 5.5. However, it is inevitable that all reinforced concrete structures will be affected.

Critical infrastructure components of the drinking water system, which are most at risk as a result of cyber-attack; treatment plants, water tanks, transmission and distribution lines, deep water wells and water intake structure. With the developing technology, the most risky attacks are seen as cyber-attacks. It can affect the entire system and can be collapsed to prevent it from rolling back. The operation of the whole system, from the water intake structure until we reach the taps in our home we talk about a system managed by the SCADA system, so it is revealed in the analysis that protection is inevitable.

Turkey must begin efforts to minimize all these risks and results urgently. The critical infrastructure of the water sector is indispensable for carrying out our daily life activities. Even short-term water shortages create chaos in society and make life

very difficult. As a result of long-term water shortages, public health is adversely affected, the inability of hospitals to carry out their activities leads to a major health crisis, environmental pollution starts to occur, water treatment cannot be done, disrupts industrial activities, school-work-home life becomes difficult, diseases begin in short life reaches a halt. We have to be aware of all of this and we need to protect our critical infrastructures and develop our system according to the new threats that jeopardize our developing technology and security.

When performing risk analyzes, appropriate methods or software should be used. All districts, provinces, regions and countries should be carried out starting from local enterprises by using like VSAT software or CARVER method. In case of interruption in any of our infrastructures connected with neighboring countries, the possible impacts should be evaluated and preparedness plans should be prepared. This may be due to our country or neighboring country, and preparation should be made in both cases. Critical infrastructure sectors should not only be evaluated within their own sector, but also all risk-dependent infrastructure should be analyzed together. All possible impacts and possible impacts should be included in the assessment. The point to note is that the problem should be solved at the source. The more accurate detections are made in local businesses, the more robust the security in the expanding ring is. The crack formed at the starting point of the system continues to spread.

Firstly, the risk analysis method / software appropriate to the facility or system should be selected or developed. The team that will carry out the risk analysis should be composed of people who are fully familiar with the site, as well as those with technical knowledge, for example the operator, engineer, maintenance technician and authorized persons of the facility to calculate the effects. Thus, when the system is unable to serve, the data that may occur, the number of wounded deaths, the number of days the system will stop, and which regions cannot serve, the data appear more clearly. As much as risk analysis, it is as important to evaluate the results correctly, to predict the effects and to perform corrective-preventive actions correctly. It is not only sufficient to present the current situation, but it is also very important to develop

improvement analysis and a comprehensive crisis management plan, but the process will be productive.

Today, threats are constantly changing and gaining a new dimension both due to the political interest wars of the countries and the developing technology. Therefore, it is not enough to identify risks and take precautions only once. Risk analyzes should be renewed at regular intervals, repeated according to changes in the system and reported to the higher authority units so that they can be adapted to the whole system.

Work should be initiated for critical infrastructures of not only water sector but all other sectors. As mentioned earlier, critical infrastructures are interdependent and gradually create risks between each other. The studies to be carried out should not be done by creating legislation on paper. Real data should be used and the actual impacts that may occur in the event of a threat occurring should be calculated. In this study, we have attempted to produce a questionnaire in the form of various scenarios, assuming assumptions, taking the available data and expert opinions, so the results may vary. In this study, we have attempted to produce a questionnaire in the form of various scenarios, accepted assumptions, taking the available data and expert opinions, so the results may vary.

REFERENCES

AFAD (2014). *Kritik altyapıların korunması – yol haritası belgesi.* Retrieved June 20, 2019, from https://www.afad.gov.tr/upload/Node/3910/xfiles/kritikaltyapi-son.pdf

Baker, G. H. (2005). *A vulnerability assessment methodology for critical infrastructure sites.* Retrieved May 8, 2017, from http://works.bepress.com/george_h_baker/2/

Baylis, J., Edmonds, A. J., Grayson, M. E., Murren, J. J., Mcdonald, J., & Scott, B. (2016). *Water sector resilience final report and recommendations.* Retrieved March 16, 2018, from https://www.dhs.gov/sites/default/files/publications/niac-water-resilience-final-report-508.pdf

Copeland, C. (2010). *Terrorism and security issues facing the water infrastructure sector.* Retrieved May 10, 2018, from https://fas.org/sgp/crs/terror/RL32189.pdf

DHS, (2017). *Critical infrastructure sectors*. Retrieved July 15, 2018, from https://www.dhs.gov/cisa/critical-infrastructure-sectors

EPA, (2016). *Ground water and drinking water.* Retrieved May 27, 2019, from https://www.epa.gov/ground-water-and-drinking-water

Eskicioğlu, F., Bilgiç, E., &Gündüz, O. (2017).*Risk analysis for Izmir drinking water system with "CARVER" method*. Proceedings of the 2th International Water and Health Congress, Antalya. 443-449.

Eskicioğlu, F., & Gündüz, O. (2017). Risk *analysis for Izmir drinking water system with "VSAT" software*. Proceedings of the 4th International Water Congress, Izmir, 587-598.

Federation of American Scientists, (2010). *Appendix d target analysis process.* Retrieved February 12, 2016, from https://fas.org/irp/doddir/army/fm34-36/appd.htm

Giannopoulos, G., Filippini, R., & Schimmer, M. (2012). *Risk assessment methodologies for critical infrastructure protection part 1: a state of the art.* Luxembourg: Publications Office of the European Union. EUR 25286 EN – 2012.

Gilette, J., Fisher, R., Peerenboom, J., & Whitfield, R. (2002). *Analyzing water/wastewater infrastructure interdependencies.* Retrieved February 18, 2016, from https://publications.anl.gov/anlpubs/2002/03/42598.pdf

İZSU, (2016). *İçme suyu üretimi, dağıtım ve kontrolü.* Retrieved July 30, 2019, from https://www.izsu.gov.tr/tr/Faaliyet/1

Leuven, L. J. V. (2011). Water/wastewater infrastructure security: threats and vulnerabilities. In *Handbook of water and wastewater system protection (27-46).* New York: Springer.

Pederson, P., Dudenhoeffer, D., Hartley, S., & Permann, M. (2006). *Critical infrastructure interdependency modeling: a survey of U.S. and international research.* Idaho: Idaho National Laboratory.

U.S. Homeland Security, (2010). *Water sector specific plan-An Annex to the National Infrastructure Protection Plan.* Retrieved February 10, 2016, from https://www.dhs.gov/publication/nipp-ssp-water-2010

Utne, I. B., Hokstad, P., Kjølle, G., Vatn, J., Tøndel, I. A., Bertelsen, D., Fridheim, H., & Røstum, J. (2008). *Risk and vulnerability analysis of critical infrastructures - the decris approach.* Retrieved July 19, 2019, from https://www.sintef.no/globalassets/project/samrisk/decris/documents/decris_paper_samrisk_final-080808.pdf

VSAT, (2017). *Download page for vulnerability self-assessment tool (VSAT Version 6.0)*. Retrieved March 3, 2017, from http://www2.epa.gov/waterriskassessment/download-page-vulnerability-self-assessment-tool-vsat

Yusta, J. M., Correa, G. J., & Lacal-Arantegui, R. (2011). Methodologies and applications for critical infrastructure protection: state-of-the-art. *Energy Policy, 39,* 6100–6119.

Zhang, Y., Yang, N., & Lall, U. (2016). Modeling and simulation of the vulnerability of interdependent power-water infrastructure networks to cascading failures. *Journal of Systems Science and Systems Engineering, 25*(1), 102-118.

Zimmerman, R. (2009). *Understanding the implications of critical infrastructure interdependencies for water.* Retrieved March 8, 2018, from https://create.usc.edu/sites/default/files/publications/understandingtheimplicationsofcriticalinfrastructureinterde_0.pdf